

Kapittel 1

Grunnleggende begreper for informasjonssikkerhet

I dette kapitlet lærer du hva informasjonssikkerhet er, og også betydningen av andre sentrale begreper relatert til informasjonssikkerhet. Det hersker dessverre en del forvirring rundt noen begreper, der denne boken tar stilling. Du lærer om denne forvirringen slik at du selv ikke blir forvirret når begrepene dukker opp i ulike betydninger og sammenhenger.

1.1 Terminologi rundt informasjonssikkerhet

Det kan være forvirrende at det benyttes mange forskjellige begreper med (delvis) samme betydning, som for eksempel datasikkerhet, IT-sikkerhet, informasjonssikkerhet, cybersikkerhet og digital sikkerhet. Nye ord skapes kontinuerlig, og ordenes popularitet endrer seg over tid. «Datasikkerhet» har vært populært fra 1980-tallet, «cybersikkerhet» dukket opp og ble populært fra 2010-tallet, mens «digital sikkerhet» ble skapt av norske myndigheter i 2019 i den hensikt å være et samlebegrep for begrepene ovenfor. Når det også rimer godt med begrepet «digitalisering», har «digital sikkerhet» fått en viss popularitet. «Informasjonssikkerhet» har hatt en jevn popularitet gjennom hele denne perioden. Dessuten er «informasjonssikkerhet» en direkte oversettelse av det engelske «information security», som er nedfelt i en rekke internasjonale standarder og rammeverk. Denne boken velger å hovedsakelig bruke ordet «informasjonssikkerhet» med betydning som stort sett overlapper med de andre begrepene.

For purister handler informasjonssikkerhet også om beskyttelse av informasjon på papir eller formidlet gjennom analoge lydbølger, mens digital sikkerhet bare omhandler beskyttelse av digital informasjon. Hvis for eksempel noen kollegaer diskuterer sensitiv informasjon mens de har lunsj på en kafé, slik at andre personer hører hva de sier, så er det strengt tatt ikke et brudd på digital sikkerhet, men et brudd på informasjonssikkerhet. Det har egentlig liten nytte å fokusere på denne forskjellen, for i praksis har begrepene den samme betydningen.

Det fins mange ulike definisjoner på datasikkerhet, cybersikkerhet og IT-sikkerhet, som typisk refererer til sikkerhet for ting som på en eller annen måte er koblet til datanett eller internett. Et eksempel er følgende definisjon som er hentet fra Wikipedia:

Datasikkerhet, cybersikkerhet eller IT-sikkerhet er beskyttelse av datasystemer og datanett mot angrep fra ondsinnede aktører som kan føre til uautorisert informasjonsavsløring, tyveri av, eller skade på, maskinvare, programvare eller data, i tillegg til avbrudd eller feil ved tjenestene de leverer.¹

1.2 Betydninger av begrepet sikkerhet

Begrepet sikkerhet er overlesset med ulike meninger på norsk, noe som kan skape forvirring. Som eksempel viser figur 1.1 nedenfor hvordan tre svært ulike engelske begreper typisk oversettes til «sikkerhet», selv om hvert engelske begrep har gode separate oversettelser til norsk.

Engelsk	Norsk	
Security	Sikkerhet	
Safety		
Certainty		
		(dårlig oversettelse)

Engelsk	Norsk	
Security	⇒ Sikkerhet	
Safety	⇒ Trygghet	
Certainty	⇒ Visshet	
		(god oversettelse)

Figur 1.1. Dårlig og god oversettelse av engelske uttrykk.

Setningene nedenfor gir eksempler på overlesset bruk av «sikkerhet» og hvordan det bedre kan uttrykkes med spesifikke begreper.

Etter bølgen av cyberangrep mot biler med alvorlige ulykker som konsekvens kan vi med sikkerhet si at sikkerhet i biler er viktig for sikkerhet i trafikken.

En bedre formulering av samme setning er:

Etter bølgen av cyberangrep mot biler med alvorlige ulykker som konsekvens kan vi med visshet si at cybersikkerhet i biler er viktig for trygghet i trafikken.

Begrepet «usikkerhet» er på tilsvarende måte overlesset med ulike meninger. For å ha et rikere språk bør «unsecure» oversettes som «usikker», «unsafe» og «insecure» som «utrygg», og «uncertain(ty)» som «uviss(het)».

Selv om «sikkerhet» og «usikkerhet» er overleskede ord, blir vi i praksis sjelden forvirret fordi vi raskt forstår den rette betydningen ut fra sammenhengen. Likevel er det språkfattig å overlesse «sikkerhet» og «usikkerhet» med ulike meninger – det er bedre å bruke ord med klare separate betydninger, noe denne boken forsøker å gjøre.

¹ Wikipedia, s.v. «Computer security», lest 28.03.2023 (min oversettelse). https://en.wikipedia.org/wiki/Computer_security.

Et tilfelle der betydningsforskjellen er avgjørende, er når vi snakker om et feilsikkert (fail secure) eller feiltrygt (fail safe) system. Et eksempel kan være en ståldør til et sikkert hvelv der låsen er styrt elektronisk. En feilsikker lås er at den automatisk går i lås hvis strømmen forsvinner, for å beskytte verdien i hvelvet. En feiltrygg dør er at den automatisk åpnes hvis strømmen forsvinner, slik at det ikke oppstår fare for at mennesker stenges inne i hvelvet.

I de fleste tilfeller er det ikke feil at «certainty» og «safety» oversettes til «sikkerhet», og de fleste ordbøker og Google translate gjør nettopp det. Likevel anbefaler denne boken å oversette «certainty» til «visshet», og «safety» til «personsikkerhet» eller «trygghet».

1.3 Hva er sikkerhet?

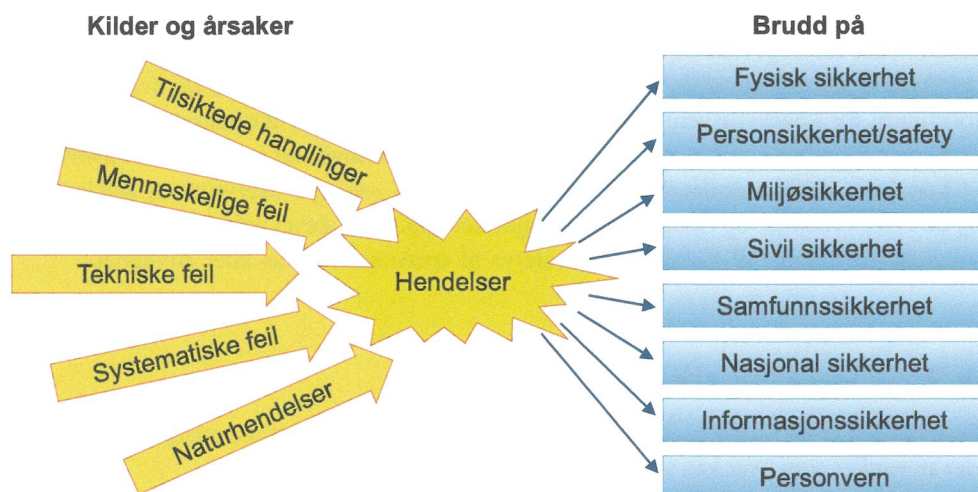
Generelt sett er sikkerhet beskyttelse av verdier mot skade, der det fins mange ulike kategorier av verdier som hver kan skades på forskjellige måter.

Sikkerhet er beskyttelse av verdier mot skade.

Sentrale verdikategorier kan for eksempel være eiendom, infrastruktur, demokrati, samfunnsorden, liv og helse, miljø, data og personinformasjon. For hver av disse verdikategoriene er det veletablerte fagområder for sikkerhet:

- **Fysisk sikkerhet** er beskyttelse av fysisk eiendom mot innbrudd, tyveri og ødeleggelse.
- **Personsikkerhet/safety/trygghet/HMS** er beskyttelse av liv og helse.
- **Miljøisikkerhet** er beskyttelse av miljøet ved å forhindre forurensning og invasjon av fremmede arter i naturen.
- **Sivil sikkerhet** er opprettholdelse av lov og orden, også kalt rettssikkerhet.
- **Samfunnssikkerhet** er beskyttelse av kritisk infrastruktur og grunnleggende funksjoner som energiforsyning, kommunikasjon og transport.
- **Nasjonal sikkerhet** er opprettholdelse av vår nasjonale suverenitet, territorielle integritet og demokratiske styreform (se definisjon fra sikkerhetsloven i avsnitt 15.3.1).
- **Informasjonssikkerhet** er beskyttelse av konfidensialitet, integritet og tilgjengelighet av informasjonsverdier (se definisjon i neste avsnitt).
- **Person(opplysnings)vern** er beskyttelse av personopplysninger gjennom krav til innsamling, lagring, sletting, deling og behandling av informasjon om personer (se kapittel 10 om personvern).

Verdi-/sikkerhetskategoriene ovenfor har ofte gjensidige avhengigheter. For eksempel er informasjonssikkerhet naturligvis helt essensielt for samfunnssikkerhet fordi kritisk infrastruktur styres av IT-systemer. I sektorer der personsikkerhet/safety er svært sentralt, benyttes begrepet «sikkerhet» typisk i betydning av «safety», mens begrepet «sikring» ofte benyttes i betydning av «informasjonssikkerhet». Olje- og gassindustrien er nettopp en slik sektor. Figur 1.2 viser at det fins ulike kilder og årsaker til sikkerhetsbrudd.



Figur 1.2. Kilder og årsaker til sikkerhetsbrudd.

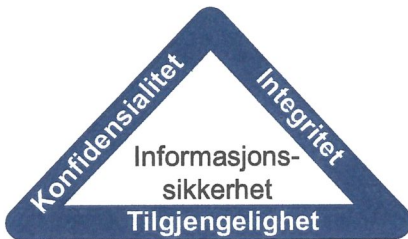
Innen fagfeltet informasjonssikkerhet fokuseres det mest på tilsluktede handlinger som årsaker til hendelser. Samtidig er det viktig å ta i betraktning at informasjonsverdier også kan skades som følge av menneskelige feil, tekniske feil, systematiske feil og naturhendelser. Systematiske feil betyr at sikkerhetsbrudd oppstår på grunn av inadekvate spesifikasjoner for systemer og prosesser. Sagt på en annen måte: Sikkerhetsbrudd oppstår nettopp fordi systemene er korrekt bygget etter spesifikasjoner som er feil. Tekniske feil er relativt lett å rette ved å sørge for at systemet er i samsvar med spesifikasjonene. Systematiske feil kan være vanskelig å rette fordi spesifikasjonene først må rettes slik at systemene kan endres, eller nye systemer må bygges. Hvis feilen allerede fins i milliarder av systemer, må disse først fases ut, som kan ta mange år. Svakheter i mobilnett er et eksempel på dette, som beskrevet i avsnitt 7.4.5.

1.4 Hva er informasjonssikkerhet?

Generelt sett er informasjonssikkerhet å beskytte informasjonsverdier mot skade. En informasjonsverdi kan være selve informasjonen, men også ressurser for representering og behandling av informasjonen. Eksempler på informasjonsverdier er data, fysisk IT-utstyr og infrastruktur, systemer, konfigureringer, programvare, applikasjoner og til og med menneskelige ressurser. Det fins altså ingen tydelig avgrensning av hva som kan være en informasjonsverdi.

Informasjonssikkerhet er beskyttelse av informasjonsverdier mot skade.

På den annen side fins det en klar definisjon på hvordan informasjonsverdier kan skades, nemlig gjennom brudd på konfidensialitet, integritet eller tilgjengelighet. Målsettingen for informasjonssikkerhet er dermed å opprettholde **K**onfidensialitet, **I**ntegritet og **T**ilgjengelighet (forkortet KIT) for informasjonsverdier. På engelsk kalles sikkerhetsmålene *Confidentiality*, *Integrity* and *Availability*, forkortet som CIA. Dette kalles ofte KIT-triaden, typisk illustrert som i figur 1.3.



Figur 1.3. KIT-triaden for informasjonssikkerhet.

En slik måte å definere informasjonssikkerhet på, eller lignende definisjoner, er å finne i en rekke standarder og rammeverk, hvor den internasjonale standarden ISO/IEC 27000² er et prominent eksempel. Denne standarden definerer informasjonssikkerhet som følger:

«Informasjonssikkerhet er beskyttelse av informasjonens konfidensialitet, integritet og tilgjengelighet. I tillegg kan andre egenskaper, f.eks. autentisitet, sporbarhet, ubestemtlig og pålitelighet, omfattes.»

(ISO/IEC 27000)

Den første setningen i definisjonen ovenfor er intuitivt enkel å forstå og stemmer med KIT-triaden, men den andre setningen bringer inn relativt avanserte begreper som kan gjøre det vanskelig å forstå nøyaktig hva som menes med informasjonssikkerhet. For å rydde opp i forvirringen er et enkelt råd rett og slett å se bort fra den andre setningen i definisjonen fra ISO/IEC 27000. Forklaringen på at den andre setningen likevel står der, er at den måtte inkluderes for å oppnå konsensus i standardiseringskomiteen. Tenk deg at representanter fra mange land rundt i verden er samlet i et standardiseringsmøte for å bli enige om en definisjon. Alle er enige om den første setningen, men noen argumenterer sterkt for at begrepene i den andre setningen også må inkluderes. I slike tilfeller kan definisjonen bli bestemt ved avstemning, der ordlyden noen ganger kan høres ut som et kompromiss.

² ISO/IEC 27000:2016 *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

En god måte å forstå definisjonen fra ISO/IEC 27000 på er at begrepene i den andre setningen støtter KIT-sikkerhetsmålene konfidensialitet, integritet og tilgjengelighet. Det er faktisk nyttig å skille mellom sikkerhetsmålene KIT og begreper som støtter KIT. Begreper som støtter KIT, kan for eksempel kalles sikkerhetstiltak, -mekanismer, -tjenester eller -kontroller. I denne boken bruker vi begrepet *sikkerhetstiltak* som oversettelse av det engelske *security control*. Eksempler på hvordan ulike sikkerhetstiltak støtter KIT, nevnes i avsnitt 1.8, som beskriver sikkerhetsmålene konfidensialitet, integritet og tilgjengelighet.

Begrepene autentisitet, sporbarhet, ubenektelighet og pålitelighet fra den andre setningen i definisjonen fra ISO/IEC 27000 er forklart senere i kapitlet.

1.5 Kilder til krav om informasjonssikkerhet

For en virksomhet er det viktig å kjenne til krav om informasjonssikkerhet, både i egen organisasjon og i forhold til andre, rett og slett for å ha god sikkerhetsstyring og for å kunne velge passende sikkerhetstiltak. Det er ledelsens ansvar å legge til rette for at virksomheten kartlegger krav om informasjonssikkerhet. Generelt fins det tre typer kilder til krav om informasjonssikkerhet:

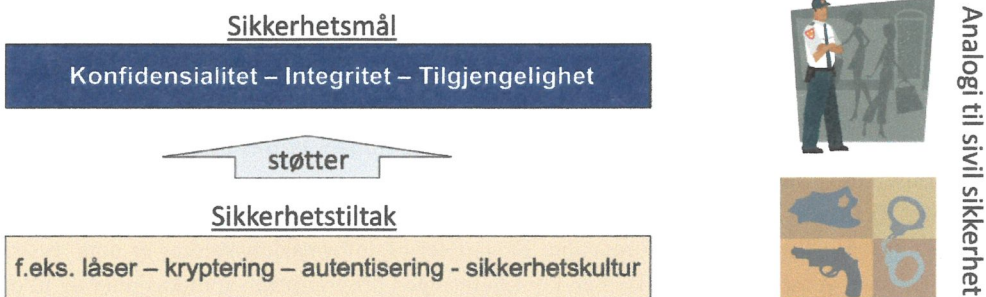
- *Krav om adekvat sikkerhet i applikasjoner og forretningsprosesser i henhold til standard praksis og forvaltning.* For hver type av systemer eller applikasjoner som implementeres og settes i drift, er det viktig å kjenne til hva som er god praksis med hensyn til å bygge inn sikkerhetsmekanismer og funksjoner. For eksempel er det standard praksis at grensesnittet mellom internett og virksomhetens datanett er beskyttet med en brannmur. Det er også standard praksis at tilgang til tjenester i egne nettverk eller til online-tjenester er beskyttet med brukerautentisering og tilgangskontroll. En konsis beskrivelse av god praksis for informasjonssikkerhet er utvalget av 13 prioriterte sikkerhetstiltak fra NSMs *Grunnprinsipper for IKT-sikkerhet*, som beskrevet i avsnitt 12.4. De fleste virksomheter vil ha stor nytte av å implementere disse. Imidlertid er det utilstrekkelig for en virksomhet å bare følge standard praksis. Ifølge CMMI-modenhetsskalaen beskrevet i avsnitt 12.6 anses en virksomhet å ha lav modenhet i styring av informasjonssikkerhet hvis den ikke i tillegg foretar egne risikovurderinger for å identifisere nødvendige sikkerhetstiltak.
- *Krav om å begrense sikkerhetsrisiko til et akseptabelt nivå.* Sikkerhetstiltak for dette formål identifiseres gjennom sikkerhetsrisikovurdering og risikohåndtering. For eksempel kan risikovurdering peke på nødvendigheten av å installere en avansert brannmur med kapasitet til å motstå DDoS-angrep, fordi sannsynlighet og konsekvenser av DDoS-angrep anses å være høye. DDoS (Distributed Denial of Service) er et overlastangrep som betyr at et nettsted blir bombardert med så mye trafikk at legitime brukere ikke når frem. Hvis vanlig praksis setter krav om en (enkel) brannmur, kan risikovurdering sette krav om en avansert «*neste generasjons*» brannmur som kan filtrere bort DDoS-trafikk. Risikovurderingen kan også peke på nødvendigheten av å innføre tofaktor-autentisering (sterk brukerautentisering) for tilgang til svært sensitive ressurser. Hvis vanlig praksis setter krav om (enkel) brukerautentisering, kan risikovurdering i tillegg sette krav om sterk brukerautentisering. Risikostyring beskrives i kapittel 14.

- *Juridisk lovbestemte, regulatoriske og kontraktmessige krav til informasjonssikkerhet.* Alle virksomheter er underlagt lover og forskrifter om informasjonssikkerhet som må overholdes, og for spesifikke sektorer og organisasjoner gjelder ofte flere lover. Det er hver organisasjons plikt å ha oversikt over hvilke juridiske krav til informasjonssikkerhet som må overholdes. Sikkerhetsloven setter for eksempel en rekke krav om informasjonssikkerhet som underlagte foretak er pliktige til å overholde. Mange regelverk, som for eksempel sikkerhetsloven, spesifiserer også at virksomheter må identifisere krav om sikkerhet ut ifra risikovurderinger, som nettopp er kilden til krav nevnt over. Regelverk for informasjonssikkerhet beskrives i kapittel 15.

Krav om informasjonssikkerhet kan være artikulert på en relativt overordnet måte, for eksempel som sikkerhetsmål i henhold til KIT, eller på en mer detaljert måte, som spesifikke sikkerhetstiltak.

Prinsippet om at sikkerhetstiltak og mekanismer støtter KIT-sikkerhetsmålene, er illustrert i figur 1.4, som også viser en analogi til hvordan sivil sikkerhet med målsetting om å opprettholde lov og orden støttes ved å ha politi og sikkerhetsvakter med egnet utstyr (tiltak).

Å si at et sikkerhetsmål skal oppfylles, sier i seg selv intet om hvordan det skal gjøres i praksis, og er i utgangspunktet uavhengig av implementering. Det er opp til de som jobber med informasjonssikkerhet i en organisasjon, å velge de best egnede tiltakene for å oppnå sikkerhetsmål for informasjonsverdier. Når valg av tiltak gjøres, velger man samtidig spesifikke tjenester og mekanismer som kan være bundet til enkelte produkter og leverandører.



Figur 1.4. Sammenheng mellom sikkerhetsmål og sikkerhetstiltak, med analogi til sivil sikkerhet.

1.6 Trusler, sårbarheter, verdier, hendelser og risikoer

Det er viktig å ha en klar begrepsforståelse for å kunne snakke presist om informasjonssikkerhet. Sentrale begreper er trusler, sårbarheter, verdier, hendelser, risikoer og tiltak. Det er også essensielt å forstå sammenhengen mellom disse begrepene, som beskrives nedenfor.

- **Trusselaktør:** En trusselaktør er en aktiv entitet som kan utløse eller gjennomføre et trusselscenario. Trusselaktører kan være intelligente entiteter med bevisst skadehensikt eller naturkrefter som er for sterke eller uforutsigbare for effektiv forebygging.
- **Trusselscenario:** Et trusselscenario er en sekvens av trinn som kan utløses eller styres av en trusselaktør, og som kan skade informasjonsverdier. Et trusselscenario er mulig å gjennomføre og kan føre til en hendelse når det fins sårbarheter (svakheter).
- **Sårbarhet:** En sårbarhet representerer en svakhet, feil eller mangel som gjør at (et trinn i) et trusselscenario kan gjennomføres, noe som dermed gjør det mer sannsynlig at en trusselaktør vil lykkes i et angrep som fører til en hendelse. En sårbarhet kan også tolkes som en mangel på sikkerhetstiltak, det vil si at sårbarheten kan fjernes ved å innføre ett eller flere sikkerhetstiltak. De tre hovedkategoriene av sårbarheter er:
 - tekniske sårbarheter, som er svakheter i systemer, nettverk, programvare og maskinvare,
 - prosesssårbarheter, det vil si svakheter i funksjoner og aktiviteter, og svakheter i sammenheng av disse,
 - menneskelige sårbarheter, som er svakheter i menneskelig bevissthet, holdning og atferd.

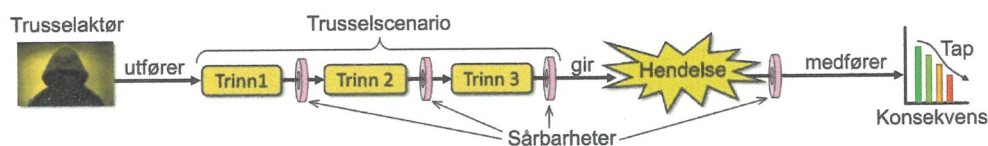
En *sårbarhetsflate* er alle mulighetene en trusselaktør kan utnytte som del av angrep. Å minske sårbarhetsflaten vil redusere risikoen, som naturligvis er ønskelig, men vil som regel ha en kostnad og kan redusere funksjonalitet, slik at det blir en avveining. Noen ganger skiller man mellom *svakheter* og *sårbarheter*, der en svakhet representerer en abstrakt type sårbarhet uten referanse til et reelt system, mens en sårbarhet er en instans av en svakhet i et spesifikt system. Dette skillet gjøres for eksempel av CVSS (Common Vulnerability Scoring System) beskrevet i avsnitt 3.3.

- **Sikkerhetstiltak:** Et sikkerhetstiltak (eng.: security control) er en måte å hindre eller bremse et trusselscenario på slik at det ikke (lett) kan gjennomføres. Å innføre sikkerhetstiltak er det samme som å fjerne sårbarheter. Det fins en rekke forskjellige tiltak som kan deles inn i kategorier, se figur 1.6. Noen norske miljøer bruker også ordet «kontroll», som er en direkte oversettelse fra engelsk.
- **Verdi:** En informasjonsverdi kan være informasjon, men også en ressurs for representering og behandling av informasjon. Eksempler på informasjonsverdier er data, fysisk IT-utstyr og infrastruktur, systemer, konfigureringer, programvare, applikasjoner og til og med menneskelige ressurser.
- **Hendelse:** En sikkerhetshendelse er at det oppstår et brudd på konfidensialitet, integritet eller tilgjengelighet (brudd på et KIT-sikkerhetsmål) for en informasjonsverdi som resulterer i en negativ konsekvens for eier av informasjonsverdien. Under risikoanalysen forsøker man blant annet å estimere sannsynlighet for at hendelser inntreffer. Det kan skilles mellom hendelser som følge av en tilsiktet handling i motsetning til hendelser som følge av andre årsaker, som feil, ulykker og naturskade. Begge typer hendelser kan gi brudd på informasjonssikkerhet, men kun den ene er forårsaket av en målrettet trusselaktør. Fagområdet informasjonssikkerhet dekker begge typer hendelser, men fokuserer mest på tilsiktede hendelser.
- **Konsekvens:** En konsekvens av en sikkerhetshendelse er en form for tap som kan ha ulike aspekter, som tappt fortjeneste/profitt (for kommersielle selskaper), tap av ytelser/

tjenester (for ikke-kommersielle organisasjoner), tap av omdømme, kostnader som følge av brudd på juridisk etterlevelse eller kostnader ved gjenoppretting av skaden etter hendelsen. Under risikoanalysen forsøker man blant annet å estimere størrelsen eller alvorligheten av konsekvensen. Ulike former for konsekvens av en sikkerhetshendelse gir også føringer for hvordan vi omtaler hendelsen. Den kan f.eks. kalles avvik, sikkerhetstruende hendelse, kompromittering eller sikkerhetsbrudd.

- **Risiko:** En informasjonssikkerhetsrisiko er en relevant kombinasjon av trussel, sårbarhet og potensiell sikkerhetshendelse som kan berøre en informasjonsverdi. Risikoidentifisering er å kartlegge slike relevante kombinasjoner. Å gjøre en risikoanalyse er å kombinere estimert sannsynlighet for en hendelse og estimert alvorlighet av konsekvensene for å beregne nivået eller størrelsen på tilhørende risiko.

Figur 1.5 viser dynamikken mellom trusselaktør, trusselscenario, sårbarhet, hendelse og konsekvens. Eksemplet i figuren indikerer sårbarheter som kan utnyttes ved ulike trinn i trusselscenarioet, som betyr at trusselen har større sannsynlighet for å nå angrepsmålet og skape en hendelse. Når hendelsen inntreffer, kan det få ulike konsekvenser avhengig av evne til gjenoppretting. Manglende sikkerhetskopi eller dårlig beredskap er også sårbarheter som typisk medfører at konsekvensene blir mer alvorlige enn de ellers ville blitt.



Figur 1.5. Dynamikken mellom trussel, sårbarheter, hendelse og konsekvens.

Et sikkerhetstiltak har typisk til hensikt å forhindre et trusselscenario, eller å redusere negative konsekvenser. Å innføre et slikt sikkerhetstiltak er det samme som å fjerne sårbarheter som utnyttes i de tilhørende trinnene i trusselscenarioet, eller å styrke cyberberedskap ved hendelser. Hensikten er å redusere sannsynlighet for at trusselscenarioet kan fullføres og gi en hendelse, og å redusere konsekvensene i tilfelle hendelsen inntreffer likevel.

1.7 Tiltak for informasjonssikkerhet

Sikkerhetstiltak kan kategoriseres på forskjellige måter, selv om de alle støtter sikkerhetsmålene konfidensialitet, integritet og tilgjengelighet (KIT) på en eller annen måte. En mulig kategorisering kan være å skille mellom forebyggende, oppdagende og korrigerende tiltak.

- **Forebyggende tiltak** skal forhindre hendelser slik at de (helst) ikke inntreffer. Eksempler er autentisering og tilgangskontroll som skal sørge for at uautoriserte ikke får tilgang til informasjon og ressurser. Denne typen tiltak kalles også «sannsynlighetsreduserende tiltak», siden de reduserer sannsynligheten for sikkerhetshendelser.

- **Oppdagende tiltak** skal gjøre det lett å oppdage angrep og hendelser. Et eksempel er IDS (Intrusion Detection System) som trigger alarmer etter bestemte kriterier. I noen tilfeller kan slike tiltak oppdage angrep på et så tidlig tidspunkt at det ennå ikke har skjedd noe sikkerhetsbrudd, men som regel dreier oppdagende tiltak seg om å redusere tiden fra hendelsen inntreffer, til korrektive tiltak kan iverksettes.
- **Korrektive tiltak** brukes for å reparere skade og gjenopprette drift etter en hendelse. Et eksempel er sikkerhetskopier som kan hentes og reinstallerer hvis driftsdata går tapt eller blir ødelagt. Et annet eksempel er å lage planer for, og øve på, cyberberedskap, slik at virksomheten er godt forberedt hvis en hendelse skulle inntreffe.

NSMs *Grunnprinsipper for IKT-sikkerhet* beskrevet i avsnitt 12.4 benytter en lignende kategorisering med 4 kategorier, som er 1) Identifisere og kartlegge, 2) Beskytte og opprettholde, 3) Oppdage, 4) Håndtere og gjenopprette.

En annen kategorisering av sikkerhetstiltak er i henhold til tematiske områder som kartlegging av verdier, risikovurdering, identitets- og tilgangshåndtering, bevissthet og opplæring, nettverkssikkerhet, programvaresikkerhet, skysikkerhet, sikker konfigurering, hendelseshåndtering osv. En slik kategorisering brukes for eksempel i CIS Security Controls,³ i NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations,⁴ og var brukt i den tidlige utgaven av standarden ISO/IEC 27002:2013.

En tredje type kategorisering er å skille mellom organisatoriske tiltak, fysiske tiltak og teknologiske tiltak, som vist i figur 1.6. En svært lik kategorisering brukes i den siste utgaven av standarden *ISO/IEC 27002:2022 Sikkerhetstiltak* beskrevet i avsnitt 12.3.4, bortsett fra at denne standarden skiller ut tiltak for personellsikkerhet som egen kategori. I figur 1.6 er personellsikkerhet inkludert i kategorien av organisatoriske tiltak, som kan være naturlig.



Figur 1.6. Kategorisering av sikkerhetstiltak.

³ <https://www.cisecurity.org/controls>.

⁴ <https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search/>.

De ulike måtene å kategorisere sikkerhetstiltak på beskrevet ovenfor dekker naturligvis de samme tiltakene – det er bare alternative måter å dele opp sikkerhetstiltakene på i forskjellige grupper/kategorier. En virksomhet må velge de tiltak som virker mest formålstjenlige for styring av informasjonssikkerhet. Dette må betraktes ut fra antatt avkastning på investering (ROI: Return on Investment), som betyr oppnådd risikoreduksjon med et sikkerhetstiltak i forhold til kostnad ved etablering og drift av tiltaket. Denne typen vurdering er nærmere beskrevet i kapittel 14. Det bør også vurderes om tiltak kan ha negative sideeffekter, noe som kan uttrykkes som en kostnad. Det er som regel nødvendig å ha sikkerhetstiltak fra alle kategoriene med hensyn til forebygging/oppdaging/korrigerende av hendelser, og med hensyn til organisatoriske/fysiske/teknologiske tiltak.

1.8 KIT-sikkerhetsmålene

Avsnitt 1.4 presenterte definisjonen på informasjonssikkerhet, som betyr å opprettholde sikkerhetsmålene konfidensialitet, integritet og tilgjengelighet, forkortet til KIT på norsk eller CIA (Confidentiality, Integrity & Availability) på engelsk. KIT-sikkerhetsmålene beskrives nedenfor.

1.8.1 Konfidensialitet

Konfidensialitet er kanskje det sikkerhetsmålet folk først og fremst tenker på i forbindelse med informasjonssikkerhet. Alle organisasjoner og privatpersoner har behov for å beskytte informasjon de besitter, mot at uvedkommende får tilgang. ISO/IEC 27000 gir en enkel definisjon:

«Konfidensialitet er egenskapen at informasjon ikke blir gjort tilgjengelig eller vist til uautoriserte individer, entiteter eller prosesser.»

(ISO/IEC 27000)

Denne definisjonen er i utgangspunktet lett å forstå, men det er likevel viktig å legge merke til begrepet «uautorisert», for hvis det er uklart hvem som er autorisert eller ikke, blir begrepet konfidensialitet faktisk meningsløst. Her hersker det en del forvirring som det må styres unna, noe vi kommer tilbake til i avsnitt 1.10 om autorisering og tilgangskontroll.

Generelle trusler mot konfidensialitet er *datatyveri* begått av eksterne aktører eller *datalekkasje* forårsaket av interne, enten ved uhell eller tilsiktet.

Sikkerhetstiltak som støtter konfidensialitet, er for eksempel følgende:

- Brukerautentisering og tilgangskontroll for å beskytte lagret informasjon
- Kryptering av data for beskyttelse under lagring eller overføring
- Sikkerhetsfunksjoner i operativsystemer for å beskytte informasjon under prosessering
- Vakter og fysisk adgangskontroll

Listen over tiltak ovenfor er overhodet ikke uttømmende. En rekke andre tiltak bidrar direkte eller indirekte til å opprettholde konfidensialitet, som f.eks. sikkerhetskultur, policyer, prosedyrer og praksis.

1.8.2 Dataintegritet

Begrepet *integritet* kan ha ulike betydninger, der særlig to typer integritet er sentrale for informasjonssikkerhet. Vi kaller disse dataintegritet og systemintegritet. Dataintegritet beskrives her, mens systemintegritet beskrives i neste avsnitt.

En god definisjon på dataintegritet fins i standarden X.800:⁵

«Integritet er egenskapen at data ikke har blitt endret eller slettet på en uautorisert måte.»

(X.800)

Definisjonen på integritet fra X.800 er intuitivt lett å forstå, og er i tråd med definisjonen på konfidensialitet fra ISO/IEC 27000 ved at den også benytter begrepet «uautorisert». For definisjonen på integritet fra X.800 er det også essensielt å vite hvem som er autorisert eller ikke, for hvis det er uklart, blir dataintegritet også meningsløst.

Generelle trusler mot dataintegritet er korrupte data, for eksempel forårsaket av eksterne aktører, eller innsidetrusler enten ved uhell eller tilsiktet. Uautorisert sletting av data eller uautorisert oppretting eller endring av data og filer utgjør også brudd på dataintegritet. Dataintegritet er i prinsippet ekvivalent med data-autentisitet, for hvis data er endret på en uautorisert måte, er dataene ikke lenger autentiske; eller omvendt, hvis data mangler autentisitet, er integriteten uviss.

Sikkerhetstiltak som støtter dataintegritet, kan være følgende:

- Brukerautentisering og tilgangskontroll for å beskytte lagret informasjon
- Kryptering eller kryptografisk sjekksum av data for beskyttelse under lagring eller overføring
- Sikkerhetskopier av data
- Vakter og fysisk adgangskontroll

Sikkerhetstiltak for dataintegritet er mange av de samme som for konfidensialitet. Listen over tiltak ovenfor er heller ikke uttømmende. En rekke andre tiltak kan også bidra direkte eller indirekte til å opprettholde dataintegritet.

⁵ X.800: *Security architecture for Open Systems Interconnection for CCITT applications* (1991).

1.8.3 Systemintegritet

En god definisjon på systemintegritet fins i standarden ISO/IEC 27000:

«Integritet er egenskapen av å opprettholde korrekthet og komplettethet av dataressurser.»

(ISO/IEC 27000)

Definisjonen på integritet fra ISO/IEC 27000 er relativt abstrakt, noe som åpner for tolkning av hva som menes med komplettethet og korrekthet, og hva som menes med dataressurs. Definisjonen refererer ikke til autoriserte entiteter, slik at det kun er implisitt hvem som bestemmer hva som er korrekt og komplett, men det naturlige er at eieren av dataressursen er den som bestemmer det. Begrepet dataressurs kan tolkes som data, slik at definisjonen dekker dataintegritet. Begrepet dataressurs kan også tolkes som systemer og applikasjoner som prosesserer data, slik at definisjonen også dekker systemintegritet. Systemintegritet betyr for eksempel at systemer, applikasjoner og nettverkskomponenter har riktig konfigurasjon, korrekt programvare og oppdatert patch-status.

Generelle trusler mot systemintegritet er misconfigurerte systemer forårsaket av eksterne trusselaktører eller av interne ved uhell eller tilsiktet, og utdatert programvare som kan være forårsaket av mangelfull forvaltning av systemer og programvare. Sikkerhetstiltak for å opprettholde integritet kan være følgende:

- Brukerautentisering og tilgangskontroll for alle, og sterk autentisering for admin-brukere
- Konfigurasjonsstyring
- Endringsledelse

En rekke andre tiltak kan også bidra direkte eller indirekte til å opprettholde systemintegritet.

1.8.4 Tilgjengelighet

Tilgjengelighet av informasjonsressurser er et essensielt sikkerhetsmål, for uten tilgjengelighet har IT-systemer ingen nytte. En god definisjon på tilgjengelighet er å finne i ISO/IEC 27000:

«Tilgjengelighet er egenskapen at data og tjenester er tilgjengelige og anvendbare ved forespørsel fra en autorisert entitet.»

(ISO/IEC 27000)

Begrepet «autorisert» er viktig å legge merke til, for hvis det er uklart hvem som er autorisert, er det uklart hvem tilgjengeligheten skal gjelde for.

Generelle trusler mot tilgjengelighet er tjenestenekt (DoS/DDoS), hindring av autorisert tilgang til ressurser og forsinkelse av tidskritiske funksjoner.

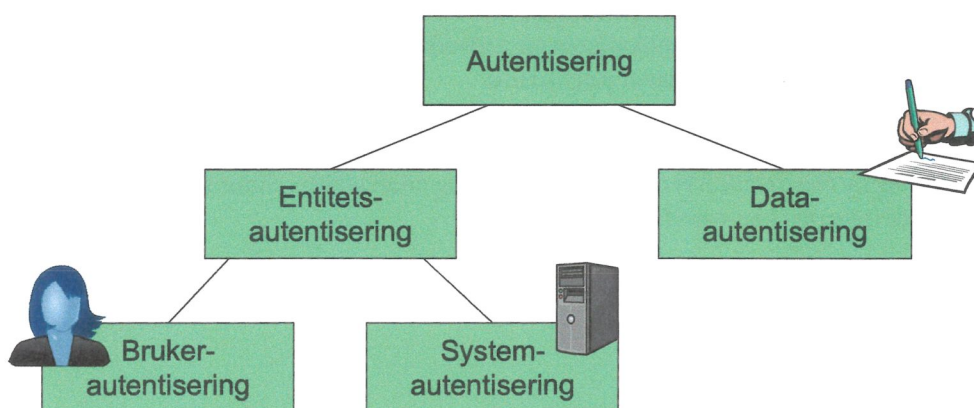
Sikkerhetstiltak som støtter tilgjengelighet, kan være filtrering av skadetraffikk, redundans av ressurser, lastdeling for prosessering, sikkerhetskopier, hendelsesrespons og beredskap.

1.9 Andre sikkerhetsmål

Ettersom standarden ISO/IEC 27000 også nevner autentisitet, sporbarhet, ubenektelighet og pålitelighet som sikkerhetsmål, er disse begrepene kort beskrevet i avsnittene nedenfor.

1.9.1 Autentisering

Autentisering er en svært viktig funksjon som støtter KIT-sikkerhetsmålene konfidensialitet, integritet og tilgjengelighet. Begrepet autentisering er relativt generelt, med flere ulike betydninger. Figur 1.7 gir en oversikt over hovedtypene av autentisering.



Figur 1.7. Hovedtyper av autentisering.

De ulike autentiseringstypene er forklart nedenfor.

Brukerautentisering

Brukerautentisering er å verifisere korrektheten av en brukers identitet.

Brukerautentisering er den sikkerhetsmekanismen vi oftest møter og bruker i omgang med våre digitale omgivelser. Typisk består brukerautentisering av to trinn: 1) oppgi bruker-ID og 2) bevis at du er den legitime bruker ved å oppgi autentikator, som for eksempel passord, engangskode med brikke eller fingeravtrykk. Brukere er tradisjonelt mennesker, men botter

(robotprogrammer) tar i økende grad rollen som brukere for å utføre rutinemessige funksjoner. I slike anvendelser gjelder autentisering og tilgangskontroll også for botter.

Generelle trusler mot autentisering er identitetstyveri, falsk identitet og falsk innlogging. Begrepet *spoofing* benyttes ofte om å forfalske identitet. Sikkerhetstiltak for å styrke autentisering er for eksempel tofaktor-autentisering basert på to uavhengige autentikatorer eller å bare sørge for å bruke sterke passord.

Angrep mot brukerautentisering er en svært vanlig angrepsvektor. Her gjelder prinsippet om at en kjede ikke er sterkere enn det svakeste ledd, det vil si at hvis bare én bruker i en organisasjon har et svakt passord, klarer angripere å få uautorisert tilgang. Sagt på en annen måte: Det er mye å hente på å sørge for at alle følger gode rutiner rundt brukerautentisering og autentikatorer.

Brukerautentisering er beskrevet i detalj i kapittel 8 om brukerautentisering og i kapittel 9 om identitets- og tilgangshåndtering.

Systemautentisering

Systemautentisering er å verifisere korrektheten av et systems identitet.

Systemer kan være webtjenere, backend-tjenere, databasetjenere, rutere, skytjenere osv. Når slike systemer kommuniserer med hverandre, er autentisering som regel integrert. Kommunikasjonen, altså utveksling av data og meldinger, følger en kommunikasjonsprotokoll som definerer hvordan meldingene skal se ut slik at systemene forstår hverandre. Sikkerhets- og autentiseringsprotokoller definerer hvordan systemer skal autentisere hverandre, og er basert på kryptografi.

Generelle trusler mot systemautentisering er falske noder i nettverk, falske datatransaksjoner, mellommannsangrep (eng. man-in-the-middle-attack) og nettverksinnbrudd.

Sikkerhetstiltak er som nevnt bruk av kryptografiske autentiseringsprotokoller for autentisering og integritet. Kommunikasjons- og sikkerhetsprotokoller for autentisering er beskrevet i kapittel 6 om nettverkssikkerhet.

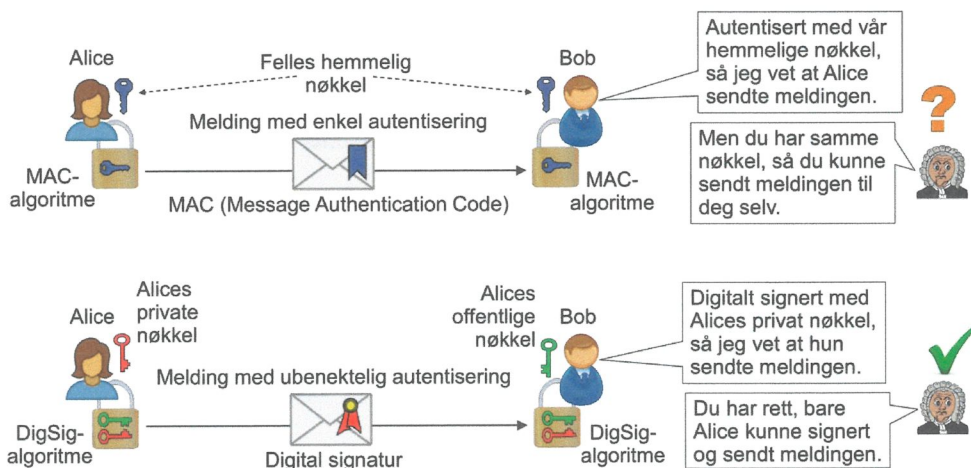
Data-autentisering

Data-autentisering er å verifisere opphav eller avsender av data.

Data er ingen entitet. Data er passive, virtuelle og uavhengige av fysisk representasjon. Data-autentisering betyr at noen ønsker å vite hvor data kommer fra, eller hvem som har generert dem. Sagt på en annen måte betyr data-autentisering å verifisere ektheten av dokumenter og informasjon og at de kan spores til en avsender eller forfatter. Mens bruker- og systemautentisering typisk bare gjelder ved innlogging eller for en enkelt økt, er det ofte krav om at data-autentisitet skal kunne verifiseres og ha gyldighet over mange år eller så lenge som mulig.

Generelle trusler mot data-autentisering er forfalskning av digitale dokumenter og forfalskning av meldinger sendt gjennom datanett. En mekanisme for data-autentisering er *MAC (Message Authentication Code)*, som er en kryptografisk sjekksum på en melding som kan verifiseres av en spesifikk mottager. En sjekksum er en bit-sekvens, typisk på 256 bits, som beregnes over et dokument av vilkårlig størrelse. Hvis en eneste bit endres i dokumentet, vil sjekksummen ikke lenger stemme. Dermed kan sjekksummen brukes til å verifisere at dokumentet ikke er blitt endret. En sterkere mekanisme for data-autentisering, og som støtter ubenektelighet, er en *digital signatur* som også er en kryptografisk sjekksum på en melding. Forskjellen er at en digital signatur kan verifiseres av tredjeparter (dvs. av hvem som helst), ikke bare av en spesifikk mottager. Begrepet ubenektelighet (ikke-benekting) betyr nettopp at autentisitet er ubenektelig fordi det eksisterer et kryptografisk bevis for at en bestemt aktør har utført en bestemt handling som kan verifiseres av tredjeparter.

For å klargjøre forskjellen mellom enkel data-autentisering med MAC, på den ene side, og ubenektelig autentisering med digital signatur, på den andre, anta en situasjon der Alice har sendt en ordre til aksjemegler Bob om å kjøpe akser i et selskap. Dagen etter synker aksjekursen kraftig, noe som vil medføre store tap for Alice. For å komme seg ut av situasjonen hevder Alice at hun aldri sendte ordren og krever transaksjonen annullert, mens Bob hevder at hun sendte ordren. Det blir rettssak for å fastslå hvem som har rett. Her er det avgjørende om ordrens autentisitet er basert på MAC eller digital signatur, slik som vist i figur 1.8. For MAC brukes felles hemmelig nøkkel delt mellom Alice og Bob til å både generere og verifisere en sjekksum for data-autentisitet. For digital signatur bruker Alice sin private nøkkel for å generere signaturen, mens Bob eller andre tredjeparter bruker hennes offentlige nøkkel for å verifisere signaturen.



Figur 1.8. Forskjell mellom enkel autentisering med MAC og ubenektelig autentisering med digital signatur.

Figur 1.8 viser at MAC beviser for Bob at Alice sendte meldingen, men at MAC ikke lar Bob bevise dette overfor tredjeparter. En digital signatur gir bevis både for Bob og tredjeparter at Alice sendte meldingen. Forskjellen er at MAC gir autentisitet, mens digital signatur gir ubenektelighet, noe som egentlig er en sterk form for autentisitet.

Bruk av digital signatur er avhengig av en *PKI (Public Key Infrastructure)*, også kalt offentlig nøkkel-infrastruktur, og er en relativt komplisert mekanisme sammenlignet med MAC, som kun trenger utveksling av en hemmelig nøkkel mellom to parter (selv om det kan være komplisert nok).

Dessverre kan hverken data-autentisering med MAC eller med digital signatur gi garanti-er for evigheten fordi de underliggende kryptografiske algoritmene har begrenset gyldighet, typisk ikke mer enn 30 år.

MAC og digital signatur beskrives i kapittel 4 om kryptografi.

1.9.2 Sporbarhet og ubenektelighet

Sporbarhet betyr at aktiviteter i et system eller datanett kan spores til noen som kan stilles til regnskap for aktivitetene.

Sporbarhet er en svært viktig funksjon for deteksjon, etterforskning og gjenoppretting av skade etter sikkerhetshendelser. Sporbarhet er basert på logging av aktiviteter i systemer og nettverk, og kartlegger hvilken bruker eller annen entitet som står bak hver logget aktivitet.

I kontekst av informasjonssikkerhet er «sporbarhet» en oversettelse av det engelske begrepet «accountability», som betyr å stå til regnskap for noe. I stedet for sporbarhet kunne en alternativ oversettelse av accountability være «regnskapelighet».

Generelle trusler mot sporbarhet er nettopp mangel på sporbarhet, det vil si at det ikke er mulig å identifisere hvem som sto bak en handling, og at det mangler tilstrekkelig bevis for å kunne anmelde en hendelse og for fremleggelse i en eventuell retts sak.

Sikkerhetsmekanismer for sporbarhet kan være autentisering av alle brukere og logging av systemhendelser. Logging kan gjøres på forskjellige måter, og kan kombineres med data-autentisering for å beskytte datalogger mot endring. Digital etterforskning (beskrevet i avsnitt 16.6) kan også bidra til sporbarhet ved at sammenhenger som ikke kommer direkte frem av logger, kan avdekkes gjennom analyse av utstyr, data og andre bevis.

Ubenektelighet er at en entitet ikke kan benekte å ha utført en handling.

Ubenektelighet (eng. non-repudiation), også kalt *ikke-benekting*, er basert på digital signatur, og betyr at den som har digitalt signert en melding, en transaksjon eller et dokument, ikke kan benekte å ha gjort nettopp det. Ubenektelighet er relatert til sporbarhet fordi en digital signatur antas å være et ubenektelig spor til hvem som har sendt en melding, utført en transaksjon eller forfattet et dokument. Imidlertid er en digital signatur aldri absolutt ubenektelig.

Hvis en person ønsker å benekte å ha utført en digital signatur, kan hen bare hevde at den private signaturnøkkelen ble stjålet, og at signaturen derfor ble utført av en annen. Digital etterforskning kan være nødvendig for å vurdere sannheten av en slik påstand.

1.9.3 Pålitelighet

Pålitelighet av et system betyr at det ikke inneholder betydelige feil eller svakheter, og at systemet har evne til å opprettholde viktig funksjonalitet selv når enkelte feil forekommer.

Pålitelighet betyr hovedsakelig evnen til å motstå ikke-tilsiktete hendelser (dvs. feil), men betyr samtidig at systemer opprettholder viktig funksjonalitet ved både tilsiktete og utilsiktede hendelser. Pålitelighet er særlig viktig for tilgjengelighet som sikkerhetsmål.

Generelle trusler mot pålitelighet er lav kvalitet i utvikling, konfigurering og drift av systemer samt spesielt manglende oppmerksomhet på sikker systemutvikling.

Tiltak for god pålitelighet er rett og slett å følge god praksis for sikker utvikling og drift av systemer, som kalles «innebygd informasjonssikkerhet», beskrevet i kapittel 11.

1.10 Autorisering og tilgangskontroll

Det er viktig med en god forståelse av begrepet autorisering ettersom definisjoner på KIT-sikkerhetsmålene beskrevet i avsnitt 1.8 er basert på hvem som er autorisert eller ikke.

Tilgangsautorisering er å spesifisere tilgangsrettigheter for brukere, roller og prosesser.

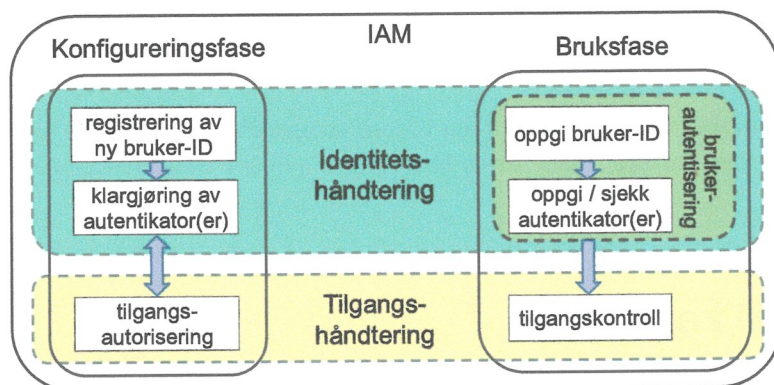
Spesifiseringer av tilgangsrettigheter kalles typisk *tilgangsregler* eller *tilgangspolicy*. Tilgangsautoriseringer er basert på hvilken rolle brukeren har i en virksomhet, og blir formalisert som regler og konfigurering i systemer for tilgangskontroll.

Autoriteter i en organisasjon har ansvar for autorisering, men autoriseringsfunksjonen kan bli delegert som f.eks. Leder → Systemadministrator → Bruker.

Tilgangskontroll er å benytte spesifiserte tilgangsrettigheter for å beslutte om tilgang til ressurser skal gis eller ikke når en autentisert bruker gjør en forespørsel om tilgang.

Brukeren må være logget inn slik at systemet kjenner identiteten og dermed kan finne gjeldende tilgangsrettigheter for å ta beslutning om brukeren skal få tilgang til forespurte ressurser.

Begrepet *IAM* (*Identity and Access Management*), eller identitets- og tilgangshåndtering, kan beskrives med en konfigureringsfase og en bruksfase, som hver består av trinn, som illustrert i figur 1.9. Brukerkonto og autentikatorer må opprettes og konfigureres før det er mulig å utføre brukerautentisering i bruksfasen. På samme måte må tilgangsautoriseringer spesifiseres og konfigureres før brukeren kan få tilgang til ressurser for å utføre oppgaver i bruksfasen. IAM knytter sammen trinnene for registrering og autorisering av brukere i konfigureringsfasen, og brukerautentisering og tilgangskontroll i bruksfasen. Brukerautentisering er beskrevet i kapittel 8, og IAM er beskrevet i kapittel 9.



Figur 1.9. Faser og trinn i IAM (identitets- og tilgangshåndtering).

I konfigureringsfasen blir nye brukere registrert med ny bruker-ID og får utdelt og klargjort nødvendige autentikator(er). Ut fra brukerens rolle i organisasjonen blir tilgangsrettigheter spesifisert i autoriseringstrinnet. En nyansatt i personalavdelingen er typisk autorisert til å lese og redigere alle ansattprofiler som inneholder lønnsinformasjon og andre personlige ting. På den annen side vil en nyansatt i salgsavdelingen som regel ikke bli autorisert for å lese ansattprofiler om kollegaer.

I bruksfasen skjer brukerautentisering under innlogging ved at brukeren oppgir bruker-ID og autentikator(er) som blir sjekket av systemet. Etter innlogging kan brukeren gjøre forespørsel om å åpne dokumenter eller bruke tjenester. Tilgangskontroll består av at systemet sjekker gjeldende autoriseringspolicy/-regler for å avgjøre om brukeren skal få tilgang til forespurte dokumenter og tjenester.

Ofte vil systemer/applikasjoner kun gjøre synlig de ressurser som brukeren er autorisert for, mens andre ganger er alle ressurser synlige, og systemet avslår tilgang dersom brukeren forespur noe hen ikke er autorisert for. Å definere autoriseringspolicy er en form for konfigurering, mens tilgangskontroll er en del av vanlig bruk. Modeller for tilgangsautorisering og tilgangskontroll er beskrevet i avsnitt 9.3.

Det er en klar forskjell mellom autorisering og tilgangskontroll. Dessverre blandes ofte disse begrepene i litteratur og lærebøker ved feilaktig å si at autorisering er det samme som tilgangskontroll. Imidlertid blir det helt absurd hvis trinnet med tilgangskontroll i figur 1.9

defineres som autorisering. Som forklart i avsnitt 1.8 ovenfor er KIT-sikkerhetsmålene konfidensialitet, integritet og tilgjengelighet definert med utgangspunkt i hvem som er autorisert eller ikke. Ved å definere autorisering som ekvivalent med tilgangskontroll ville enhver person som faktisk får tilgang, per definisjon være autorisert, enten denne personen er en genuin bruker eller en hacker. Det ville gjøre KIT-sikkerhetsmålene, og informasjonssikkerhet generelt, helt meningsløse. Dette kan illustreres med følgende scenario:

Tenk deg at du urettmessig får tak i en annen persons passord, som du bruker til å stjele informasjon fra vedkommendes brukerkonto. Din kriminelle handling blir oppdaget, du blir anmeldt for uautorisert uthenting av informasjon, og det blir rettssak. Når aktor ber deg om å forklare din handling, tar du frem en lærebok om informasjonssikkerhet (ikke denne!) der det for eksempel står: «Etter innlogging vil systemet autorisere brukeren for tilgang til dataressursene.» Du argumenterer med at du logget deg inn, og at du dermed var autorisert for tilgang til ressursene.

Basert på en slik lærebok har du logisk sett rett i denne argumentasjonen, men det spørs likevel om du hadde vunnet saken. Aktor kunne for eksempel referere til læreboken du nå holder i hånden.

Oppgaver til kapittel 1

1.1 Tilgangsautorisering

- a. X.800 er en standard for sikkerhetstjenester i OSI (Open Systems Interconnection). Søk og finn X.800-standarden, eller besøk <https://www.itu.int/rec/T-REC-X.800-199610-I!Amd1/en>. Les definisjonene av konfidensialitet, integritet og autorisering i X.800. Er definisjonene av konfidensialitet og integritet fra X. 800 meningsfulle i forhold til hvordan autorisering er definert? Hvorfor eller hvorfor ikke?
- b. Hvordan er autorisering definert på Wikipedia? <https://en.wikipedia.org/wiki/Authorization>
- c. Forklar om definisjoner av konfidensialitet, integritet og tilgjengelighet (KIT) i standardene X.800 og ISO/IEC 27000 gir mening på bakgrunn av Wikipedias definisjon av autorisering.

1.2 Eksempler på angrep som kan gi brudd på KIT

Beskriv eksempler på angrep som kan forårsake sikkerhetsbrudd for hvert KIT-sikkerhetsmål, og mulige tiltak som kan forhindre angrepene. Angrepsbeskrivelsene skal være svært abstrakte, som f.eks. «en hacker stjeler et passord og overtar brukerkontoen til en annen person».

- a. Konfidensialitet
- b. Integritet
- c. Tilgjengelighet

1.3 Trusler mot IAM (identitets- og tilgangshåndtering)

En enkel metode for å identifisere trusler er å spørre «Hva kan gå galt?» eller «Hvordan kan dette angripes?».

- a. Nevn relevante trusler mot (trinnene i) konfigureringsfasen av IAM (identitets- og tilgangshåndtering).
- b. Nevn relevante trusler mot (trinnene i) bruksfasen av IAM (identitets- og tilgangshåndtering).

Kapittel 2

Angrepsvektorer og skadevare

Læringsmålene for dette kapitlet er at du skal få en oversikt over de vanligste angrepsvektorene og de vanligste formene for skadevare. Angrepsvektorer er praktiske metoder og kanaler som benyttes av trusselaktører for å påvirke og angripe verdier hos en virksomhet. En angrepsvektor er generelt sett det samme som et trusselscenario, som er definert i avsnitt 1.6. Skadevare er data og programkode som trusselaktøren overfører til og/eller kjører i infrastrukturen til virksomheten som angripes, og som kan resultere i skade på virksomhetens informasjonverdier.

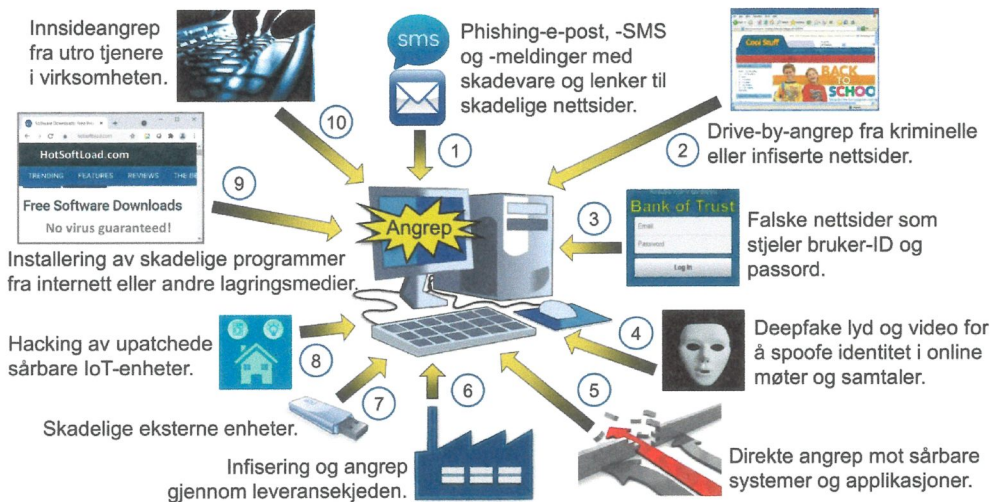
2.1 Angrepsvektorer

En *angrepsvektor* er en måte å utføre angrep på, eller en måte å hacke på. Et angrep benytter typisk en eller flere kanaler for kommunikasjon, tilgang eller påvirkning for å sende skadelig innhold og/eller utføre skadelig aktivitet i virksomhetens infrastruktur. Hensikten med et angrep er typisk å infisere eller ødelegge systemer og nettverk, eller å stjele eller ødelegge data. Angrepsvektorer utnytter sårbarheter, inkludert for eksempel menneskelig mangel på bevissthet gjennom sosial manipulering. Angrepsvektorer er generelt sett det samme som trusler. Når man foretar trusselmodellering, som betyr å kartlegge mulige og relevante cybertrusler mot egen virksomhet, er klassiske angrepsvektorer det første man bør tenke på. Trusselmodellering er nærmere beskrevet i kapittel 11 om innebygd informasjonssikkerhet, og i kapittel 14 om risikostyring.

Den vanligste angrepsvektoren i dag er phishing, som består av å sende skadevare eller lenke til skadelige nettsider gjennom villedende e-post og andre direkte meldinger som f.eks. SMS, messenger- og chattemeldinger. Den farligste sårbarheten for denne typen angrep er mangel på kunnskap og bevissthet hos oss brukere, slik at vi lar oss lure til å klikke på farlige lenker, åpne skadelige dokumenter eller installere skadevare.

Brannmurer og antivirusfilter kan til en viss grad blokkere mot slike angrepsvektorer, men det fins ingen metoder som gir 100 % beskyttelse. En forsvarsmetode kan fort bli ut-

datert, ettersom hackere kontinuerlig forbedrer og utvikler nye angrepsmetoder. Figur 2.1 viser eksempler på typiske angrepsvektorer. Hver angrepsvektor kan benyttes separat eller i kombinasjon med andre for å øke angrepspotensen ytterligere.



Figur 2.1. Vanlige angrepsvektorer.

Listen over angrepsvektorer i figur 2.1 er naturligvis ikke uttømmende. DDoS (Distributed Denial of Service) er også en betydelig angrepsvektor (se avsnitt 6.4.3). Noen litt mer spesielle angrepsvektorer er for eksempel avlytting av elektromagnetisk utstråling fra digitalt utstyr (se avsnitt 3.10), avlytting av mobiltelefoner med IMSI-fangere (se avsnitt 7.4.3), eller å stjele identiteter med forfalsket biometri (se avsnitt 8.5.3).

Trusselaktører er svært innovative, og nye angrepsvektorer og metoder utvikles kontinuerlig. Samtidig er klassiske angrepsmetoder fremdeles svært potente, og de forbedres stadig. De nummererte angrepsvektorene illustrert i figur 2.1 er beskrevet i avsnittene nedenfor.

2.1.1 Phishing

Phishing, også kalt nettfisking, er en type sosial manipulering som også er beskrevet i avsnitt 13.4. En phishing-e-post er for eksempel formulert for å lure mottageren til å oppgi sensitiv informasjon, til å besøke en falsk nettside eller til å installere skadevare. Navn og e-postadresse for avsender er ofte *spoofet*, det vil si forfalsket, noe som teknisk er enkelt å utføre. Hvis offeret klikker på en lenke til et falskt nettsted, kan angriperen observere alt offeret foretar seg, og kan utføre et mellommannsangrep mot det legitime nettstedet. Mellommannsangrep betyr at den falske nettsiden sender input fra brukeren videre til den ekte nettsiden, og det samme i motsatt retning, som gjør at angriper kan observere og endre data i kommunikasjonen. Massephishing er når samme phishing-e-post blir sendt til mange, som typisk er lett å avsløre fordi innholdet som regel er irrelevant for mottagerne. Spydfishing er når en phishing-e-post blir spesiallaget for en enkelt utvalgt mottager, som dermed høyner sannsynlighet for

at mottageren blir lurt. Fra omtrent år 2020 er phishing den desidert vanligste angrepsvektoren for cyberangrep og datakriminalitet på internett. Andre meldingstyper som SMS eller chattemeldinger kan også benyttes for denne typen sosial manipulering. For eksempel kan telefonnummer til den som ringer, eller til avsender av SMS bli spoofet, slik at vi alltid må vurdere om SMS-meldinger er ekte, eller om den som ringer er den hen gir seg ut for å være. Mangel på kunnskap og bevissthet er den farligste sårbarheten for denne typen angrep. Den beste beskyttelsen er altså å lære å kjenne igjen tegn på phishing, og å være skeptisk.

2.1.2 Drive-by-angrep

Drive-by-angrep er når en nettside sender skadevare til klienten automatisk og uten bruker-interaksjon. Skadevaren kan stjele personlig informasjon som bruker-ID og passord, eller ta kontroll over klienten. Kriminelle nettsteder eies og driftes av angripere, mens infiserte nettsteder er legitime nettsteder der angripere har klart å installere skadelige elementer. Kriminelle nettsteder ser ut som legitime nettsteder. Drive-by-angrep foregår gjennom skjult nedlasting av skadevare til klienten. Det spesielle med drive-by-angrep er at brukeren ikke trenger å klikke på noe, eksplisitt laste ned noe eller åpne noe vedlegg for at klienten skal bli infisert. Brukeren trenger bare å besøke nettsiden for å bli angrepet. *Skadereklame* er reklame som inneholder skadelige skript eller lenker til andre kriminelle eller infiserte nettsteder.

2.1.3 Falske nettsider

Falske nettsider kan være nesten umulig å skille fra ekte nettsider. Brukere kan bli villedet til å besøke en falsk nettside for eksempel gjennom phishing-e-post, gjennom andre falske eller infiserte nettsider eller gjennom skadereklame. En bruker som har havnet på en falsk nettside, kan bli lurt til å oppgi bruker-ID og passord eller annen sensitiv informasjon.

2.1.4 Deepfake

Vi er vant til å kjenne igjen stemmer og ansikter når vi snakker med folk i den fysiske verden. I den virtuelle verden har vi frem til nå kunnet anta med nesten absolutt visshet at stemmen vi hører gjennom telefon, eller ansiktet vi ser i et online-møte, faktisk tilhører den personen som vi kjenner fra før. Men snart kan vi ikke lenger ta det for gitt. Teknologi basert på maskinlæring tvinger oss til å være mer skeptiske til hvem vi tror vi ser og hører online. Verktøy basert på maskinlæring gjør det mulig for en angriper å snakke på en måte som høres ut som deg, eller opptre i et videomøte med ansikt og stemme som deg. Slike forfalskninger kalles *deepfake*, som refererer til at falsk lyd og bilde genereres av teknologi basert på *dype neuralnettverk* (DNN). Dette kalles også *dyplæring*, som er teknologien bak roboter, autonome kjøretøy og ansiktsgjenkjenning. Denne teknologien kan dessverre også benyttes for cyberkriminalitet, for eksempel ved å spoofe identitet til personer i telefonsamtaler eller online-møter. En angriper kan f.eks. spoofe identiteten til virksomhetens direktør under et online-møte, og gi en ansatt med høye autorisasjoner instruks om å overføre en stor pengesum til en konto kontrollert av angriperen. Alternativt kan angriperen spoofe identiteten til en ansatt i en bedrift under et videomøte, og sende en chattemelding med en link til en skadelig nettside. Fordi kollegaer kjenner og stoler på den ansatte, vil de typisk klikke på lenken. Det fins allerede eksempler på slike angrep, og virksomheter må i økende grad være oppmerksomme på denne angrepsvektoren i tiden fremover.

2.1.5 Direkte angrep mot sårbare systemer og applikasjoner

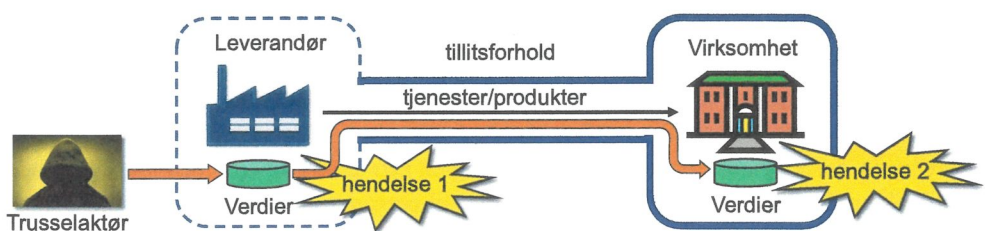
Systemer og applikasjoner som ligger online, er eksponert for trusler fra hele internett. Slike systemer og applikasjoner har ofte sårbarheter som enten er ukjente for system- og programvareleverandører, eller som er kjent, men som virksomheten ikke har rukket å patche. To klassiske angrepsmåter mot sårbare applikasjoner er SQL-injeksjon og XSS (Cross Site Scripting), som er beskrevet i avsnitt 11.7. Angrep og utnyttelse av slike sårbarheter gjøres typisk med automatiserte verktøy gjennom internett.

Passwordspraying betyr at angriperen prøver å logge inn på et stort antall kontoer med standard eller typiske passord. En konto blir vanligvis låst etter tre forsøk med feil passord, men angriperen kan omgå denne hindringen med passwordspraying. Når en ny server installeres, har admin-kontoen ofte et standard passord. Hvis dette passordet ikke endres, er serveren lett å kompromittere.

Automatisk spredning av skadevare kan skje for eksempel gjennom en *dataorm* som automatisk sprer seg til andre computere gjennom datanett og internett. En dataorm utnytter ukjente eller upatched sårbarheter for å infisere en computer, og bruker denne som vert for å skanne og infisere andre computere. Dette utløser en kjedereaksjon som kan gi eksponentiell spredning på kort tid. Foruten å beslaglegge betydelig båndbredde gjennom spredningen kan dataormer ha tilsiktede skadevirkninger.

2.1.6 Leveransekjedeangrep

Et *leveransekjedeangrep* er at trusselaktøren først angriper og kompromitterer produkter og tjenester hos en leverandør, som deretter gjør det mulig å angripe leverandørens kunder. Dette er altså et to-trinnsangrep. En virksomhet som i utgangspunktet har god styring av informasjonssikkerhet i egen infrastruktur, kan likevel være sårbar hvis en angriper for eksempel klarer å installere en skjult bakdør i programvare som virksomheten kjøper av en leverandør. En trusselaktør som klarer å installere en bakdør i programvaren til en programvareleverandør, vil lett kunne angripe alle kunder som benytter samme programvare. På den måten kan leveransekjedeangrep være svært potente. Prinsippet for leveransekjedeangrep er illustrert i figur 2.2.



Figur 2.2. Leveransekjedeangrep.

Som vist i figuren skjer det to sikkerhetshendelser i rekkefølge. Den første hendelsen er når trusselaktøren angriper leverandøren der for eksempel en skjult bakdør eller løsepengevirus blir installert i programvaren som leverandøren utvikler og selger. Ved angrep mot en leve-

randør vil trusselaktøren vanligvis fokusere på å manipulere programvare utviklet av leverandøren, men kan også forsøke å stjele passord, API-nøkler, brannmurregler, kryptografiske nøkler, sertifikater, CRM-data og annen konfidensiell informasjon. I tillegg kan trusselaktøren forsøke å kompromittere maskinvare og prosesser for digital signatur.

Den andre sikkerhetshendelsen skjer når trusselaktøren utnytter kompromittert programvare eller maskinvare ved å skaffe seg uautorisert tilgang til virksomhetens systemer, eller ved å gjennomføre et løsepengangrep.

Fra et sikkerhetsperspektiv representerer leveransekjedene en del av angrepsflaten til virksomheten. Avhengigheten av lange og komplekse leveransekjeder har ført til en dramatisk forstørrelse av angrepsflaten til den typiske virksomheten de siste årene.⁶ Enhver entitet som bidrar i en leveransekjede, har mulighet til å påvirke sikkerheten lenger opp i leveransekjeden. Jo lenger og mer kompleks leveransekjeden er, desto vanskeligere er det å få oversikt over trusler og sårbarheter, og desto vanskeligere er det å håndtere sikkerhetshendelser.

Leveransekjedesårbarhet og *leveransekjederisiko* er betegnelser på sårbarheter og sikkerhetsrisiko knyttet til leveransekjeden. I kapittel 14 beskrives risikostyring på den måten at omfanget av sikkerhetstiltak skal være proporsjonalt med størrelsen på sikkerhetsrisikoen. Når sikkerhetsrisikoen hos virksomheten er mye høyere enn hos leverandøren, oppstår det en markedssvikt ved at leverandøren ikke ser risikoen hos virksomheten, og dermed ikke har insentiv til å innføre sikkerhetstiltak proporsjonalt med størrelsen på risiko hos virksomheter som er kunder av leverandøren. Dette er et fundamentalt problem som bare kan løses ved at virksomheter gjennom avtaler krever at leverandører holder et adekvat sikkerhetsnivå, og at det foretas revisjon av leverandørenes sikkerhetsprogram.

En variant av leveransejedeangrep er hvis leverandøren selv er en trusselaktør mot sine kunder. Det kan for eksempel skje hvis myndighetene i en stat tvinger en nasjonal leverandør til å legge skult spionvare eller skulte bakdører inn i systemer som selges til andre land. Frykten for denne typen angrep gjør at mange land nå tar forholdsregler. For Norges del kan det bety at leverandører av utstyr til kritisk infrastruktur må ligge i et land som Norge har sikkerhetspolitisk samarbeid med. Sikkerhetsloven § 9-4 gir regjeringen mulighet til å ekskludere produsenter og leverandører etter dette prinsippet. Dette var nettopp tilfellet da norske teleoperatører i 2019 ble nektet å kjøpe utstyr for 5G-nettet fra det kinesiske selskapet Huawei. Antagelig gjelder det samme prinsippet i for eksempel Kina og Russland, det vil si at de er forsiktige med å bruke amerikansk IKT-utstyr i sin kritiske infrastruktur.

Sikkerhet i digitale leveransekjeder beskrives i avsnitt 11.9.

2.1.7 Skadelige eksterne enheter

Skadelige eksterne enheter kan f.eks. kobles til USB-kontakten og brukes i angrep. For eksempel kan enheten inneholde skadeware som brukeren kanskje installerer av nysgjerrighet. En annen angrepsmulighet er at en USB-minnepinne konfigureres som en HID-enhet (Human Interface Device), som lurer datamaskinen til å tro at den er et tastatur og sender en strøm av tastetrykk som utgjør skadelige kommandoer. Et *drop-angrep* er når angriperen legger igjen skadelige USB-minnepinner på steder som kafeer, og venter på at noen finner dem og plugges dem inn i en datamaskin. Ved lading av mobilenheter gjennom en USB-kontakt

6 <https://www.telenor.no/om/digital-sikkerhet/2020/artikler/nettene-blir-lange.jsp>.

på offentlige steder, er en mulig trussel at USB-kontakten angriper enheten som beskrevet over. Derfor bør USB-kondom alltid benyttes for lading gjennom offentlige ladekontakter. Et USB-kondom sperrer all dataoverføring og tillater kun lading.

2.1.8 Hacking av upatched sårbare IoT-enheter

IoT-enheter er separate fysiske enheter med en innebygd minicomputer som kobles trådløst til et nettverk gjennom wifi, mobilnett (4G/5G) eller blåtann (eng. Bluetooth), og har muligheten til å sende og ta imot data. IoT betyr *tingenes internett*, som betyr at de danner nettverk for å automatisere hjemme- og industrioppgaver. De kan overføre sensordata eller ta imot kommandoer for å utføre funksjoner. IoT-enheter kan kategoriseres i tre hovedgrupper: for forbrukere, for bedrifter og for industrianlegg.

I et smarthjem kan IoT-enheter registrere og reagere på en persons tilstedeværelse. Når du kommer kjørende hjem, kommuniserer bilen med garasjen for å åpne porten. Når du går inn i huset, blir termostaten justert til ønsket temperatur, og belysningen satt til intensitet og farge etter tiden på dagen og været ute.

Mens vanlige datamaskiner med fullverdige operativsystemer som Windows eller Linux får jevnlig sikkerhetsoppdateringer og patching av programvarefeil, blir IoT-enheter som regel aldri oppdatert etter at de er produsert og levert. Fravær av fullverdige operativsystemer i IoT-enheter gjør det teknisk vanskelig eller umulig å foreta online oppdatering av programvare.

Det er et faktum at programvare alltid har sårbarheter og feil som jevnlig blir oppdaget, og som kan utnyttes av trusselaktører for hacking. Når IoT-enheter aldri blir oppdatert, er det opplagt at de står lagelig til for å bli hacket, fordi sårbarheter som oppdages, aldri blir fjernet. Dermed kan et smarthjem eller industrianlegg bli hacket gjennom sårbare IoT-enheter som er koblet til internett og eksponert for trusselaktører i hele verden.

2.1.9 Uvitende installering av skadevare

Installering av skadelige programmer kan skje gjennom nettsteder eller andre lagringsmedier som trusselaktører bruker under et cyberangrep. Brukeren kan bli lurt til å installere skadevare i den tro at programvaren er legitim. Det fins en rekke ulike typer skadelig programvare, som beskrevet i avsnitt 2.2. Trojaner (trojansk hest) er en type skadevare som faktisk har en nyttig funksjon, men som samtidig har skjulte skadelige funksjoner.

2.1.10 Innsideangrep

Innsideangrep er angrep som begås av en ansatt eller annen person som er autorisert for tilgang til virksomhetens systemer og data. Begrepet *utro tjener* benyttes typisk om slike personer. Innsideangrep kan være svært skadelige fordi angriperen har kjennskap og tilgangsrettigheter til systemer og verdier slik at typiske sikkerhetstiltak har begrenset nytte. I tillegg kan innsideangrep være svært vanskelig å oppdage fordi angriperen ofte vet hvordan spor kan skjules. Innsideangrep er beskrevet nærmere i kapittel 13 om sikkerhetskultur.

2.2 Skadevare

Skadevare (skadelig programvare) er programvare med tilsiktede skadelige funksjoner. Programvare som forårsaker utilsiktet skade på grunn av feil, er bare dårlig programvare. Vanligvis er skadevare laget med hensikt å bli brukt som del av et angrep. Skadevare kan også være legitim programvare som blir brukt som del av et angrep. Derfor er det ikke alltid entydig hva som er skadevare, fordi det avhenger av hvilket perspektiv vi inntar. Det kan godt hende at programvare produsert av seriøse firmaer blir betraktet som skadevare hvis den i det skjulte handler mot interessene til brukeren. Som eksempel kan vi nevne at Sony i 2005 distribuerte et rootkit lagret på musikk-CD-er for å forhindre kopiering av musikk. Dette rootkittet skapte sikkerhetssårbarheter som igjen ble utnyttet av andre angripere. Sonys ingeniører tenkte antagelig at dette var nyttig programvare, men for brukerne var det helt opplagt skadevare.

Fil-løs skadevare er en paraplybetegnelse på skadevare som ikke lagres på disk i form av en fil, men kun lagres og kjøres i systemminnet. Det betyr at skadevaren forsvinner når systemet stenger ned eller restarter. Tradisjonelle virus og trojanere er en form for skadevare som lagres på disk, mens exploits og skadelige JavaScript er fil-løse. Figur 2.3 viser de vanligste typer skadevare.



Figur 2.3. Vanlige typer skadevare.

De nummererte typene skadevare illustrert i figur 2.3 er beskrevet i de respektive avsnittene nedenfor.

2.2.1 Datavirus

Den opprinnelige betydningen av begrepet *datavirus* er skadelig programkode som infiserer andre legitime programmer ved at koden legges til og flettes inn i de andre programmene. Dette er analogt med biologiske virus, som flettes inn i vanlige celler i kroppen. Dataviruset utfører sin skadelige funksjon bare når det infiserte programmet kjøres. At et virus er flettet

inn i et annet program, gjør det spesielt vanskelig å fjerne, og selv de beste antivirusprogrammene sliter med å gjøre dette korrekt. Rene datavirus er uvanlige i dag, og utgjør mindre enn 10 % av all skadevare.

Vær oppmerksom på at begrepet «virus» ofte brukes som en generell betegnelse på alle typer skadevare, noe som kan være forvirrende.

2.2.2 Løsepengevirus

Løsepengevirus er en type skadevare som i første trinn krypterer alle eller et utvalg kritiske data på offerets systemer, slik at data og applikasjoner blir utilgjengelige. Dette er altså en form for tjenestenektangrep som fører til brudd på sikkerhetsmålet tilgjengelighet. Angriperen følger opp første trinn med å foreta utpressing og kreve løsepenger for å utlevere dekrypteringsnøgkelen. Teknisk sett er dette ikke et «datavirus» i tradisjonell forstand, men typisk en trojaner som utfører krypteringen. Begrepet «løsepengevirus» er blitt vanlig på norsk, der «virus» tolkes mer generelt som skadevare. Kryptovirus er et annet navn på løsepengevirus, nettopp fordi det krypterer og låser ned data. En viktig beredskap mot løsepengevirus er å ta regelmessige sikkerhetskopier (eng. backup) av alle viktige data, og ha gode gjenopprettingsrutiner. Sikkerhetskopier bør lagres frakoblet nettverket dersom dette er mulig, for å forhindre at disse blir angrepet. Gjenopprettingsrutiner må testes regelmessig, for eksempel én gang per år, for å verifisere at de faktisk virker, og for at rutineene er innøvd hvis det virkelig skjer en hendelse.

Doxing er offentliggjøring av personlig informasjon eller sensitiv informasjon om en virksomhet uten individenes eller virksomhetens samtykke. Doxing gjøres vanligvis gjennom internett og utføres av ulike grunner, inkludert online utpressing. Trusselaktører kan bruke løsepengevirus til å stjele sensitiv informasjon og true med doxing, altså å utpresse virksomheten ved å kreve løsepenger for å ikke publisere informasjonen offentlig.

Ved denne typen utpressing nytter det ikke med sikkerhetskopier. Det kan være svært alvorlig og utfordrende for virksomheter å håndtere slike former for utpressing hvis det omfatter sensitive personopplysninger. Det beste er å sørge for gode preventive sikkerhetstiltak som kan forhindre at datainnbrudd og tyveri av data skjer i det hele tatt.

2.2.3 Spionvare

Spionvare er programmer som spionerer på brukeren ved å samle inn forskjellige typer informasjon. En *tastaturlogger* (eng. keylogger) er en type spionvare som logger tastetrykk, slik at angriperen kan stjele passord og annen sensitiv informasjon. Slike programmer blir ofte installert gjennom en form for sosial manipulering kombinert med en av angrepsvektorene beskrevet i forrige avsnitt, og slik spionvare starter som regel opp hver gang systemet starter.

En type spionvare som vanligvis ikke regnes som direkte kriminell, er at nettsider samler inn forskjellige typer informasjon om brukere, som kan selges og brukes til markedsføring mot brukerne. GDPR, beskrevet i kapittel 10, regulerer den typen innsamling av data i EU/EØS, men er dessverre vanskelig å håndheve.

2.2.4 Bott-programvare

Bott-programvare utfører automatiserte oppgaver på kommando fra en kommandoenhet. En computer med bott-programvare kalles en *bott* (eng.: bot), og kan like godt være en privat computer som en computer i en bedrift. Alle typer computere med internett-tilknytning kan

bli infisert og bli til en bott, også IoT-enheter. Navnet kommer fra «robot», altså noe som jobber selvstendig og automatisk. Bott-programvare kan brukes til legitime formål, for eksempel som søkemotorer for å utføre indeksering. Dessverre brukes bott-programvare ofte som skadevare av angripere. Bott-skadevare er typisk selvreplicherende, og er i stand til å motta kommandoer fra en sentralisert eller distribuert bott-gjeter. Angripere infiserer computere i stort antall for å lage et *bottnett* som er samlingen av alle infiserte bott-computere kontrollert av en bott-gjeter. Størrelsen på bottnett varierer fra noen hundre til flere millioner infiserte computere. Et bottnett kan utføre forskjellige typer angrep, for eksempel DDoS-angrep (se avsnitt 6.4.3) eller utvinning av kryptovaluta (se avsnitt 4.13.2). For utvinning av kryptovaluta brukes elektrisitet og beregningsressurser i de infiserte bott-computerene. For DDoS-angrep brukes de infiserte bott-computerene til å sende trafikk mot angrepsmål på internett. Aktører som kontrollerer store bottnett, driver ofte bottnett-utleie som en måte å generere inntekt på. Dette gjør at hvem som helst som har samvittighet til å gjøre seg til en kriminell, dessverre kan utføre DDoS-angrep billig og enkelt.

2.2.5 Exploit

Exploit, også kalt *utnyttelseskode*, er et lite program, en streng med data, en fil eller en sekvens med kommandoer som utnytter en eller flere feil eller sårbarheter i en programvare, maskinvare eller annet datautstyr for å trigge korrumpert eller unormal oppførsel. En exploit trigger typisk en *buffer overflow*, som er beskrevet i avsnitt 3.5. Angriperens hensikt med å trigge slik oppførsel er å få kontroll over et system, laste ned bakdører, få uautorisert tilgang eller å utføre et tjenestenektangrep. For å finne sårbarheter som kan brukes til å lage exploits, brukes ofte fuzzing, som er beskrevet i avsnitt 11.3.5.

2.2.6 Makro-virus

Skadelige Office-makroer kan ligge i Office-dokumenter. Makroer brukes for å automatisere funksjoner i Office-dokumenter. Imidlertid kan angripere gjemme skadelige Office-makroer i Office-filer sendt som vedlegg til phishing-e-post. Disse filene bruker navn som er ment å lokke eller skremme folk til å åpne dem, og ser typisk ut som fakturaer, kvitteringer, juridiske dokumenter, osv. Tidligere kjørte Office-makroer automatisk, men ikke nå lenger. Nå må angriperen lure brukere til å aktivere makroer for at de skal kunne kjøre.

2.2.7 Trojaner

Trojanere maskerer seg som legitime programmer som faktisk (eller tilsynelatende) har nyttige funksjoner, men som samtidig har skjulte skadelige funksjoner. Trojanere er populære blant hackere og har stort sett tatt over etter datavirus. Trojanere blir typisk lastet ned fra kriminelle eller infiserte nettsteder, eller kommer som et vedlegg til phishing-e-post. Brukeren blir lurt til å tro at programmet er nyttig, og velger eksplisitt å installere det. Det er ironisk at falske antivirusprogrammer er en utbredt type trojaner.

Begrepet «trojaner» kommer fra gresk mytologi, der soldater fra Athen under angrep mot byen Troja skjulte seg inne i en stor hesteskulptur av planker som var plassert utenfor byen. Innbyggerne i Troja dro hesteskulpturen inn i byen i den tro at det var en gave. Om natten snek de athenske soldatene seg ut og åpnet byporten slik at den athenske hær kunne storme inn og ta byen.

2.2.8 Dataorm

Dataormer er selvstendige programmer som sprer seg selv til andre computere innen et datanett eller over hele internett på en automatisk måte, som regel uten at brukere må gjøre noe som helst. Dataormer klarer dette ved at de kobler seg til andre vertsnoder og utnytter sårbarheter i programmer som er eksponert til internett. Det som gjør dataormer så ødeleggende, er deres evne til å spre seg uten brukerdeltagelse. Virus og trojanere krever i det minste at en bruker starter et program. Den beryktede *SQL Slammer-or*men utnyttet en buffer overflow-sårbarhet i databasetjeneren Microsoft SQL. I januar 2003 infiserte ormen omkring 75 000 Microsoft SQL-tjenere på omtrent 10 minutter, noe som viser dens eksponentielle spredningshastighet.

2.2.9 Rootkit

Rootkit er en type programvare som gjør at angriperen får uautoriserte root/admin- tilgangrettigheter, og dermed full kontroll over systemet. Spredning og installering av rootkit skjer ofte gjennom en form for sosial manipulering kombinert med en angrepsvektor. Rootkit kan også brukes til å skjule annen skadevare, for eksempel spionvare og tastaturloggere. En exploit er ofte et rootkit.

2.2.10 Bakdør

Bakdør er en skjult metode for å omgå normal autentisering og tilgangskontroll i et system. Bakdører har legitime bruksområder, som å gi produsenten av systemer og programvare en måte å foreta vedlikehold og service på. En bakdør kan også brukes av angripere for å få uautorisert tilgang til systemer. Den kan være en skjult del av et program, et eget program, kode i fastvaren til maskinvaren eller en del av operativsystemet. En skadebakdør kan for eksempel bli installert av en trojaner eller av en exploit.

2.2.11 Skadelige JavaScript

Skadelige JavaScript kan komme fra ulike nettsider. De fleste nettsider inneholder JavaScript som automatisk lastes ned og kjører i nettleseren når en bruker besøker nettsiden. Vanligvis er JavaScript helt legitimt og brukes til avanserte funksjoner på en nettside, men det kan også utføre skadelige funksjoner, som å laste ned et exploit fra et nettsted kontrollert av angriperen. JavaScript kan også misbrukes til å få nettleseren til å utvinne kryptovaluta for angriperen eller til å stjele sensitiv informasjon som sendes til angriperen. Skadelige JavaScript kan bli injisert i nettsider gjennom XSS-angrep, beskrevet i avsnitt 11.7.2. Ettersom JavaScript utføres automatisk og helt uten interaksjon når brukeren besøker en nettside, er JavaScript typisk brukt til drive-by-angrep.

2.2.12 Logisk bombe

En logisk bombe er skadevare som trigger en ondsinnet funksjon når spesifiserte betingelser er oppfylt. En trusselaktør kan for eksempel være en ansatt i en virksomhet som lager en logisk bombe i form av et dataprogram som begynner å slette filer dersom den ansattes lønn stoppes, som typisk vil skje dersom hen skulle miste jobben.

Ulike typer skadevare, som virus og ormer, inneholder ofte logiske bomber som utfører en bestemt funksjon på et forhåndsdefinert tidspunkt eller når en annen betingelse er oppfylt. Denne teknikken kan brukes av et virus eller en orm for å få fart og spre seg før det blir lagt merke til. Når skadevare er programmert til å angripe vertssystemet på bestemte datoer, kalles det ofte *tidsbomber*.

Oppgaver til kapittel 2

2.1 Angrepsvektorer

- Hva er den vanligste angrepsvektoren for cyberangrep?
- Hvordan kan deepfake-stemme og video brukes i cyberangrep?
- Hvordan kan USB-enheter som f.eks. (ligner på) en minnepinne, brukes for å angripe en datamaskin?

2.2 Leveransekjedeangrep

- Forklar hva som menes med leveransekjedeangrep.
- Beskriv eksempler på leveransekjedeangrep som har skjedd i de siste årene.
- Hvilke tiltak kan en virksomhet benytte for å redusere leveransekjederisiko?

2.3 Bottnett

- Hva er et bottnett?
- Hva er et DDoS, og hvordan kan et bottnett brukes til å gjøre et DDoS-angrep?
- Mirai er en skadevare som ble brukt til å «ta ned» internett i store deler av USA gjennom et angrep på en DynDNS en dag i oktober 2016. Beskriv kort Mirai og hvordan dette angrepet ble utført.

8

Kapittel

Brukerautentisering

I dette kapitlet lærer du om metodene for brukerautentisering, som typisk deles inn i tre kategorier: 1) noe du vet, 2) noe du har, og 3) noe du er. Til slutt lærer du om autentiseringsrammeverk, som danner grunnlag for å spesifisere krav til brukerautentisering i e-forvaltning, det vil si i statlige/offentlige online-tjenester, der Norge følger den europeiske eIDAS-forordningen, som spesifiserer tre ulike autentiseringsnivåer avhengig av tjenestens sensitivitet.

8.1 Hva er brukerautentisering?

Brukerautentisering betyr at en bruker må bevise eierskap til en digital identitet for å logge inn i et system eller for å få tilgang til applikasjoner og tjenester beskyttet av tilgangskontroll. Brukerautentisering skal forhindre at uautoriserte entiteter får tilgang.

En bruker i denne sammenheng er ikke nødvendigvis begrenset til å være en person, men kan også være et fysisk system, eller til og med en logisk prosess implementert i programvare, som kan kalles en *bott* (fra robot).

Fordi fysiske personer er juridiske entiteter, gjør brukerautentisering det mulig å kunne stille personen til regnskap for handlinger utført med denne spesifikke identiteten. Det betyr at brukerautentisering støtter sporing og regnskapelighet av aktiviteter i systemer og nettverk.

For å knytte fysiske personer til en digital identitet er det nødvendig å ha identitetsforvaltning med krav til tilstrekkelig dokumentasjon for den fysiske personens identitet. Eksempler på slike krav er beskrevet i NIST SP 800-63-3 *Digital Identity Guidelines – Enrollment and Identity Proofing Requirements*.

En *autentikator* er et element som beviser brukerens eierskap til en identitet ved innlogging. En autentikator kan være et passord, en brikke/enhet eller en biometrisk prøve. Kjennskap til riktig passord, bruk av en brikke/enhet eller anvendelse av biometri tolkes av systemet som bevis for at brukeren er rettmessig eier av identiteten. Det kan naturligvis skje feil, for eksempel ved at en uautorisert person har stjålet et passord, eller at en autentikator er forfalsket.

8.2 Autentiseringsmetoder

Autentikatorer kan deles inn i tre hovedkategorier:

- Noe du *vet* – kunnskapsbaserte autentikatorer, som typisk er passord.
- Noe du *har* – eierskapsbaserte autentikatorer, som typisk er brikker/enheter.
- Noe du *er* – egenskapsbaserte autentikatorer, som typisk er biometri.

Ved å benytte flere metoder samtidig kan autentiseringen styrkes betraktelig, dvs. at viss-heten om korrekt autentisering øker. *Sterk autentisering* er typisk basert på at to eller flere metoder benyttes samtidig. Dette kalles tofaktor- eller flerfaktor-autentisering. De tre kategoriene av autentikatorer er beskrevet i avsnittene nedenfor.

8.3 Kunnskapsbaserte autentikatorer: passord og lærte mønster

Med kunnskapsbaserte autentikatorer menes passord som huskes, eller mønster som en bruker er i stand til å gjengi. Det vanligste er passord, men det kan også være andre ting som kan læres og huskes, som for eksempel å gjengi et bevegelsesmønster, en sekvens med handlinger eller elementer på et bilde. Passord var den første type autentikator som ble implementert for innlogging til systemer, og er fremdeles mye brukt. Dette avsnittet fokuserer på passord, som er et interessant tema.

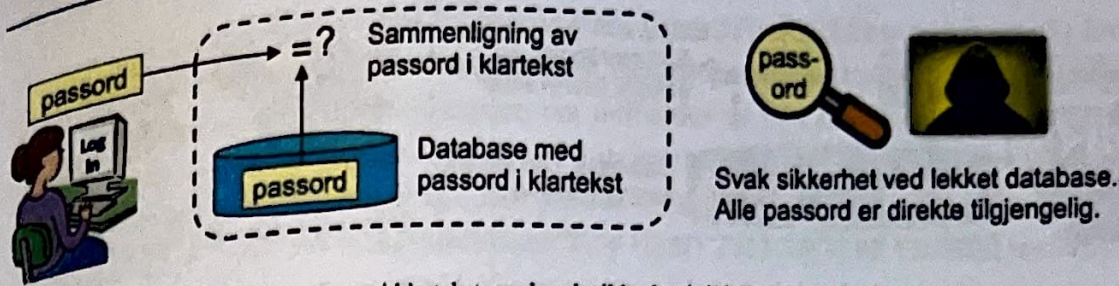
Ulemper med passord er blant annet at de

- er lette å dele med andre (med vilje eller ikke)
- er lette å glemme (kan bli belastning for helpdesk)
- ofte er lette å gjette (bl.a. med cracke-verktøy)
- kan stjeles av skadevare eller en tastaturlogger koblet mellom tastatur og datamaskin
- kan skrives ned (som er både bra og ikke bra)

Fordelen med passord er at det er relativt enkelt og billig å implementere. Prinsippet for brukerautentisering med passord er at bruker oppgir et passord og at systemet eller applikasjonen sjekker om passordet er riktig. Selv om det høres enkelt ut, er det utfordrende å lage sikre løsninger.

8.3.1 Beskyttelse av passord mot cracking

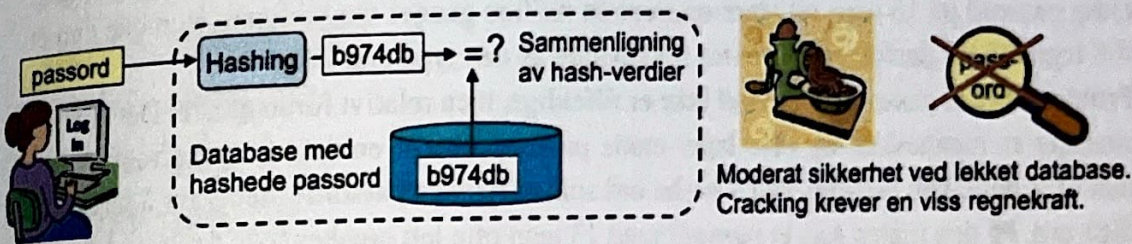
Figur 8.1 viser prinsippet for sjekking av passord lagret i klartekst. Det antas naturligvis at passordet krypteres hvis det sendes gjennom datanett eller internett. Et alvorlig og vedvarende sikkerhetsproblem er at passordfiler og -databaser blir lekket eller stjålet. Hvis passordene ligger lagret i klartekst, har angriperne som får tak i en lekket database, direkte tilgang til alle passordene. Figuren viser at dette gir svak sikkerhet i tilfelle databasen lekkes.



Figur 8.1. Sjekking av passord lagret i klartekst, med svak sikkerhet i tilfelle lekket database.

Selv om det fremdeles forekommer, er det svært dårlig praksis å implementere brukerautentisering med passord lagret i klartekst, som vist i figur 8.1.

En forbedret metode er at alle passord hashes før de lagres i passorddatabasen. Når brukeren ved innlogging oppgir passord, må det naturligvis også hashes før det sammenlignes med den lagrede hash-verdien i databasen, som vist i figur 8.2. Også her er det antatt at passordet er kryptert hvis det sendes gjennom datanett eller internett. Figuren viser at det gir moderat sikkerhet i tilfelle databasen lekkes, fordi det er relativt vanskelig for angriperen å finne passord ut fra hash-verdier.



Figur 8.2. Sjekking av passord lagret som hash-verdier, med moderat sikkerhet i tilfelle lekket database.

Metoden for å finne et passord ut fra en hash-verdi kalles «passord-cracking». Denne metoden går ut på å hashe alle mulige ord helt til det fins en hash-verdi som er lik den lagrede hash-verdien for passordet. Da er nettopp dette ordet passordet, eller i alle fall et passord som virker. Angripere fant raskt ut at det var effektivt å lagre gigantiske tabeller med hash-verdier og tilhørende ord for alle mulige ord opp til en viss størrelse. Dermed kunne et passord lett crackes med et enkelt oppslag i hash-tabellen. Selv om denne metoden for lagring av passord fremdeles brukes i noen applikasjoner, er den ikke å anbefale.

Den beste metoden for lagring av passord er at passord «saltes» før de hashes og lagres i passorddatabasen. *Salting* betyr at det legges til en tilfeldig bitstreng (f.eks. 8 byte) til passordet før det hashes. Saltverdien lagres sammen med hash-verdien i databasen. Når brukeren ved innlogging oppgir passord, må det naturligvis også hashes sammen med saltverdien før det sammenlignes med den lagrede saltede hash-verdien i databasen, som vist i figur 8.3. Det antas at passordet krypteres hvis det sendes gjennom datanett eller internett. Figuren viser at det gir god sikkerhet i tilfelle databasen lekkes, fordi det er svært ressurskrevende for angriperen å finne passord ut fra saltede hash-verdier.



Figur 8.3. Sjekking av passord lagret som saltet hash-verdi, som gir god sikkerhet i tilfelle lekket database.

Når passord lagres som saltede hash-verdier, må angripere bruke store ressurser for å cracke passord fra en lekket database. Det er ikke lenger mulig å bruke ferdiglagede hash-tabeller, fordi det ville kreve en egen hash-tabell for hver mulige saltverdi. Hvis saltverdien for eksempel er 8 byte, trengs det 2^{64} ulike hash-tabeller, noe som ikke er praktisk mulig å produsere.

Angripere kan likevel forsøke å cracke enkelte passord de anser som verdifulle, ved å investere i utstyr med stor regnekraft og kjøpe store mengder strøm. Hvor mye tid og strøm som trengs for å cracke et enkelt passord, avhenger naturligvis av kvaliteten på passordet. Et tilfeldig passord med 8 tegn kan antagelig crackes på noen timer med kraftig utstyr. Et tilfeldig passord på 13 tegn vil være omtrent en million ganger vanskeligere å cracke enn et med 8 tegn, og vil derfor være utenfor rekkevidde av den type cracking.

Problemet er at passord som regel ikke er tilfeldige, men relativt forutsigbare. Det er fordi mennesker er mennesker, og ofte lager enkle passord som er enkle å huske. Crackere har funnet ut at dette kan utnyttes ved å hashe ord som er typiske passord i stedet for å hashe tilfeldige ord. På den måten kan et passord med 13 tegn ofte lett crackes hvis det har en typisk regelmessighet til å være et passord laget av et menneske. Utfordringen for oss mennesker er å lage passord som mennesker typisk ikke lager, og samtidig klare å huske dem. Da forstår vi umiddelbart at passord ikke er enkelt.

Passord-cracking gjøres også av systemeiere for å sjekke kvaliteten på brukerpasord i egen organisasjon. Hvis de lykkes i å cracke et passord, blir brukeren bedt om å skifte til et bedre passord.

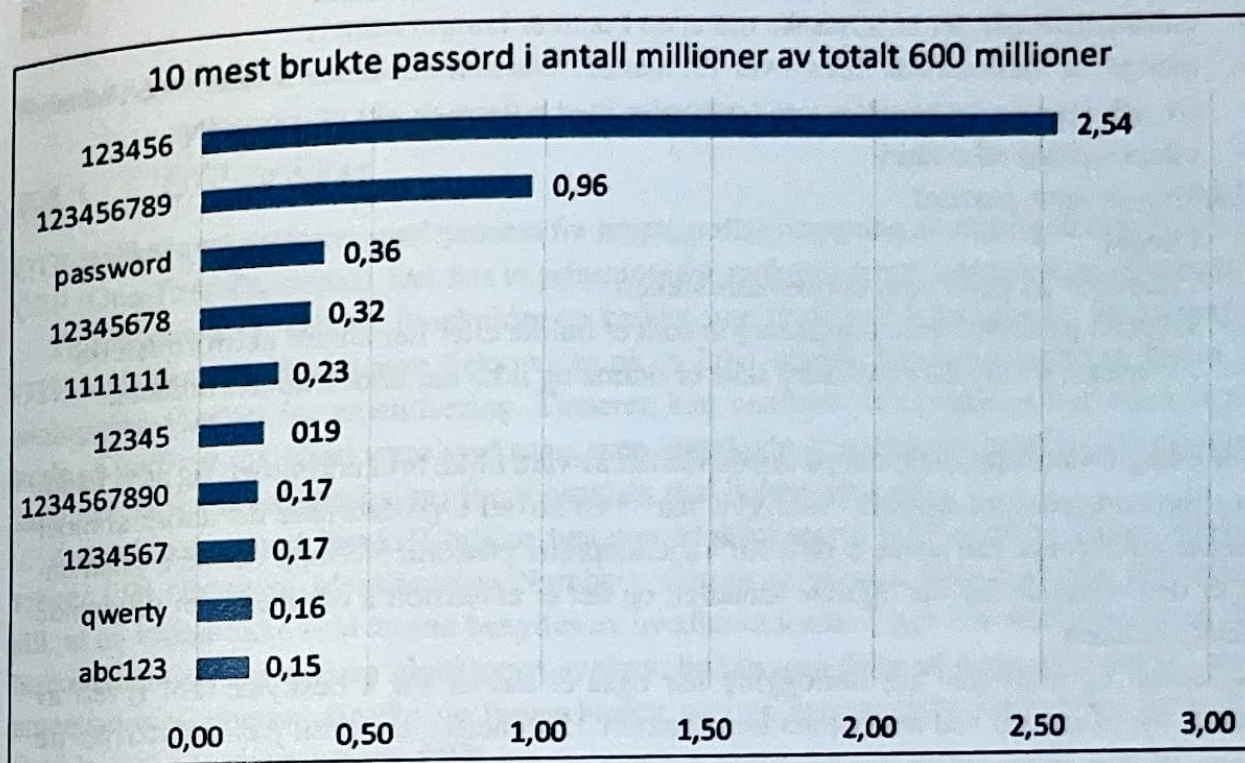
Passordfiler og -databaser lagres på forskjellige lokasjoner avhengig av system og nettverkskonfigurasjon. Noen eksempler er følgende:

- Linux: Passord lagres lokalt i filen `/etc/shadow`, som har rent tekstformat. Kun Root-brukere har tilgang til å lese/endre.
- Windows: Passord lagres lokalt i SAM-databasen (Security Account Manager) i filen `\windows\system32\config\sam`, som har NTLM-format. Kun admin har tilgang.
- Datanett: I nettverksmiljøer er det som regel en egen applikasjon som lagrer passord. Windows-applikasjonen AD (Active Directory) er svært utbredt. Linux-applikasjonen LDAP (Lightweight Directory Access Protocol) er brukt i noen Linux-baserte nettverk.

Passorddatabaser på internett er blitt lekket og stjålet helt siden internett ble oppfunnet. Forskere samler og analyserer slike passorddatabaser for å forstå hvordan vi kan lage bedre passord og også gjøre det mulig for folk å finne ut om deres passord er stjålet.

Nettstedet *Have I Been Pwned?*²⁹ tilbyr en gratis tjeneste for å sjekke om en personlig brukerkonto og/eller passord er blitt kompromittert. Nettstedet samler inn og analyserer hundrevis av databasedumper med informasjon om milliarder av lekkede brukerkontoer, og lar brukerne søke etter sin egen informasjon ved å skrive inn brukernavnet eller e-postadressen. Det er også mulig å sjekke om et spesifikt passord er på listen over kompromitterte passord. Nettstedet ble opprettet av sikkerhetsekspert Troy Hunt i 2013, og er en verdifull ressurs for å bekjempe identitetstyveri og brudd på personvern på internett.

Nettstedet har samlet inn over 600 millioner passord som er funnet blant de kompromitterte brukerkontoene, der mange passord går igjen. Figur 8.4 viser de 10 mest brukte passordene, der «123456» er det desidert mest brukte passordet og forekommer 2,54 millioner ganger.



Figur 8.4. Mest brukte passord av totalt 600 millioner ulike passord.³⁰

2,54 millioner av 600 millioner utgjør 0,4 % av alle de innsamlede passordene. Det betyr at en angriper kan prøve å logge seg på forskjellige fremmede brukerkontorer med passordet «123456» og gjennomsnittlig få uautorisert tilgang ved omtrent 1 av 250 forsøk.

Det kan antas at mange av de 600 millioner passordene er relativt gamle, fordi de stammer fra gamle lekkasjer. De fleste nye applikasjoner krever en viss lengde og kvalitet på passord, slik at mange av passordene i figur 8.4 antageligvis ikke ville blitt god tatt.

²⁹ <https://haveibeenpwned.com/>.

³⁰ Basert på datasett fra 2020 fra <https://haveibeenpwned.com/>.

8.3.2 Råd om sterke passord

Nedenfor er noen generelle råd om sterke passord for beskyttelse mot cracking og identitetstyveri.

- Aldri gjenbruke passord. Hvis et passord gjenbrukes, og passordet lekkes og crackes fra en tjeneste, kan angripere stjele brukerens identitet på alle andre tjenester der samme passord er brukt.
- Minimum 13 tegn passord for viktige kontoer.
- Ikke bruk vanlige ord, navn eller fødselsdato som del av et passord.
- Bruk flere kategorier av tegn: store/små bokstaver, tall og spesialtegn.
- Endring av passord:
 - umiddelbart når det er mistanke om at en konto er kompromittert
 - med jevne mellomrom, f.eks. hver 13. måned, hvis kontoen anses å være svært sensitiv, eller passordet benyttes i en omgivelse med potensielt økt eksponering
 - ellers sjelden eller aldri
- Lagring av egne passord:
 - i hodet
 - i klartekst på papir som oppbevares sikkert
 - kryptert på digital enhet/applikasjon som er online eller har annen nettforbindelse
 - i klartekst på digital enhet som ikke er online og ikke har annen nettforbindelse

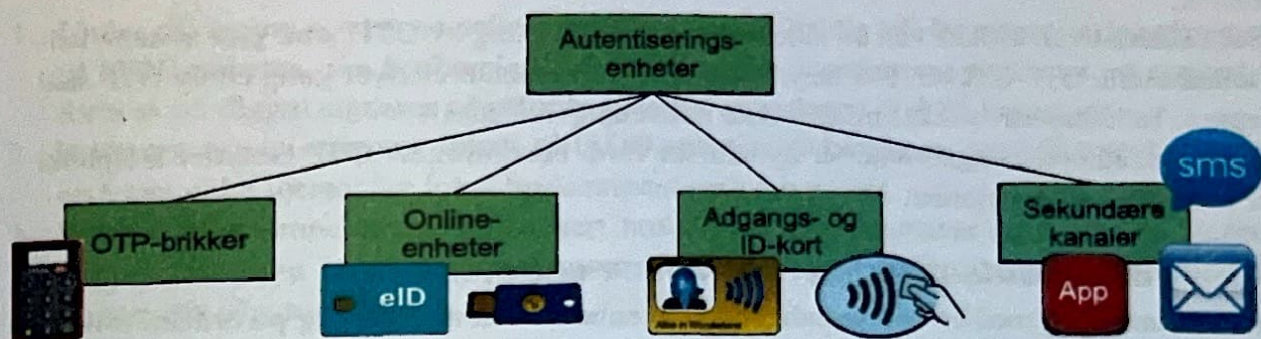
Det er viktig å være oppmerksom på sensitiviteten av våre ulike brukerkontoer, og at vi håndterer tilhørende passord deretter. Vanligvis har vi en hoved-e-postadresse dit andre kontoer og nettapplikasjoner kan sende e-post for å gjenopprette passord. Nettopp denne e-postkontoen er den viktigste for vår digitale identitet, og det er essensielt å håndtere det tilhørende passordet sikkert.

Systemer og nettsteder for innlogging har også et ansvar for å beskytte mot tyveri av passord, for eksempel ved at kontoen blir sperret i 15 minutter, hvis feil passord skrives tre ganger. På den måten vil en angriper ikke kunne prøve mange passord manuelt eller automatisk på kort tid.

8.4 Eierskapsbaserte autentikatorer: enheter

Brikker og andre enheter som brukeren eier eller kontrollerer, kan danne grunnlag for sterk brukerautentisering. Disse enhetene kan inneholde kryptografiske komponenter med variable input-parametere som gjør at en slik autentikator betegnes som dynamisk. Styrken med dynamiske autentikatorer er at hver autentisering er unik, slik at det er umulig å forfalske autentisering ved å kopiere og gjenta dataoverføring fra en tidligere autentisering. Brikker er ofte designet for å være tuklingsbestandige, noe som gjør dem svært vanskelige å klonere eller forfalske. En autentiseringsenhet kan også være en sekundær kanal som brukeren kontrollerer. E-post eller SMS er vanlige sekundærkanaler, selv om disse kanalene har svak sikkerhet. Kommunikasjon med SIM-kortet i brukerens mobiltelefon kan være en sikker se-

kundærkanal. Hovedtyper av autentiseringsenheter vises i figur 8.5. Disse beskrives separat i avsnittene nedenfor.



Figur 8.5. Hovedtyper av autentiseringsenheter.

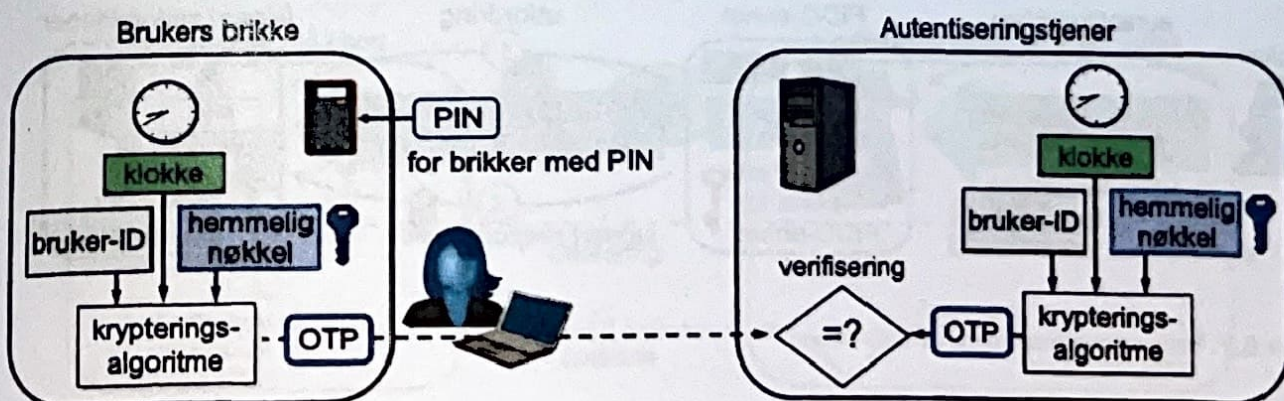
8.4.1 OTP-brikker

OTP-brikker synkroniseres med tjeneren for kryptografisk beregning av engangskoder, også kalt OTP (One-Time-Password). Det fins to prinsipper for synkronisering: tidsbasert og tellerbasert.

Tidsbaserte OTP-brikker inneholder en klokke som brukes til å beregne en tidsavhengig OTP-kode (engangskode) som f.eks. vises på en liten skjerm. Brukeren kopierer koden til innloggingsvinduet for autentisering. Tjeneren kan verifisere om brukeren har sendt riktig kode. Klokkene må alltid være synkrone, men hver kode er gyldig for et tidsvindu på noen minutter. Brikken trenger batteri for at klokken skal holdes synkron.

Autentisering med BankID-brikke benytter klokkebaserte OTP-brikker. Noen brikker krever PIN (Personal Identification Number), som er et passord eller kode for aktivering slik at en brikke ikke skal kunne benyttes av uvedkommende. Figur 8.6 viser prinsippet for brukerautentisering med en klokkestyrt synkron brikke som deler en hemmelig nøkkel med autentiseringstjeneren. Brikke og tjener bruker samme symmetriske krypteringsalgoritme for å beregne en tidsavhengig OTP.

I internettsjangongen kalles en autentiseringstjener ofte en IdP (Identity Provider), særlig i forbindelse med føderert identitetshåndtering beskrevet i neste kapittel.



Figur 8.6. Brukerautentisering med synkron brikke og symmetrisk algoritme.

Verifisering gjøres ved at autentiseringstjeneren sjekker om mottatt OTP er lik beregnet OTP. Hvis mottatt OTP fra brukeren er lik OTP beregnet av autentiseringstjeneren, er dette bevis for at brukeren er i besittelse av OTP-brikken, noe som igjen indikerer at brukeren er autentisk.

Som alternativ til klokke kan en teller brukes for beregning av OTP, som gjør at dette kalles tellerbaserte OTP-brikker. Det betyr at en teller inkrementeres hver gang en ny OTP skal beregnes. Tellerbaserte brikker trenger ikke nødvendigvis batteri.

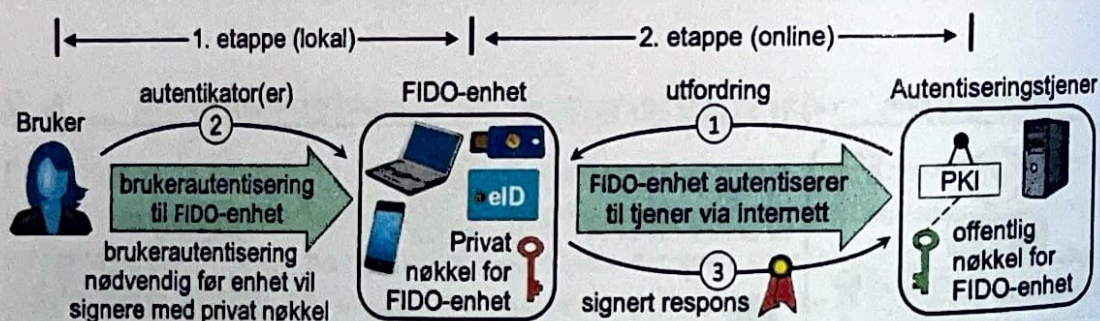
Synkrone autentiseringsbrikker er dynamiske fordi beregning av OTP benytter tidspunkt eller tellerverdi som variabler.

8.4.2 Brukerautentisering med online-enheter

Brukerautentisering med en online-enhet betyr at enheten autentiserer seg på brukerens vegne til en autentiseringstjener på internett. Online-enheten kan være en separat brikke som for eksempel en USB-enhet eller smartkort som plugges inn, eller en brikke som kommuniserer med klientterminalen via NFC eller blåtann. Alternativt kan online-enheten være innebygd i en klientterminal som f.eks. i en smarttelefon eller en datamaskin, både som maskinvare og programvare. Uansett format vil online-enheten utveksle kryptografiske meldinger med en autentiseringstjener gjennom internett. Denne utvekslingen av kryptografiske meldinger mellom enheten og autentiseringstjeneren foregår online med en kryptografisk autentiseringsprotokoll basert på digital signatur, som vist i figur 8.7.

Vanligvis vil online-enheten først autentisere brukeren lokalt før den i sin tur foretar online-autentisering, slik at dette er en totrinns-autentisering. Første autentiseringsetappe er lokal brukerautentisering som typisk er basert på biometri eller PIN. For biometri kan multimodal biometrisk autentisering benyttes, for eksempel med gjenkjenning av både fingeravtrykk, ansikt og stemme. Andre autentiseringsetappe består av online-autentisering mot autentiseringstjeneren.

FIDO (Fast Identity Online)³¹ er en industriallianse som standardiserer autentisering med online-enheter, og som forvalter sertifisering av FIDO-godkjente enheter. Visjonen bak FIDO er, som navnet sier, at brukerautentisering til online-tjenester skal kunne foregå raskt og enkelt. Brukerautentisering i henhold til FIDO 2.0-standard er vist i figur 8.7.



Figur 8.7. Brukerautentisering med FIDO-enhet.

31 <https://fidoalliance.org/>.

Meldingsutvekslingen med nummererte piler i figur 8.7 er beskrevet nedenfor. Anta at FIDO-enheten er koblet til eller er integrert med brukerplattformen, som f.eks. kan være en smarttelefon eller laptop.

1. Under pålogging sendes en *utfordring* i form av et tilfeldig tall fra autentiseringstjeneren til FIDO-enheten, via brukerplattformen. Autentiseringstjeneren forventer en respons i form av en digital signatur på utfordringen for at brukeren skal bli logget inn.
2. Brukeren autentiserer seg lokalt til FIDO-enheten. Avhengig av krav til autentiseringsnivå kan ulike former for lokal brukerautentisering benyttes.
3. Etter at FIDO-enheten har autentisert brukeren lokalt, genereres og sendes en signert respons tilbake til autentiseringstjeneren. Brukeren logges inn ved korrekt verifisering av responsens digitale signatur.

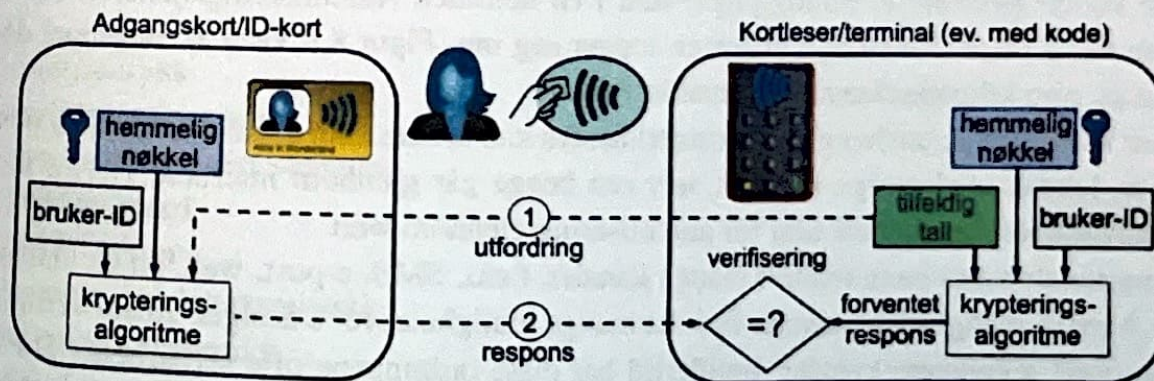
Autentisering med en online-enhet krever at enheten har en privat kryptografisk nøkkel, og at den tilhørende offentlige nøkkelen kan distribueres til autentiseringstjenere. En PKI er naturligvis nødvendig for å garantere autentisitet i denne type distribusjon av offentlige nøkler. Policyen rundt brukerautentisering med online-enheter setter typisk krav til godkjenning av enhetene.

I Norge tilbyr Buypass og Commfides autentiseringsordninger blant annet for ID-porten, Altinn og HelseID basert på online-enheter, enten som separate brikker (smartkort, USB-brikke, FIDO-brikke) eller som en mobilapp. Det er viktig å legge merke til at styrken til denne typen brukerautentisering avhenger av online-enhetens sikkerhet, noe som skaper et ekstra ledd som krever tillit.

8.4.3 Adgangs- og ID-kort

Adgangskort er typisk et smartkort som benytter NFC for kommunikasjon med en kortleser. NFC (Near Field Communication) er en teknologi for overføring av radiosignaler mellom enheter over avstander på noen centimeter. Denne og lignende teknologi brukes ikke bare for adgangskort, men også for berøringsfrie betalingskort, pass og ID-kort. Alternativt kan kortet settes inn i en kortleser med elektrisk kontakt. Sammen med kortet kan det også benyttes en PIN-kode.

Et NFC-kort kan motta og sende data. Eksemplet i figur 8.8 viser at kortleser sender et tilfeldig tall som utfordring til NFC-kortet, som krypterer utfordringen og returnerer en respons som verifiseres av kortleseren. Verifiseringen består i å sammenligne mottatt respons med beregnet forventet respons.



Figur 8.8. Utfordring-respons-autentisering med NFC-kort mot kortleser.

I eksemplet i figur 8.8 brukes en symmetrisk algoritme med hemmelig nøkkel. En annen mulighet er å bruke en asymmetrisk algoritme med et privat/offentlig nøkkelpar og en utfordring-respons-protokoll som i figur 8.7. Pass og nasjonalt ID-kort benytter nettopp utfordring-respons basert på privat/offentlig nøkkel. Kortleseren kan være avanserte terminaler som benyttes for passkontroll på flyplasser, eller kan være en smarttelefon med NFC. Den private nøkkelen ligger i passet/ID-kortet, og den offentlige nøkkelen i kortleseren/terminalen. Her brukes en egen PKI for å garantere autentisitet av den offentlige nøkkelen i kortleser/terminal. Utfordring-respons-protokollen gjør at kortleser/terminal kan autentisere pass/ID-kort. Autentisering med denne type adgangs- og ID-kort er dynamisk fordi det tilfeldige tallet i utfordringen er uforutsigbart og varierer hver gang.

Elektroniske pass og ID-kort er også designet slik at de kan autentisere kortleser/terminal. Dette er for at pass/ID-kort ikke skal gi fra seg sensitiv informasjon som for eksempel fingeravtrykkmal til en uautorisert terminal. Denne autentiseringen benytter en separat utfordring-respons-protokoll som går motsatt vei, det vil si med privat nøkkel lagret i kortleser/terminal og offentlig nøkkel i pass/ID-kort. PKI for pass forvaltes av ICAO (International Civil Aviation Organization).

Pass og nasjonalt ID-kort brukes hovedsakelig for å autentisere oss når vi krysser grenser på reise, mens eID benyttes når vi autentiserer oss for tilgang til online offentlige tjenester. Under arbeidet med nasjonalt ID-kort ble det diskutert om nasjonalt ID-kort skulle kunne benyttes for eID, men den ideen ble droppet. For at nasjonalt ID-kort samtidig skulle være eID, måtte kortet i praksis også være en slags BankID-brikke, og Politidirektoratet måtte samtidig bli en eID-leverandør. Å få til noe slikt ble vurdert å være for komplisert, og ble derfor ikke implementert.

8.4.4 Sekundære kanaler

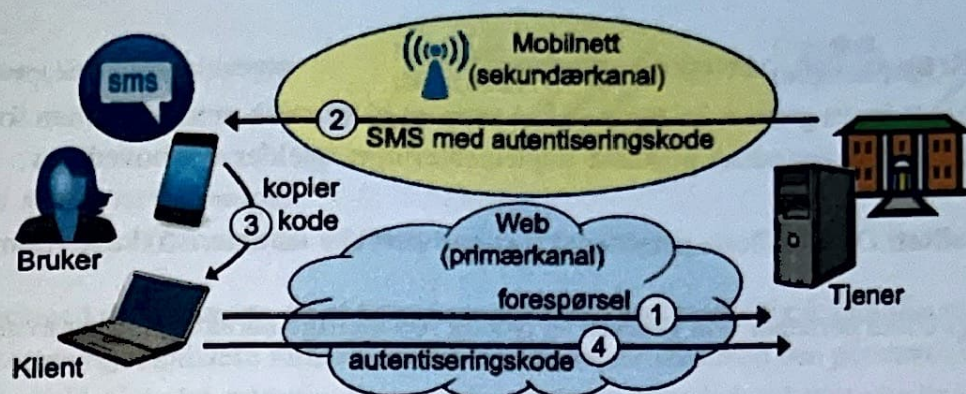
Hvis web-kommunikasjon betraktes som en *primærkanal*, kan SMS betraktes som en *sekundærkanal*. Slike sekundærkanaler kan støtte autentisering gjennom primærkanalen. Autentiseringstjeneren kan for eksempel sende en kode som SMS til brukerens telefon. Telefonnummer har moderat sterk autentisitet ved at abonnenter må bevise identitet for å få et telefonnummer.

Man bør likevel være oppmerksom på mulige sårbarheter som kan gjøre det mulig for en angriper å urettmessig overta kontrollen over et annet telefonnummer, og angrep som gjør det mulig å kapre SMS-meldinger, som beskrevet i avsnitt 7.4.3.

I en autentiseringsordning der brukeren mottar en kode via SMS, skal brukeren typisk returnere koden gjennom et innloggingsvindu i en nettleser. Autentiseringstjeneren tolker dette som bevis på at den riktige brukeren logger seg inn. Figur 8.9 viser et eksempel der SMS brukes som sekundærkanal for autentisering.

Enhver kanal som er uavhengig av primærkanalen kan brukes som sekundærkanal. E-post og web er faktisk uavhengige kanaler, selv om begge går gjennom internett. Derfor kan e-post benyttes som sekundærkanal for autentisering gjennom web.

En smarttelefon kan bære relativt mange kanaler, f.eks. SMS, e-post, web, NFC, blåtann og USB. Med så mange ulike kanaler fins det mange muligheter for å designe autentiseringsordninger med sekundære kanaler. Imidlertid har disse ordningene ofte sårbarheter. For at autentisering med sekundærkanaler skal kunne støtte høyt autentiseringsnivå, må sekundærkanalen være sikker mot avlytting, kapring og mellommannsangrep. Autentisering med se-



Figur 8.9. Autentisering gjennom sekundærkanal, med SMS i dette eksemplet.

kundærkanaler er dynamisk fordi autentiseringstjeneren sender forskjellige og uforutsigbare koder for hver ny autentisering.

BankID på mobil ble innført i 2009, og utfaset i 2023. BankID på mobil benyttet SIM (beskrevet i avsnitt 7.4.6) som sekundærkanal. Her ble det sendt et par referanseord, som for eksempel «Klein Paraply» til SIM-brikken via teleoperatøren og presentert til brukeren på mobilen. De samme referanseordene ble vist på nettsiden, der brukeren måtte verifisere at de stemte overens. Bruk av SIM er en svært sikker sekundærkanal, og gir høyt autentiseringsnivå. Grunnen til at BankID på mobil ble utfaset, er blant annet at ordningen var avhengig av teleoperatørene, som tok betaling for å sende meldinger til SIM-brikken. BankID-appen er uavhengig av teleoperatørene, noe som gir IdP-er og banker større fleksibilitet, og gjør forvaltning av autentisering enklere. Imidlertid kan installering av BankID-appen skape problemer for brukere, mens BankID på mobil ikke krevde installering av en app. BankID-appen er basert på samme prinsipp som FIDO (beskrevet i avsnitt 8.4.2).

8.5 Egenskapsbaserte autentikatorer: biometri

Biometrisk autentisering er automatiserte metoder for å verifisere en persons identitet basert på fysiologiske egenskaper. Det fins en rekke ulike metoder som på fagspråket kalles biometriske modaliteter, der velkjente modaliteter er blant annet

- fingeravtrykk
- ansiktsgjenkjenning
- øye-/netthinne-/iris-skanning
- håndgeometri
- håndsignatur
- stemme-/talekarakteristikk
- tastetrykkdynamikk
- ganglag

8.5.1 Krav til biometriske systemer

Det fins nær sagt ingen grenser for hva som kan være en biometrisk modalitet, men for at en modalitet skal kunne anvendes i praktiske implementeringer, gjelder syv hovedkrav:

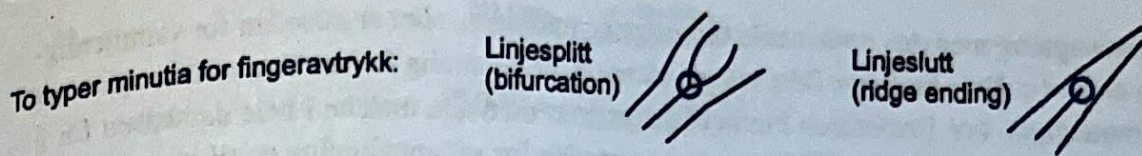
1. **Universalitet:** De aller fleste personer skal kunne uttrykke karakteristikkene for modaliteten.
2. **Særpreget:** Ulike personer skal generelt ha tydelig forskjellige karakteristikkene av modaliteten.
3. **Permanens:** Karakteristikkene av modaliteten for en person skal stort sett holde seg uendret over lang tid.
4. **Målbarhet:** Karakteristikkene for modaliteten skal være lett å innhente og måle på en kvantitativ måte.
5. **Ytelse:** Hastigheten på innhenting av målinger for karakteristikkene, hastigheten på analysen av målingene og hvor lav ressursbruk som er tilstrekkelig for å oppnå ønsket hastighet.
6. **Aksept:** I hvilken grad folk er villige til å akseptere bruken av en bestemt biometrisk modalitet.
7. **Beskyttelse mot presentasjonsangrep:** Evnen til å beskytte mot, og detektere, forsøk på å lure det biometriske systemet med forfalskede karakteristika. Dette er relatert til PAD (Presentation Attack Detection), som er beskrevet i avsnitt 8.5.3.

Biometriske maler og prøver representerer svært sensitive data der konfidensialitet er viktig. I de fleste tilfeller regnes biometriske data som personopplysninger, slik at man må ta hensyn til personvern og GDPR når man tar i bruk et system med biometrisk autentisering. Hvis biometriske opplysninger behandles «*med det formål å entydig identifisere en fysisk person*», som jo er det vanlige, skal det betraktes som særlige kategorier i henhold til GDPR. I slike tilfeller må den behandlingsansvarlige tilfredsstille et av behandlingsgrunnlagene beskrevet i GDPR Art. 9 for at behandlingen skal være lovlig. Hvis biometriske maler og prøver for en bruker kun samles inn og prosesseres lokalt på brukerens enhet, er det relativt enkelt å beskytte biometriske data. Hvis biometriske data fra mange brukere lagres og prosesseres sentralt, kreves det strenge sikkerhetstiltak for å beskytte slike data.

8.5.2 Virkemåte og komponenter i biometriske systemer

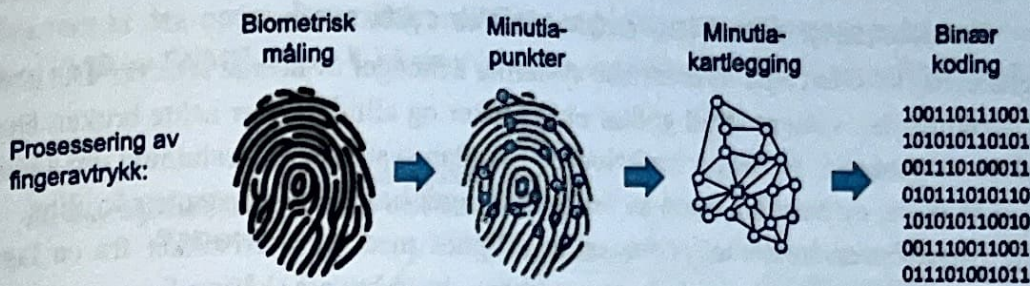
Formatet på biometriske målinger er svært ulike og avhenger av modalitet. For stemmegjenkjenning gjøres lydopptak der sekvenser av lydfrekvenser analyseres og sammenlignes. For fingeravtrykk lages et todimensjonalt bilde av linjene i huden på en finger, der linjenes geometri analyseres og sammenlignes. Målinger for en spesifikk modalitet kan beskrives med et sett med karakteristika (features).

Prosessering av fingeravtrykk er basert på å detektere og kartlegge såkalte *minutia*, der det fins to forskjellige typer, som vist i figur 8.10.



Figur 8.10. Minutia for fingeravtrykk.

Ved tradisjonell prosessering av et fingeravtrykk analyseres bildet for å identifisere linjer og for å detektere og lokalisere minutia. Hvert minutia registreres med den geometriske plasseringen i forhold til andre minutia. Denne informasjonen blir til slutt kodet og uttrykt binært, som vist i figur 8.11.



Figur 8.11. Prosessering av fingeravtrykk fra biometrisk måling til binær kode.

For autentisering med fingeravtrykk må hver bruker først registrere sitt fingeravtrykk for å lage en fingeravtrykkmal. Kvaliteten på den innsamlede fingeravtrykkmalen er avgjørende for nøyaktigheten av biometrisk autentisering. Systemet vil derfor verifisere om kvaliteten er tilfredsstillende før en fingeravtrykkmal med karakteristika legges inn i databasen. Ved autentisering vil brukeren legge fingeren på en sensor som registrerer et bilde av fingeren med linjer i huden. Sensoren sender bildet til neste komponent, som ekstraherer karakteristika fra prøven. Disse blir til slutt sendt til komparatoren, som sammenligner karakteristika fra den innhentede prøven med karakteristika fra fingeravtrykkmalen i databasen. Figur 8.12 viser sammenhengen mellom disse generelle komponentene.



Figur 8.12. Generelle komponenter for et biometrisk system.

Et system som vist i figur 8.12 kan brukes for å sammenligne med metodene «en-til-en» eller «en-til-mange». Hvis applikasjonen har mange brukere, er det vanlig at brukeren oppgir identitet, slik at biometrisystemet kan hente malen for en enkelt bruker fra databasen for

sammenligning med den innhentede biometriske målingen, som er metoden for sammenligning en-til-en. Hvis brukeren ikke oppgir identitet, er det mulig for det biometriske systemet å sammenligne den innhentede biometriske prøven med alle malene i hele databasen for å identifisere malen med størst likhet, som er metoden for sammenligning en-til-mange.

Det er svært ressurskrevende å anvende et biometrisk system med en-til-mange som metode. Imidlertid er dette nettopp metoden som benyttes i kriminalteknisk etterforskning, der en innhentet biometriske prøve sammenlignes med maler fra alle mulige mistenkte for å etablere bevis.

Tradisjonelt ble spesifikke måleparametere benyttet for sammenligning av biometriske prøver. I nyere systemer benyttes mest maskinlæring for å sammenligne biometriske prøver og beregne skåring for å ta beslutning om brukerautentisering.

8.5.3 Kvalitetsaspekter ved biometriske systemer

Nøyaktigheten og kvaliteten på biometriske systemer avhenger av mange faktorer. Det er ønskelig at et biometrisk system alltid godtar ekte bruker og alltid avviser uekte bruker. Dessverre er dette uoppnåelig. Nedenfor beskriver vi hvordan systemet tar beslutning om å godta eller avvise brukere, og hvordan raten av feilbeslutninger bestemmer systemets kvalitet.

Karakteristika fra en innhentet prøve sammenlignes med karakteristikk fra en lagret mal. Sammenligningen gir skåring S . Jo større likhet, desto høyere skåring S .

Terskelverdi T avgjør om systemet definerer prøven som *match*, som betyr at prøven ligner på malen og det antas at brukeren er ekte, eller *non-match*, som betyr at prøven ikke ligner på malen og det antas at brukeren er uekte.

Match (antatt ekte bruker) er når $S \geq T$

Non-match (antatt uekte bruker) er når $S < T$

Det er imidlertid mulig at systemet feilaktig gir match for uekte bruker og non-match for ekte bruker. Det fins fire alternativer:

- True Match: match for ekte bruker $\rightarrow$ ekte bruker godtas (sann positiv)
- True Non-Match: non-match for uekte bruker $\rightarrow$ uekte bruker avvises (sann negativ)
- False Match: match for uekte bruker $\rightarrow$ uekte bruker godtas (falsk positiv)
- False Non-Match: non-match for ekte bruker $\rightarrow$ ekte bruker avvises (falsk negativ)

Kvaliteten på biometriske systemer testes ved å la et stort antall ekte og uekte brukere forsøke å autentisere seg. At en ekte bruker autentiserer seg, betyr at brukeren forsøker å logge inn på sin egen konto. At en uekte bruker autentiserer seg, betyr at brukeren som forsøker å logge inn, ikke er registrert i systemet, eller at brukeren er registrert, men forsøker å logge inn på en annen brukers konto. På den måten samles statistikk over hvor ofte hvert av de fire alternativene ovenfor forekommer. To viktig statistiske mål er *FMR* (*False Match Rate*), som er raten av falske positiv, og *FNMR* (*False Non-Match Rate*), som er raten av falske negativ. Disse kan uttrykkes som følger:

$$FMR = \frac{\text{antall False Match}}{\text{antall uekte brukere}}$$

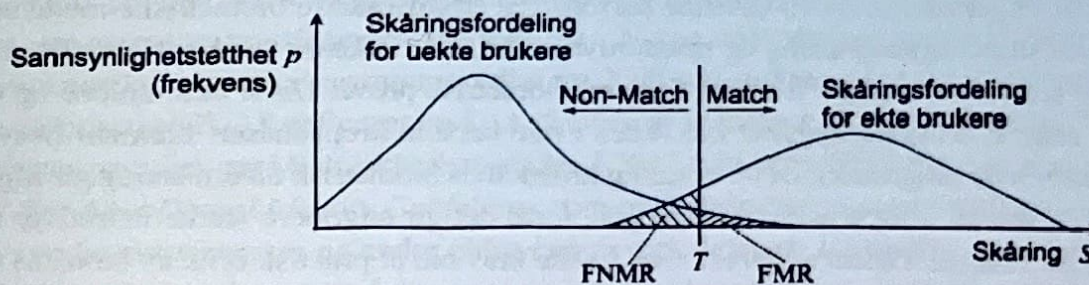
$$FNMR = \frac{\text{antall False Non-Match}}{\text{antall ekte brukere}}$$

Terskelverdien T bestemmer balanse mellom FMR og FNMR.

Hvis terskelverdien T heves, blir det vanskeligere for uekte brukere å få match, slik at antall falske positive går ned og FMR reduseres, noe som er bra. Imidlertid blir det også vanskeligere for ekte brukere å få match, slik at antall falske negative går opp og FNMR øker, noe som ikke er bra.

Hvis terskelverdien T senkes, blir det lettere for uekte brukere å få match, slik at antall falske positive går opp og FMR øker, noe som ikke er bra. Samtidig blir det også lettere for ekte brukere å få match, slik at antall falske negative går ned og FNMR reduseres, noe som er bra.

Hva som er den optimale terskelverdi T for et biometrisk system, er altså en avveining mellom FMR og FNMR. Figur 8.13 viser hvordan terskelverdien T påvirker FMR og FNMR.



Figur 8.13. Betydning av terskelverdien T for FMR og FNMR.

Kurvene representerer statistiske fordelinger av skåringer for henholdsvis ekte og uekte brukere etter testing med mange brukere. Høyden på kurvene representerer (tetthet av) sannsynlighet p for at en ekte eller uekte bruker oppnår en gitt skåring S . Størrelsen på de skraverede områdene på figur 8.13 representerer FMR og FNMR.

EER (Equal Error Rate) er når $FMR = FNMR$, dvs. $EER = FMR = FNMR$. Generelt sett er terskelverdien for EER den optimale terskelverdien, men systemeier må likevel avgjøre hvilken av FMR og FNMR det skal tas mest hensyn til. EER er samtidig et mål for kvaliteten på et biometrisk system – dvs. jo lavere EER, desto bedre kvalitet.

Imidlertid betyr lav EER slett ikke at systemet ikke kan lures. Fordelingen av skåringer for uekte brukere i figur 8.13 reflekterer ikke at de forsøker å lure systemet – de er bare uekte brukere.

Hvis angripere virkelig forsøker å lure et biometrisk system, og har nødvendige ressurser og kompetanse, vil de som regel alltid lykkes. Begrepet PAD (Presentation Attack Detection) uttrykker i hvilken grad angrep på biometriske systemer med forfalsket input kan forhindres og detekteres. Dessverre er det vanskelig å oppnå robust PAD, særlig når angripere tar i bruk AI (Artificial Intelligence) for å etterligne ansikter og stemmer.

Generelt sett er biometriske autentiseringssystemer relativt sårbare for angrep, og bør ikke brukes alene for sensitive applikasjoner. Sammen med andre metoder for autentisering kan biometri gi god sikkerhet, og samtidig gi god brukervennlighet.

8.5.4 Trygghetsaspekter ved biometriske systemer

Det kan være aktuelt å sette krav til personsikkerhet ved bruk av biometriske systemer, etter som brukeren involveres fysisk. Et mulig angrep på biometriske systemer kan være å tvinge en person til å avgi en biometrisk prøve, eller å stjele kroppsdeler som brukes for biometrisk autentisering. I Kuala Lumpur i 2005 hugget biltyver av en del av førerens venstre pekefinger for å starte hans S-klasse Mercedes Benz utstyrt med fingeravtrykksnøkkel.³² I USA i 2023 er det rapportert om flere tilfeller der kriminelle har dopet ned ofre for å låse opp deres smart-telefoner og få tilgang til deres bankkontoer med ansiktsgjenkjenning.³³ I alle tilfellene dreier det seg om kroppsbaserte biometriske modaliteter, det vil si at en kroppsdelt, som for eksempel ansikt eller finger, benyttes for autentisering. Slike modaliteter kan benyttes selv om brukeren er bevisstløs, slik at det er relativt enkelt å tvinge frem en biometrisk prøve. Det er for eksempel enkelt å få et fingeravtrykk fra en sovende person. Ved atferdsbaserte biometriske modaliteter derimot, som stemmegjenkjenning og tastaturdynamikk, må brukeren være bevisst, slik at det ikke er like lett for en angriper å tvinge frem en biometrisk prøve. Disse eksemplene og vurderingene viser at brukers trygghet kan settes i fare dersom kroppsbasert biometri benyttes utenfor kontrollerte omgivelser. Dette er særlig kritisk hvis biometrisk autentisering gir tilgang til betydelige verdier eller sensitiv informasjon, fordi det gir angripere sterke insentiver til å fysisk angripe brukere. Derfor er det relevant å sette krav om at praktisk bruk av biometri skal være trygt, og ikke utsetter brukeren for uforholdsmessig stor fysisk fare.

8.6 Flerfaktor-autentisering

Å basere autentisering på bare én av metodene beskrevet i avsnitt 8.2 vil aldri kunne gi sterk autentisering. Sagt på en annen måte vil én autentiseringsmetode alene ikke kunne skape høy visshet om at en autentisert bruker faktisk er den ekte brukeren. For å oppnå sterk autentisering må to eller flere metoder benyttes samtidig. Dette kalles *flerfaktor-autentisering*, der faktorene er de ulike autentiseringsmetodene som benyttes i en ordning.

2FA (tofaktor-autentisering), som uttales «tofa», har lenge vært brukt for høyt sensitive tjenester, og brukes i økende grad også for tjenester med moderat sensitivitet. En typisk tofaktor-kombinasjon er å benytte en dynamisk autentiseringsenhet (brikke eller sekundærkanal) sammen med et statisk passord.

De største hindringene for å ta i bruk 2FA er økte kostnader og utfordringer med god brukervennlighet. Imidlertid gjøres det mye innovasjon i utviklingen av rimelige og samtidig brukervennlige metoder for autentisering. BankID-appen anses som mer brukervennlig enn tradisjonell BankID, samtidig som det gir høy autentiseringsstyrke. Dette er et eksempel på vellykket implementering av tofaktor-autentisering.

32 <http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm>.

33 <https://www.nytimes.com/2023/03/29/nyregion/indictments-nyc-gay-bars-homicide.html>.

For tilbydere av online-tjenester kan det være vanskelig å velge passende autentiseringsordning. I neste avsnitt beskriver vi rammeverk for autentisering som nettopp skal være til hjelp for å tilpasse en autentiseringsordning til sensitiviteten av tjenesten.

8.7 Veiledere for autentisering

Myndigheter i alle land går i økende grad over til e-forvaltning (e-Governance), som betyr digitalisering av offentlige tjenester. God autentisering er viktig når innbyggere må logge seg inn for å få tilgang til offentlige tjenester. En ordning for brukerautentisering i e-forvaltning kalles eID. Det er naturlig at eID-ordninger harmoniseres mellom alle offentlige tjenester, både nasjonalt innen hvert land og regionalt som i EU. Norge og mange andre land har derfor publisert veiledere for autentisering til bruk i offentlig sektor. *Veileder for identifikasjon og sporbarhet i elektronisk kommunikasjon med og i offentlig sektor*, publisert av DigDir i 2022, følger eIDAS-forordningen fra EU implementert som *lov om elektroniske tillitstjenester*, som trådte i kraft 15. juni 2018. Begrepet «tillitstjeneste» er EU-sjargong for PKI-baserte sertifiserings- og autentiseringstjenester. Merk at det i Norge noen ganger fremdeles refereres til det gamle norske autentiseringsrammeverket fra 2008 som definerer fire autentiseringsnivåer.

Det europeiske eIDAS definerer tre LoA (Levels of Assurance) for autentisering,³⁴ dvs. tre autentiseringsnivåer, også kalt sikkerhetsnivåer. I 2017 publiserte NIST ny utgave av veilederen *SP 800-63-3 Digital Identity Guidelines*, som også definerer tre autentiseringsnivåer. Det gamle norske rammeverket og andre eldre rammeverk definerte typisk fire autentiseringsnivåer. Imidlertid viste det seg at det laveste nivået, med betydningen «liten eller ingen visshet om korrekt identitet», ikke hadde noen praktisk anvendelse for e-forvaltning. Moderne rammeverk for autentisering har derfor bare tre autentiseringsnivåer. Tabell 8.1 viser noen relevante veiledere og standarder for autentisering og hvordan de definerer autentiseringsnivåer.

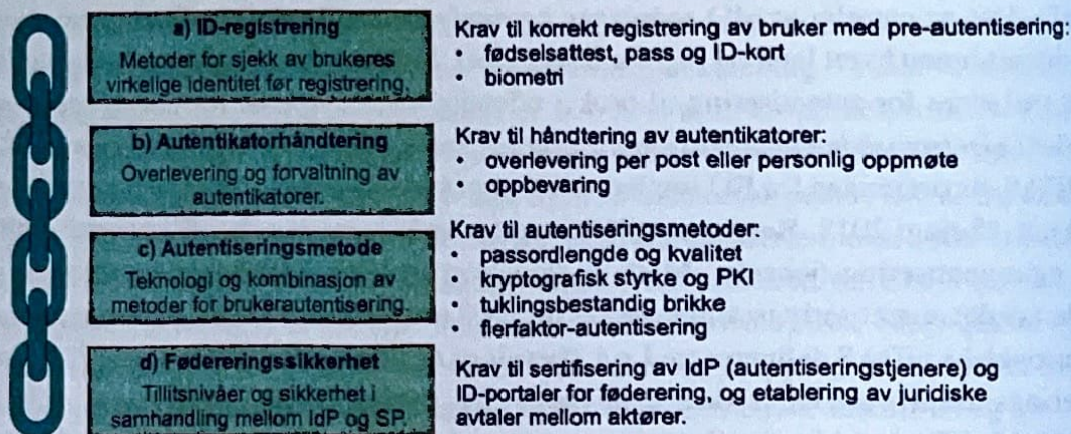
Tabell 8.1. Veiledere og standarder for autentisering

Veileder/standard for autentisering		Autentiseringsnivåer			
Veileder for identifikasjon og sporbarhet DigDir 2022			Lavt	Betydelig	Høyt
Assurance levels for electronic identification means eIDAS, EU 2018			Low	Substantial	High
SP 800-63-3 Digital Identity Guidelines NIST, USA 2017			Assurance Level 1	Assurance Level 2	Assurance Level 3
IS 29115 Entity authentication assurance framework ISO/IEC 2013		Low (1)	Medium (2)	High (3)	Very High (4)

Det er interessant å se i tabell 8.1 at veilederne/standardene gir sprikende navn på hvert autentiseringsnivå. Ved å lese de ulike dokumentene viser det seg likevel at kravene for hvert nivå er relativt godt harmonisert.

34 <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS+Levels+of+Assurance>.

Slike veiledere/standards definerer typisk fire kategorier av krav til autentisering. For at en ordning skal oppnå et visst autentiseringsnivå, må kravene for det nivået i alle kategorier oppfylles. Figur 8.14 viser de fire kategoriene av krav til autentisering, med eksempler fra hver kategori. Kjettinglenken viser metaforisk at autentiseringen ikke kan være sterkere enn det svakeste ledd, det vil si det svakeste sett med oppfylte krav i hver kategori. Enkelt forklart betyr det at korrekt autentisering typisk er avhengig av fire komponenter (kategorier): a) korrekt registrering av brukere, b) forsvarlig håndtering av autentikatorer, c) tilstrekkelig robust autentiseringsmetode, d) sikkerhet i ID-føderering.



Figur 8.14. Kategorier av krav til autentisering.

Det er verdt å nevne at kun det amerikanske SP 800-63-3 beskriver kategori d) med krav til fødereringssikkerhet. Den norske veilederen inkluderer ikke kategori d) med fødereringssikkerhet fordi veilederen bygger på eIDAS-forordningen der fødereringssikkerhet ikke nevnes. Imidlertid bør krav til fødereringssikkerhet absolutt inkluderes ettersom ID-føderering brukes i alle eID-ordninger, som beskrevet i neste kapittel. Forhåpentlig vil krav til ID-føderering tas med i den reviderte forordningen fra EU.

Nedenfor er en forenklet beskrivelse av krav for hvert autentiseringsnivå, som er omtrent like i den europeiske eIDAS-forordningen, den amerikanske veilederen SP 800-63-3 og i den norske veilederen for identifikasjon og sporbarhet.

- **Lavt** – 1-faktoraautentisering, f.eks. statisk passord mottatt personlig eller via post til brukerens offisielle postadresse.
- **Betydelig** – 2-faktoraautentisering (2FA), f.eks. statisk passord og i tillegg engangskoder mottatt via post til brukerens offisielle postadresse, alternativt via SMS (norsk ordning: MinID).
- **Høyt** – 2-faktoraautentisering (2FA), f.eks. statisk passord, og i tillegg fysisk brikke mottatt ved personlig oppmøte, alternativt app på mobil (norske ordninger: Commfides, Buy-pass, BankID-brikke, BankID-app).

Tilbydere av offentlige digitale tjenester kan benytte slike standarder og veiledere for autentisering som grunnlag for å velge autentiseringsnivå og metoder for autentisering. Når en tjeneste er vurdert til å ha høy, betydelig eller lav sensitivitet, setter rammeverkene krav til hva som kreves av en passende ordning for brukerautentisering. Tilbydere av offentlige digitale tjenester kan være fristet til å alltid velge høyeste autentiseringsnivå, men de må også huske at høyere autentiseringsnivå gir større kompleksitet og kostnader ved utrulling og forvaltning. Derfor er det viktig at autentiseringsnivået er tilpasset sensitivitetsnivået for tjenesten. Vurdering av en tjenestes sensitivitet og valg av passende autentiseringsnivå er en viktig del av risikostyring for tjenesten.

Phishingangrep er en trussel som eksisterende autentiseringsmetoder i liten grad gir beskyttelse mot. Et mellommannsangrep betyr for eksempel at brukeren blir lurt til å sende autentikatorer til en falsk tjenestetilbyder eller autentiseringstjener, som videresender autentikatorene til den genuine tjenestetilbyderen/autentiseringstjeneren. For å stoppe slike angrep forskes det på å utvikle phishingresistent autentisering. Det kan for eksempel gjøres ved at autentikatorer blir en dynamisk funksjon av identiteten og/eller IP-adressen til tjenestetilbyderen/autentiseringstjeneren, slik at autentikatorer ikke kan videresendes fra den falske til den ekte tjenestetilbyderen/autentiseringstjeneren. I arbeidet med ny revidert utgave av den amerikanske *SP 800-63-3 Digital Identity Guidelines* nevnes det at phishingresistente autentiseringsmetoder blir et krav for det høyeste autentiseringsnivået.

I 2021 startet EU prosessen med revidering av eIDAS-forordningen som antagelig vil skifte navn til forordning for digital identitet (eng. digital identity act), også kalt eID-forordningen. Den reviderte forordningen vil blant annet beskrive et europeisk rammeverk for eID. Norge har hatt en god eID-ordning helt siden autentisering med fødselsnummer og BankID ble innført i 2004. De andre nordiske landene og en del andre EU-land har også gode eID-ordninger, men det gjelder ikke alle land i EU. Hensikten med å innføre europeisk eID er blant annet å tvinge alle EU-land til å innføre gode eID-ordninger for sine innbyggere, og at disse ordningene skal fungere over landegrensene.

Den nye eID-forordningen vil også beskrive en såkalt *digital identitetslommebok* (eng. digital identity wallet), også kalt ID-lommebok. En ordning for ID-lommebok vil gjøre at hver innbygger skal kunne bruke en app tilknyttet sin eID som gjør det enkelt å presentere dokumentasjon i form av *verifiserbare akkreditiver* (eng. verifiable credentials) i ulike sammenhenger. Et verifiserbart akkreditiv er et digitalt signert dokument som tredjeparts mottagere kan verifisere autentisiteten og ektheten av. Verifiserbare akkreditiver kan for eksempel være sertifiseringer, vitnemål, karakterutskrifter, referanser, attester, lisenser, tillatelser, vaksinasjoner og medisinske prøveresultater. En velfungerende ordning for ID-lommebok har potensial til å effektivisere forvaltning av denne typen dokumenter, og til å forhindre dokumentforfalskning. EU diskuterer også begrepet *selv-suveren identitet* (SSI) (eng. self-sovereign identity), som betyr at hver innbygger skal kunne definere og forvalte sin egen eID med forankring i blokkjeder (se avsnitt 5.4). En ordning for SSI ville gjøre det mulig å benytte en selvdefinert identifikator i stedet for fødselsnummeret, for tilgang til e-forvaltningstjenester. Visjonene om ID-lommebok og selv-suveren identitet er temmelig ambisiøse, så det kan ta noen år før den nye eID-forordningen blir ferdig.

Oppgaver til kapittel 8

8.1 Passord

- a. Hvorfor bør passord ikke lagres i klartekst på autentiseringstjeneren?
- b. Hva menes med passordsalting, og hva er hensikten med det?
- c. Hvilken kjent tjeneste på internett brukes for å sjekke om en bruker-ID (og passord) kan være stjålet? Sjekk om en av dine egne bruker-ID-er kan være stjålet, og endre passordet hvis den er det.
- d. Nevn en grunn til at passord aldri bør gjenbrukes.

8.2 Biometri

- a. Forklar hvordan kvaliteten på et system for biometrisk autentisering kan uttrykkes med EER.
- b. Hvis et biometrisk system konfigureres med svært lav FMR (False Match Rate), hva er konsekvensen for FNMR (False Non-Match Rate)?
- c. Se for deg et system som er konfigurert med svært lav FMR. I hvilken grad gjør det at systemet er robust mot tilsiktet forfalskning (eng. presentation attack)?

8.3 Veileder for autentisering

- a. Hva er formålet med å ha en veileder/forordning for e-autentisering?
- b. Hvilken veileder/forordning for e-autentisering gjelder for Norge?
- c. Nevn norske autentiseringstjenester som tilfredsstiller krav til høyeste autentiseringsnivå.

Kapittel 9

IAM – identitets- og tilgangshåndtering

I dette kapitlet lærer du hvordan brukerautentisering beskrevet i forrige kapittel settes i system for å lage avanserte ordninger som gir god brukervennlighet og skalerbarhet på internett. *Identitetshåndtering* er begrepet som dekker slike avanserte ordninger for brukerautentisering.

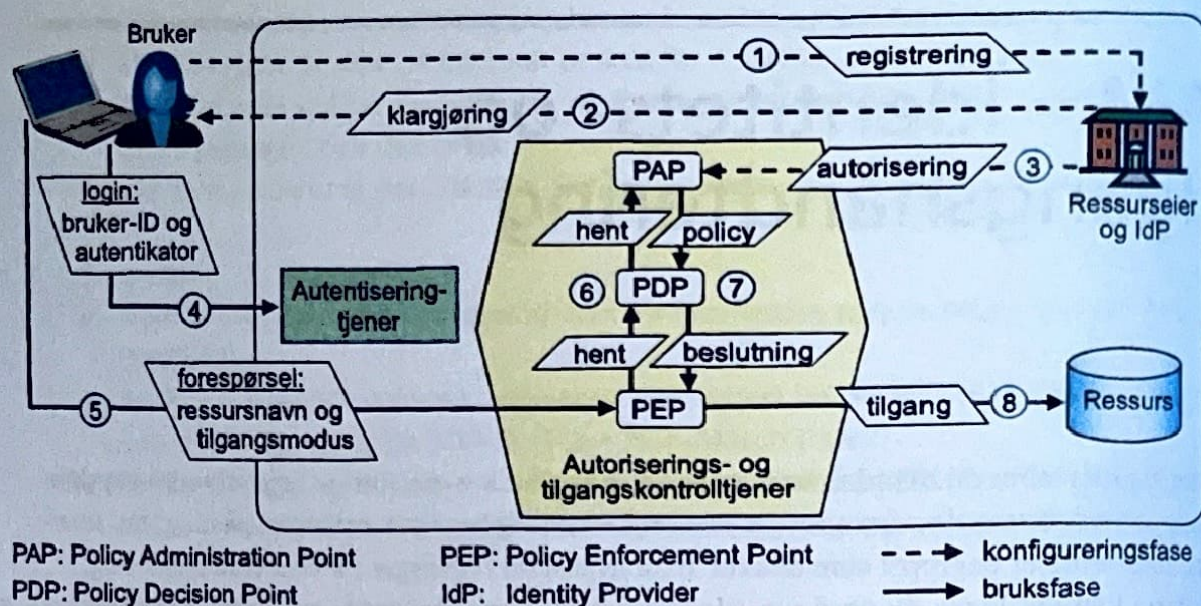
I dette kapitlet lærer du også om *tilgangshåndtering*, som består av metoder som sørger for at autentiserte brukere kun får tilgang til data og tjenester de er autorisert for.

9.1 Definisjon av IAM

Forkortelsen IAM (Identity and Access Management) betyr «identitets- og tilgangshåndtering», som dekker de to generelle funksjonene som består av identitetshåndtering og tilgangshåndtering (se figur 1.9). Identitetshåndtering fokuserer på registrering og autentisering av brukeridentiteter. Selv om en bruker er blitt autentisert, er det begrenset hvilke ressurser brukeren skal ha tilgang til. Tilgangshåndtering fokuserer nettopp på tilgangsbasert autorisering for registrerte brukere, og deretter på kontroll av tilgang til data og ressurser basert på autoriseringen. Det fins flere modeller for tilgangskontroll, tradisjonelt kalt *sikkerhetsmodeller*, som er metoder for å kontrollere autentiserte brukeres tilgang til ressurser. Identitetshåndtering og tilgangshåndtering er knyttet tett sammen i praktiske implementeringer. En god definisjon på IAM er artikulert av Gartner:³⁵

«Identitets- og tilgangshåndtering (IAM) er sikkerhetsdisiplinen som sørger for at de rette individene får tilgang til de riktige ressursene til rett tid, og med riktige hensikter.»

Mens figur 1.9 fremstiller IAM på en relativt abstrakt form bestående av en konfigureringsfase og en bruksfase, viser figur 9.1 en alternativ fremstilling av IAM i form av et typisk IAM-scenario.



Figur 9.1. IAM-scenario.

Hvert trinn av IAM i figur 9.1 er beskrevet nedenfor.

Konfigureringsfasen

1. Brukerens identitet og bruker-ID registreres av autentiseringstjener (IdP).
2. IdP klargjør autentikator(er) som overføres til bruker.
3. Ressurseier autoriserer bruker ved å spesifisere tilgangspolicy og -regler i PAP (Policy Administration Point). En autoriseringspolicy kan endres over tid, og kan bestemmes ut fra hvilke oppgaver brukeren for øyeblikket skal utføre.

Bruksfasen

4. Bruker-login med bruker-ID og autentikator.
5. Bruker gjør forespørsel om tilgang til ressurs.
6. Funksjonen for tilgangskontroll henter tilgangspolicy fra PAP.
7. PDP (Policy Decision Point) foretar en beslutning om tilgang.
8. PEP (Policy Enforcement Point) håndhever beslutningen og tillater eller avviser tilgang.

Konfigureringsfasen og bruksfasen foregår parallelt. Det vil typisk være behov for å endre tilgangsautorisasjoner eller å klargjøre nye autentikatorer for en bruker samtidig som bruker-kontoen er i aktiv bruk.

Konfigureringsfasen og bruksfasen av IAM vises i figur 9.1 med henholdsvis stiplede og heltrukne piler, slik at trinn 1–3 er en del av konfigureringsfasen, mens trinn 4–8 er en del

av bruksfasen. Fra et annet perspektiv består identitetshåndtering av trinn 1, 2 og 4, mens tilgangshåndtering består av trinn 3, 5, 6, 7 og 8.

At brukeren gjør en tilgangsforespørsel i trinn 5, betyr ikke nødvendigvis at brukeren eksplisitt spesifiserer ressursnavn og tilgangsmodus. I praksis er det avhengig av applikasjoner hvordan bruker gjør en tilgangsforespørsel. Nedenfor skisseres tre ulike måter å gjøre tilgangsforespørsel på:

- Tilgang kan gis automatisk etter autentisering uten at brukeren trenger å gjøre en forespørsel. Tilgangskontroll og autentisering er dermed kombinert i ett trinn.
- Applikasjonen kan være konfigurert slik at den kun viser ressurser som brukeren er autorisert for. På den måten består tilgangskontrollen av at applikasjonen viser ressurser som brukeren er autorisert for, og skjuler ressurser som brukeren ikke er autorisert for.
- Applikasjonen kan vise, eller la brukeren velge, alle ressurser som applikasjonen kan tilby, uansett om brukeren er autorisert for tilgang eller ikke. Tilgangskontroll skjer når brukeren faktisk gjør en forespørsel, som vist i figur 9.1.

Betegnelsene PAP, PDP og PEP representerer abstrakte funksjoner, og ikke nødvendigvis konkrete programvaremoduler. Disse funksjonene er spesifisert i XACML-standard (eXtensible Access Control Markup Language) publisert av OASIS. Denne standarden kan brukes for implementering av ABAC (Attribute-Based Access Control), som er en modell for tilgangskontroll beskrevet i avsnitt 9.3 nedenfor.

Scenarioet for IAM i figur 9.1 er relativt enkelt, og skalerer dårlig for tilgang til tjenester på internett. Identitetsfødering er blitt en sentral komponent i moderne IAM-arkitekturer, som beskrevet i neste avsnitt. Avanserte modeller for tilgangshåndtering er beskrevet i avsnitt 9.3.

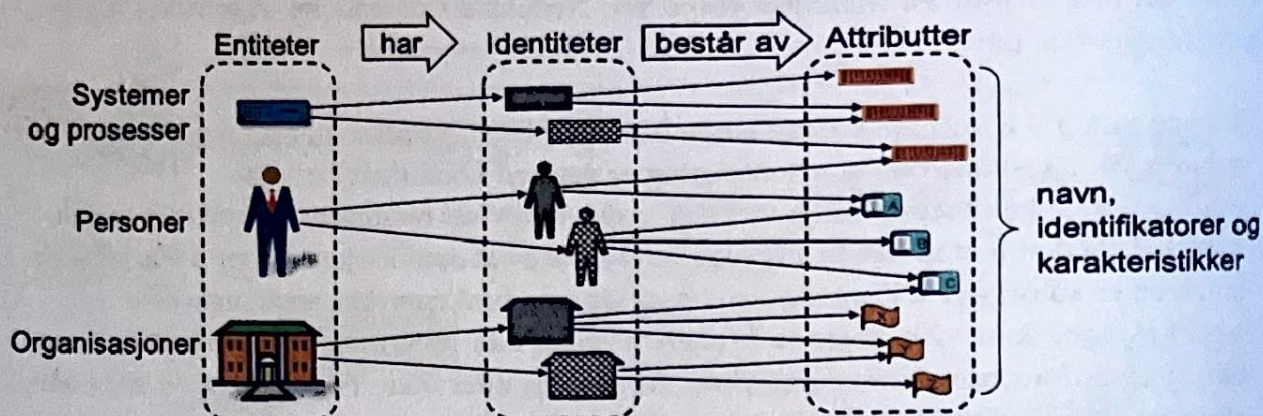
9.2 Identitetshåndtering

Identitetshåndtering består i å registrere identiteter og autentisere brukere basert på deres identiteter. Det fins ulike modeller for identitetshåndtering, der silomodellen er en klassisk og gammeldags modell, mens fødererte modeller er moderne med hensyn til økt brukervennlighet og fleksibilitet. Siden det er nyttig å ha en klar forståelse av hva identitet betyr, blir dette beskrevet i neste avsnitt.

9.2.1 Identitet

I dagligtale har begrepet «identitet» flere betydninger. Det er en fordel å ha en relativt presis definisjon på identitet for å kunne beskrive IAM på en konsistent måte. Vi må ta utgangspunkt i entiteter som har en fysisk, juridisk eller prosessuell eksistens. *Entiteter* kan være mennesker, organisasjoner, systemer eller til og med systemprosesser i minnet på et system. En slik entitet kan bli gitt en identitet som gjør det mulig å referere til entiteten. Etymologisk har begrepet «identitet» betydningen «den samme som forrige gang», som nettopp betyr at vi kan kjenne igjen entiteten basert på identiteten. Egentlig er en identitet bare et sett med attributter som beskriver eller er tilordnet entiteten. Et typisk attributt er et navn, men det kan

også være en fødselsdato, adresse eller nær sagt hvilken som helst opplysning relatert til en entitet. Figur 9.2 viser sammenhengen mellom entiteter, identiteter og attributter.



Figur 9.2. Sammenheng mellom entitet, identitet og attributter.

Ulike entiteter og ulike identiteter kan ha felles attributter. For eksempel kan to personer eller et firma og en person ha samme adresse. Imidlertid har to personer hvert sitt fødselsnummer, mens et firma har et entydig foretaksnummer, noe som gjør det mulig å skille identitetene fra hverandre.

Det er vanlig at hver identitet har et entydig attributt som representerer en identifikator eller databasenøkkel innenfor et navnerom. Et norsk fødselsnummer er en entydig identifikator innenfor navnerommet av fødselsnummer i domenet til folkeregisteret. Et vanlig navn er derimot ikke nødvendigvis entydig innenfor navnerommet av personlige navn, siden det for eksempel fins mange personer ved navn Per Hansen. Brukerkontoer har alltid et entydig navn innenfor domenet hvor en konto er registrert. I dagligtale er det vanlig å kalle et slikt entydig navn for brukeridentitet eller bruker-ID. Sammen med bruker-ID kan det registreres tilleggsattributter, som vanlig navn, adresse osv., og selve identiteten består egentlig av hele settet med attributter. Et identitetsdomene består av identiteter registrert med entydig bruker-ID og andre attributter.

En entitet kan ha flere identiteter, der hver identitet har sitt eget sett med attributter. Det er mulig å ha flere identiteter innenfor samme domene hvis hver identitet har en separat bruker-ID, men dette er uvanlig, og er ofte ansett som uheldig fra et sikkerhetsperspektiv. På den annen side er det svært vanlig å ha flere ulike identiteter innenfor forskjellige domener, som f.eks. ulike online-tjenester.

Et navnerom er sentralisert når det forvaltes av en enkelt entitet, for eksempel navnerommet av bruker-ID-er til alle ansatte i et firma eller navnerommet av fødselsnummer som forvaltes av folkeregisteret. Et navnerom er distribuert når det forvaltes av forskjellige entiteter. Navnerom for telefonnummer og e-postadresser er distribuerte fordi de forvaltes i fellesskap av ulike entiteter.

En IdP (Identity Provider) er en autentiseringstjener som forvalter et register over bruker-ID for hver bruker og foretar brukerautentisering. Legg merke til at en IdP ikke nødvendig-

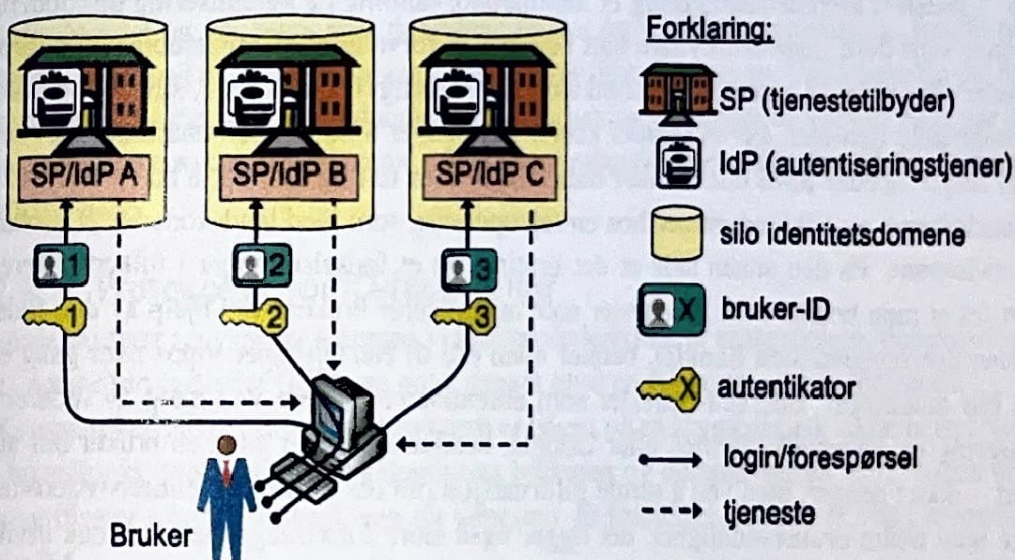
vis forvalter navnerommet av bruker-ID-er. Navnet IdP kan være forvirrende fordi det bokstavelig betyr «identitetstilbyder», mens en IdP i virkeligheten foretar brukerautentisering. For eksempel benyttes fødselsnummer som bruker-ID for autentisering med BankID. Her er folkeregisteret den som forvalter navnerommet, mens BankID er den som foretar brukerautentisering med fødselsnummeret som bruker-ID. BankID er altså IdP, mens folkeregisteret forvalter navnerommet med bruker-ID-er.

Kombinasjonen av ulike navnerom og IdP-er danner grunnlag for silo- og fødererte modeller for identitetshåndtering, som beskrives i avsnittene nedenfor.

9.2.2 Silomodell for identitetshåndtering

Silo-identitetshåndtering betyr at tjenestetilbyder selv utfører autentisering av sine brukere.

I den klassiske silomodellen for identitetshåndtering forvalter hver organisasjon et register over egne brukeridentiteter og foretar autentisering av disse. Med andre ord er tjenestetilbyder SP (Service Provider) og autentiseringstjener IdP (Identity Provider) en del av samme organisasjon. På den måten danner hver organisasjon sin egen silo for registrering og autentisering av brukere, der ulike siloer er isolert fra hverandre. En bruker som ønsker tjenester fra flere organisasjoner, må opprette en brukerkonto med separat autentikator i hvert silodomene, som vist i figur 9.3.



Figur 9.3. «Use-case» med silomodell for identitetshåndtering.

En fordel med silomodellen fra brukerens perspektiv er at den gir godt personvern som følge av at silodomener er isolerte. På den måten er utveksling av personinformasjon mellom domener ikke en del av arkitekturen. Fra perspektivet til tjenestetilbydere er dette en ulempe

fordi de ofte ønsker å utveksle informasjon om brukerne, som naturligvis alltid må skje på lovlig måte med samtykke og saklig grunnlag, osv. ifølge GDPR.

Silomodellen er også enkel å implementere for tjenestetilbydere, men gir dårlig brukervennlighet. Før internett – i en verden uten online-tjenester – var silomodellen det eneste fornuftige. Det viste seg etter hvert at silomodellen skalerte dårlig til det globale internett. På 2000-tallet ble det etablert mange nye online-tjenester som krevde innlogging. I begynnelsen ble disse tjenestene implementert med silomodellen, som gjorde det nødvendig for brukere å opprette en separat identitet og et separat passord for hver eneste tjeneste, noe som medførte identitetsoverlast (identity overload) og passordutmattelse (password fatigue) hos brukerne.

Undersøkelser viste at brukere som egentlig var interessert i å bruke en online-tjeneste, ofte ikke gjorde det likevel fordi de rett og slett ikke orket å opprette enda en identitet med enda et passord.

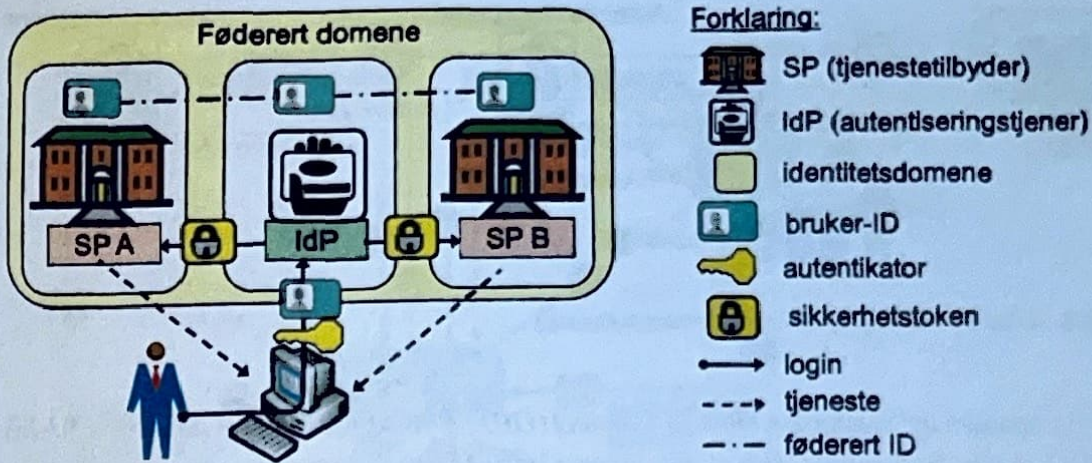
Mens silomodellen fremdeles er berettiget og fornuftig i mange sammenhenger, er føderert identitetshåndtering blitt svært utbredt på internett.

9.2.3 Føderert identitetshåndtering

Føderert identitetshåndtering betyr at samme bruker-ID benyttes hos ulike tjenestetilbydere og at brukerautentisering utføres av eksterne autentiseringstjenere.

Føderert identitetshåndtering er svært fleksibel på den måten at modulære komponenter kan brukes til å bygge forskjellige arkitekturer som er tilpasset bruksområde og forretningsprosess. I føderert identitetshåndtering er identitetsforvaltning og autentisering distribuerte funksjoner som flere tjenestetilbydere kan benytte. Å forvalte et identitetsdomene, et brukerregister eller tilby en autentiseringsfunksjon har naturligvis en kostnad, slik at dette ofte er kommersielle tjenester. For eksempel koster det penger å ha et telefonnummer selv om du aldri ringer, sender SMS eller bruker data. Du betaler rett og slett for å ha en identitet i identitetsdomenet av telefonnummer hos en teleoperatør, som med landskoder er et globalt identitetsdomene. På den annen side er det gratis å ha et fødselsnummer i folkeregisteret, bortsett fra at man betaler skatt. Tjenester som autentiserer brukere ved hjelp av den fødererte autentiseringstjenesten BankID, betaler noen øre til eierselskapet Vipps hver gang en bruker blir autentisert. Internett-tjenester som autentiserer brukere ved hjelp av fødererte autentisering fra Facebook, Twitter, eller Google, betaler også hver gang en bruker blir autentisert – ikke i penger, men ved å samle informasjon om oss brukere. Identitetsføderering gir ikke bare bedre brukervennlighet, det ligger også store forretningsinteresser bak utviklingen av slike tjenester.

En relativt enkel arkitektur er for eksempel en sentralisert føderering der en autentiseringstjener, IdP (Identity Provider), forvalter et brukerregister og foretar autentisering av alle brukere. Etter en autentisering vil IdP sende et sikkerhetstoken til andre tjenestetilbydere som forteller dem at en bruker med en viss bruker-ID er blitt autentisert, slik at de kan la brukeren få tilgang til tjenesten. Figur 9.4 viser et enkelt use-case der en bruker autentiserer seg til en sentralisert IdP og deretter får tilgang til tjenester fra både SP A og SP B.



Figur 9.4. Enkelt use-case med føderert identitetshåndtering.

For at SP A og SP B skal kunne godta og verifisere sikkerhetstokenet fra IdP i figur 9.4, må de på forhånd ha opprettet et teknisk og forretningsmessig samarbeid, som f.eks. utveksling av kryptografiske nøkkelsertifikater og inngåelse av juridiske avtaler. Dette er en forutsetning for alle identitetsføderasjoner, noe som skaper en viss kompleksitet.

ID-føderering er beslektet med SSO (Single Sign-On), som betyr at en enkelt innlogging er tilstrekkelig for tilgang til mange ulike tjenester fra forskjellige tilbydere. Kerberos er navnet på en teknologi for SSO utviklet på 1980-tallet ved MIT i USA som fremdeles er i utstrakt bruk. Kerberos er basert på en sentralisert AS (Authentication Service), et KDC (Key Distribution Center) og en TGS (Ticket Granting Service). Når brukeren autentiserer til AS, vil brukeren deretter implisitt være autentisert for andre tjenester internt i datanettet ved hjelp av kryptonøkler og «tickets» som tjenestene mottar og verifiserer automatisk. Imidlertid er Kerberos begrenset til et enkelt datanett, og skalerer ikke til internett. Ved å betrakte det fødererte domenet i figur 9.4 som et datanett hos en organisasjon ligner scenarioet på et use-case basert på Kerberos, der IdP tilsvarende AS/TGS i Kerberos og et sikkerhetstoken tilsvarende en Kerberos-ticket.

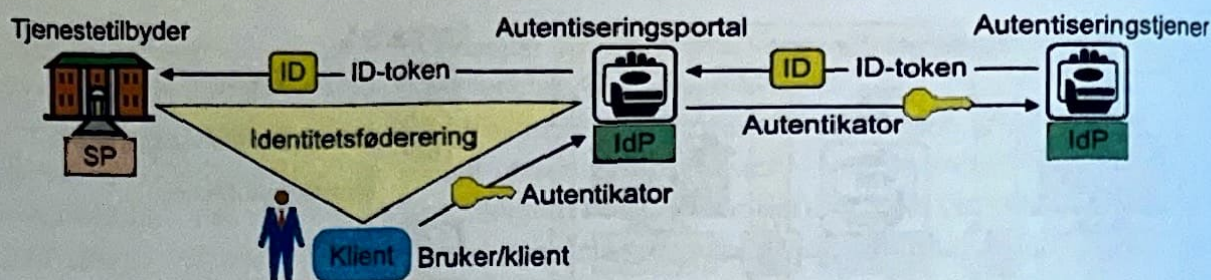
9.2.4 Protokoller for ID-føderering

Sentrale entiteter som spiller sammen i identitetsføderering, er bruker/klient, tjenestetilbyder (SP), autentiseringstjener (IdP), og noen ganger også en ID-portal som mellomledd.

Kommunikasjon mellom disse entitetene er basert på en kryptografisk sikkerhetsprotokoll der hovedfunksjonene er at IdP autentiserer brukeren og deretter sender et ID-token til SP, som verifiserer tokenet før brukeren får tjenesten. Et forenklet scenario er vist i scenarioene i figur 9.5.

Både autentiseringsportalen og autentiseringstjeneren i figur 9.5 regnes som IdP. Eksempler på autentiseringsportaler i Norge er ID-porten, Altinn, HelseID og FEIDE. Merk at det ikke alltid brukes en autentiseringsportal slik at autentiseringstjener sender ID-tokenet direkte til tjenestetilbyder.

Frem til ca. 2018 var SAML (Security Assertion Markup Language) den mest brukte standard/protokoll for identitetsføderering. SAML regnes nå som gammeldags, og er i stor



Figur 9.5. Roller og meldingsutveksling i identitetsføderering.

grad blitt erstattet av standarden *OpenID Connect (OIDC)*, som er beskrevet nedenfor. SAML og OIDC er ikke kompatible, slik at alle aktører innenfor en føderasjon må endre teknologi samtidig for å skifte standard, noe som kan være komplisert. I Norge brukes nesten utelukkende OIDC i dag. En annen standard fra begynnelsen av 2000-tallet er WS-Federation, som fikk lite gjennomslag på tross av at den ble utviklet av prominente selskaper som Microsoft og IBM.

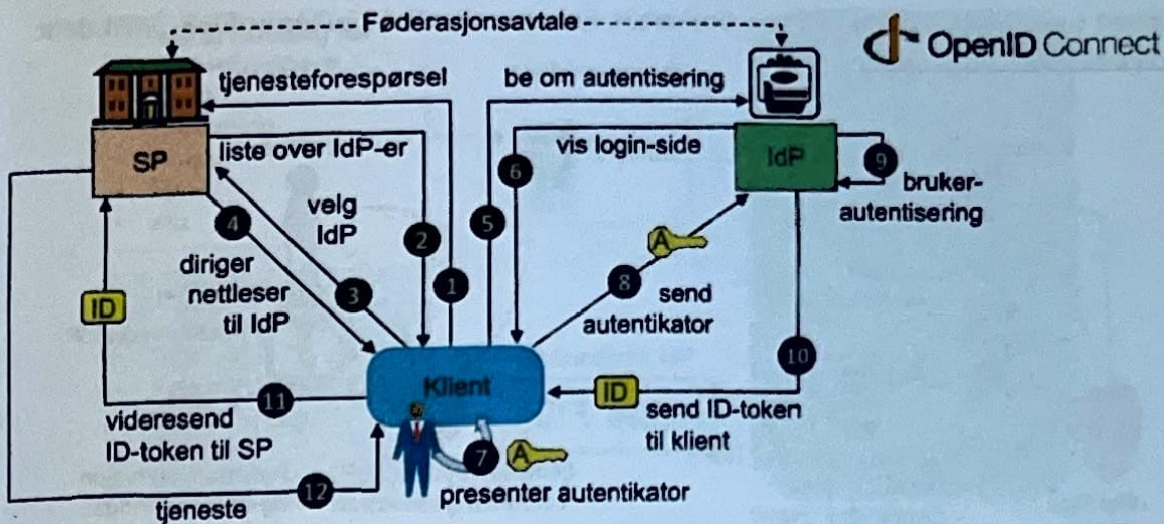
De ulike standardene for identitetsføderering spesifiserer forskjellige meldingsformater og metoder (profiler) for meldingsutveksling og anvendelse, noe som betyr at de ikke er kompatible. Alle entiteter i en føderasjon må altså ha installert applikasjonsmoduler basert på samme standard, ellers kan de ikke snakke sammen. Ulike standarder danner en teknisk hindring for å integrere forskjellige identitetsføderasjoner. Selv om to identitetsføderasjoner kanskje er basert på samme standard, spiller i tillegg mange politiske, juridiske og økonomiske føringer inn, noe som gjør at ulike identitetsføderasjoner som regel er atskilt. Tilgang til e-forvaltningstjenester gjennom ID-porten og tilgang til online-tjenester gjennom Facebook er for eksempel to separerte identitetsføderasjoner, selv om begge er bygd med OIDC. Vi kan ikke levere skattemeldingen ved å logge inn med Facebook, og vi kan ikke leie en leilighet på Airbnb ved å logge inn gjennom ID-porten.

9.2.5 OpenID Connect

OpenID Connect (OIDC) er en del av OAuth, som beskrives i avsnitt 9.4, eller mer presist: OpenID er en spesifikk metode («scope») ved bruk av OAuth til brukerautentisering. Identitetsføderasjoner basert på OIDC er f.eks. online sosiale nettverk som Facebook, Twitter og Google, der disse har rollen som IdP-er. OAuth bruker den generelle betegnelsen autentiseringstjener, som i tilfelle OIDC er en IdP (autentiseringstjener). Den statlige ID-porten er en annen føderasjon som benytter OIDC. Et sentralt element i OIDC-protokollen er sikkerhetstokenet *ID-token*, som er en kryptografisk melding og bekreftelse på at brukeren er autentisert. Meldingsutveksling i autentiseringsprotokollen OIDC er vist i figur 9.6.

Trinnene i scenarioet i figur 9.6 er beskrevet i figuren, og trenger derfor ikke en separat forklaring. OIDC spesifiserer forskjellige typer meldingsflyt (eng. message flows), der figur 9.6 viser såkalt *implisitt meldingsflyt*. Melding (5) i figur 9.6 inneholder «scope = OpenID», som gjør at IdP genererer et ID-token i melding (10).

Når vi sammenligner scenarioet for brukerautentisering basert på OpenID Connect i figur 9.6 med scenarioet for brukerautentisering basert på silomodellen i figur 9.3, ser vi at identitetsføderering medfører bemerkelsesverdig større kompleksitet. Imidlertid er denne kom-



Figur 9.6. Føderert autentisering med OpenID Connect.

pleksiteten transparent for oss brukere, og vi opplever bare økt brukervennlighet ved at vi lett får tilgang til mange ulike tjenester med bare én bruker-ID og autentikator.

I tillegg til brukerautentisering trengs naturligvis policyer og modeller for tilgangskontroll for «tilgang på tvers» mellom institusjoner, som for eksempel betyr å definere hva overlege *L* på sykehus *H* skal få tilgang til om pasient *P* på fastlegekontor *F*. Dette er et komplisert tema – ikke bare teknisk, men også juridisk og politisk. Tilgangskontroll beskrives i avsnitt 9.3 nedenfor.

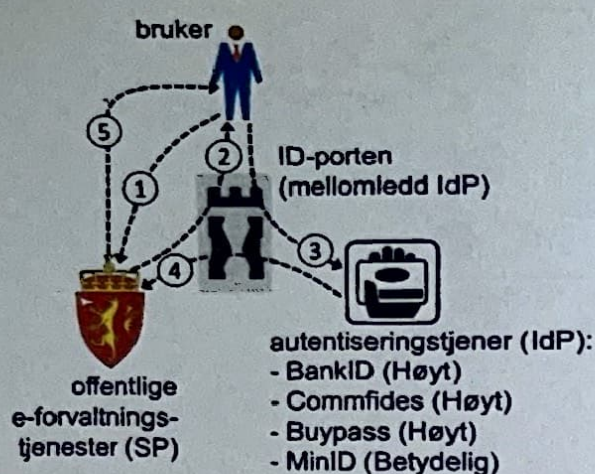
9.2.6 Identitetsføderasjonene ID-porten, Altinn og FEIDE

eID er en ordning for føderert autentisering til bruk i e-forvaltning.

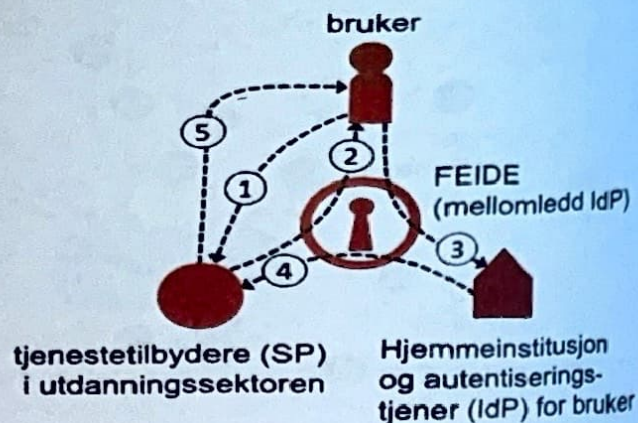
En IdP som benyttes i e-forvaltning, kalles en eID-leverandør. For eksempel er BankID den mest prominente eID-leverandøren i Norge, mens MinID, Buypass og Commfides brukes i mindre grad.

Identitetsføderasjoner som er basert på OIDC-protokollen, er for eksempel den statlige ID-porten for tilgang til offentlige e-forvaltningstjenester og FEIDE (Felles Elektronisk IDentitet) for tilgang til tjenester innen utdanningssektoren. Figur 9.7 viser forenklete scenarioer for ID-porten og FEIDE, som generelt er like, bare med forskjellige aktører som SP-er og IdP-er. Selv om ID-porten og FEIDE begge er basert på OIDC-protokollen, er de separate identitetsføderasjoner. For eksempel kan vi ikke logge inn med FEIDE for å levere skattemeldingen, ei heller logge inn gjennom ID-porten for å bestille en bok fra universitetsbibliotek. Grunnen til at disse føderasjonene lever separate liv, er at de er basert på ulike identifikatorer. Når vi logger på gjennom ID-porten, benytter vi vårt fødselsnummer, mens vi benytter vårt brukernavn på skole/universitet når vi logger på gjennom FEIDE. Hver skole

og hvert universitet lagrer vanligvis brukerens fødselsnummer i brukerprofilen, men dette brukes ikke for autentisering.



ID-porten: e-forvaltning for Innbyggere



FEIDE (Felles Elektronisk IDentitet) for utdanning

Figur 9.7. Separate OIDC-baserte føderasjoner: ID-porten og FEIDE.

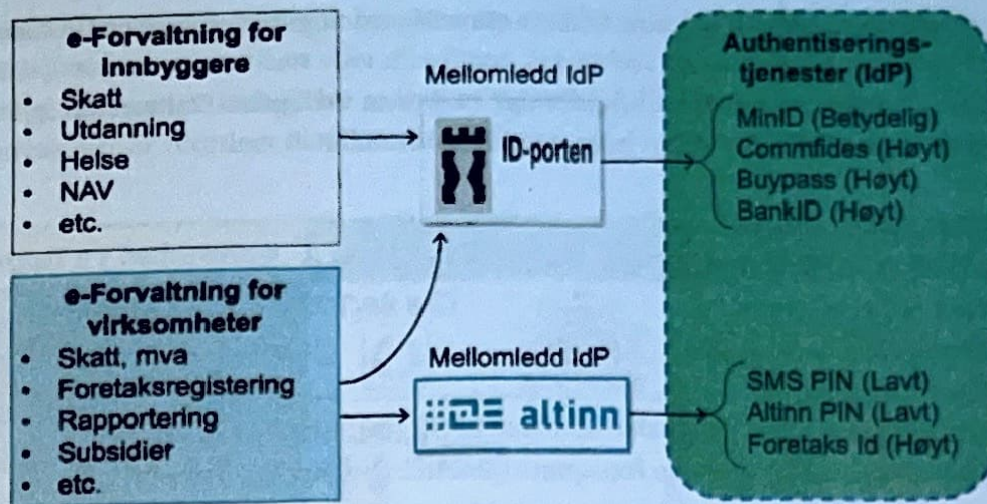
Meldingsutvekslingen i scenarioene i figur 9.7 er beskrevet nedenfor.

1. Bruker forespur tjeneste hos SP.
2. SP viser login-vindu med alternative IdP-er til bruker.
3. Bruker velger IdP, oppgir bruker-ID og autentikator(er) i påloggingsvinduet, som sendes til IdP.
4. IdP autentiserer bruker og sender ID-token og brukerattributter via portal/mellomledd til SP.
5. SP sjekker token og attributter, og yter den forespurte tjenesten i henhold til policy.

Autentiseringsnivåene for ID-porten i figur 9.7 er spesifisert etter *Veileder for identifikasjon og sporbarhet i elektronisk kommunikasjon med og i offentlig sektor*. Dette tilsvarer autentiseringsnivåene i den europeiske eIDAS-forordningen, som Norge har tilpasset seg.

ID-porten er en offentlig autentiseringsportal for både innbyggere og foretak i Norge. En annen offentlig autentiseringsportal er Altinn, som gir tilgang til e-forvaltningstjenester for virksomheter. I praksis kan virksomheter også benytte ID-porten, men gjennom Altinn kan foretak benytte spesielle virksomhetsidentifikatorer og autentiseringsmetoder som ikke er tilgjengelige for innbyggere. For virksomheter kan denne arkitekturen virke forvirrende, men de finner fort ut hvordan skatt og regnskap skal rapporteres. Figur 9.8 viser hvilke IdP-er (autentiseringstjenester) som gjelder for ID-porten, og hvilke som gjelder for Altinn. Figuren viser også at e-forvaltningstjenester for virksomheter og foretak også er tilgjengelig gjennom ID-porten.

Autentiseringsnivåene for IdP-er i både ID-porten og Altinn er vist i forhold til *Veileder for identifikasjon og sporbarhet i elektronisk kommunikasjon med og i offentlig sektor*, publisert av DigDir. Listen over IdP-er er ikke uttømmende, ettersom dette er kommersielle tjenester og nye IdP-er kommer på markedet og nye autentiseringsordninger tilbys. Innen



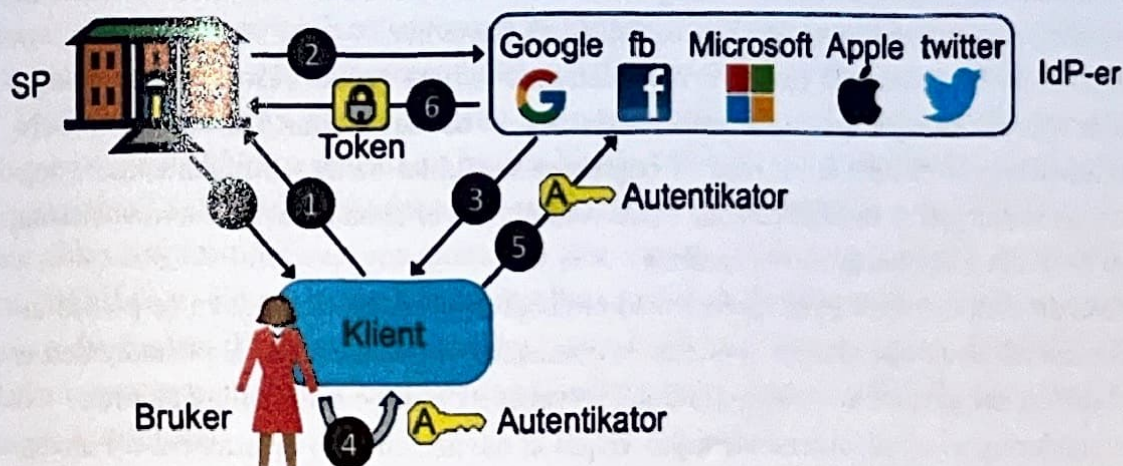
Figur 9.8. Sammenheng mellom ID-porten og Altinn, med IdP-er og autentiseringsnivåer (eIDAS).

helsesektoren er HelseID en IdP-portal tilsvarende ID-porten og Altinn. HelseID benytter noen av de samme bakenforliggende autentiseringstjenestene som vist i figur 9.8, og benytter i tillegg andre IdP-er.

For å bli en IdP må autentiseringsordningen akkrediteres. I Norge er Nkom (Norsk kommunikasjonsmyndighet) myndigheten som akkrediterer IdP-er for autentisering i henhold til autentiseringsnivåene spesifisert i DigDirs *Veileder for identifikasjon og sporbarhet*.

9.2.7 Identitetsføderasjonene Facebook, Twitter, Google etc.

Det er mange andre *identitetsføderasjoner* som er basert på OAuth og OpenID Connect-standard, for eksempel har Facebook, Twitter, Apple, Microsoft og Google etablert seg som IdP-er for tilgang til kommersielle tjenester på internett. Figur 9.9 viser et forenklet scenario for identitetsføderering som er vanlig for tilgang til tjenester på internett, der f.eks. Google, Facebook og Twitter er prominente IdP-er. Det er vanlig at en SP registrerer brukere med e-postadresse som bruker-ID, og lar brukere velge hvilken IdP de ønsker å bruke for autenti-



Figur 9.9. Forenklet scenario for identitetsføderasjoner basert på OpenID Connect.

sering. Det er naturligvis en forutsetning at den samme e-postadressen er bruker-ID både hos SP og IdP.

Meldingsutvekslingen i scenarioet i figur 9.9 er beskrevet nedenfor. Dette er en forenklet versjon av scenarioet i figur 9.6 ved at noen meldinger er utelatt.

1. Bruker forespør en tjeneste hos SP.
2. SP videresender nettleteren til IdP for autentisering.
3. IdP viser innloggingsvindu.
4. Bruker presenterer autentikator.
5. Autentikator sendes til IdP.
6. IdP verifiserer autentikator og sender ID-token til SP (egentlig via klient).
7. SP sjekker ID-tokenet og yter den forespurte tjenesten i henhold til policy.

Autentiseringsnivåene hos IdP-er på internett følger ikke retningslinjene til for eksempel DigDir's *Veileder for identifikasjon og sporbarhet*, eIDAS eller NISTs *SP 800-63-3 Digital Identity Guidelines*. De regnes heller ikke som eID-leverandører fordi de ikke brukes til autentisering i e-forvaltning. Disse IdP-ene tilbyr likevel 2-faktoraутentisering (2FA) gjennom sekundærkanaler som f.eks. med mobilapp eller autentiseringskode via SMS.

9.2.8 Kategorisering av identitetsføderering

Identitetsføderering er svært mangfoldig, slik det kommer frem i beskrivelsen av ulike standarder og arkitekturer i foregående avsnitt. Det kan derfor være utfordrende å gi en logisk kategorisering av identitetsføderinger. Nedenfor gjør vi likevel et forsøk på å gi en generell kategorisering.

Vi tar utgangspunkt i to aspekter:

1. Om navnerommet for bruker-ID forvaltes av en sentral aktør eller av mange aktører på en distribuert måte.
2. Om en føderasjon kun har én sentralisert IdP for hver bruker-ID, eller om IdP-rollen som utfører autentisering av en bruker-ID, er distribuert over flere aktører.

Vi har snakket mye om IdP-rollen i tidligere avsnitt, men lite om rollen som forvalter av navnerom og dets betydning, så en slik diskusjon kan passe her.

Et navnerom for bruker-ID definerer mengden med mulige bruker-ID-er. Det er viktig å være klar over hvilken juridisk og kommersiell status et navnerom har. Det norske fødselsnummeret definerer et navnerom med et begrenset sett ulike navn (fødselsnummer) som forvaltes av staten gjennom Skatteetaten. Fødselsnummeret er altså et sentralisert navnerom, nettopp fordi det forvaltes av en enkelt aktør.

E-postadressen definerer et navnerom med et ubegrenset antall ulike navn (e-postadresser) som forvaltes av alle aktører som eier et domenenavn på internett. E-postadressen er altså et distribuert navnerom, nettopp fordi det forvaltes av mange forskjellige aktører.

Ved etablering av en identitetsføderasjon velges et navnerom som er praktisk for anvendelsen. Noen ganger passer et sentralisert navnerom best, mens andre ganger passer et distribuert navnerom best. Det må også velges om det passer å ha sentralisert autentisering

eller om det er formålstjenlig å ha ulike og dermed distribuerte IdP-er for autentisering. Kombinasjonen av sentralisert eller distribuert navnerom, og sentralisert eller distribuert autentisering, danner fire kategorier som vist i figur 9.10, der eksempler på prominente identitetsføderasjoner er tilordnet de ulike kategoriene.

Kategori av føderering	Sentralisert navnerom	Distribuert navnerom
Sentralisert autentisering	Tysk eID  AADHAAR 	FEIDE  eduroam 
Distribuert autentisering	ID-porten  altinn  HelseID 	Google  Microsoft  twitter  fb  Apple  Europeisk eID 

Figur 9.10. Kategorier av identitetsføderering, med eksempler.

Nedenfor gis en forklaring på hvorfor hver identitetsføderasjon vist i figur 9.10 nettopp er tilordnet en spesifikk kategori.

Det tyske nasjonale ID-kortet fungerer også som eID for tilgang til e-forvaltning og en rekke private tjenester. ID-kortet kobles til smarttelefonen ved å holde kortet mot telefonen slik at de kan kommunisere via NFC (Near Field Communication). Autentiseringsprotokollen ligner på FIDO2 beskrevet i avsnitt 8.4.2. eID i Tyskland har en identifikator (ID-kortnummer) bestående av 9 tegn (bokstaver og tall) i et sentralisert navnerom, og har *Bundesportal.de* som sentralisert statlig IdP (eID-leverandør).

Aadhaar (fra hindu: «grunnlag») er et tolvstifret unikt identitetsnummer for innbyggere i India, som lagres i en profil sammen med personens biometriske og demografiske data. Dataene samles inn av UIDAI (Unique Identification Authority of India), en lovpålagt myndighet opprettet i januar 2009 av regjeringen i India. Aadhaar er verdens største biometriske ID-system, med over en milliard registrerte personer i en sentralisert database. Aadhaar tilsvarer folkeregisteret i Norge, altså med et sentralisert navnerom av identiteter. Samtidig er UIDAI en sentralisert IdP som utfører autentisering av brukere for tilgang til alle e-forvaltningstjenester i India.

FEIDE og Eduroam har distribuerte navnerom med bruker-ID definert av hver utdanningsinstitusjon. I Norge registreres bruker-ID for studenter, elever og ansatte i norske utdanningsinstitusjoner. I Eduroam defineres en bruker-ID på samme måte som i FEIDE, dvs. av hver utdanningsinstitusjon, men globalt og ikke bare nasjonalt. Autentisering er sentralisert i både FEIDE og Eduroam fordi en bruker bare kan bli autentisert av den utdanningsinstitusjonen der bruker-ID-en er registrert. Det kunne imidlertid være mulig at utdanningsinstitusjoner outsourcer autentiseringstjenesten til ulike aktører, som dermed ville gjøre autentiseringen distribuert.

ID-porten, Altinn og HelseID er autentiseringsportaler som benytter bakenforliggende IdP-er for selve brukerautentiseringen, for eksempel BankID, Buypass og Commfides. Fød-

selsnummer er navnerom for ID-porten og HelseID, mens foretaksnummer er navnerom for Altinn. Fødselsnummer forvaltes av Skatteetaten, mens foretaksnummer forvaltes av Brønnøysundregistrene, som begge er sentraliserte navnerom. Samtidig kan personer og foretak benytte ulike IdP-er for autentisering mot ID-porten, Altinn og HelseID, som dermed betyr at disse har distribuert autentisering.

Imidlertid er det et problem, blant annet for personvern, at ansatte i private og offentlige virksomheter ofte må benytte personlig fødselsnummer for brukerautentisering i jobbsammenheng. Innenfor NHN (Norsk helsenett) fins for eksempel helsepersonellnummeret, som er et sentralisert navnerom som er forvaltet av NHN. Et helsepersonellnummer er ikke et fødselsnummer, selv om fødselsnummeret ligger som et attributt i brukerprofilen. Helsepersonellnummer kunne i teorien bli brukt som identifikator ved brukerautentisering hos helseinstitusjoner. På den måten kunne helsepersonell autentisere seg innenfor NHN i henhold til sin jobbrolle og få tilgang til data og ressurser fra ulike helseinstitusjoner. Å kunne skille mellom rollen som privatperson (med fødselsnummer) og helsepersonell (med helsepersonellnummer) ville være nyttig, ikke bare for personvern, men for å skille mellom ulike ansvarsroller. En grunn til at helsepersonellnummer ikke benyttes for brukerautentisering i helsesektoren er blant annet at de typiske IdP-ene for eID i Norge, som er BankID, Buypass og Commfides, ikke er forberedt på å kunne konsumere helsepersonellnummer med separate autentikatorer. For å få til noe slikt trengs nye løsninger og prosesser med en tilhørende forretningsmodell for å dekke de ekstra kostnadene.

Identitetsføderasjonen av sosiale nettverk, der nettstedet som Google, Facebook eller Twitter spiller rollen som IdP-er, kan kategoriseres som å ha et distribuert navnerom fordi en SP lar brukere registrere seg med alle slags e-postadresser og telefonnummer fra forskjellige domener og land. Brukere som benytter en vilkårlig e-postadresse eller telefonnummer for tilgang til internett-tjenester, kan velge ulike IdP-er som dermed er distribuerte. For eksempel kan en bruker få tilgang til tjenester fra en SP ved å autentisere gjennom IdP-ene Google, Facebook, Twitter eller andre tilsvarende nettsteder som tilbyr å ta rollen som IdP.

EU-kommisjonen planlegger innføring av europeisk eID, som kan bli en realitet rundt midten av 2020-tallet. Vi kan anta at en slik identitet blir basert på et distribuert navnerom av bruker-ID-er, der ulike land forvalter hver sin undermengde av navnerommet. Vi kan også anta at ulike autentiseringstjenester vil kunne foreta brukerautentisering innenfor hvert lands navnerom. Teknisk sett vil hver slik autentiseringstjeneste være en IdP, selv om identitetene forvaltes av hvert lands myndigheter. Hvis disse antagelsene er riktige, vil denne identitetsføderasjonen ha likhetstrekk med identitetsføderasjonen av sosiale nettverk i figur 9.10. Et mulig fremtidig scenario i en slik identitetsføderasjon er en EU/EØS-innbygger som benytter en e-forvaltningstjeneste utenfor sitt eget land. Ved innlogging vil brukeren først velge hvilket land bruker-ID-en hører til, og deretter velge autentiseringstjeneste. En norsk innbygger vil velge bruker-ID fra Norge, som typisk vil være fødselsnummeret. Deretter velger den norske brukeren en av autentiseringstjenestene vist i figur 9.8. I et slikt scenario vil det være mulig at samme person kan ha flere bruker-ID-er fra ulike land, og kanskje til og med flere bruker-ID-er i samme land. Fra et perspektiv om å forhindre trygdesvindler og andre former for kriminalitet vil det være ønskelig å knytte sammen ulike bruker-ID-er for samme person. Fra et personvernperspektiv vil det være ønskelig å ikke knytte sammen en persons ulike bruker-ID-er. Dermed blir det en politisk debatt om ulike eID-er for en person skal knyttes sammen.

9.3 Tilgangskontroll

At en bruker er korrekt autentisert innenfor et datanett eller av en tjenestetilbyder, betyr ikke at brukeren dermed har tilgang til alle ressurser som forvaltes innenfor datanettet eller av tjenestetilbyderen. Tilgangskontroll er sikkerhetsfunksjonen som sørger for at brukere bare får tilgang til ressurser de på forhånd er blitt autorisert til. I avsnittene nedenfor beskrives metoder og modeller for å kontrollere tilgang til ressurser.

I terminologien for tilgangskontroll representerer *subjekt* en entitet som forespør tilgang, og *objekt* ressursen som subjektet ønsker tilgang til. En tilgangsforespørsel betyr for eksempel at subjektet forsøker å åpne en fil for å lese/redigere, åpne en filkatalog for å se hva som ligger der, eller å starte/utføre en applikasjon. Subjektet er typisk en bruker, men kan også være et system eller en prosess. Det er ofte relevant at en forespørsel om tilgang til en ressurse også spesifiserer *tilgangsmodus*, som f.eks. lese, skrive eller utføre, men dette er ofte implisitt. Det er antatt at tilgangsautorisering allerede er spesifisert i konfigureringsfasen, som vist i figur 9.1 og figur 1.9, det vil si at det er spesifisert attributter for tilgang i profilene for subjekt og/eller objekt. Når subjektet gjør en tilgangsforespørsel, vil tilgangskontrollfunksjonen i figur 9.1 sjekke relevante tilgangsattributter og ta en beslutning om tilgang skal tillates eller avvises.

Modeller for tilgangskontroll kalles tradisjonelt «sikkerhetsmodeller», som stammer fra 1970-tallet, da nettopp tilgangskontroll var den viktigste sikkerhetsfunksjonen. Klassiske modeller er DAC (Discretionary Access Control), MAC (Mandatory Access Control) og RBAC (Role-Based Access Control), som alle fremdeles er utbredt. Imidlertid skalerer disse modellene relativt dårlig til moderne forretningsprosesser med identitetsfødering, «tilgang på tvers» og utstrakt samhandling mellom ulike organisasjoner. En mer moderne og fleksibel modell for tilgangskontroll er derfor ABAC (Attribute-Based Access Control), som egentlig er en generalisering av alle de tidligere nevnte modellene. I tillegg kommer distribuert tilgangsstyring. Alle disse modellene beskrives i avsnittene nedenfor.

9.3.1 DAC: Navnebasert tilgangskontroll

DAC (Discretionary Access Control) er en modell for tilgangskontroll basert på subjektnavn og objektnavn. Det betyr generelt at regler for tilgang uttrykkes på formen «*subjekt X har tilgang til objekt Y med tilgangstype Z*». Dette er tilgangsautorisasjoner som kan kalles policy eller regler. Figur 9.11 viser et enkelt eksempel med en ACL (Access Control List) som spesifiserer tilgangsautorisasjoner for brukere. Et viktig spørsmål er om regelen skal lagres som en del av subjektprofilen, som en del av objektprofilen eller separat. Reglene kan for eksempel lagres som en del av objektprofilen, det vil si som metadata for en fil eller domene. Reglene kan også lagres i subjektprofilen for brukere, f.eks. ved å spesifisere hvilke domener en bruker tilhører og skal ha tilgang til.

	Objekt-navn	
	HR	Sag
Subjekt-navn	Ola Glomstulen	lese, skrive
	Kari Hakadalen	lese, skrive

Figur 9.11. Navnebasert tilgangskontroll.

I Windows og Linux er DAC implementert som ACL (Access Control List), eller «tilgangskontrollliste» på norsk. Hvert objekt har en ACL som spesifiserer hvilke subjekter som er autorisert for tilgang og med hvilken tilgangsmodus. Det er imidlertid ikke mulig å spesifisere individuelle subjekter, kun tre kategorier: *eier*, *gruppe* og *andre*. Med denne granulariteten kan eier spesifisere tilgangsrettigheter for seg selv, for en gruppe subjekter og for alle subjekter. Individuelle subjekter kan legges inn i gruppen. For hvert objekt kan det spesifiseres tilgangsrettigheter for hver kategori med en eller flere av tilgangsmodusene *lese* (read), *skrive* (write) og *utføre* (execute). På lignende måte kan det spesifiseres tilgangsrettigheter til filkataloger.

Den engelske betegnelsen DAC reflekterer at eieren av filen kan spesifisere etter eget ønske hvem som skal ha tilgang til filen, derav ordet «discretionary», som her betyr «etter eierens ønske». DAC-betegnelsen stammer fra 1980-tallet, da DAC-tilgangsmodeller først ble implementert i systemer. Alle operativsystemer støtter DAC, som er den mest utbredte modellen for tilgangskontroll både i sivil og militær sektor.

9.3.2 MAC: Merkebasert tilgangskontroll

MAC (Mandatory Access Control) er en modell for tilgangskontroll basert på merker/label på subjekter (brukere), og merker/label på objekter (data og tjenester). Sikkerhetsklarering for en bruker uttrykkes med subjektmerke, og sikkerhetsgradering av informasjon uttrykkes med objektmerke. Sikkerhetsloven beskriver fire graderinger, som i synkende rekkefølge er følgende:

STRENGT HEMMELIG

HEMMELIG

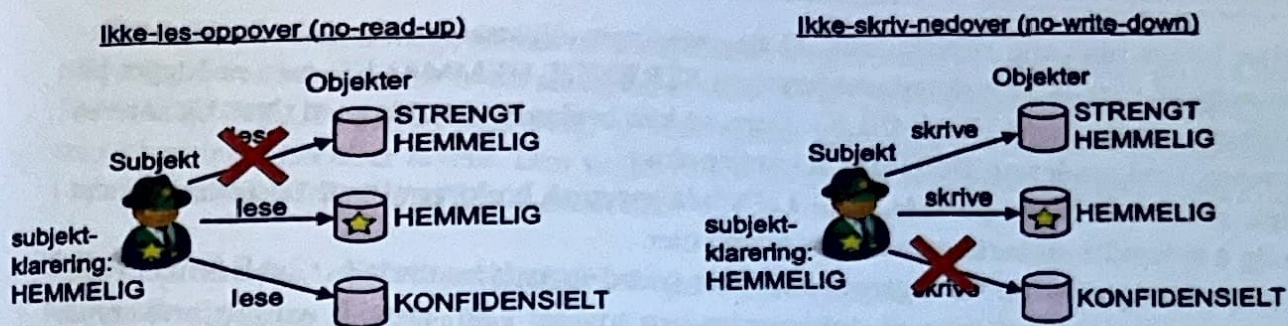
KONFIDENSIELT

BEGRENSET

Dokumenter som ikke er graderte, kalles UGRADERT, som strengt tatt ikke er en gradering, men som ofte påføres dokumenter i miljøer hvor det ellers håndteres en høy andel graderte dokumenter for å markere et tydelig skille mellom gradert og ikke-gradert informasjon. Det fins mange ulike graderingsskalaer som er spesifisert i andre lovverk eller av andre land.

Tilgangskontroll basert på MAC betyr generelt at tilgangskontrollfunksjonen sammenligner subjektmerket med objektmerket for å ta beslutning om tilgang. Den engelske betegnelsen MAC reflekterer at tilgangsregelen er obligatorisk (mandatory), på den måten at eieren av filen ikke kan spesifisere etter eget ønske hvem som skal ha tilgang til filen – det er nemlig merkene som dikterer hvem som har tilgang. MAC-betegnelsen stammer fra 1980-tallet, da MAC-tilgangsmodeller først ble implementert i systemer.

Den mest vanlige modellen, eller sett med regler, for sammenligning av subjekt- og objektmerker kalles *Bell-LaPadula* etter forfatterne David Elliott Bell og Leonard J. LaPadula, som først beskrev denne modellen. Bell-LaPadula beskriver relativt mange ulike regler, men de to viktigste kalles «ikke-les-oppover» (no-read-up) og «ikke-skriv-nedover» (no-write-down), som illustrert i figur 9.12. Begge reglene er illustrert med et subjekt som har sikkerhetsklarering HEMMELIG og et sett objekter med ulike graderinger.



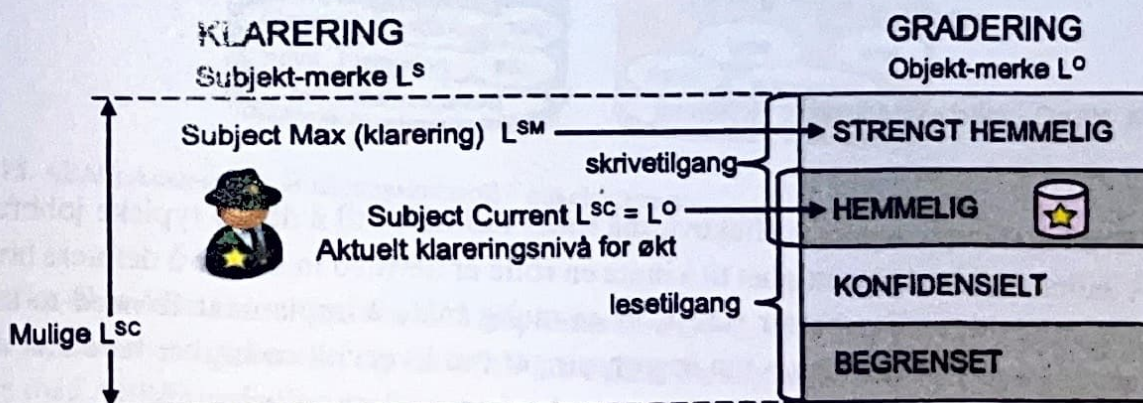
Figur 9.12. MAC-tilgangsregler fra Bell-LaPadula-modellen.

Regelen «ikke-les-oppover», illustrert til venstre i figur 9.12, er intuitivt lett å forstå. Hvis en person er klarert for HEMMELIG, kan personen lese dokumenter med samme eller lavere gradering, men ikke dokumenter med høyere gradering. Denne regelen hindrer lekkasje av høyt gradert informasjon til personell med lavere sikkerhetsklarering.

Regelen «ikke-skriv-nedover» er ikke like intuitiv og trenger en forklaring. Logikken er at en person med høy sikkerhetsklarering kanskje har høyt gradert informasjon i hodet. Hvis denne personen kunne skrive informasjonen fra hodet til dokumenter med lav sikkerhetsgradering, som personell med lav sikkerhetsgradering kan lese, ville det forårsake lekkasje av høyt gradert informasjon til personell med lav sikkerhetsklarering.

I praksis er det ikke hvilken informasjon en bruker har i hodet, som er relevant for «ikke-skriv-nedover», men hvilke andre dokumenter som brukeren har åpnet samtidig i en aktiv pålogget økt. «Ikke-skriv-nedover» skal forhindre at brukeren kopierer informasjon fra et høyt gradert dokument til et lavt gradert dokument under økten.

Hvis en bruker ønsker å både lese og skrive samtidig på ulike dokumenter, er det klart at alle dokumentene og brukeren må ha samme sikkerhetsgradering/klarering. Det må imidlertid ikke være slik at en bruker med høyeste sikkerhetsklarering dermed bare kan arbeide med (lese og skrive) dokumenter med høyeste sikkerhetsgradering – brukeren må kunne arbeide med alle dokumenter gradert på samme nivå eller lavere nivå enn sikkerhetsklareringen. Dette gjøres ved at det defineres en subjekt-max-label som er lik sikkerhetsklareringen, og en subjekt-current-label som brukeren velger ved pålogging, der subjekt-current kan ha samme



Figur 9.13. Praktisk bruk av Bell-LaPadula ved at bruker velger subjekt-current-label for en økt.

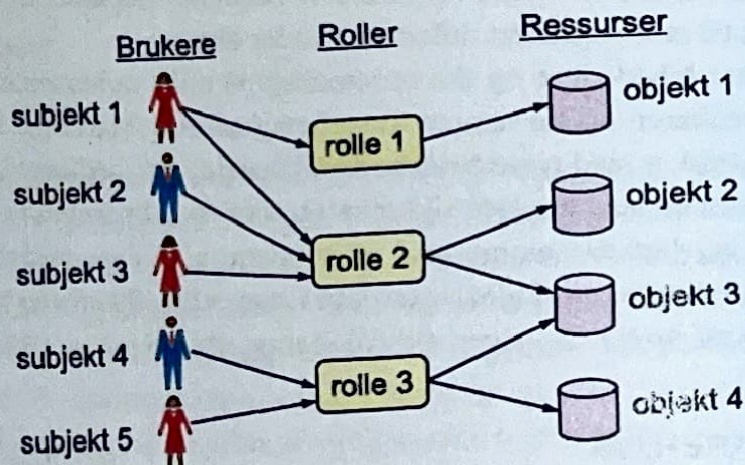
nivå eller lavere nivå enn subjekt-max. Dette prinsippet illustreres i figur 9.13, der brukeren har subjekt-max-label (sikkerhetsklarering) STRENGT HEMMELIG, men er logget på med subjekt-current-label HEMMELIG. Dermed kan brukeren arbeide med (lese og skrive) dokumenter med gradering HEMMELIG under økten.

Tilgangskontroll basert på MAC/Bell-LaPadula er typisk brukt i militære systemer der det er vanlig å behandle sikkerhetsgraderte dokumenter.

Et annet viktig prinsipp for tilgangskontroll er «need-to-know», det vil si at en bruker bare skal være autorisert for tilgang til dokumenter hen trenger i sitt arbeid, uansett brukerens sikkerhetsklarering. DAC kan brukes for å implementere need-to-know, som i praksis betyr at ansatte blir autorisert for tilgang til forskjellige domener av data og tjenester i virksomheten. På den måten blir MAC som regel kombinert med need-to-know basert på DAC. Neste avsnitt beskriver RBAC, som er et annet prinsipp som også benyttes sammen med MAC og DAC.

9.3.3 RBAC: Rollebasert tilgangskontroll

Vedlikehold av tilgangsrettigheter krever mye arbeid i organisasjoner. Etter som medarbeidere endrer jobbfunksjon, må gamle tilgangsrettigheter fjernes og nye legges til. En interessant tilnærming er at tilgangsrettigheter defineres for roller og ikke for enkeltbrukere. I stedet spesifiseres det mulige roller som brukere kan ta ved pålogging, og som gjør at brukeren under den økten automatisk får alle tilgangsrettigheter som er definert for rollen. Denne modellen for tilgangskontroll kalles *RBAC (Role-Based Access Control)*, som er rollebasert tilgangskontroll på norsk. Figur 9.14 illustrerer et enkelt eksempel med tilgangsrettigheter basert på RBAC.



Figur 9.14. RBAC – rollebasert tilgangskontroll.

For at RBAC skal implementeres effektivt, må roller defineres til å dekke typiske jobbfunksjoner. Å definere en brukers rettighet til å innta en rolle er dermed indirekte å definere brukerens tilgangsrettigheter til ressurser. RBAC er en mulig måte å implementere need-to-know på i organisasjoner. Det kan legges inn begrensninger om hvorvidt en bruker bare kan innta en enkelt rolle i en økt, eller om det skal være mulig å innta flere roller samtidig.

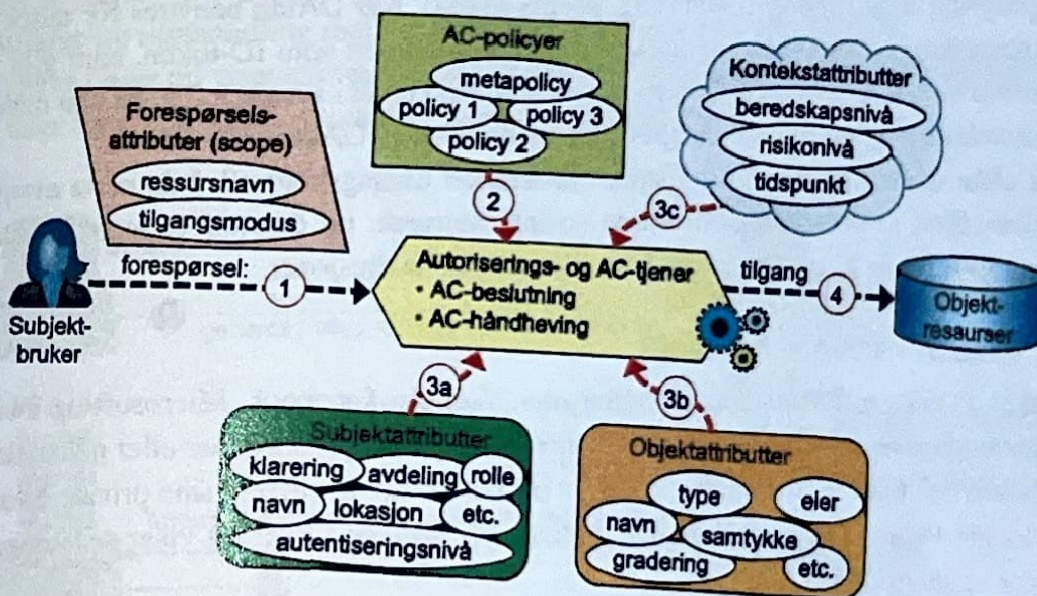
RBAC har sine fordeler, men i praksis viser det seg ofte at det er nødvendig å definere veldig mange roller, og at det krever betydelig arbeid å vedlikeholde tilgangsrettigheter for roller.

Det er interessant å legge merke til at MAC kan implementeres med RBAC på den måten at det defineres en rolle for hvert sikkerhetsnivå av STRENGT HEMMELIG, HEMMELIG, KONFIDENSIELT og BEGRENSET, og at en bruker kan velge en rolle som tilsvarer brukers klareringsnivå eller lavere. Den valgte rollen for en økt er dermed subjekt-current-label i henhold til MAC/Bell-LaPadula-modellen.

9.3.4 ABAC: Attributtbasert tilgangskontroll

Mange forskjellige aspekter kan være relevante for å spesifisere tilgangsrettigheter. DAC, MAC og RBAC beskrevet ovenfor fokuserer for eksempel på navn, labeler eller roller. I tillegg kan det være relevant å ta med kontekst som geografisk lokasjon, tid på døgnet, hverdag/helg, beredskapsnivå og driftsstatus. Ved å betrakte alle disse tingene som attributter kan det defineres regler for tilgangskontroll som nettopp kan ta hensyn til alle slags attributter, som dermed blir til ABAC (Attribute-Based Access Control).

Med ABAC kan organisasjoner spesifisere tilgangsautorisering basert på alle slags attributter relatert til subjekt, objekt, tilgangsmodus, kontekst og selve policyen (reglene) som gjelder for en forespørsel om tilgang. Hovedkategorier av attributter er dermed forespørselsattributter, subjektattributter, objektattributter, kontekstattributter og AC-policyer (Access Control Policies). AC-policyene kan betraktes som reglene for å tolke de andre attributtene for å ta en beslutning om tilgang. Systemer kan automatisk foreta og håndheve tilgangsbetring basert på disse attributtene. Figur 9.15 illustrerer et enkelt ABAC-eksempel der tilgang er basert på attributtene nevnt ovenfor.



Figur 9.15. ABAC: Attributtbasert tilgangskontroll – enkelt scenario.

Legg merke til at ABAC kan brukes til å implementere DAC, MAC og RBAC, noe som betyr at ABAC er den mest generelle og fleksible modellen for tilgangskontroll. DAC kan implementeres med ABAC ved at både subjekt- og objektattributt kan være navn, og AC-policyen rett og slett er en ACL (Access Control List). MAC kan implementeres med ABAC ved at subjekt- og objektattributter kan være labeler med klarering og gradering, og policyen rett

og slett er Bell-LaPadula. RBAC kan implementeres ved at et sett med roller defineres som proxyer bestående av både et rolleobjekt som brukersubjekter har tilgang til, og et rollesubjekt som har tilgang til objektressurser, slik at subjektbrukeres tilgang til objektressurser går indirekte via rolleproxyen.

Implementering av løsninger basert på ABAC har økt raskt i utbredelse etter 2010. Sammen danner ABAC og føderert identitetshåndtering grunnlaget for fleksible og skalerbare løsninger for tilgangshåndtering og samhandling i distribuerte omgivelser.

I en distribuert infrastruktur kan det være nødvendig å innhente attributter fra forskjellige organisasjoner. Et typisk eksempel er NHN (Norsk helsenett), der helsepersonell kan gjøre forespørsler om tilgang til pasientdata fra andre institusjoner enn der de selv jobber. Først må brukeren autentiseres gjennom identitetsføderasjonen HelseID og deretter gjøre en forespørsel om tilgang. Deretter må en autorisasjonstjener hente inn relevante attributter og policyer for å ta en beslutning om å gi eller avvise tilgang til ressursen. En mulig arkitektur for tilgangskontroll i en distribuert omgivelse er typisk basert på OAuth, som beskrives i neste avsnitt.

9.4 OAuth og distribuert tilgangsstyring

OAuth er en åpen standard som beskriver hvordan nettsteder eller applikasjoner kan få tilgang til og utveksle ressurser seg imellom ved at ressurseier gir samtykke om det og delegerer tilgangsrettigheter på en sikker måte. Første versjon av OAuth-protokollen ble publisert i 2010 gjennom IETF (Internet Engineering Task Force).

I OAuth kan sikkerhetstokenet representere forskjellige ting (ha forskjellig «scope»), som for tilgangsstyring er et tilgangstoken (eng. access token). Når OAuth benyttes for autentisering, er betydningen («scopet») av sikkerhetstokenet definert som ID-token, som gjør at protokollen blir til OIDC (OpenID Connect), slik som beskrevet i avsnitt 9.2.5. På den måten er OIDC-protokollen egentlig bare en spesifikk anvendelse av OAuth-protokollen.

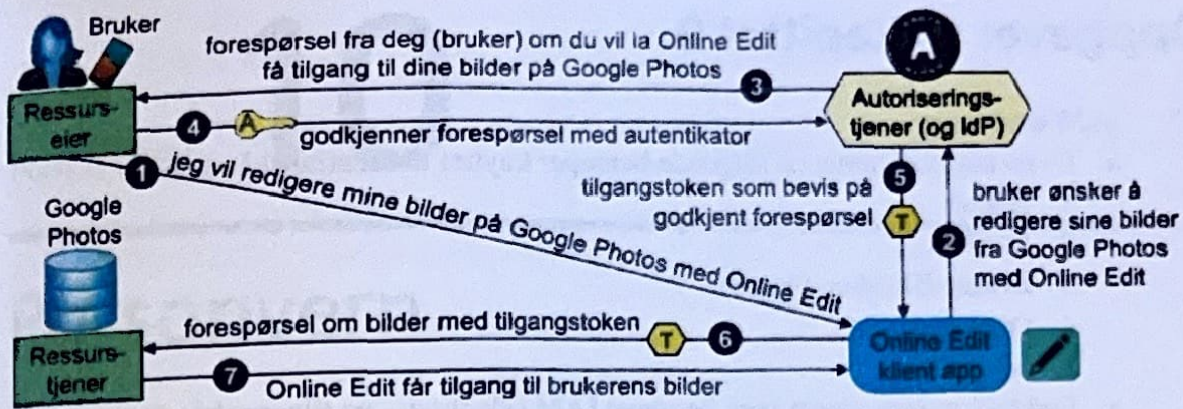
Det fins ulike scenarier der OAuth støtter distribuert tilgangskontroll. I de neste avsnittene beskrives først et scenario med online sosiale nettverk, og deretter et scenario med samhandling for tilgang til pasientjournaler mellom helseinstitusjoner.

9.4.1 OAuth i sosiale nettverk

OAuth brukes av alle store nettsteder, som Amazon, Google, Facebook, Microsoft og Twitter, for å dele brukernes ressurser/informasjon med tredjeparts-applikasjoner eller nettsteder. Som eksempel viser figur 9.16 et scenario der en bruker ønsker å redigere sine private bilder lagret på Google Photos med en tredjeparts online app. Tallene i hver pil viser sekvensen, slik at figuren er selvforklarende.

Motivasjonen bak utviklingen av OAuth var nettopp scenarier som vist i figur 9.16, fordi det er fleksibel protokoll som danner grunnlaget for betydningsfulle forretningsprosesser og forretningsmodeller på internett.

Samtidig kan OAuth være svært invaderende med hensyn til våre persondata. Selv om vi teknisk sett gir samtykke gjennom OAuth til at tjenestetilbydere på internett kan utveksle data om oss, klarer de fleste av oss ikke å fatte utstrekningen av hva vi gir samtykke til, og at det antagelig benyttes i handel med persondata.



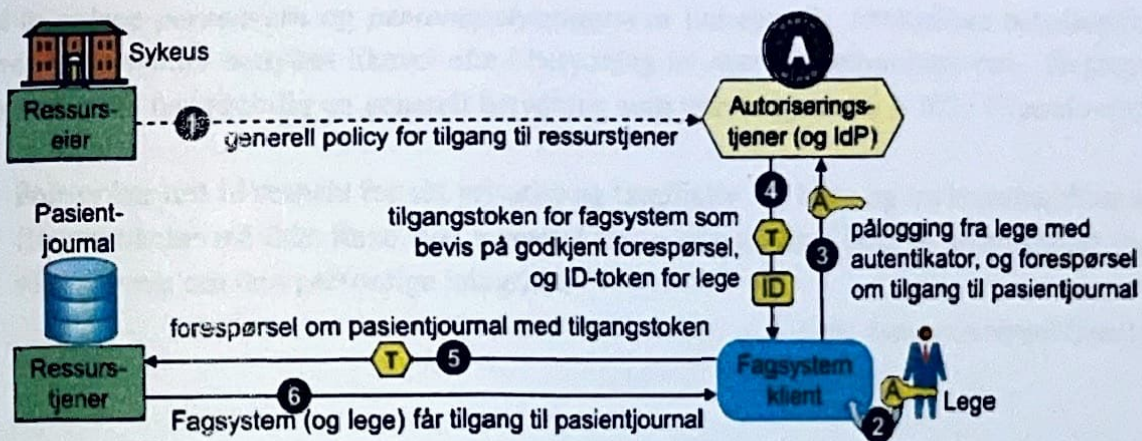
Figur 9.16. OAuth brukt for å dele informasjon mellom online nettsteder.

9.4.2 OAuth for tilgang og samhandling mellom helseinstitusjoner

OAuth har anvendelse innenfor alle slags sektorer, ikke bare kommersielle internett-tjenester. En utfordring for behandling av pasienter er for eksempel at pasientdata om samme person kan være lagret hos forskjellige helseinstitusjoner, f.eks. fastleger, sykehus eller patologilaboratorier. Utveksling av pasientdata er underlagt streng kontroll, og krever ofte samtykke. OAuth og OIDC kan nettopp benyttes for å effektivisere utveksling av pasientdata på en sikker måte.

Figur 9.17 viser en mulig måte OAuth kan brukes i Norsk helsenett (NHN) for samhandling og «tilgang på tvers» mellom helseforetak i Norge. NHN er et norsk statsforetak etablert og eid av Helse- og omsorgsdepartementet med oppdrag å utvikle og drifte nasjonal IKT-infrastruktur for samhandling mellom aktørene i helse- og omsorgssektoren.

Tallene i hver pil viser sekvensen, slik at figuren er selvforklarende. Autoriseringstjeneren kan være basert på ABAC-modellen beskrevet i avsnitt 9.3.4.



Figur 9.17. OAuth for distribuert tilgangskontroll og samhandling i helsesektoren.

En variant av scenarioet i figur 9.17 er hvis ressurseier ønsker en en finkornet styring av tilgang for brukere ved hver tilgangsforespørsel, i stedet for tilgangsstyring basert på en generell policy for alle brukere som sendes i melding 1. Da vil autoriseringstjeneren og ressurseier utveksle meldinger tilsvarende melding 3 og 4 i figur 9.16.

Oppgaver til kapittel 9

9.1 IAM-begreper

- a. Gi en kort forklaring på følgende begreper knyttet til identitetshåndtering:
 1. Entitet
 2. Identitet
 3. Bruker-ID (identifikator)
 4. Digital identitet
 5. Autentikator
- b. Forklar hva som menes med begrepet IAM (identitets- og tilgangshåndtering).

9.2 Silomodell og føderert modell

- a. Beskriv silomodellen for identitetshåndtering.
- b. Beskriv fordeler og ulemper ved silomodellen.
- c. Beskriv generelt den fødererte modellen for identitetshåndtering.
- d. Beskriv fordeler og ulemper ved den fødererte modellen.

9.3 ABAC: Attributtbasert tilgangskontroll

Attributtbasert tilgangskontroll, eller ABAC (Attribute-Based Access Control), er en fleksibel modell for tilgangskontroll.

- a. Nevn fem kilder for attributter i ABAC.
- b. Forklar hvordan DAC kan implementeres med ABAC.
- c. Forklar hvordan MAC kan implementeres med ABAC.
- d. Forklar hvordan RBAC kan implementeres med ABAC.

Personvern

I dette kapitlet lærer du først forskjellen mellom personvern og personopplysningsvern, og behovet for å finne en balanse mellom overvåking og skjerming. Deretter får du innblikk i industrien bak sporing på internett, med noen råd om hvordan man kan beskytte seg. Videre lærer du om hvordan personopplysninger beskyttes gjennom den europeiske GDPR-forordningen (General Data Protection Regulation). Til slutt lærer du å vurdere om det er nødvendig å gjennomføre en DPIA (Data Protection Impact Assessment), og selve gjennomføringen av DPIA, som er noe virksomheter må vurdere og eventuelt gjennomføre for å behandle personopplysninger på lovlig vis i henhold til GDPR.

10.1 Hva er forskjellen mellom personvern og personopplysningsvern?

De to ordene *personvern* og *personopplysningsvern* har egentlig forskjellige betydninger, men «personvern» benyttes likevel ofte i betydning av «personopplysningsvern». Begrepet «personvern» har egentlig en generell betydning som uttrykt gjennom § 102 i Grunnloven:

Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon. Husransakelse må ikke finne sted, unntatt i kriminelle tilfeller. Statens myndigheter skal sikre et vern om den personlige integritet.

§ 102. Kongeriket Norges Grunnlov

Grunnlovens § 102 er faktisk basert på FNs verdenserklæring om menneskerettigheter og Den europeiske menneskerettighetskonvensjonen:

Ingen må utsettes for vilkårlig innblanding i privatliv, familie, hjem og korrespondanse, eller for angrep på ære og anseelse. Enhver har rett til lovens beskyttelse mot slik innblanding eller slike angrep.

FNs verdenserklæring, artikkel 12

Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse.

Artikkel 8-1 i Den europeiske menneskerettskonvensjonen

Lekk merke til at Grunnlovens § 102 nevner «(...) respekt for (...) kommunikasjon», som typisk er personlig, slik at det nettopp betyr å ha respekt for *personopplysninger*.

Personopplysningsvern er dermed en spesiell type personvern som dreier seg om kommunikasjon og behandling av personopplysninger. Begrepet er dermed vinklet mot det å ha respekt for persondata, som er svært viktig for vår personlige integritet. Personopplysningsvern dekker aspekter som muligheten til selv å vite og kontrollere når, hvordan og hvor mye informasjon om egen person som spres til andre parter.

Norge har en lov som kalles *lov om behandling av personopplysninger* (*personopplysningsloven*), som trådte i kraft i 2018. Ettersom kortversjonen av tittelen nettopp er personopplysningsloven, er det naturlig at begrepet «personopplysningsvern» er begrepet som denne loven dekker. Formelt sett stemmer det, men i de fleste sammenhenger benyttes «personvern» som begrep for det som dekkes av personopplysningsloven. Denne unøyaktigheten i begrepsbruk er svært innarbeidet i det norske språket, og er nok vanskelig å vende. Hvis vi tar i betraktning at «opplysning» har tre stavelser som er tungt å måtte uttale mange ganger, forstår vi at folk ofte foretrekker å si «personvern» i stedet for «personopplysningsvern». På den måten er «personvern» i praksis blitt ekvivalent med «personopplysningsvern». Vi velger å følge denne praksisen, slik at vi i resten av denne boken bruker begrepet «personvern» i betydningen «personopplysningsvern».

10.2 Personvern i den digitale tidsalderen

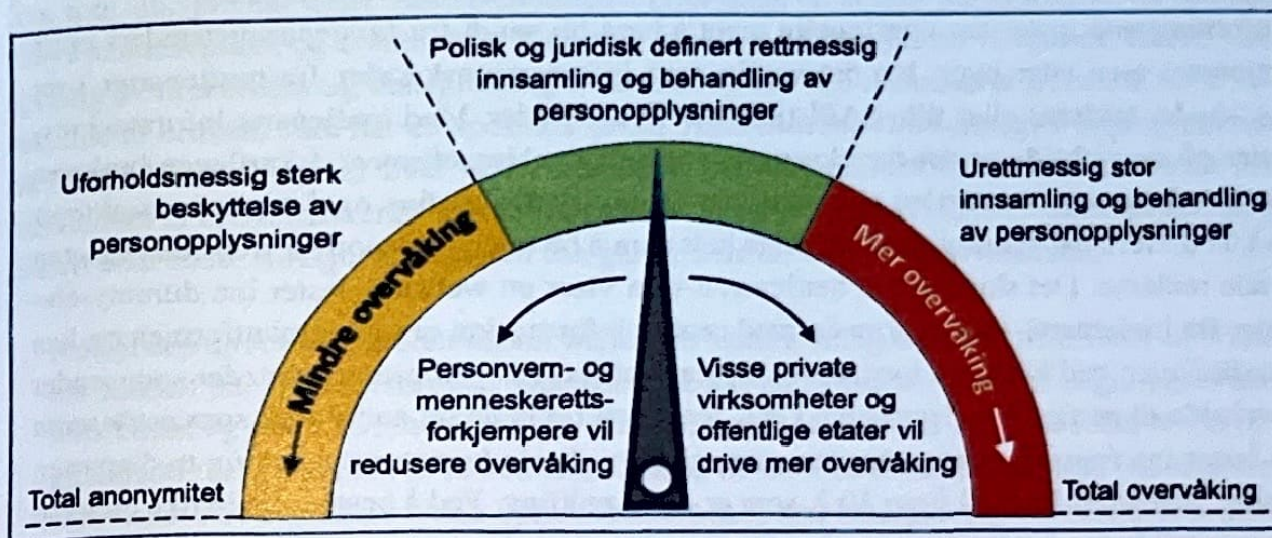
Økt digitalisering av samfunnet fører til raskt økende produksjon og deling av personopplysninger. Tidligere var personopplysninger som regel eksplisitt definerte og relativt statiske kategorier som adresse, skole, arbeidsplass, helseopplysninger og medlemskap i foreninger. Nå som nesten alle våre aktiviteter har en digital komponent, genereres og lagres personopplysninger dynamisk og kontinuerlig, og gir et massivt potensial for overvåking.

La oss først betrakte en situasjon der massiv innsamling av personopplysninger finner sted. På den ene siden kan det støtte nye forretningsprosesser, effektivisere forvaltningen og gjøre privatliv og arbeidsliv praktisk. Det gir også politimyndigheter enorme muligheter for å etterforske kriminalitet og håndheve lov og orden. På den andre siden kan det gi alvorlige negative konsekvenser hvis private virksomheter og myndigheter kan drive massiv innsamling og behandling av personopplysninger. Mulige negative konsekvenser er at det raskt vil krenke vår integritet, skape uønsket oppmerksomhet mot oss, gjøre at vårt privatliv blir utlevert, føre til diskriminering og gi myndigheter mulighet for maktmisbruk og undertrykking som kan true vårt demokrati.

La oss så betrakte en situasjon der det foregår svært begrenset innsamling av personopplysninger. På den ene siden vil innbyggere kunne være i fred, slippe uønsket oppmerksomhet og i mindre grad frykte maktmisbruk og undertrykking fra myndighetene. På den andre siden vil det også ha alvorlige negative konsekvenser. Det vil for eksempel hindre utvikling av smarte forretningsprosesser, gjøre forvaltning ineffektiv, og det vil forhindre effektiv etterforskning av kriminalitet. Nettopp kriminelle har stor interesse av å beskytte sine person-

opplysninger ved å opptre anonymt og ikke legge igjen spor når de begår lovbrudd, slik at de ikke kan spores opp. At kriminelle og terrorister har et uforholdsmessig sterkt personvern, vil forhindre håndheving av lov og orden, som igjen kan true vårt demokrati.

På bakgrunn av betraktningene over er det opplagt at vi må finne en balanse, som illustrert med overvåkingsbarometeret i figur 10.1. Forskjellige kulturer, land og regioner har ulike oppfatninger av hvor denne balansen bør ligge, og det bør skilles mellom myndigheter og private virksomheter som aktører for overvåking. Kina er et eksempel der statens politikk er å ha et høyt overvåkingstrykk fra myndighetene. I motsatt ende av skalaen er EU/EØS en region som gjennom GDPR har bestemt at vi skal ha et relativt lavt overvåkingstrykk både fra myndigheter og private. Når det oppstår uenighet om tolkning av spesifikke caser i forhold til loven, blir det avgjort med rettssaker, som er et grunnleggende demokratisk prinsipp.



Figur 10.1. Overvåkingsbarometeret.

Selv om GDPR definerer hva som er akseptabel behandling av personopplysninger, er loven relativt vanskelig å håndheve. Det er fordi innsamling og behandling av personopplysninger foregår i virksomheters private systemer som tredjeparter har lite innblikk i. Ettersom behandling av personopplysninger danner grunnlag for svært lønnsomme forretningsprosesser, er det fristende for virksomheter å drive mer overvåking enn det som egentlig er tillatt etter loven. Ettersom det fins et stort antall virksomheter, er det nærmest umulig for Datatilsynet å oppdage brudd på GDPR, unntatt i tilfeller der en hendelse blir rapportert.

10.3 Personverninvaderende teknologier

Det fins mange metoder og teknologier for innsamling av personopplysning, hvorav noen metoder virker invaderende ved å samle informasjon om oss og spore våre aktiviteter. Avsnittene nedenfor beskriver noen personinvaderende teknologier og noen teknologier og metoder som styrker personvern.

10.3.1 Sporing med informasjonskapsler

Reklameindustrien generer stor profit basert på personopplysninger, fordi det muliggjør målrettet markedsføring som har høyere påvirkningskraft enn den ellers ville hatt. Web-industrien og reklameindustrien har derfor utviklet svært avanserte metoder for innsamling av data om og sporing av brukere på nett. Cookies, også kalt informasjonskapsler, er et sentralt teknisk element for innsamling av brukerdata.

En informasjonskapsel er en datafil som lastes ned og lagres på brukers klient (smarttelefon eller laptop) når brukeren åpner en nettside, og som returneres til nettstedet ved hver påfølgende brukeraktivitet.

Informasjonskapselen brukes for eksempel til å lagre innloggingsdetaljer, huske hva brukeren har gjort på nettstedet, eller holde orden på handlekurven i nettbutikker. Nettstedet som sender informasjonskapselen, kan tilpasse tjenestene sine ut fra dens innhold.

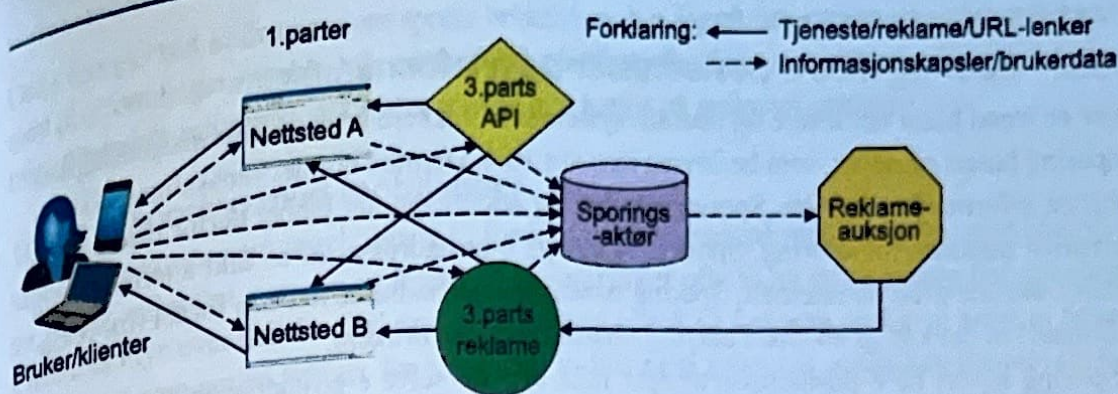
Informasjonskapsler var opprinnelig ment å bare bli sendt fra førstepartnettsteders egne webtjenere, men etter hvert ble det vanlig med informasjonskapsler fra tredjeparter som f.eks. sender reklame eller tilbyr API-tjenester til nettsteder. Med tredjeparts-informasjonskapsler på en webside er det for eksempel mulig for reklamefirmaer å kartlegge brukers aktivitet på tvers av nettsteder, slik som vist i figur 10.2. Det fins også tredjeparts-aktører som kun driver med sporing av brukerdata helt uten å ha noen funksjon på websiden og uten å sende reklame. Det skjer ved at nettleseren som viser en webside, laster inn dummy-elementer fra tredjeparts-aktører som dermed mottar informasjon om klientplattformen og kan spore brukeren ved å lagre informasjonskapsler i brukerens nettleser. Nettsteder som sender en webside til nettleseren, legger inn URL-lenker til reklame og andre ting som nettleseren selv laster inn fra tredjeparter. At elementer på en webside kommer direkte fra tredjeparter, kommer ikke klart frem på figur 10.2, som er en forenkling. Ved å bestemme hvilke elementer som skal lastes fra tredjeparter, har førsteparts-nettsteder en viss makt med hensyn til å styre omfang av sporing.

Nettsteder kjøper typisk tilleggsfunksjoner gjennom tredjeparts-API-er (Application Programming Interface). Slike API-tjenester kan for eksempel være Google Analytics, som monitorerer trafikk og aktivitet på nettsider, tjenester for å ta imot betaling, eller tjenester som tilpasser innhold. Slike API-tjenester kan også formidle informasjonskapsler, og dermed innhente brukerdata på samme måte som reklame.

Mange stusser over hvordan det er mulig at de først søker eller leser om en ting gjennom en spesifikk kanal eller plattform, og deretter mottar reklame om samme ting gjennom en annen kanal eller klientplattform. Forklaringen ligger i at data om samme bruker spores på tvers av nettsteder og klientplattformer. Det er som regel lett å matche informasjonskapsler om samme bruker basert på sammenfallende innhold. Figur 10.2 viser hvordan informasjon om samme bruker flyter via ulike nettsteder og tredjeparter, og til slutt aggregeres av sporingssentiteter som sammenstiller data om samme bruker.

For å effektivisere reklamering på web ble programmatisk reklameformidling og reklameauksjon i sanntid tatt i bruk fra 2007.³⁶ Nettsteder kan tilby annonseplass til reklameformid-

³⁶ Reuben Binns (2022). Tracking on the Web, Mobile and the Internet of Things. *Foundations and Trends in Web Science*, 8(1-2), 1-113.



Figur 10.2. Informasjonskapsler til å samle brukerdata for reklameauksjon.

lere som auksjonerer disse annonseplassene. Hver gang en bruker har klikket på en nettside, tilbys annonseplass, og annonsører byr automatisk for å kjøpe denne visningen. Takket være sporing av brukerdata og auksjonering av annonseplass kan annonsører nå betale for å vise reklame til brukere som har en spesifikk profil. Annonsørenes budstrategier er programmert på forhånd, som betyr at hver reklameauksjon kun tar millisekunder. Innenfor dette lille tidsvinduet er et overraskende stort antall aktører involvert i en kompleks, automatisk koreografert budrunde. Auksjonsprosessen foregår i tre trinn, som forklart nedenfor.

1. Auksjonen åpnes ved at annonsører mottar en budutlysning om en nettside som en bruker har klikket på. Budutlysningen spesifiserer URL-en til siden, nettstedkategorien, brukers klient og nettleser, én eller flere brukeridentifikatorer som budgivere kan bruke til å gjenkjenne en bruker fra en annen kontekst, og deretter informasjonskapsler om brukeren som f.eks. kan inkludere antatt kjønn, interesser, fysisk lokasjon (by eller GPS-koordinater) og andre ting.
2. Selve auksjonen foregår automatisk basert på de konkurrerende annonsørenes programmatisk budgivningsstrategier, som er spesifisert basert på budutlysningen og ytterligere data om brukeren som budgiver har kunnet hente fra andre sporingskilder.
3. Til slutt vinner den høystbydende annonsør auksjonen, og formidler automatisk reklamen som integreres i nettsiden som presenteres til brukeren, i håp om at brukeren ser og kanskje klikker på reklamen.

Denne type innsamling og behandling av brukerdata er svært inngripende, og er samtidig obskur for de fleste. Det er interessant å vurdere dette i forhold til GDPR. Selv om et nettsted innhenter samtykke, ville de ikke kunne oppfylle krav til åpenheten rundt reklameauksjoneringen, og vil ikke kunne påse at alle de involverte aktørene har et adekvat sikkerhetsnivå for beskyttelse av brukerdata. På det grunnlaget kan man argumentere med at denne industrien antagelig bryter prinsippene i GDPR.

Et enda mer dystert scenario er hvis en lignende mekanisme for målrettet påvirkning benyttes for å manipulere politiske valg, slik det skjedde under presidentvalget i USA i 2016. Entiteter som er lagelig plassert i økosystemet for informasjonsflyt på internett, kan kartlegge brukers profiler og politiske holdninger svært nøyaktig gjennom aggregering, sporing og analyse av data fra forskjellige kilder.

10.3.2 Sporing med e-postadresser og telefonnummer

Det er en trend blant nettlesere og operativsystemer å blokkere bruk av informasjonskapsler og sporing basert på apper, som beskrives i avsnitt 10.4. Dermed blir det vanskeligere å spore basert på informasjonskapsler. Sporingsaktører og reklamebyråer jobber derfor med å finne alternative metoder for sporing. Sporing basert på e-postadresser er et slikt alternativ som brukes i økende grad på internett. Sporing basert på e-postadresse har den fordel (for reklamefirmaer) at det kan gi en enkel entydig identifisering av brukere.

Sporing basert på e-postadresse trenger ikke benytte selve e-postadressen for å matche samme bruker på forskjellige nettsteder. I stedet genereres et slags adressefingeravtrykk av e-postadressen som dermed utgjør et pseudonym. På den måten kan brukerdata utveksles sammen med e-postpseudonymet slik at sporingsaktører kan matche brukerdata fra forskjellige kilder. For å beskytte sin forretningsmodell kan tilbydere av slike pseudonym-identifikatorer diversifisere hver brukers identifikator for ulike mottagere (f.eks. reklamebyråer), slik at mottagere ikke kan samarbeide seg imellom ved å utveksle identifikatorer med tilhørende brukerdata.

Telefonnummer utgjør også en unik adresse som kan benyttes til sporing på samme måte som e-postadresser. Imidlertid er sporing med telefonnummer mindre utbredt enn med e-postadresse, fordi vi i mindre grad benytter telefonnummer som identifikator på internett.

10.3.3 Sporing med plattformfingeravtrykk

Nettlesere sender informasjon om innstillinger og karakteristikker om klientplattformen til webtjeneren for at denne skal kunne tilpasse hvordan nettsider best kan presenteres. For eksempel sender nettleseren informasjon om grafikkoppløsning på klientplattformen, slik at størrelse og oppløsning av bilder kan tilpasses. Andre eksempler på slike attributter er hvilke plugins som er installert, hvilke bokstavfonter som er installert, og hvilken tidssone som er satt. Ved å kombinere disse og andre attributter er det mulig å unikt identifisere en nettleser og plattform med stor sannsynlighet. Som analogi er det mulig å spore en enkelt bil uten å bruke bilnummeret, men bare basert på bilmerke, modell, farge, dekktype, montert ekstrautstyr, omtrentlig kjørelengde, og kanskje ved å kartlegge riper i lakken.

Antall og typer av attributter avgjør hvor unikt hvert plattformfingeravtrykk er. Antagelig er en stor andel av «fingeravtrykk» helt unike, slik at det i praksis kan brukes til entydig identifisering av en bruker. Det fins online tjenester for å sjekke hvor unik en plattform er, f.eks. EFF sin *Cover Your Tracks*.³⁷

I motsetning til informasjonskapselbasert sporing, som innebærer å påvirke måten nettleseren fungerer på, og som etterlater spor ved å plassere en informasjonskapsel, skjer sporing med plattformfingeravtrykk skjult i bakgrunnen på tjenersiden, som derfor er vanskeligere å oppdage og forhindre.

Sporing av plattformfingeravtrykk gjøres i stor skala, og komplementerer sporing med informasjonskapsler og e-postadresser. Både førsteparts-nettsteder og tredjeparts-API- og reklameleverandører driver sporing av plattformfingeravtrykk. Hvis en bruker sletter informasjonskapsler fra en nettleser, kan plattformfingeravtrykk brukes til å regenerere informasjonskapsler.

37 <https://coveryourtracks.eff.org/>.

Dette foregår ved at firmaer som sporer brukerdata, har lagret informasjonskapsler indeksert med plattformfingeravtrykk. Når en spesifikk plattform detekteres, er det en enkel sak å hente frem tilhørende informasjonskapsler som på nytt lagres på brukeren nettleser.

10.3.4 Sporing med mobilapper

Mobilapper krever som regel tilgang til forskjellige ressurser på mobilenheten, som kontakter, bilder, mikrofon, kamera og lokasjon. Vi samtykker ofte til alt en mobilapp ber om uten å tenke så mye over det, fordi vi ønsker å ta appen i bruk så fort som mulig og antar at dette er ressurser som appen trenger for å fungere. Vi blir også spurt om appen kan benytte disse ressursene kun når den brukes, eller hele tiden, dvs. også når den ikke brukes. Anbefalingen er helt klart å bare la en app bruke ressurser når appen er i bruk, men selv da samler mange apper betydelige mengder informasjon som sendes til selskapet som står bak appen, og til tredjeparter. Dette i seg selv er både et personvernproblem og et sikkerhetsproblem.

I mars 2023 kom anbefalingen fra Justis- og beredskapsdepartementet, og fra Nasjonal sikkerhetsmyndighet, om at statlig ansatte ikke får installere appene TikTok og Telegram på sine mobiltelefoner og andre digitale enheter eid av arbeidsgiveren. Teknisk sett er TikTok og Telegram som alle andre apper – de samler data for de funksjonene de tilbyr, og de får tilgang de ber om og som brukeren godtar. Forskjellen er at TikTok er kinesisk-eid og Telegram er russisk-eid, og at både Kina og Russland regnes som trusselaktører innenfor cyberdomenet. Lovgivningen i Kina forplikter kinesiske virksomheter å utlevere all informasjon som myndighetene måtte be om. Tilsvarende lovgivning eller praksis gjelder antagelig i Russland.

Fra et dystert perspektiv kan man forestille seg at apper kan skru på mikrofon eller kamera for å spionere, noe som teknisk sett er mulig. Apper kan få tilgang til både brukernes persondata, og virksomhetsinformasjon som er lagret på mobilenheten eller som mobilenheten har tilgang til gjennom nett.

En app som TikTok sender ikke bare mediefiler fra TikTok-appen til TikToks datasenter. Apper har felles tilgang til data som er lagret i felles områder, som kontakter, bilder, meldinger og dokumenter. TikTok kan også kopiere den type informasjon fra brukernes enheter og laste det opp til TikToks datasenter. Hvis kinesiske myndigheter ber om det, kan de få den type informasjon utlevert.

Men det er feil å utelukkende være skeptisk til TikTok og Telegram; man burde også forholde seg skeptisk til de fleste apper. Det eksisterer en stor overvåkningsindustri for både mobilapper og vanlige nettsider med informasjonskapsler som samler inn store mengder informasjon til sammenstilling, analyse og videresalg.

På samme måte som nettsider har informasjonskapsler fra tredjeparter som samler informasjon om brukerne, inneholder de fleste apper også API-funksjoner fra tredjeparter som Alphabet (Google), Meta (Facebook), Twitter, Verizon, Microsoft, Amazon og andre Big Tech-selskaper. Når API-funksjoner fra tredjeparter er innebygd i en app, kan de sende brukerdata tilbake til tredjepartene. Slike API-funksjoner gjør det enklere å utvikle apper med avanserte funksjoner, og kan brukes til å sende reklame til brukeren, slik at app-tilbydere også kan tjene penger på det.

De store mengdene brukerdata som samles inn på denne måten, brukes primært til kommersiell målrettet reklame tilsvarende prosessen vist i figur 10.2. Imidlertid kan mange slike innsamlede datasett kjøpes av hvem som helst, også av kriminelle eller statlige aktører, og

på den måten benyttes som kilde for rekognosering og frikildeetterretning (OSINT) som del av et APT-angrep (se avsnitt 17.1.2). På den måten er reklameindustrien ikke bare en trussel mot personvern, men også en ressurs som kan utnyttes av kriminelle og statlige trusselaktører. Det beste rådet er å ha så få apper som mulig installert på mobilenheter. Apper som ikke lenger brukes, bør slettes.

10.4 Blokkering av sporing

Som reaksjon på sporings- og reklameindustriens stadig mer personinngripende teknologier utvikles det også teknologier og metoder som styrker personvern ved å beskytte mot og forhindre invaderende sporing.

Eksplisitt varslings- og valgfrihet om, å gi samtykke til sporing med informasjonskapsler avhenger av at førsteparts-nettsteder iverksetter tiltak mot tredjeparters ønske om sporing. I denne sammenheng bør vi ta i betraktning at førsteparts-nettsteder ofte er avhengige av tredjeparters tjenester for funksjonalitet og inntekter, slik at det kan mangle insentiver for at førsteparts-nettsteder faktisk innfører slike tiltak.

Innenfor EU/EØS setter GDPR krav om å innhente samtykke fra bruker for å spore med informasjonskapsler. Dessverre kan prinsippet om samtykke feile i praksis når brukeren går lei av å klikke for å endre innstillinger av informasjonskapsler, eller nettstedet samler inn mer enn det brukeren faktisk har, eller tror hen har, gitt samtykke til. For å komme unna denne frustrerende situasjonen ønsker mange brukere å benytte teknologier på klientsiden som effektivt hindrer sporing uansett. Blokkeringsteknologier i nettleseren er mest brukt. Sporingsblokkere er blitt implementert både av nettleser-plugins som Ghostery, Disconnect, Adblock, Adblock Plus, Privacy, Badger og andre, samt er innebygde i vanlige nettlesere som Safari, Firefox, Chrome og Edge. Standard innstilling gir ikke alltid maksimal blokkering, men for eksempel «balansert blokkering» som i Microsoft Edge. Derfor kan det være nødvendig for brukere å justere innstilling for blokkering av tredjeparts-informasjonskapsler. Blokkering av sporing er typisk basert på lister over IP-adresser til tredjeparts-sporingsaktører. Store aktører som Google har annonsert at deres nettleser Chrome aktivt vil blokkere sporing med informasjonskapsler fra 2024, men det er uvisst om det faktisk vil skje, og om det bare er et tiltak som er ment å støtte en ny forretningsmodell for reklame på internett.

Mange typer nettleser-plugin er laget for å blokkere både reklame og informasjonskapsler fra tredjeparts-aktører. Begge typer blokkering forhindrer forretningsprosesser hos tredjeparts-aktører. Som motreaksjon kan disse for eksempel varsle førsteparts-nettsteder og bedømme om å sperre webtjenester for brukere som blokkerer reklame, eller redusere funksjonalitet for brukere som blokkerer informasjonskapsler.

En måte å forhindre sporing med e-postadresser på er å benytte ulike e-postadresser for forskjellige tjenester. Imidlertid er dette svært upraktisk fordi vi da måtte huske hvilke e-postadresser vi benytter for ulike tjenester, og dessuten huske ulike passord relatert til hver e-postadresse. Imidlertid fins tjenester som automatisk genererer ulike alias e-postadresser, som f.eks. *Apple Hide My Email* og *Firefox Relay*. Å benytte ulike telefonnummer for å blokkere sporing av telefonnummer er enda mer upraktisk, og vil dessuten være dyrt fordi det koster å ha et telefonabonnement.

For å blokkere sporing med plattformfingeravtrykk må man å ta drastiske skritt, som å stadig skifte klientplattform (skifte ut PC og mobiltelefon) og endre nettlesere, og hele tiden endre IP-adresse ved å bruke VPN-løsninger. For de fleste er dette for upraktisk.

Kampen mellom aktører som ønsker å spore, og brukere som forsøker å unngå sporing på web, vil alltid være som en katt-og-mus-lek. Forretningsmodeller basert på sporing av brukere er enormt profitable, slik at sterke markedskrefter vil drive innovasjon for utvikling av nye avanserte metoder for sporing.³⁸ Dessverre ligger det ikke særlig store økonomiske insentiver bak å utvikle teknologier som hindrer sporing og styrker personvern. GDPR, som beskrives i de neste avsnittene, er ment å kompensere for denne skjevheten, og gjenopprette balansen mellom personverninteresser og markedsinteresser.

10.5 GDPR og personopplysningsloven

For tradisjonell informasjonssikkerhet eksisterer forretningsmodeller og insentiver for at organisasjoner selv innfører tiltak for å redusere sikkerhetsrisiko. I kontrast til tradisjonell informasjonssikkerhet eksisterer det egentlig ingen naturlig forretningsmodell for organisasjoner for å ivareta personopplysningsvern. Sagt på en annen måte: Uten regulering ville organisasjoner hatt få insentiver for å sørge for personopplysningsvern. I EU eksisterer det sterk politisk vilje til nettopp å beskytte innbyggers integritet gjennom personopplysningsvern, noe som har resultert i innføringen av GDPR. Dette har vært en politisk og juridisk prosess som har gjort GDPR til en særegen modell for personopplysningsvern. GDPR er juridisk orientert, og kan virke relativt innviklet og vanskelig å forstå fra et IT-perspektiv.

Uavhengig av GDPR fins det en rekke tilnærminger for å styrke personvern i digitale omgivelser. Slike teknologier går gjerne under navnet *PET* (*Privacy Enhancing Technologies*). Typiske PET er teknologier for anonymisering og pseudonymisering. Vi fokuserer ikke på PET i denne boken.

GDPR (General Data Protection Regulation) er en EU-forordning som skal styrke og harmonisere personvernet i EU og EØS gjennom regler for behandling av personopplysninger. På norsk kalles GDPR for *Personvernforordningen*. Dette navnet er igjen en unøyaktighet, for egentlig burde det hete «Personopplysningsvernforordningen», men det ville nok være for mye å forvente av noen å uttale et slikt ord. I denne boken bruker vi betegnelsen «GDPR» i stedet for det unøyaktige ordet «Personvernforordningen».

En EU-forordning er en lov som har bindende virkning i alle medlemsland i EU, det vil si at hvert medlemsland øyeblikkelig må innføre forordningen som lov slik den er når den trer i kraft, uten anledning til å endre en eneste artikkel. Det står i kontrast til EU-direktiver, som medlemslandene har frihet til å implementere på sin egen måte over tid. I den grad en EU-forordning eller et EU-direktiv er relevant for EØS-landene (deriblant Norge), kan EØS-landene velge å ta det inn i sine lovverk. Bindende virkning av en EU-forordning for hvert EØS-land er når alle EØS-landene samlet har godtatt forordningen. EØS-landene valgte å godta GDPR, men det skjedde først noen måneder etter at forordningen trådte i kraft i EU.

38 Zuboff, S. & Schwandt, K. (2019). *The age of surveillance capitalism*. Profile Books Ltd.

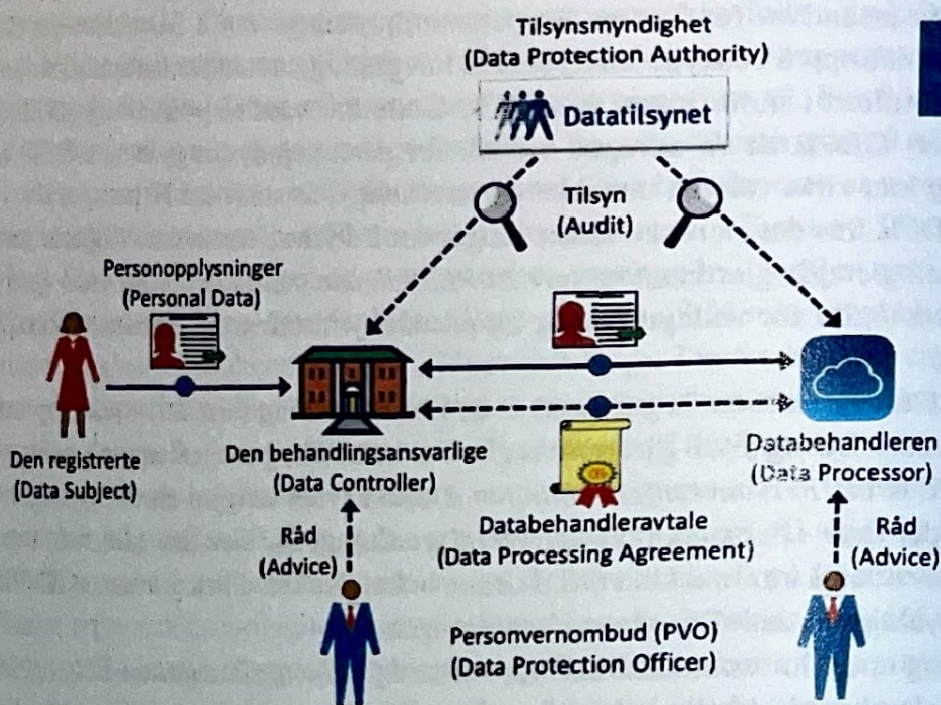
Selv om GDPR er en forordning, åpner den for en rekke nasjonale tilpasninger som i Norge er innlemmet i personopplysningsloven, men som ikke er en del av GDPR. Som eksempel sier GDPR Art. 84 at hvert medlemsland skal bestemme strafferammen overfor individer i tilfelle det begås grove brudd på GDPR. Som nasjonal tilpasning har Norge, gjennom personopplysningsloven § 48, satt strafferammen til bøter og/eller fengsel inntil 1 år (3 år ved særdeles skjerpene omstendigheter).

GDPR gjelder først og fremst innen EU/EØS, men omhandler også behandling av personopplysninger som skjer utenfor EU eller overføring av personopplysninger ut av EU.

I EU ble GDPR vedtatt å tre i kraft 25. mai 2018, som erstatning for det tidligere Personvern direktivet. I Norge ble personopplysningsloven, som omfatter GDPR, vedtatt å tre i kraft 20. juli 2018, samtidig med de andre EØS-landene.

10.6 Roller i GDPR

GDPR beskriver et sett med roller som har ulike rettigheter, plikter og ansvarsområder, som vist i figur 10.3.



Figur 10.3. Roller i GDPR.

Rollene definert i GDPR er beskrevet i avsnittene nedenfor.

10.6.1 Den registrerte og tilhørende personopplysninger

En *registrert* er en naturlig person som enten

- 1) er innbygger/statsborger i EU/EØS,
- 2) befinner seg i EU/EØS, eller
- 3) har personopplysninger om seg lagret i EU/EØS.

Personopplysninger er «enhver opplysning om en identifisert eller identifiserbar fysisk person (den registrerte)» (GDPR Art. 4, nr.1). Følgende beskrivelse av hva som er personopplysninger, er hentet fra Datatilsynets websider:³⁹

Personopplysninger er alle opplysninger og vurderinger som kan knyttes til deg som enkeltperson. Typiske personopplysninger er navn, adresse, telefonnummer, e-post og fødselsnummer. Et bilde regnes som en personopplysning dersom personer kan gjenkjennes, og lydopptak kan være personopplysninger selv om ingen navn blir nevnt i innspillingen. Biometri slik som fingeravtrykk, irismønster og hodeform (for ansiktsgjenkjenning) er også personopplysninger.

Videre er en dynamisk IP-adresse i gitte tilfeller også definert som personopplysning. Registreringsnummeret på en bil kan være en personopplysning hvis det kan knyttes til en bestemt person, men ikke hvis det står på en firmabil som benyttes av flere.

Opplysninger om atferdsmønstre er også regnet som personopplysninger. Opplysninger om hva du handler, hvilke butikker du går i, hvilke tv-serier du ser på, hvor du fysisk beveger deg i løpet av en dag, og hva du søker etter på nettet, er alt sammen eksempler på dette. En av de nyere utfordringene for personvernet er nemlig det at vi legger igjen så mange digitale spor – ofte uten å vite om det eller tenke over det.

Datatilsynet

GDPR definerer også *særlige kategorier personopplysninger* (ofte kalt sensitive personopplysninger), som hvis de samles inn og behandles, skaper særlig høy risiko for den registrertes *rettigheter og friheter*. Derfor er behandling av slike opplysninger i utgangspunktet forbudt i henhold til GDPR Art. 9, nr. 1. Det gjelder opplysninger om

rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning eller fagforeningsmedlemskap, samt behandling av genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person, helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering.

Imidlertid spesifiserer Art. 9 et sett med unntak der det likevel er tillatt å behandle særlige kategorier personopplysninger.

Det som menes med «rettigheter og friheter», er først og fremst rettighetene som beskrives i GDPR Art. 12–22, men også rettigheter nedfelt i Grunnloven, FNs menneskerettighe-

³⁹ <https://www.datatilsynet.no/rettigheter-og-plikter/personopplysninger/>.

ter og Den europeiske menneskerettighetskonvensjonen, som blant annet beskriver retten til privatliv, kommunikasjonsvern, ytringsfrihet, religionsfrihet, retten til å organisere seg, og frihet fra diskriminering.

10.6.2 Den behandlingsansvarlige

Den *behandlingsansvarlige* er typisk eieren av tjenesten eller applikasjonen som behandler personopplysninger. Den behandlingsansvarlige bestemmer formålene for, og på hvilken måte, personopplysningene behandles. Sagt omvendt: Hvis en organisasjon bestemmer «hvorfor» og «hvordan» personopplysningene skal behandles, er den behandlingsansvarlig.

Det er mulig at behandlingsansvaret deles mellom flere organisasjoner som i fellesskap bestemmer «hvorfor» og «hvordan» personopplysninger skal behandles. Felles behandlingsansvar må innebære en ordning som beskriver deres respektive forpliktelser for å overholde GDPR, som for eksempel hvem som utfører DPIA (se nedenfor).

Begrepet *ansvarlig* er tvetydig på norsk, og kan enten bety å ha som oppgave eller å stå til regnskap. Tolkningen av ansvar er nærmere beskrevet i avsnitt 15.1.2. I GDPR er betydningen av begrepet *behandlingsansvarlig* den som står til regnskap (eng. *accountable*) overfor de registrerte og overfor Datatilsynet vedrørende behandlingen av personopplysninger.

10.6.3 Databehandleren

Databehandleren er en tredjepart som har som oppgave å behandle personopplysninger på vegne av den behandlingsansvarlige.

Databehandlerens plikter overfor den behandlingsansvarlige må spesifiseres i en databehandleravtale. For eksempel må avtalen angi hva som skjer med personopplysningene når forretningssamarbeidet er avsluttet. En typisk aktivitet for databehandleren er å tilby IT-løsninger, inkludert skylagring. Databehandleren kan bare utlevere deler av behandlingen til en underleverandør, som dermed også blir en databehandler hvis det foreligger skriftlig forhåndsgodkjenning fra den behandlingsansvarlige.

10.6.4 Personvernombudet

Personvernombudet gir råd til behandlingsansvarlige eller databehandleren om forpliktelser som virksomheten har etter personvernloven. Alle virksomheter kan ha personvernombud. Personvernombudet deltar i DPIA (se nedenfor).

Dersom den behandlingsansvarlige er en offentlig etat (med visse unntak) eller en organisasjon med over 250 ansatte, må det oppnevnes et personvernombud. Det samme gjelder databehandlere hvor kjerneoppgaven er behandling av personopplysninger. Andre organisasjoner kan selv vurdere om det er hensiktsmessig å oppnevne et personvernombud. Rollen som personvernombud kan kombineres med andre roller, eller kan være utelukkende som personvernombud, etter behov.

10.6.5 Tilsynsmyndigheten og straff ved overtredelse av GDPR

Tilsynsmyndigheten er en uavhengig offentlig myndighet i hvert medlemsland i EU/EØS som fører tilsyn av organisasjoners etterlevelse av GDPR. Tilsynsmyndigheten gir råd og behandler klager om brudd på GDPR. Datatilsynet er tilsynsmyndighet i Norge.

En tilsynsmyndighet kan straffe overtredelse av GDPR med bøter eller fengsel. GDPR sier eksplisitt at noen overtredelser er mer alvorlige enn andre, og spesifiserer derfor to kategorier bøter.

De mindre alvorlige overtredelsene kan føre til et gebyr på opptil € 10 millioner eller 2 % av selskapets verdensomspennende årlige inntekt, avhengig av hvilket beløp som er høyest. Overtredelser av denne typen er typisk at den behandlingsansvarlige eller databehandleren ikke har fulgt riktig prosedyre for inngåelse av databehandleravtale eller utførelse av DPIA.

De mer alvorlige overtredelsene er de som strider mot selve prinsippene om retten til privatliv og retten til å bli glemt, som er kjernen i GDPR. Denne typen overtredelser kan resultere i et gebyr på opptil € 20 millioner eller 4 % av selskapets verdensomspennende årlige inntekt, avhengig av hvilket beløp som er høyest. Overtredelser av denne typen er typisk at den behandlingsansvarlige samler inn, behandler og videre sender personopplysninger uten lovlig grunnlag, uten samtykke, uten å gi innsyn eller uten sletting etter at behandlingen er avsluttet. Alvorlige tilsiktede overtredelser av GDPR kan også gi fengselsstraff for ansvarlige ledere og direktører. Likeså kan det gis fengselsstraff for grov uaktsomhet med å sikre sensitive eller store mengder personopplysninger mot tyveri og uautorisert innsyn.

Hensikten med de relativt drakoniske straffene er å virke avskrekkende mot overtredelse av GDPR. Det er et problem at overtredelser av GDPR kan være svært vanskelig å oppdage, fordi det kan foregå skjult i private datanett. De drakoniske straffene er nettopp ment å kompensere for vanskeligheten med å overvåke og håndheve overholdelse av GDPR.

10.7 Spesielt relevante artikler i GDPR

GDPR består i alt av 99 artikler. Denne boken beskriver kort syv av disse artiklene som er spesielt relevante fra perspektivet om å designe IT-løsninger med adekvat sikkerhet og personvern. Følgende artikler beskrives i avsnittene nedenfor.

- Artikkel 5: Prinsipper for behandling av personopplysninger
- Artikkel 6: Behandlingens lovlighet
- Artikkel 25: Innebygd personvern og personvern som standardinnstilling
- Artikkel 32: Sikkerhet ved behandlingen
- Artikkel 35: Vurdering av personvernkonsekvenser (DPIA)
- Artikkel 45 og 46 om overføring av personopplysninger til land utenfor EU/EØS

10.7.1 Artikkel 5: Prinsipper for behandling av personopplysninger

Art. 5 kan betraktes som et sammendrag av hele GDPR. Denne artikkelen definerer hva som menes med begrepet personvern i henhold til GDPR, og definerer syv kortfattede prinsipper som skal være lette å huske. Disse prinsippene er kort beskrevet nedenfor.

- **Art. 5.1.a: Lovlighet, rettferdighet og åpenhet**

Med *lovlighet* menes for det første at det fins et *behandlingsgrunnlag* for behandlingen, der Art. 6 i GDPR beskriver spesifikke behandlingsgrunnlag. Den behandlingsansvarlige må begrunne at behandlingen faller inn under minst ett av behandlingsgrunnlagene

beskrevet i Art. 6. Derneft avhenger lovligheit også av at behandlingen er i samsvar med alle de andre artikkelene i GDPR, og her er det mye å passe på. For eksempel krever Art. 32 at det som standardinnstilling kun skal samles inn og behandles et minimum av personopplysninger som er nødvendig for formålet. Art. 32 krever at lagring og behandling av personopplysninger er underlagt adekvate sikkerhetstiltak. Hvis personopplysninger blir overført til land utenfor EU/EØS, kreves et *overføringsgrunnlag* som beskrives i Art. 44 og 46. Dette er bare noen eksempler.

Med *rettferdighet* menes det som befolkningen i EU/EØS generelt oppfatter som rettferdig. Dette prinsippet er altså noe vagt, og kan juridisk sett bli benyttet til å fange opp det som ikke spesifiseres konkret av andre artikler i GDPR.

Med *åpenhet* menes at den registrerte skal ha innsyn i om det behandles personopplysninger om hen, hvilke opplysninger som behandles, og hva formålet er. Dette er avgjørende for at den registrerte skal kunne benytte seg av de andre rettighetene som GDPR gir, som retten til å få sine opplysninger korrigert, eller å trekke tilbake samtykke og få sine opplysninger slettet.

- **Art. 5.1.b: Formålsbegrensning**

Med formålsbegrensning menes at personopplysninger kun behandles for spesifikke og legitime formål. Alle behandlingsformål av personopplysninger skal beskrives presist og forklares på en måte som gjør at alle berørte har samme forståelse av formålene. At et formål er legitimt, betyr at det skal ha et rettslig grunnlag og at det skal være i samsvar med øvrige etiske og rettslige samfunnsnormer. Personopplysninger som er samlet inn for et spesifikt formål, kan ikke gjenbrukes til formål som er uforenelig med det opprinnelige formålet.

- **Art. 5.1.c: Dataminimering**

Med dataminimering menes at innsamling og bruk av personopplysninger i behandlingen skal begrenses til det som er nødvendig for å realisere formålet med behandlingen. Dersom personopplysninger ikke er nødvendige for å oppnå formålet, skal de heller ikke samles inn. Videre skal hver applikasjon bare benytte og hente personopplysninger som er nødvendig for behandlingen, selv om virksomheten kanskje har lagret et større sett med personopplysninger.

- **Art. 5.1.d: Riktighet**

Personopplysninger som behandles, skal være korrekte sett opp mot behandlingens formål. Dette kan for eksempel være avgjørende for at helsepersonell skal kunne gi riktig behandling. Hvis aspekter ved en person endres, skal personopplysninger om disse aspektene oppdateres. Dette betyr at den behandlingsansvarlige må sørge for å straks rette personopplysninger som er utdaterte eller feil, eller slette personopplysninger som ikke kan rettes.

- **Art. 5.1.e: Lagringsbegrensning**

Prinsippet om lagringsbegrensning betyr at personopplysninger skal slettes eller anonymiseres når de ikke lenger er nødvendige for formålet de ble innhentet for. Imidlertid er

det ikke alltid klart når formålet er oppnådd. For eksempel ved ansettelser der flere personer har søkt på samme stilling, skal normalt søknader til de som ikke ble ansatt, slettes når stillingen er besatt. Men i tilfelle den nyansatte ombestemmer seg etter kort tid, vil det være praktisk at virksomheten kan se nærmere på neste person på listen og tilby stillingen til denne uten å måtte utlyse stillingen på nytt. Dessuten fins en rekke andre lover som setter krav til oppbevaring av personopplysninger, blant annet for etterforskning av kriminalitet og for arkivering av regnskapsdokumenter.

• **Art. 5.1.f: Integritet og konfidensialitet**

Dette prinsippet fokuserer på tradisjonell informasjonssikkerhet, som betyr at personopplysninger må beskyttes med adekvate sikkerhetstiltak. Selv om det ikke nevnes eksplisitt, bør tilgjengelighet inkluderes her, slik at dette prinsippet betyr KIT for personopplysninger.

• **Art. 5.2: Ansvar**

Prinsippet om ansvar betyr at virksomheter står til regnskap for å sørge for at behandlingen av personopplysninger skjer i samsvar med GDPR. På engelsk kalles dette prinsippet «accountability», som også kan oversettes med regnskapelighet eller «å stå til regnskap», se forklaring i avsnitt 15.1.2. Å vise ansvarlighet betyr at virksomheten dokumenterer alle relevante aspekter ved behandlingen, som formål, behandlingsgrunnlag, typer personopplysninger, DPIA og risikovurderinger osv., og at dokumentasjonen kan legges frem ved tilsyn. Det betyr også at den behandlingsansvarlige ikke skal kunne fraskrive seg ansvar ved brudd på GDPR, selv om hendelsen for eksempel ligger hos en databehandler. For å vise ansvarlighet må virksomheter opptre proaktivt ved å etablere nødvendige organisatoriske og tekniske tiltak som trengs for å etterleve GDPR.

10.7.2 Artikkel 6: Behandlingens lovlighet

Art. 6 er sentral i GDPR ved at den beskriver et sett med kategorier av formål for behandling av personopplysninger. Enhver behandling av personopplysninger må forklares i forhold til en av kategoriene. Art. 6 har 4 avsnitt, hvorav avsnitt 1 som inneholder bokstaver a) til f), er gjengitt nedenfor.

Avsnitt 1. Behandlingen er bare lovlig dersom og i den grad minst ett av følgende vilkår er oppfylt:

- den registrerte har samtykket til behandling av sine personopplysninger for ett eller flere spesifikke formål,
- behandlingen er nødvendig for å oppfylle en avtale som den registrerte er part i, eller for å gjennomføre tiltak på den registrertes anmodning før en avtaleinngåelse,
- behandlingen er nødvendig for å oppfylle en rettslig forpliktelse som påhviler den behandlingsansvarlige,
- behandlingen er nødvendig for å verne den registrertes eller en annen fysisk persons vitale interesser,
- behandlingen er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt,

- f. behandlingen er nødvendig for formål knyttet til de berettigede interessene som forfølges av den behandlingsansvarlige eller en tredjepart, med mindre den registrertes interesser eller grunnleggende rettigheter og friheter går foran og krever vern av personopplysninger, særlig dersom den registrerte er et barn.

GDPR, Art. 6

Avsnitt 1. bokstav f) får ikke anvendelse på behandling som utføres av offentlige myndigheter som ledd i utførelsen av deres oppgaver.

For å illustrere anvendelsen av Art. 6 ser vi på noen caser nedenfor.

- *Case 1: Et privat sykehus har behov for å behandle personopplysninger om en pasient som er ubevisst og trenger øyeblikkelig behandling.*

Her fins to mulige grunnlag:

- Bokstav d): Pasientens vitale interesser tilsier at sykehuset kan behandle personopplysninger uten samtykke eller annen avtale.
- Bokstav c): Sykehuset kan ha en rettslig forpliktelse å gi behandling for å redde liv.

- *Case 2: Et forsikringsselskap har behov for å behandle personopplysninger om kunder og andre personer av interesse for å etterforske og avdekke mulig forsikringssvindel.*

Her fins to mulige grunnlag:

- Bokstav f): Forsikringsselskaper har en berettiget interesse av å forhindre svindel og bør derfor kunne behandle relevante personopplysninger for det formål, uten samtykke eller annen avtale.
- Bokstav e): Det kan anses å være i allmennhetens interesse å forhindre forsikringssvindel.

- *Case 3: Virksomheten har en nettside, og ønsker å spore besøkende med informasjonskapsler.*

Her fins to mulige grunnlag:

- Bokstav a): Virksomheten har ingen kontrakt med brukeren (den registrerte). Derfor er samtykke et adekvat behandlingsgrunnlag.
- Bokstav f): Virksomheten kan argumentere med at den har et berettiget grunnlag for å bruke informasjonskapsler, men her er formålet avgjørende. Hvis det er for å støtte sikkerhet og pålitelighet i tjenesten, er det OK. Hvis det er for å sende reklame, er det ikke OK.

10.7.3 Artikkel 25: Innebygd personvern

Art. 25 omhandler *innebygd personvern*, som generelt betyr at det skal tas hensyn til personvernprinsippene fra Art. 5 i alle faser av livssyklusen til en tjeneste eller applikasjon som behandler personopplysninger. Disse fasene kan beskrives som *kravspesifisering, design, koding,*

testing, idriftsetting og forvaltning. Art. 25 består av tre punkter som er sammenfattet nedenfor, det vil si at teksten nedenfor ikke er ordrett slik den står i Art. 25, men bare et sammendrag.

1. Det skal gjennomføres tekniske og organisatoriske tiltak med sikte på en effektiv gjennomføring av prinsippene for vern av personopplysninger, f.eks. dataminimering, og for å integrere de nødvendige garantier i behandlingen for å oppfylle kravene i denne forordning og verne de registrertes rettigheter.
2. Den behandlingsansvarlige skal gjennomføre egnede tekniske og organisatoriske tiltak for å sikre at det som standard bare er personopplysninger som er nødvendige for hvert spesifikke formål med behandlingen, som behandles. Nevnte forpliktelse får anvendelse på den mengden personopplysninger som samles inn, omfanget av behandlingen av opplysningene, hvor lenge de lagres og deres tilgjengelighet.
3. En godkjent sertifiseringsmekanisme i henhold til Art. 42 *Sertifisering* kan brukes som en faktor for å påvise at kravene fastsatt i nr. 1 og 2 i denne artikkel overholdes.

Punkt nr. 2 ovenfor setter krav om at nettstedet og apper i sin standardinnstilling kun skal samle inn personopplysninger som er nødvendige for tjenesten brukeren forespør. Dette er spesielt relevant for nettsteders bruk av informasjonskapsler (cookies) og for mobilappers innsamling av informasjon fra sensorer og andre apper. Når vi går til nettsteder, blir vi som brukere ofte spurt om hvilke typer informasjonskapsler vi godtar. Ifølge punkt nr. 2 ovenfor skal standard innstilling alltid være færrest mulige informasjonskapsler, men det virker som om mange nettsteder synder mot dette, slik at vi er tvunget til å klikke oss frem til valg av informasjonskapsler for å velge bort de unødvendige. På samme måte er det mange mobilapper som synder mot punkt nr. 2 ved at de henter inn mange flere typer informasjon enn det som er nødvendig for appens egentlige funksjon og tjeneste til brukeren. Dette er opplagt brudd på Art. 25, og det kan argumenteres for at Datatilsynet og de andre tilsynsmyndighetene i EU/EØS ikke håndhever denne artikkelen. Det burde ikke være nødvendig å klikke på noe som helst på nettsider for at innstillingen skal settes til minimum.

10.7.4 Artikkel 32: Sikkerhet ved behandlingen

KIT-sikkerhetsmålene konfidensialitet, integritet og tilgjengelighet er også viktige for beskyttelse av personopplysninger. Art. 32 definerer nettopp krav om KIT for personopplysninger. Art. 32 består av fire punkter som er sammenfattet nedenfor, det vil si at teksten nedenfor ikke er ordrett slik den står i Art. 32, men bare et sammendrag.

1. Den behandlingsansvarlige og databehandleren skal gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, herunder blant annet evne til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene.
2. Ved vurderingen av egnet sikkerhetsnivå skal det særlig tas hensyn til risikoene forbundet med behandlingen.
3. Overholdelse av godkjente atferdsnormer som nevnt i Art. 40 *Atferdsnormer (Codes of Conduct)* eller en godkjent sertifiseringsmekanisme som nevnt i Art. 42 *Sertifisering* kan brukes som en faktor for å påvise at kravene i nr. 1 i denne artikkel er oppfylt.

4. Den behandlingsansvarlige og databehandleren skal treffe tiltak for å sikre at enhver fysisk person med autorisert tilgang behandler nevnte opplysninger bare etter instruks fra den behandlingsansvarlige, med mindre unionsretten eller medlemsstatenes nasjonale rett krever at vedkommende gjør dette.

Å opprettholde KIT-sikkerhetsmålene for personopplysninger er essensielt. Personopplysninger er svært attraktive mål for trusselaktører. For eksempel kan personopplysninger være verdifulle for

- statlige aktører som driver spionasje for å skaffe kunnskap om viktige personer
- kriminelle aktører som vil tjene penger gjennom utpressing ved å true med offentliggjøring av sensitive personopplysninger

Denne typen sikkerhetshendelser kan få svært alvorlige konsekvenser. Punkt nr. 1 og 2 setter krav til sikkerhet for behandlingen av personopplysninger basert på risikovurdering i forhold til KIT-sikkerhetsmålene. Sannsynlighet og konsekvens av sikkerhetshendelser som skader personopplysninger, skal inngå i slike risikovurderinger. Risikovurdering for informasjonssikkerhet beskrives i kapittel 14 nedenfor.

10.7.5 Schrems II-dommen og Artikkel 45 og 46 om overføring av personopplysninger til land utenfor EU/EØS

Dette avsnittet dekker begge artiklene nedenfor som er nært relatert:

- Art. 45: Overføringer på grunnlag av en beslutning om tilstrekkelig beskyttelsesnivå
- Art. 46: Overføringer som omfattes av nødvendige garantier

Ifølge Art. 45 kan EU-kommisjonen vurdere at tredjestater, dvs. land eller territorier utenfor EU/EØS, sikrer et beskyttelsesnivå som gir minst like godt vern av personopplysninger som GDPR. Dette kalles en *adekvansbeslutning*, som betyr at et lands personvernlovgivning er funnet adekvat. Art. 45 sier at en virksomhet kan overføre personopplysninger til slike stater uten å kreve en særlig godkjenning. EU-kommisjonen utarbeider en liste over slike tredjestater, og per 2023 besto listen av følgende stater: Andorra, Argentina, Canada, Færøyene, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Sveits, Storbritannia, Sør-Korea og Uruguay.

For land som ikke omfattes av en adekvansbeslutning, kan Art. 46 anvendes. Denne artikkelen setter krav til at virksomheter selv må vurdere om det er trygt å overføre personopplysninger til spesifikke databehandlere i stater utenfor EU/EØS.

Frem til 2020 sto også USA på listen over land med adekvansbeslutning, basert på en lovgivning kalt Privacy Shield. Imidlertid ble EU-kommisjonen saksøkt av Max Schrems fordi han mente at USAs Privacy Shield ikke var adekvat. Max Schrems fikk medhold, og dommen kalles Schrems II fordi han gjennom den tidligere Schrems I-dommen hadde fått erklært som inadekvat den tidligere amerikanske lovgivningen Safe Harbour.

Grunnlaget for Schrems II er at amerikanske myndigheter gjennom et sett med lover kan kreve innsyn i personopplysninger om innbyggere i EU/EØS når personopplysningene ligger lagret under amerikansk jurisdiksjon. Disse lovene er:

- *FISA Section 702 (Foreign Intelligence Surveillance Act)* åpner for å innhente etterretning om ikke-amerikanske personer som ikke befinner seg i USA.
- *Executive Order 12333* regulerer all amerikansk utenlandsk etterretningsvirksomhet, inkludert aktiviteter som faller utenfor FISA, f.eks. utført utenlands mot ikke-amerikanske personer. Etterretningsvirksomheten kan foregå hemmelig.
- *Presidential Policy Directive 28* åpner for masseinnhenting av (person)data for overvåking uten at berørte personer er spesifikt mistenkt eller utpekt som interessante. Dog kan innhentede data kun benyttes for nasjonal sikkerhet, og ikke f.eks. til industrispionasje.

Som følge av Schrems II ble adekvansbeslutningen om USA opphevet i 2020, slik at overføring av personopplysninger til USA må baseres på Art. 46. I praksis må virksomheten selv vurdere om kategorier av personopplysninger og typer behandling kan gjøres av tjenesteleverandøren i USA på en måte som ikke bryter personvernprinsippene i Art. 5 og GDPR generelt.

Elementer som må vurderes, er for eksempel sensitivitet av personopplysningene, og i hvilken grad innhenting og behandling av personopplysningene vil være en målsetting for amerikansk myndigheter i henhold til FISA Section 702, Executive Order 12333 eller PPD 28. Kryptering og anonymisering kan være en løsning for IaaS og PaaS, men er upraktisk ved bruk av SaaS. Krypteringsnøkler lagret i USA gir ingen beskyttelse fordi amerikanske myndigheter kan kreve disse utlevert. Admin-tilgang fra USA betyr overføring selv om data er lagret i EU/EØS.

Mange virksomheter i EU/EØS overfører store mengder personopplysninger, i mange tilfeller sensitive personopplysninger, til USA, noe som tilsier at virksomhetene bør gjøre grundige vurderinger av overføringsgrunnlaget. De store skyleverandørene er amerikanske, og Microsoft Office 365 er en tjeneste som svært mange virksomheter benytter. De fleste kunder av O365 behandler antagelig relativt sensitive personopplysninger i denne tjenesten, som i mange tilfeller burde tilsi at bruk av O365 egentlig er ulovlig. For eksempel har Sverige besluttet at statlige myndigheter ikke kan bruke O365 på grunn av Schrems-II-dommen.

Det ville naturligvis vært svært disruptivt hvis Datatilsynet og tilsynsmyndighetene i Europa skulle begynne å forby bruk av O365 og en del andre amerikanske skytjenester for behandling av personopplysninger. At virksomheter fortsatt får lov til å benytte O365, reflekterer at pragmatiske og økonomiske interesser noen ganger veier tyngre enn rent juridiske argumenter. Imidlertid hadde det vært en gylden mulighet for å stimulere europeisk IT-industri å forby bruk av visse amerikanske skytjenester for behandling av personopplysninger fordi de bryter med GDPR.

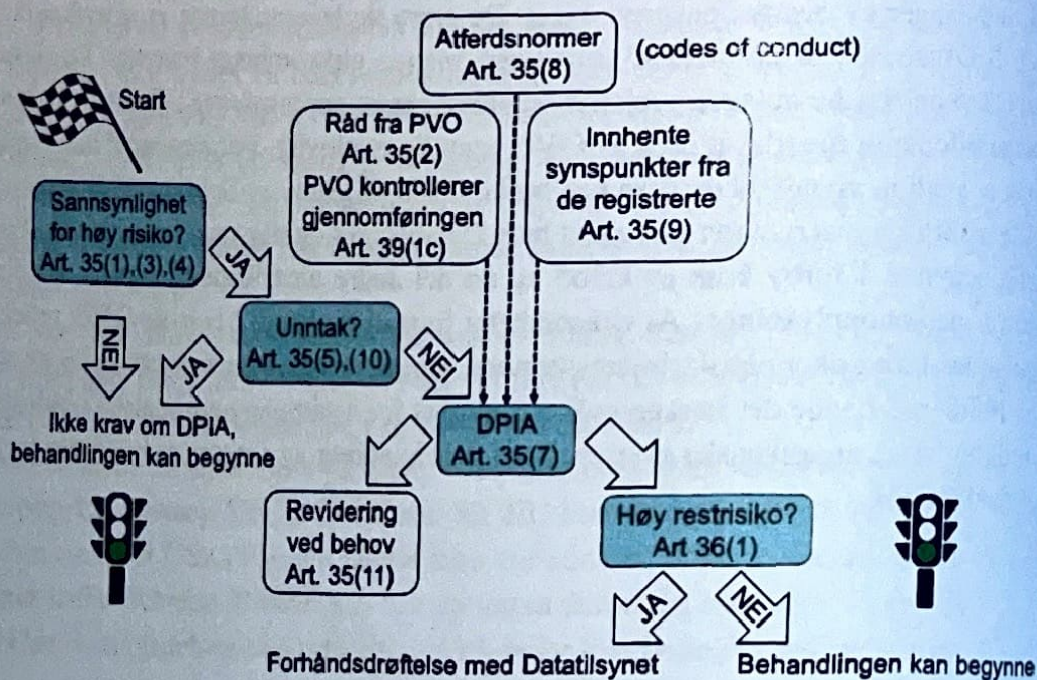
10.8 Artikkel 35: Vurdering av personvernkonsekvens – DPIA

Art. 35 sier at virksomheter må vurdere mulige negative personvernkonsekvenser, og eventuelt redusere disse til et akseptabelt nivå, før virksomheten idriftsetter en tjeneste eller applikasjon som behandler personopplysninger. Dette kalles *vurdering av personvernkonsekvenser* på norsk, vanligvis forkortet til *DPIA* (Data Protection Impact Assessment). Det norske ordet er litt upresist – det burde egentlig hete «vurdering av personopplysningsvernkonsekvenser», men det ville nok være for mye å forvente av noen å uttale et slikt ord. De fleste sier bare DPIA. Beskrivelsen nedenfor oppsummerer og utfyller Datatilsynets egen DPIA-veileder.

10.8.1 Prosessen rundt DPIA

Prosessen rundt DPIA starter øverst til venstre og slutter nederst til høyre som vist i figur 10.4. Før en DPIA utføres, skal det først vurderes om en DPIA i det hele tatt er nødvendig, noe som gjøres ved å vurdere om det er sannsynlig at behandlingen vil medføre en høy risiko for personvern. Dette kan betraktes som er forarbeid til DPIA. Selv om behandlingen anses å medføre høy risiko for personvern, fins visse unntak, som for eksempel behandling som er nødvendig for nasjonal sikkerhet, siden det har prioritet over personvern.

Selve DPIA går ut på å vurdere om den planlagte behandlingen kan få uforholdsmessig negative konsekvenser for de registrerte, og om omfanget av behandling av personopplysninger kan begrunnes ut fra behovet for å kunne oppfylle formålet med behandlingen. Hvis negative konsekvenser er uforholdsmessig store (risikoen for personvern er stor) og omfanget av behandlingen er større enn nødvendig, skal det foreslås hvordan omfanget kan reduseres, eller hvordan de negative konsekvensene (risikoen for personvern) på annen måte kan reduseres til et akseptabelt nivå.



Figur 10.4. Prosess rundt DPIA.

Som resultat av en DPIA vil det foreligge en rapport med vurdering av restrisiko. Hvis ledelsen hos den behandlingsansvarlige vurderer at restrisikoen er uforholdsmessig høy, men samtidig ikke ser hvordan den kan reduseres uten at det setter alvorlige begrensninger for behandlingens formål, kan den behandlingsansvarlige be om forhåndsdrøftelse med Datatilsynet. Hvis ledelsen derimot finner at restrisikoen er lav og akseptabel, kan det besluttes å begynne behandlingen av personopplysninger etter det spesifiserte formålet.

10.8.2 Når er det nødvendig å utføre en DPIA?

Ifølge Art. 35 skal den behandlingsansvarlige foreta en DPIA dersom det er sannsynlig at behandlingen vil medføre en høy risiko for fysiske personers *rettigheter og friheter*, idet det tas hensyn til behandlingens *art, omfang, formål og sammenhengen* den utføres i.

Eksempler på behandlingens art er at:

- det er vanskelig for de registrerte å utøve sine rettigheter
- det er uforutsigbarhet, liten åpenhet og uvisshet om ivaretagelse av prinsipper
- det planlegges systematisk behandling
- det planlegges behandling av særlige kategorier personopplysninger
- det er et skjevt maktforhold mellom de registrerte og den behandlingsansvarlige
- det tas i bruk teknologi som kan skape nye typer konsekvenser

Eksempler på behandlingens omfang er:

- antall registrerte involvert (tall eller prosent)
- volumet av data (antall variabler, detaljer)
- lagringstid (kort, tidsavgrenset, permanent)
- geografisk omfang (lokalt, regionalt, nasjonalt, internasjonalt, globalt)

Eksempler på behandlingens formål er:

- kontrollformål
- behandling for å ta beslutninger som får betydning for den registrerte
- å treffe avgjørelser om enkeltpersoner basert på systematisk og omfattende analyse av personopplysninger

Eksempler på behandlingens sammenheng er:

- forventning om konfidensialitet (helse, velferd og arbeidsforhold)
- forventning om privatliv (hjem, rekreasjon)
- behandling av personopplysninger fra ulike datasett som er innsamlet for ulike forhold

Ved uvisshet om det er nødvendig å gjennomføre en DPIA, anbefales det å gjøre det uansett som et nyttig verktøy for at behandlingsansvarlig får visshet om at de overholder personvernforordningen og for å ha dokumentasjon i tilfelle klage fra de registrerte eller tilsyn fra Datatilsynet. Det er absolutt nødvendig å utføre DPIA

- ved systematisk og omfattende vurdering av personlige forhold når opplysningene brukes til automatiserte avgjørelser,

- ved behandling av særlige kategorier av personopplysninger i stor skala, og
- ved systematisk overvåking av offentlig område i stor skala.

10.8.3 Trusselaktører som element i vurdering av risiko

Når risiko for personvern skal vurderes, er det alltid nyttig å ha en oppfatning om hvem som er trusselaktøren. For tradisjonell vurdering av sikkerhetsrisiko og konsekvenser av sikkerhetshendelser er det typisk antatt at trusselaktører er kriminelle organisasjoner, terrorister eller (fiendtlige) statlige aktører, som vist til venstre i figur 10.5. For vurdering av konsekvenser av brudd på personvern i henhold til DPIA er det nødvendig å anta at trusselaktøren er den behandlingsansvarlige eller databehandleren, som vist til høyre i figur 10.5.

Trusselaktører:

- script kids
- hacktivisme
- organisert kriminalitet
- terrorisme
- statlige cyberoperasjoner

Trusler er f.eks.:

- brudd på KIT for personopplysninger
- tyveri og publisering av personopplysninger



Trusselaktører:

- den behandlingsansvarlige
 - databehandleren
- Trusler er f.eks.:**
- manglende behandlingsgrunnlag
 - urettmessig diskriminering
 - re-identifisering
 - lagring lenger enn nødvendig



→ Risikovurdering ifølge art. 32.

→ DPIA ifølge art. 35.

Figur 10.5. Ulike trusselaktører som element i vurdering av sikkerhetsrisiko (t.v.) og DPIA (t.h.).

Det paradoksale ved DPIA er at den behandlingsansvarlige og databehandleren som utfører DPIA, samtidig er de potensielle trusselaktørene. Dette er som «å sette bukken til å passe havresekken», som i utgangspunktet virker som en dårlig idé. Likevel går DPIA nettopp ut på at behandlingsansvarlige og databehandlere skal vurdere seg selv med hensyn til egen planlagt behandling av personopplysninger. De har som oppgave å vurdere risiko på vegne av de registrerte.

10.8.4 Hvem skal utføre DPIA?

Den behandlingsansvarlige har overordnet ansvar for utførelsen av en DPIA, men selve arbeidet kan delegeres til andre. CISO (Chief Information Security Officer) og PVO (personvernombud) kan anbefale at en DPIA gjennomføres, og bidra i prosessen. Teamdeltagere for utførelsen av DPIA er f.eks. følgende:

- Personvernombudet
- Representant(er) for den behandlingsansvarlige
- Representant(er) for databehandlere
- Representant for de registrerte dersom dette er relevant, for å få synspunktene fra de registrerte
- Generelt: Relevante aktører og eventuelt eksperter på området

DPIA-teamet bør forvisse seg om at behandlingen i utgangspunktet er lovlig og oppfyller grunnkrav som følger av øvrige bestemmelser i GDPR. En DPIA må gjennomføres forut for behandlingen og bør startes så tidlig som mulig. Dette er en kontinuerlig prosess, slik at DPIA skal gjentas ved betydelige endringer i behandlingen, for eksempel ved å inkludere nye typer personopplysninger og nye typer beslutninger basert på personopplysninger. Det er god praksis å definere og dokumentere følgende:

- Roller og ansvarsområder for behandlingen
- Hvis relevant – hvorfor det skal gjennomføres en behandling i strid med de registrertes synspunkter og interesser
- Hvis relevant – hvorfor det ikke innhentes synspunkter fra de registrerte

10.8.5 Trinnene i DPIA

Utførelse av en DPIA består hovedsakelig av følgende fem (eventuelt seks) trinn:

1. Lag en systematisk beskrivelse av den planlagte behandlingen og formålet med behandlingen.
2. Foreta en vurdering av om behandlingen er nødvendig og står i rimelig forhold til formålene.
3. Gjør en vurdering av risikoene for de registrertes rettigheter og friheter.
4. Spesifiser de planlagte tiltakene for å håndtere risikoene og å påvise at GDPR overholdes.
5. Få ledelsens validering av DPIA.
6. Forhåndsdrøftelse med Datatilsynet.

I praksis vil DPIA-teamet først lage et utkast til systematisk beskrivelse, deretter gjøre en iterasjon over punktene 2)–4) til det vurderes at «behandling ikke får konsekvenser for den registrertes rettigheter og friheter», og til slutt redigere endelig versjon av den systematiske beskrivelsen, som valideres av ledelsen i punkt 5). Hvert trinn er beskrevet i detalj nedenfor.

1. Systematisk beskrivelse

Dette trinnet består av å lage en systematisk beskrivelse av den planlagte behandlingen og formålet med behandlingen. Her skal man gjennomgå og kvalitetssjekke oversikten og beskrivelsen av behandlingen med hensyn til

- behandlingens art, omfang, formål og sammenhengen behandlingen utføres i,
- mottagere, dataflyt og lagring,
- funksjonell beskrivelse av behandlingen og alle aktiva, og
- aktuelle referanser for dokumentering av behandlingen.

Ved beskrivelse av behandlingen skal det spesifiseres formål for hver type personopplysning, og hvorfor behandlingen ikke kan gjøres uten den. Målsettingen for dette trinnet er at den behandlingsansvarlige har fullstendig oversikt over behandlingen og gjør en kvalitetssjekk på at beskrivelsene som er gjort, er komplette og tydelige.

2. Vurdering av proporsjonalitet

Dette trinnet består av å vurdere om behandlingsaktivitetene er nødvendige og står i rimelig forhold til formålene (proporsjonalitet). Dette gjøres ved å vurdere

- behandlingsgrunnlag
- formål(ene)
- om det er vurdert å gjøre dataminimering
- om det fins kvalitetskontroll for riktighet av personopplysningene
- om det er spesifisert rimelig lagringsbegrensning
- om de registrertes rettigheter og friheter er tilstrekkelig ivaretatt

Hvis mulig skal man foreslå tiltak som forbedrer måten man ivaretar personvernprinsippene og de registrertes rettigheter og friheter på.

Målsettingen for dette trinnet er å kvalitetssikre at den foreslåtte behandlingen er nødvendig og står i et rimelig forhold til formålene for å etterleve GDPR.

3. Vurdering av restrisiko

Dette trinnet består av å vurdere risikoene for de registrertes rettigheter og friheter. Dette baseres på følgende punkter:

- Vurder potensielle negative konsekvenser av mangelfullt personvern. Eksempler på konsekvenser er at
 - det mangler åpenhet rundt behandlingen av personopplysninger
 - det samles inn mer personopplysninger enn nødvendig for formålet
 - personopplysninger som behandles, ikke er korrekte
 - personopplysninger lagres lenger enn nødvendig for formålet
 - den registrerte mangler informasjon til å gjøre et informert valg
 - den registrerte ikke får innsyn i lagrede personopplysninger
 - den registrerte ikke får korrigert eller slettet sine personopplysninger
 - det ikke er lagt til rette for dataportabilitet
 - de registrertes rettigheter ikke ivaretas ved profilering
 - behandlingen kan resultere i diskriminering
 - behandlingen begrenser ytringsfrihet og religionsfrihet
- Anslå konsekvensenes sannsynlighet og vurder resulterende alvorlighet for hver risiko.

Målsettingen for dette trinnet er å kjenne risikoen for de registrertes rettigheter og friheter.

4. Forslag om tiltak

Dette trinnet består av å foreslå og spesifisere tiltak for å håndtere risikoene og for å påvise at GDPR overholdes. Eksempler på tiltak er:

- samle inn mindre personinformasjon,
- redusert behandling av personinformasjon,
- tillatt rett til reservasjon,

- løpende informasjon, flere kanaler.
- særskilt tilrettelagt innsynsportal,
- automatisk sletting,
- anonymisering,
- forklarlig AI,
- alternativ manuell prosedyre for beslutning.

Målsettingen for dette trinnet er å ha en behandling som ikke får konsekvenser for de registrertes rettigheter og friheter.

5. Ledelsens validering og beslutning

Ledelsen må ha kunnskap om at behandlingen kan medføre høy risiko for den registrertes rettigheter og friheter, som dermed setter krav om DPIA. Ledelsen må også ha kunnskap om den gjennomførte DPIA-en, identifiserte risikoer og tiltak som er foreslått. Å ikke gjennomføre DPIA, å utføre DPIA feil eller ikke rådføre seg med korrekte instanser kan innebære administrative bøter fra Datatilsynet.

Basert på DPIA-rapporten kan ledelsen typisk velge en av tre mulige beslutninger:

1. DPIA er godkjent og validert, som betyr at behandling kan starte opp.
2. DPIA er godkjent på betingelse av forbedringer, med forklaring på hvilke forbedringer som forventes. Dette gjør at ledelsen vil motta en revidert DPIA.
3. DPIA er avvist, som betyr at virksomheten beslutter å ikke gjennomføre behandlingen.

Det er nødvendig å anmode om forhåndsdrøftelse med Datatilsynet i tilfelle DPIA er behandlet i ledergruppen mer enn én gang, og det ikke er funnet tilfredsstillende tiltak for å redusere risikoen tilstrekkelig, mens motivasjonen om å behandle personopplysninger fremdeles er stor.

Virksomheten må dokumentere at risikoen ikke kan reduseres. Beslutningen om å be om forhåndsdrøftelse skal tas av ledelsen.

6. Forhåndsdrøftelse

Ved høy risiko, som ikke kan reduseres, skal Datatilsynet involveres i forhåndsdrøftelser. Det stilles krav til dokumentasjon som skal sendes inn, og at behandlingsansvarlige har fulgt Datatilsynets veiledning.

Maksimum behandlingstid hos Datatilsynet er normalt åtte uker, men i særlige tilfeller kan behandlingen ta ytterligere seks uker.

Målsetting med forhåndsdrøftelse er å finne en god løsning for behandlingen av personopplysninger som ikke medfører høy risiko for de registrertes rettigheter og friheter med hensyn til personvern.

10.9 Varsling ved brudd på personopplysningssikkerhet

Art. 4 nr. 12 definerer *brudd på personopplysningssikkerheten* som et brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet.

Dette dreier seg altså om brudd på KIT-sikkerhetsmålene for personopplysninger. Slike hendelser kan være svært alvorlige hvis det for eksempel angår mange personer, eller hvis sensitiv informasjon er lekket.

Ved brudd på personopplysningssikkerheten har den behandlingsansvarlige plikt til å varsle Datatilsynet uten ugrunnet opphold, og om mulig innen 72 timer. Tre dager kan virke som god tid, men det er mye som må gjøres. Det må innhentes informasjon, vurderes om det i det hele tatt skal sendes varsel til Datatilsynet, artikulere innholdet i varsel og ikke minst sende inn varselet gjennom Altinn av en autorisert person.

72-timersfristen bør overholdes – hvis ikke må årsak til forsinkelsen oppgis i meldingen. Merk at varslingen kan gis trinnvis ved at den behandlingsansvarlige gir løpende oppdatering av hendelsen.

Foruten plikt om varslings til Datatilsynet bør den behandlingsansvarlige på et passende tidspunkt varsle de registrerte og pressen på en kontrollert måte.

10.10 Terminologi for personvern

Med utgangspunkt i at den norske tilsynsmyndigheten heter «Datatilsynet», ville det vært naturlig å bruke betegnelsen «persondata» for det Datatilsynet driver tilsyn med. Derfor virker det ulogisk at det kalles «personopplysninger». Alternativt kunne tilsynsmyndigheten bli kalt «Personopplysningstilsynet», men det klinger klønete. Datatilsynet bør absolutt beholde sitt nåværende navn, men «persondata» burde brukes i stedet for «personopplysninger». Det er intuitivt opplagt at Datatilsynet driver tilsyn med persondata, som dermed burde reflekteres i terminologien.

I *Personvernforordningen*, som er det norske navnet på GDPR, brukes begrepene «personvern» og «personopplysningsvern» om hverandre, noe som er inkonsekvent. Den logiske følgen av å si «persondata» ville vært å bruke betegnelsen «datavern», som dermed ville vært en direkte oversettelse av «data protection». På tilsvarende måte kunne GDPR oversettes med «Datavernforordningen», som er relativt kort og velklingende. Videre kunne DPIA oversettes med «vurdering av datavernkonsekvens», som også er relativt kort og klingende. Ikke minst kunne loven hatt navnet «datavernloven» i stedet for «personopplysningsloven».

De engelske betegnelsene «data controller» og «data processor» speiler hverandre på en naturlig måte, noe som ikke er like tydelig med de norske betegnelsene «den behandlingsansvarlige» og «databehandleren». Det engelske ordet «to control» betyr «å styre», slik at det hadde vært naturlig å oversette «data controller» med «databestyrer». Dermed kunne «databestyrer» og «databehandler» speile hverandre på en naturlig måte.

Dessuten er det misvisende å antyde at bare den behandlingsansvarlige er «ansvarlig». Databehandleren har også et ansvar, som er å behandle data på oppdrag fra «databestyreren». Se avsnitt 15.1.2 for en diskusjon rundt betydninger av begrepet ansvarlig.

Den politiske og juridiske prosessen bak GDPR har produsert en særegen terminologi. Denne terminologien er i utgangspunktet artikulert på engelsk, og senere oversatt til respektive språk i medlemslandene i EU/EØS. Representanter fra Datatilsynet og andre eksperter har dermed fungert som et slags språkråd for å definere ny norsk terminologi. I denne prosessen har de til en viss grad vært bundet av allerede definert terminologi fra tidligere lover og forskrifter,⁴⁰ men det kan likevel diskuteres hvor vellykket deler av den norske GDPR-terminologien er.

Oppgaver til kapittel 10

10.1 Roller

- Kan en entitet være databehandler og samtidig ha en rolle som behandlingsansvarlig for den samme behandlingen? Begrunn svaret.
- Kan en entitet være behandlingsansvarlig uten å oppnevne et personvernombud? Begrunn svaret.

10.2 Samtykke

- Kan den registrerte gi samtykke til innsamling og behandling av personopplysninger uten at den behandlingsansvarlige har definert et formål for behandlingen? Begrunn svaret.

Tenk deg at du gjør lydopptak av en samtale mellom dine kollegaer eller venner. Vurder følgende spørsmål i forhold til dette:

- Hvordan bør du informere de som er til stede under lydopptaket?
- Hvordan kan du bruke lydopptaket senere, med tanke på å spille det av (i) for de som var til stede under opptaket og (ii) for andre som ikke var til stede?
- Kan man si at noen eier lydfilen eller innholdet av lydfilen?

10.3 Outsourcing

En norsk IT-bedrift som behandler personopplysninger, beslutter å legge lagring og behandling av personopplysninger til en skytjeneste lokalisert i utlandet.

- Er dette lov, ifølge GDPR, og hvordan skiller GDPR mellom regioner der «utlandet» ligger?
- Hva må bedriften gjøre for å kunne outsource lagring og behandling av personopplysninger?

40 <https://www.regjeringen.no/no/dokumenter/veiledning-om-lov-og-forskriftsarbeid/id87536/>.

Innebygd informasjonssikkerhet

I dette kapitlet lærer du hva som menes med innebygd informasjonssikkerhet og innebygd personvern. Du lærer også om sikker systemutvikling, applikasjonssikkerhet og sikkerhet i skyen, som nettopp er tre viktige elementer i innebygd informasjonssikkerhet.

Begrepene *innebygd informasjonssikkerhet* og *innebygd personvern* (egentlig «person-opplysningsvern») ble tatt i bruk omtrent fra 2010, og er etter hvert blitt svært utbredt. Ettersom det kan være vanskelig å intuitivt forstå hva som menes med betegnelsen «innebygd» i denne sammenhengen, forklares dette kort i avsnittene nedenfor.

11.1 Innebygd informasjonssikkerhet

Innebygd informasjonssikkerhet (eng.: *security by design*) betyr generelt at det tas eksplisitt hensyn til informasjonssikkerhet i hele livssyklusen til programvareprodukter og applikasjoner.

Et selskap som tidlig oppdaget behovet for innebygd informasjonssikkerhet, var Microsoft. Versjoner av Microsoft Windows før Windows Vista (2006), Windows 7 (2009), Windows 8 (2012) og Windows 10 (2015) hadde svært mange sårbarheter, som ble utnyttet i stor skala av trusselaktører når alle datamaskiner etter hvert ble koblet til internett. For Microsoft ble det raskt tydelig at beskyttelsen av brukere mot skadelig programvare ville kreve en helt ny tilnærming til sikkerhet enn de hadde hatt inntil da. *Microsoft Security Development Lifecycle (SDL)* var et resultat av behovet for å anvende en metodikk som er lett for utviklere å forstå, og som gjorde dem i stand til å praktisere sikker programvareutvikling på en konsistent måte. SDL-metodikken ble innført av Microsoft i 2004 og brukt internt frem til 2008, da SDL-metodikken også ble publisert offentlig. SDL-metodikken består av syv faser listet i tabell 11.1. Microsoft SDL er et godt eksempel på innebygd informasjonssikkerhet.

Tabell 11.1. Fasene i Microsoft SDL (Security Development Lifecycle)

Fase	Norsk	Engelsk
1	Opplæring	Training
2	Krav	Requirements
3	Design	Design
4	Koding	Implementation
5	Test	Verification
6	Produksjonssetting	Release
7	Forvaltning	Response

Microsoft SDL er blitt en integrert del av programvareutviklingsprosessen hos Microsoft, og benyttes av mange andre selskaper verden rundt. Utvikling, implementering og konstant forbedring har gjort at SDL har modnet til å bli en veldefinert og praktisk anvendbar metodikk.

To andre metodikker for innebygd informasjonssikkerhet er BSIMM (Building-Security-In Maturity Model) og SAMM (Software Assurance Maturity Model), som begge ble lansert rundt 2009.

11.2 Innebygd personvern

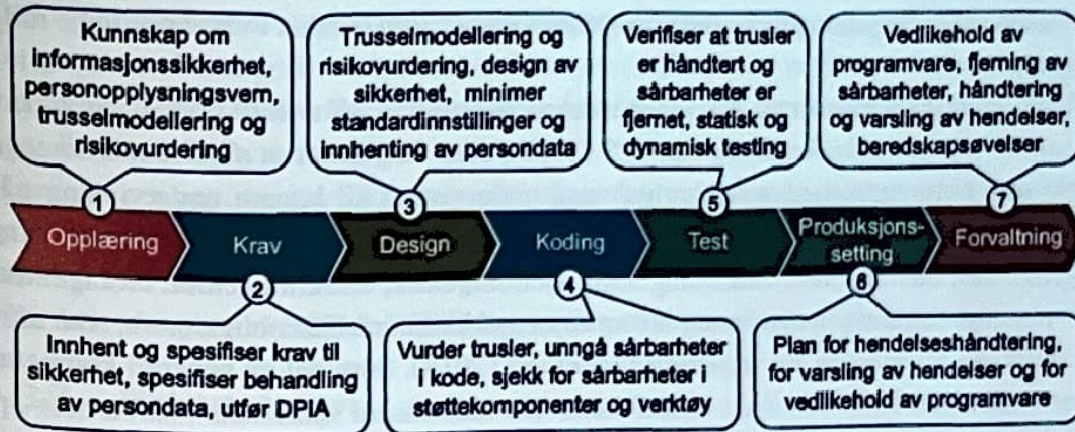
Innebygd personvern er definert i GDPR Art. 25 *Innebygd personvern og personvern som standardinnstilling*, som er beskrevet i avsnitt 10.7.3. Hovedprinsippene for innebygd personvern i henhold til GDPR Art. 25 er å minimere innsamling og behandling av persondata i forhold til formålet med applikasjonen, og at applikasjoner som standardinnstilling ikke skal samle inn og behandle persondata uten de registrertes samtykke.

Ettersom GDPR Art. 25 er artikulert i juridisk sjargong som gjør den relativt vanskelig tilgjengelig for utviklere av programvare og applikasjoner, har Datatilsynet publisert en veileder kalt *Programvareutvikling med innebygd personvern*⁴¹ som er mer lettest og samtidig mer utfyllende. Denne veilederen er inspirert av Microsoft SDL ved at den beskriver de samme syv fasene som i tabell 11.1. Det er svært fornuftig at veilederen fra Datatilsynet er harmonisert med Microsoft SDL, fordi begge på en naturlig måte har samme livssyklus, og fordi det gjør det enkelt for organisasjoner å integrere innebygd informasjonssikkerhet og innebygd personvern. Veilederen fra Datatilsynet har inkludert hensyn til personvern i alle syv faser slik at den dekker både innebygd informasjonssikkerhet og personvern. De syv fasene er beskrevet i neste avsnitt.

41 <https://www.datatilsynet.no/regelverk-og-skjema/veiledere/programvareutvikling-med-innebygd-personvern/>.

11.3 De syv fasene av innebygd informasjonssikkerhet

Livssyklusen for programvaresystemer kan beskrives med en prosess bestående av syv faser som kombinerer både Microsoft SDL og Datatilsynets veileder *Programvareutvikling med innebygd personvern*. Denne prosessen er illustrert i figur 11.1.



Figur 11.1. Prosess for innebygd informasjonssikkerhet og personvern.

Hver fase av prosessen i figur 11.1 er beskrevet i avsnittene under. Detaljer om sikker programvareutvikling som dekker fasene Design, Koding og Test er nærmere beskrevet i avsnitt 11.4 om sikker programvareutvikling.

11.3.1 Opplæring

Målsettingen for opplæring er at alle som deltar i utvikling og drift av digitale tjenester og applikasjoner, skal ha basiskunnskap og forståelse for informasjonssikkerhet og personvern samt risiko tilknyttet dette. Det er naturligvis ønskelig at medarbeidere har med seg denne kompetansen fra utdanningen. Hvis medarbeidere mangler nødvendig kompetanse, har arbeidsgiver ansvar for at de ansatte skaffer seg denne kompetansen. Den enkelte ansatte må vite når og hvorfor informasjonssikkerhet og personvern er viktig i sine arbeidsoppgaver, og hva som bør gjøres for å ivareta sikkerhet og personvern.

Dette er egentlig en selvfølge. Som analogi ville det være uforsvarlig å utdanne bygningsarkitekter og -ingeniører uten å gi dem kunnskap om brannsikkerhet, fordi arkitekter og ingeniører da kunne ha bygd brannfeller inn i våre bygninger. På samme måte er det uforsvarlig å utdanne informatikere og dataingeniører uten obligatoriske kurs om informasjonssikkerhet, fordi de ferdigutdannede da nødvendigvis ville bygd en sårbar IKT-infrastruktur.

Dessverre fins det fremdeles mange IT-designere verden rundt som mangler nødvendig kompetanse i informasjonssikkerhet rett og slett fordi det ikke var pensum der de studerte. Denne situasjonen har vært typisk også i Norge. Universiteter og høyskoler har hatt studieprogrammer innen informatikk og IT siden 1980-tallet, men det var først etter år 2000 at disse studieprogrammene så smått begynte å inneholde valgfag innen informasjonssikkerhet.

Utviklingen gikk svært sakte og holdt nesten på å gå bakover før den for alvor skjøt fart etter 2018.

I regjeringens *Nasjonal strategi for informasjonssikkerhet*⁴² (2012) ble ikke informasjonssikkerhet i utdanningen nevnt med et eneste ord. Stortingsmelding nr. 18 (2014–2015) *Konsentrasjon for kvalitet — Strukturreform i universitets- og høyskolesektoren*⁴³ fokuserte blant annet på å redusere kostnader i høyere utdanning ved å konsentrere undervisning av små fagfelt til enkelte læresteder. Informasjonssikkerhet ble ansett å være et lite fagfelt som kun burde undervises ved ett enkelt lærested. Disse planene ble heldigvis stoppet, men det viser ignoransen rundt betydningen av informasjonssikkerhet som hersket i visse politiske miljøer den gangen.

Vi spoler raskt fremover til *Nasjonal strategi for digital sikkerhet*⁴⁴ (2019) og *Nasjonal strategi for digital sikkerhetskompetanse*⁴⁵ (2019), som fremhever at *digital sikkerhet* (nytt begrep som betyr informasjonssikkerhet) skal undervises i all høyere undervisning og på alle læresteder, og til og med i videregående skole og i grunnskolen. I ingeniørutdanningen (byggingeniør, dataingeniør, elektroingeniør, kjemiingeniør, maskiningeniør, bioingeniør og HMS-ingeniør) er kompetanse innen informasjonssikkerhet nå blitt obligatorisk, som uttrykt i *Forskrift om rammeplan for ingeniørutdanning*⁴⁶ (2018). Som del av generell kompetanse krever forskriften blant annet at: «kandidaten kan identifisere sikkerhets-, sårbarhets-, personverns- og datasikkerhetsaspekter i produkter og systemer som anvender IKT.» Denne forskriften sier med andre ord at en betingelse for at et studieprogram i et ingeniørfag skal bli godkjent, er at studentene lærer om informasjonssikkerhet og personvern.

Det skjedde altså en radikal holdningsendring hos norske myndigheter mellom 2015 og 2018. Til slutt forsto regjeringen viktigheten av innebygd sikkerhet i digitaliseringen av samfunnet, og at dette arbeidet må starte med utdanningen.

Opplæring om sikker bruk av internett bør starte allerede når barn begynner å bruke internett. Barn må tidlig lære å se seg for både til høyre og venstre før de går over veien, ellers blir de overkjørt. Metaforisk må barn også lære å se seg for til høyre og venstre på internett, ellers vil de fort bli overkjørt av identitetstyveri, svindel og personvernovertramp.

Mange ungdommer er svært interessert i å utforske hva som er mulig med etisk hacking, og blir ofte flinke i dette. Det er svært viktig at disse ungdommene tidlig lærer hvor grensen går mellom lovlig og ulovlig hacking. Det fins mange eksempler på ungdommer som i utgangspunktet har gode intensjoner med å hacke en virksomhet for å vise virksomheten at den har sårbare systemer, for deretter å bli anmeldt til politiet av den samme virksomheten. Dette vil typisk være svært traumatisk og demotiverende for en ungdom som ellers med sitt talent kunne ha gjort stor nytte og bli verdsatt. For å unngå slike tragiske tilfeller bør ungdom få kunnskap om hvor grensen går for lovlig etisk hacking.

42 <https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-informasjonssikkerhet/id710469/>.

43 <https://www.regjeringen.no/no/dokumenter/meld.-st.-18-2014-2015/id2402377/>.

44 <https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-digital-sikkerhet/id2627177/>.

45 <https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-digital-sikkerhetskompetanse/id2627189/>.

46 <https://www.regjeringen.no/contentassets/389bf8229a3244f0bc1c7835f842ab60/ny-forskrift-om-rammeplan-for-ingeniorutdanning-fastsatt-18.05.18.pdf>.

11.3.2 Krav til informasjonssikkerhet og personvern

Å ta hensyn til informasjonssikkerhet og personvern er et grunnleggende aspekt ved utvikling av systemer, applikasjoner og tjenester. Sikkerhetskrav må kontinuerlig oppdateres for å gjenspeile endringer i nødvendig funksjonalitet, endringer i trussellandskapet og endringer i lover og forskrifter, som beskrevet i avsnitt 1.5. Det optimale tidspunktet for å definere sikkerhetskrav er i den innledende design- og planleggingsfasen, da dette gjør det mulig for utviklingsteamet å integrere sikkerhet på måter som minimerer hvordan det påvirker funksjonalitet og brukeropplevelse. Faktorer som påvirker sikkerhetskravene, er blant annet lovkrav og bransjekrav, beste praksis i industrien, interne standarder og praksis, erfaring fra tidligere hendelser og kjente trusler. Disse kravene bør kartlegges slik at et helhetlig sett med krav kan legges til grunn for systemdesign.

For krav om applikasjonssikkerhet er beste praksis i industrien definert gjennom OWASP Top 10 og OWASP ASVS (Application Security Verification Standard), som beskrives i avsnitt 11.6.2.

For krav om personvern bør GDPR legges til grunn, som beskrevet i kapittel 10.

11.3.3 Sikkert design

Målsettingen med sikkert design er å oppnå et sluttprodukt som er mest mulig herdet og robust mot eksisterende og fremtidige sikkerhetstrusler.

En viktig del av designfasen er å spesifisere «sikre funksjoner», ved at funksjonene er godt designet med hensyn til sikkerhet. For å oppnå dette vil utviklere ofte stole på sikkerhetsfunksjoner, som kryptografi, autentisering, logging osv. I mange tilfeller har valg eller implementering av sikkerhetsfunksjoner vist seg å være så komplisert at design eller implementeringsvalg sannsynligvis vil føre til sårbarheter. Derfor er det avgjørende at designere har god kompetanse i bruk av slike funksjoner, og at disse brukes konsekvent og med en forståelse av beskyttelsen de gir.

For å unngå sårbarheter i det planlagte systemet er det viktig å gjøre trusselmodellering, som betyr å identifisere måter en angriper kan misbruke tilgangspunkter til funksjoner og dataflyt eller andre aspekter ved systemet på. Identifiserte trusler med potensial for å skape sikkerhetshendelser reflekterer at det fins svake punkter og sårbarheter. Etter trusselmodelleringen er neste trinn å foreslå hvordan designet kan forbedres for å fjerne eller redusere sårbarhetene, noe som er ekvivalent med å stoppe identifiserte trusselscenarioer.

11.3.4 Sikker koding

Målsettingen med sikker koding er å unngå at sårbarheter bygges inn i systemet under programvareutviklingen, og at alle sikkerhetsfunksjoner fungerer i henhold til krav og design.

Moderne programvareutvikling benytter i stor grad tredjeparts-komponenter (både kommersiell og åpen kildekode). Når tredjeparts-komponenter velges, er det viktig å forstå hvilken innvirkning en sikkerhetssårbarhet i disse kan ha på sikkerheten til systemet de er integrert i. Det er essensielt å ha oversikt over alle funksjoner, API-er, tredjeparts-bibliotek og moduler som brukes i programvareutviklingen. Komponenter som vurderes som usikre, skal forbyes, og de som er utdaterte eller inneholder kjente sårbarheter, skal oppdateres. Verktøy for kodeskanning kan benyttes for å identifisere sårbare komponenter. Kartlegging av sårbar-

heter i funksjoner og moduler kan for eksempel gjøres med verktøy som OWASP Dependency Check.⁴⁷ Dette verktøyet oppdager kjente, offentliggjorte sårbarheter i programvarebiblioteker som benyttes av et program.

Statisk analyse av kildekoden før kompilering er skalerbar metode for å verifisere at regler for sikker koding følges. Automatiske verktøy for kodeanalyse og kodegjennomgang gjør denne jobben effektivt. I tillegg anbefales det å gjøre en manuell gjennomgang av koden, selv om denne metoden kan være tidkrevende. Identifiserte forbudte funksjoner kan eventuelt erstattes med sikre alternativer.

Fra et personvernperspektiv bør koden sjekkes for å deaktivere unødig sporing, logging og innsamling av personopplysninger.

11.3.5 Sikkerhetstesting av programvare

Målsettingen med sikkerhetstesting er å avdekke sårbarheter som er forblitt uoppdaget gjennom design og kodefasene slik at disse kan fjernes. Gjennom sikkerhetstesting oppnås større visshet om at koden ivaretar sikkerhet og personvern på tilstrekkelig måte. Det fins ulike former for testing; dynamisk testing, fuzz-testing og penetrasjonstesting beskrives nedenfor.

Dynamisk testing/sårbarhetsanalyse

Dynamisk testing av den fullstendige programvaren sjekker funksjonaliteten som først blir synlig når alle komponenter er integrert og kjører sammen. Dynamisk testing gjøres hovedsakelig ved å bruke verktøy, men også ved manuell gjennomgang, som analyserer hvordan programvaren oppfører seg i ulike situasjoner. Testingen skal for eksempel verifisere at brukerne kun får tilgang til den informasjonen og funksjonaliteten de er autorisert for, og at forsøk på å tilegne seg uautorisert informasjon logges som sikkerhetsfeil. Typiske sårbarheter som bør testes mens programvaren kjøres, er XSS (Cross-Site Scripting) og SQL-injeksjon, som beskrives nærmere i avsnitt 11.7.

Fra et personvernperspektiv er det relevant å teste økthåndtering, tilgangskontroll og bruk av informasjonskapsler for å verifisere at personopplysninger ikke kan hentes ut via brukere som ikke er logget inn.

Penetrasjonstesting

Penetrasjonstesting, ofte kalt *pentesting*, er å gå et skritt videre etter sårbarhetsanalyse. En penetrasjonstest er et autorisert simulert angrep utført for å evaluere sikkerheten til systemet. Testen utføres for å identifisere sårbarheter, og deretter potensialet for angriper til å utnytte sårbarhetene for å skaffe tilgang til systemets funksjoner og data. Begrepet *etisk hacking* er omtrent synonymt med penetrasjonstesting. Pentesting er nærmere beskrevet i avsnitt 17.3.

Sikkerhets- og pentesting krever også en vurdering av om et system kun har testdata eller om det har produksjonsdata med faktiske personopplysninger. Med andre ord: Sikkerhets- og penetrasjonstesting kan være en personvernutfordring i seg selv.

47 <https://owasp.org/www-project-dependency-check/>.

Fuzz-testing

Fuzz-testing betyr å fremprovosere feil i programvaren ved å gi korrupte inputverdier i form av tilfeldig og misformet data i alle mulige input-felt til programvaren. Dette gjøres ved bruk av automatiske verktøy, som også analyserer hvordan programvaren feiler. Dersom programvaren har flere grensesnitt, bør hvert enkelt av dem testes, både enkeltvis og hvis mulig i kombinasjon.

Det kan nevnes at fuzz-testing også er måten angripe oppdager nulldagssårbarheter som kan benyttes til å lage potente angrepsverktøy. Fuzzing utgjør en hel industri der aktive deltagere er både programvareutviklere og trusselaktører, samt aktører som kun har som mål å selge sårbarheter til programvareutviklere eller trusselaktører, avhengig av hvem som betaler mest, og aktørens etiske holdning.

11.3.6 Produksjonssetting

Produksjonssetting er en viktig fase og milepel i et systems livssyklus. To viktige trinn i denne fasen er å beskrive en plan for vedlikehold og hendelseshåndtering samt å formelt godkjenne at programvaren settes i produksjon.

Plan for drift, vedlikehold og hendelseshåndtering

Programvare må driftes og vedlikeholdes kontinuerlig. Før produksjonssetting må det defineres en prosedyre for drift som inkluderer oppdatering og patching både av egenutviklet programvare og av tredjeparts-kode. Det skal etableres en prosedyre for avviksrapportering og hvordan avvik følges opp.

Før produksjonssetting må det også etableres en plan for hendelseshåndtering relatert til programvaren. Dette temaet er også beskrevet i avsnitt 16.4. Planen bør definere ressurser eller responsmiljø som kan håndtere hendelser. Planen bør også beskrive håndtering av hendelser som følge av sårbarheter i kode arvet fra tredjeparter.

Responskapasiteten bør defineres ut fra kritikaliteten. For eksempel vil programvare relatert til akuttbehandling innen helse sannsynligvis kreve rask respons 24/7. Kanaler for varsling av hendelser skal defineres i planen. Sikkerheten i selve varslingskanalene bør også vurderes i henhold til sensitiviteten av innholdet i varslinger. Dersom hendelsen omfatter konfidensialitets-, integritets- eller tilgjengelighetsbrudd relatert til personopplysninger, skal virksomheten varsle Datatilsynet innen 72 timer og den registrerte umiddelbart.

Planen bør definere kriterier for å klassifisere ulike hendelser. Håndtering av en hendelse kan for eksempel være å detektere, analysere, rapportere, håndtere og normalisere. Videre bør planen beskrive logging av data relatert til hendelseshåndteringen, inkludert hvilke føringer personvernregelverket legger for dette. Til slutt bør planen omfatte rutiner for evaluering av selve hendelseshåndtering («lessons learned»), for å støtte kontinuerlig forbedring av prosessen rundt hendelseshåndtering.

Formell godkjenning av produksjonssetting

Forut for formell godkjenning av produksjonssetting bør det verifiseres og dokumenteres at alle krav til sikkerhet og personvern er oppfylt, og at identifiserte sårbarheter er fjernet i tilstrekkelig grad.

Virksomheten må definere hvem som har godkjenningsmyndighet. Sikkerhetsleder eller tilsvarende rolle er ansvarlig for å godkjenne at sikkerhetskrav er implementert og fungerer

etter hensikten. Personvernombud eller tilsvarende rolle er ansvarlig for å godkjenne at alle definerte personvernkrav er tilfredsstillt.

All relevante data og dokumentasjon fra hele utviklingsløpet skal arkiveres. Dette er viktig for å opprettholde kvalitet i arbeidet med informasjonssikkerhet og personvern, og for å ha et grunnlag for revisjon eller tilsyn.

11.3.7 Forvaltning

Forvaltning av IT-systemer består av mange ulike aktiviteter. Disse aktivitetene kan deles inn i to hovedkategorier, der *drift og vedlikehold* er den ene og *avviks- og hendelseshåndtering* er den andre. Disse er beskrevet nedenfor.

Drift og vedlikehold av programvaren

Prosedyrer og rutiner for drift og vedlikehold av programvaren skal følges. Det inkluderer blant annet rutiner for hvordan personvern og sikkerhet skal ivaretas over tid. Etter som programvaren videreutvikles, kan det være nødvendig å gjenta sikkerhetstester, sårbarhetsanalyser og penetrasjonstesting av programvare, infrastruktur og nettverk. Det bør også gjennomføres regelmessige revisjoner for å dokumentere samsvar med relevante regelverk med krav om informasjonssikkerhet. Generelt bør organisasjonen ha et styringssystem for informasjonssikkerhet (ISMS: Information Security Management System) som omfatter anskaffelse, forvaltning, drift og vedlikehold av programvare. ISMS beskrives i kapittel 12.

Feil som oppdages gjennom avviksrapportering eller på andre måter, må følges opp rutinemessig. Logging er viktig for monitorering av systemer og nettverk, men kan produsere enorme mengder data og kan i seg selv utgjøre et brudd på personvern dersom det ikke er beskrevet og vurdert i planen for behandling av personopplysninger. Derfor er det viktig å definere hva som kan og skal logges, og at loggene sikres. Å logge medfører en forpliktelse om å faktisk benytte loggene for trusselletterretning og for å benytte loggene til å følge opp hendelser. Selv om logging av personopplysninger i utgangspunktet er lovlig, er det viktig å påse at de ikke eksporteres til andre applikasjoner og blir gjort tilgjengelig for andre enn de som har tjenstlig behov.

Virksomheten må være forberedt på å håndtere hendelser, avvik og angrep som kan medføre konfidensialitets-, integritets- og tilgjengelighetsbrudd relatert til personopplysninger. Den bør ha et responssenter som kan håndtere hendelser og gi ut oppdateringer, veiledning og informasjon til brukere og berørte.

Avviks- og hendelseshåndtering

Avvik og hendelser skal rapporteres via de kanaler som er beskrevet i planen for hendelseshåndtering. Det skal være enkelt for brukere av programvaren å rapportere inn feil, sårbarheter og mangler, slik at programvaren kontinuerlig kan forbedres og videreutvikles.

Plan for hendelseshåndtering skal i utgangspunktet følges, men når en akutt hendelse oppstår, kan hendelsens karakter medføre endringer i hvordan planen følges. Selve planen skal vedlikeholdes og forbedres etter behov. Responsteamet skal etter planen vite hvem de skal kontakte etter behov for å utføre nødvendige oppgaver. Planen bør også definere hvilke prioriteringer som gjelder, og hvordan beslutninger skal tas når det virkelig er krise. For at

dette skal fungere knirkefritt i praksis, trenger de ansatte regelmessige øvelser. Evaluering av hendelser bør følge planen.

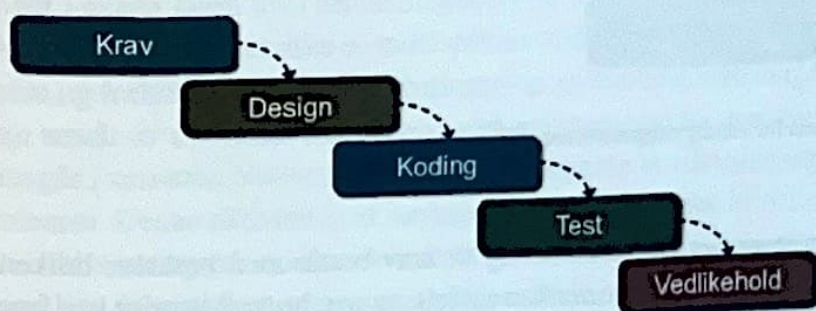
En mer detaljert beskrivelse av avviks- og hendelseshåndtering gis i kapittel 16.

11.4 Sikker programvareutvikling

Det fins mange ulike metodikker for programvareutvikling, der *fossefallmetoden* er en tradisjonell og gammeldags metodikk, mens *smidig programvareutvikling* er en moderne metodikk. Disse er kort beskrevet nedenfor.

11.4.1 Fossefallmetoden

Fossefallmetoden for programvareutvikling består av fem sekvensielle faser, der hver fase avhenger av resultatene fra den forrige fasen. Denne metoden er illustrert i figur 11.2. Legg merke til at fasene i fossefallmetoden er de samme som fem av fasene i modellen for innebygd informasjonssikkerhet og personvern beskrevet i avsnitt 11.3.



Figur 11.2. Fossefallmetoden for programvareutvikling.

Betegnelsen «fossefall» betyr metaforisk at dette er en enveisprosess, på tilsvarende måte som at vann ikke renner oppover. Hvis nødvendig er det naturligvis mulig å gå tilbake til en tidligere fase for å gjøre endringer, men det er vanskelig og medfører relativt store kostnader.

I programvareprosjekter er det nesten alltid behov for å gjøre endringer underveis. Etter som fossefallmetoden per definisjon ikke er iterativ og ikke tar hensyn til behov for å gjøre endringer underveis, har den en tendens til å være rigid og ufleksibel. Det er likevel en velstrukturert metode, som ble tatt i bruk allerede på 1970-tallet for utvikling av programvare.

Sikker programvareutvikling i henhold til Microsoft SDL (beskrevet i avsnitt 11.1) passer direkte sammen med fossefallmetoden. Med andre ord er beste praksis for sikker programvareutvikling med fossefallmetoden å følge Microsoft SDL.

11.4.2 Smidig programvareutvikling

Smidig programvareutvikling er et paraplybegrep som dekker forskjellige metoder for programvareutviklere som tar hensyn til kontinuerlige endringer basert på spesifikke prinsipper som ble skissert i *Manifestet for smidig programvareutvikling* (Manifesto for Agile Soft-

ware Development).⁴⁸ Hovedprinsippene består av tidlig og kontinuerlig levering av programvaremoduler, enkel håndtering av endringer, hyppig levering av fungerende produksjonsprogramvare, oppdragsgivere og utviklere som jobber sammen, motivering av utviklere og rikelige ressurser til å lykkes. Smidig utvikling fokuserer på samarbeid ansikt-til-ansikt og skulder-til-skulder samt måling av fremgang gjennom fungerende programvare. Smidig utvikling antar at et selvorganisert team er best egnet til å utvikle gode arkitekturer, krav og design. Smidig utvikling oppmuntre til selvinnsikt og evne til å justere og forbedre prosessen deretter. Figur 11.3 illustrerer en generell prosess for smidig programvareutvikling.



Figur 11.3. Prosess for smidig programvareutvikling.

Planlegging av systemet og spesifisering av krav består av å beskrive brukerhistorier som systemet skal støtte. Brukerhistorier kan endres, og nye brukerhistorier kan legges til. Utviklingen foregår i iterative sykluser som ofte kalles en sprint, med typisk varighet fra en uke til en måned. For hver sprint velges en eller flere brukerhistorier. I løpet av en sprint skal det gjøres design, planlegging, koding, testing, utgivelse og vurdering av de nye modulene i programvaren. Når det ikke lenger gjenstår brukerhistorier å implementere, er systemet ferdig.

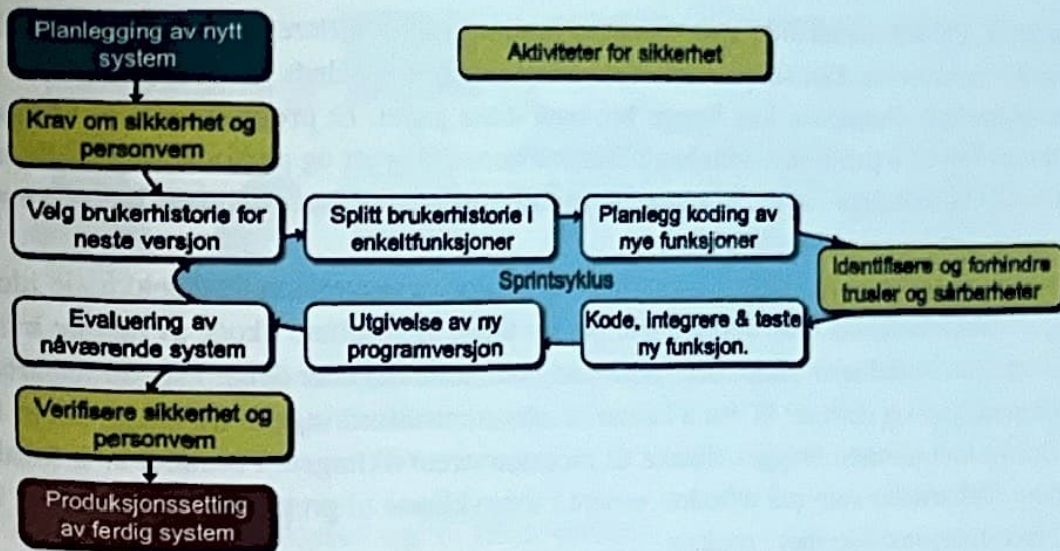
11.4.3 Sikker smidig programvareutvikling

For å oppnå innebygd sikkerhet i smidig programvareutvikling passer det ikke å følge prosessen med syv faser fra figur 11.1 direkte, siden den ikke er iterativ. Det som trengs, er å utvide den iterative prosessen for *smidig programvareutvikling* til å inkludere sikkerhetsaktiviteter, på samme måte som Microsoft SDL utvider fossefallmetoden til å inkludere sikkerhetsaktiviteter. En slik utvidet prosess for sikker smidig programvareutvikling er illustrert i figur 11.4.

De gule fasene representerer sikkerhetsaktiviteter i prosessen for sikker smidig programvareutvikling. Det er hovedsakelig tre tilleggsaktiviteter som fokuserer på sikkerhet:

- «Krav om sikkerhet og personvern» er samme aktivitet som i fase 2 i prosessen for innebygd informasjonssikkerhet og personvern i figur 11.1. Denne innledende aktiviteten

48 <https://www.agilealliance.org/agile101/the-agile-manifesto/>.



Figur 11.4. Prosess for sikker smidig programvareutvikling.

skal sørge for at grunnleggende krav til sikkerhet og personvern kartlegges. Utførelse av DPIA inngår i denne fasen hvis behandlingen av persondata anses å medføre høy risiko (GDPR Art. 35 nr. 1), men er ikke et standardkrav ved all behandling av persondata.

- «Identifisere og forhindre trusler og sårbarheter» er en aktivitet som inngår i hver sprint. Aktiviteten består av trusselmodellering og sårbarhetsanalyse for den nye funksjonaliteten som inngår i sprinten. Nødvendige tiltak skal sørge for at relevante trusler og sårbarheter elimineres. Denne aktiviteten er nærmere beskrevet i avsnitt 11.5.1.
- «Verifisere sikkerhet og personvern» er en aktivitet som utføres når systemet ellers anses å være komplett, før systemet settes i produksjon. Mens hver sprint inneholder en aktivitet for testing, skal det gjøres en avsluttende test og vurdering av systemet for å verifisere at krav om sikkerhet og personvern er oppfylt.

Tilleggsaktivitetene for sikkerhet gjør nødvendigvis at sikker smidig programvareutvikling er litt mindre smidig enn tradisjonell smidig programvareutvikling. Imidlertid er sikkerhet og personvern ufravikelige krav for bærekraftig programvareutvikling i en kontekst av økende eksponering mot cybertrusler, noe som betyr at den prisen må vi betale.

11.4.4 Sikkerhets-champion

Selv om det bør forventes at alle deltagere i et team for (sikker) smidig programvareutvikling har kompetanse i informasjonssikkerhet, er det kanskje for mye å forvente at alle skal være eksperter i å identifisere trusler og sårbarheter. Derfor er det vanlig å utpeke én person til å ha rollen som *sikkerhets-champion*.

I tillegg til å være medlem i utviklingsteamet er en sikkerhets-champion den personen i teamet som har et særskilt ansvar for å se programvaren fra perspektivet til de som jobber med sikkerhetsadministrasjon i IT-drift. Dette kan være en utfordrende rolle, gitt det tradisjonelle skillet mellom IT-drift og programvareutvikling.

Folk som jobber med sikkerhet i IT-drift, har vanligvis en begrenset forståelse av hvordan programvareutviklere jobber, og deres utfordringer med å lage programvare som er fri for

sårbarheter. På den annen side undervurderer programvareutviklere ofte hvordan feil i kode-linjene de produserer, kan skape sikkerhetsutfordringer for IT-drift.

En sikkerhets-champion kan bygge bro over dette gapet. Et programvareutviklingsteam kan øke evnen til å produsere innebygd informasjonssikkerhet og personvern hvis de har en sikkerhets-champion på laget. Å jobbe i team betyr nettopp at hver deltager har ulike roller, fordi det er mer rasjonelt og effektivt.

Fordeler med å ha en dedikert sikkerhets-champion er raskere og mer dekkende identifisering av sikkerhetshull, som dermed kan fjernes tidlig og resultere i kode av høyere kvalitet. Det er også en fordel at en sikkerhets-champion har innblikk i eller deltar i sikkerhetsarbeidet i administrasjon og drift av IT for å kunne se sikkerhetsutfordringene fra begge sider. Erfaring derfra kan dermed bringes tilbake til programvareutviklingen. Formålet er å forhindre kostbare sårbarheter som må utbedres senere i livssyklusen til programvaren. Dette er innebygd informasjonssikkerhet i praksis.

11.5 Identifisering av trusler under programvareutvikling

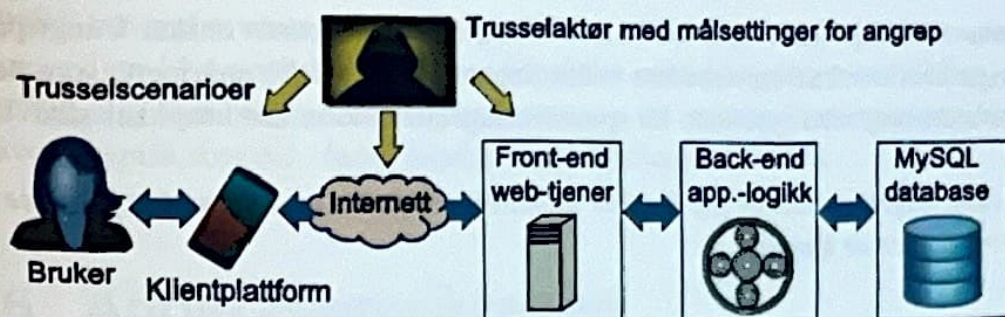
Mange trusler og sårbarheter er først mulig å identifisere under implementering og koding av systemer. I sikker smidig programvareutvikling gjøres trusselmodellering som del av hver sprintsyklus, som illustrert med aktiviteten til høyre i figur 11.4. Aspekter ved denne aktiviteten beskrives i avsnittene nedenfor.

11.5.1 Trusselmodellering

Trusselmodellering består av å kartlegge mulige måter et system eller en prosess kan misbrukes og angripes på.

Et system kan i utgangspunktet angripes på uendelig mange måter, men ikke alle er like relevante og plausible. Utfordringen er nettopp å identifisere de mest relevante angrepsmåtene. Angrep kan skje gjennom alle grensesnitt til systemet og omgivelsene systemet er berørt av. Figur 11.5 viser et eksempel med en front-end web-tjener og tilkoblet omgivelse, som har en rekke grensesnitt som et angrep potensielt kan gå gjennom.

Et utviklingsteam må gjøre så godt de kan for å identifisere relevante trusselscenarioer (mulige angrepsmåter), noe som kan være utfordrende. En nyttig tilnærming er å *tenke som en angriper* og beskrive angriperens målsettinger som *angriperhistorier*, på samme måte som at brukerens målsettinger kan beskrives som *brukerhistorier*. De neste to avsnittene beskriver likhetstrekk mellom brukerhistorier og bruksmønster (use-caser) på den ene siden og angrephistorier og trusselscenarioer på den andre.



Figur 11.5. Mulige angrep gjennom grensesnitt til et system og dets omgivelser.

11.5.2 Brukerhistorier og bruksmønster

Kravspesifikasjon i smidig programvareutvikling er i stor grad basert på å beskrive brukerhistorier. For hver sprintsyklus velger utviklingsteamet en eller flere brukerhistorier som skal implementeres.

- En *brukerhistorie* betrakter systemet fra brukerens perspektiv og beskriver hva brukeren ønsker å utføre. Dette kan uttrykkes med den generelle setningen nedenfor:

Som [bruker] ønsker jeg [funksjon] for å oppnå [resultat].

Vi ser for oss at utviklingsteamet jobber med å implementere et nettapotek kalt *ApoNett*. Brukerhistorier kan representere målsettinger for kunder eller for ansatte, som alle ønsker å utføre ulike ting med systemet. For kunder kan en spesifikk brukerhistorie uttrykkes slik:

Som registrert kunde hos ApoNett ønsker jeg å kunne bestille reseptbelagte medisiner.

- Et *bruksmønster* (use case) betrakter systemet fra designerens og utviklerens perspektiv. Et bruksmønster er en beskrivelse av et sett med interaksjoner mellom moduler i et system, mellom systemer eller mellom systemer og aktører, som vist i figur 11.5. Resultatet av å utføre et bruksmønster er at det oppnås en målsetting for en aktør eller et system.

11.5.3 Angriperhistorier og trusselscenarioer

Hvis man ser bort fra de dystre aspektene ved en trusselaktør, og kun ser på trusselaktøren som en entitet med målsettinger, kan disse målsettingene beskrives som *angriperhistorier*, som i strukturen ligner brukerhistorier.

- En *angriperhistorie* betrakter systemet fra angriperens perspektiv og beskriver hva angriperen ønsker å utføre. Dette kan uttrykkes med den generelle setningen nedenfor:

Som [angriper] ønsker jeg [funksjon] for å oppnå [resultat].

Vi antar at nettapoteket ApoNett er satt i drift, og at angriperen ønsker å angripe dette. Angriperhistorier kan representere målsettinger for potensielle angripere, som ønsker å utføre ulike ting med systemet. En spesifikk angriperhistorie kan uttrykkes slik:

Som angriper ønsker jeg å stjele identiteter til brukere av ApoNett for å se hvilke medisiner de kjøper.

- Et trusselscenario (misbruksmønster eller misuse case) betrakter systemet fra perspektivet til en trussel ekspert som designer måter et system kan angripes på. Et trusselscenario er en beskrivelse av et sett med interaksjoner mellom moduler i et system, mellom systemer eller mellom systemer og aktører, som vist i figur 11.5, der deler av interaksjonene kontrolleres av en trusselaktør. Resultatet av et trusselscenario er at trusselaktøren oppnår en målsetting, som fra offerets perspektiv er en sikkerhetshendelse med negative konsekvenser.

Ved å betrakte et trusselscenario på samme måte som et bruksmønster kan det være enklere for utviklingsteamet å identifisere ulike trusselscenarioer. En annen metode for å identifisere trusler er STRIDE, som beskrives i neste avsnitt.

11.5.4 STRIDE trusselmodellering i programvareutvikling

STRIDE er en tilnærming for trusselmodellering som utføres som del av programvareutviklingen, typisk sammen med design eller koding. STRIDE er utformet av Microsoft og er relativt utbredt i programutviklingsmiljøer. Ordet STRIDE er forbokstavene for seks kategorier av sikkerhetstrusler, som vist i tabell 11.2.

Tabell 11.2. STRIDE trusselmodellering

Forbokstav	Trusselkategori	Beskrivelse	Sikkerhetsbrudd
S	Spoofing Identitetstyveri	Kan en angriper få uautorisert tilgang ved å stjele en annens identitet?	Brudd på autentisitet
T	Tampering Tukling	Kan en angriper endre data som prosesseres av systemet?	Brudd på integritet
R	Repudiation Benekting	Kan en angriper benekte misbruk uten at vi kan bevise misbruket?	Brudd på ubenektelighet
I	Information disclosure Datatyveri og -lekkasje	Kan en angriper få tilgang til konfidensielle og personlige data?	Brudd på konfidensialitet
D	Denial of service Tjenestenekt	Kan en angriper blokkere eller minske tilgjengeligheten til systemet?	Brudd på tilgjengelighet
E	Elevation of privilege Utvidede tilganger	Kan en angriper oppnå utvidede tilganger som en privilegert bruker?	Brudd på tilgangskontroll

Høyre kolonne i tabell 11.2 viser hvilket sikkerhetsmål som hver trussel forårsaker et brudd på. STRIDE er ment å være til hjelp når et utviklingsteam forsøker å identifisere trusler mot et system. Sagt på en annen måte er STRIDE ment som en hjelp til å svare på spørsmålet om hva som kan gå galt i systemet man jobber med.

STRIDE kan typisk brukes som del av aktiviteten «Identifisere og forhindre trusler og sårbarheter» i figur 11.4, som viser prosessen for sikker smidig programvareutvikling. STRIDE kan selvfølgelig også brukes sammen med prosessen for innebygd informasjonssikkerhet og personvern, typisk som del i fase 3 (design) og 4 (koding) i figur 11.1.

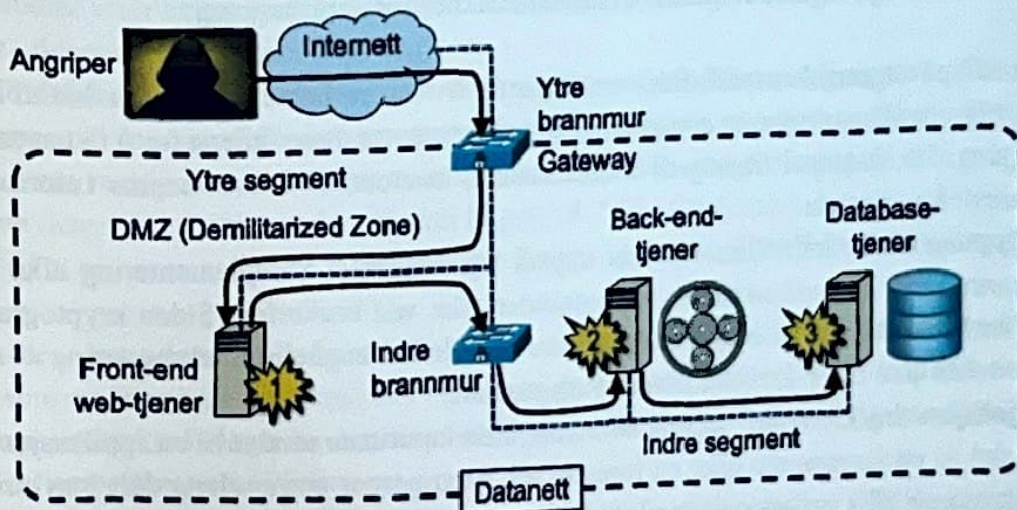
11.6 Applikasjonssikkerhet

Applikasjonssikkerhet fokuserer på sikkerhet i klient- og tjenerapper som kommuniserer over internett. Som oftest kommuniserer applikasjoner over HTTP-protokollen med portnummer 80 eller HTTPS-protokollen med portnummer 443. Kontinuerlig innovasjon produserer stadig mer avanserte online-tjenester som kommuniserer på denne måten, og det er en stor utfordring å opprettholde adekvat sikkerhet når kompleksiteten øker.

11.6.1 Web-applikasjoners eksponering mot trusler

I datanett som tillater trafikk med HTTP og HTTPS, må den ytre brannmuren nødvendigvis ha åpne portnummer 80 og 443, som betyr at applikasjoner på front-end webtjenere er direkte eksponert mot hele internett gjennom disse portene. Samtidig kommuniserer front-end webtjenere med back-end-tjenere og databaser. Selv om den trafikken typisk filtreres gjennom interne brannmurer, vil en intern brannmur typisk slippe gjennom trafikk fra front-end webtjenere til back-end-tjenere og databaser fordi det er en nødvendig del av applikasjonenes virkemåte.

Hvis det fins sårbarheter i applikasjoner i front-end webtjeneren, er det lett å se for seg hvordan en angriper kan utnytte slike sårbarheter og deretter angripe back-end-tjenere, som vist i figur 11.6.



Figur 11.6. Angrep gjennom sårbarheter i web-applikasjoner.

Klienter som kommuniserer med applikasjonstjenere, er også eksponert mot denne typen trusler fordi de kan angripes når de kontakter sårbare applikasjoner.

Eksempel på angrep som bygger på mønsteret i figur 11.6, er bl.a. SQL-injeksjon og XSS beskrevet i avsnitt 11.7.

Flere initiativer har tatt fatt i den store utfordringen med å opprettholde god sikkerhet i internettapplikasjoner, der OWASP nok er den mest prominente.

11.6.2 OWASP: The Open Web Application Security Project

OWASP (*Open Web Application Security Project*)⁴⁹ er en ideell organisasjon som har som mål å forbedre sikkerheten til applikasjoner og tjenester på internett. Gjennom åpenhet skal organisasjoner og sluttbrukere lett kunne få råd, veiledning og verktøy for å styrke applikasjonssikkerhet og ta informerte beslutninger om reelle sikkerhetsrisikoer i applikasjoner.

Bedrifter, utdanningsinstitusjoner og enkeltpersoner fra hele verden er involvert i OWASP-samfunnet, som produserer fritt tilgjengelig informasjonsmateriell, metoder, verktøy og teknologier.

OWASP har en rekke parallelle prosjekter, der noen har pågått lenge og er svært modne, mens andre er mer umodne. Det er opp til frivillige å starte og delta i prosjekter.

To av de mest modne prosjektene i OWASP er *OWASP Top 10* og *OWASP ASVS*.

11.6.3 OWASP Top 10

OWASP Top 10 er en veileder som rangerer de ti mest kritiske sikkerhetsrisikoene for nett-applikasjoner. Veilederen gir også råd om hvordan sårbarhetene og risikoene kan forhindres. Veilederen er utarbeidet av sikkerhetsekspertter fra hele verden. Risikoen er rangert og basert på hyppigheten av oppdagede sikkerhetsfeil, alvorlighetsgraden av sårbarhetene og potensielle konsekvenser. Formålet med veilederen er å forklare de mest utbredte sikkerhetsrisikoene og hvordan de kan forhindres, slik at utviklere av applikasjoner kan unngå sårbarhetene og minimere risikoene. Med jevne mellomrom på noen år foretar OWASP en revisjon av listen over hva de anser som de ti mest alvorlige sikkerhetsrisikoene. Den siste revisjonen ble foretatt i 2021, og rangerer følgende sikkerhetsrisikoer for applikasjoner:

1. **Brudd på tilgangskontroll:** Begrensninger for hva autentiserte brukere har lov til å gjøre, blir ofte ikke håndhevet riktig. Angriperen kan utnytte disse feilene for å få uautorisert tilgang, for eksempel tilgang til andre brukeres kontoer, til å lese sensitiv informasjon eller til å endre data.
2. **Kryptografiske feil:** Slike feil kan oppstå ved svakheter i implementering eller konfigurering av kryptofunksjoner, kryptonøkler eller ved brukerfeil. Siden kryptografiske systemer skal beskytte sensitive data, fører slike feil uunngåelig til eksponering av sensitive data som f.eks. kredittkortnumre og passord.
3. **Injeksjon:** Injeksjonsfeil oppstår når manipulert input-data sendes til en applikasjon som en del av en kommando eller en forespørsel. Angriperens manipulerede data kan lure applikasjonen til å utføre utilsiktede og uautoriserte handlinger. Forskjellige varianter av injeksjon er SQL-, NoSQL-, OS- og LDAP-injeksjon.
4. **Usikkert design:** Denne kategorien representerer manglende, utilstrekkelig eller svakt sikkerhetsdesign. Usikkert design er ikke det samme som usikker implementering, de

⁴⁹ <https://owasp.org/>.

har forskjellige årsaker og må derfor unngås på forskjellige måter. Et sikkert design kan fortsatt ha implementeringsfeil som fører til sårbarheter som kan utnyttes. Ei heller kan et usikkert design fikses med en perfekt implementering. Sikkert design er en kultur og metodikk som kontinuerlig evaluerer trusler og sørger for at systemet eller applikasjonen er designet for å motstå kjente angrepsmetoder.

5. **Feilkonfigurert sikkerhet:** Feilkonfigurert sikkerhet er svært vanlig, og vanskelig å unngå helt. Det kan være en usikker standardkonfigurasjon som ikke endres, åpen skylagring, feilkonfigurerte HTTP-hoder eller feilmeldinger som avslører sensitiv informasjon.
6. **Sårbare og utdaterte komponenter:** Dette kan være utdaterte moduler, programbiblioteker og API-er som mangler sikkerhetsoppdateringer, eller der produsenten har sluttet å foreta oppdateringer. Mangelfull oppdatering og lang oppdateringssyklus kan ofte føre til sårbare komponenter. I tilfelle av en kjent sårbarhet som ikke patches, vil organisasjonen være sårbar i lang tid.
7. **Brudd på identifisering og autentisering:** Autentisering og styring av økter implementeres ofte feil, slik at angripere for eksempel kan kompromittere passord, nøkler eller informasjonskapsler for å stjele identiteter eller ta over kontrollen av en økt.
8. **Brudd på programvare- og dataintegritet:** Slike sikkerhetsfeil kan oppstå når applikasjonen eller infrastrukturen ikke beskytter mot integritetsbrudd. Et eksempel på dette er når en applikasjon henter plugins, biblioteker eller moduler fra upålitelige kilder og innholdsleveringsnettverk (CDN). Slike brudd kan også oppstå ved automatisk oppdatering av programvare uten å autentisere den nye versjonen. Dette gjør det mulig for angripere å laste opp sine egne oppdateringer. Løsningen på denne risikoen er typisk å anvende digital signatur av data og programvare.
9. **Utilstrekkelig sikkerhetslogging og -monitorering:** Utilstrekkelig logging og monitorering, kombinert med manglende eller ineffektiv integrering med hendelsesrespons, gjør det mulig for angripere å gjøre ugagn uten å bli oppdaget eller bli stilt til regnskap. Studier viser at gjennomsnittlig tid til å oppdage en sikkerhetshendelse er over 200 dager fra tidspunktet angrepet først begynte.
10. **Forfalskning av forespørsel mot server (Server-Side Request Forgery):** SSRF er en type angrep som misbruker serveren slik at klienten (som er angriperen) kan hente ut, eller kan manipulere, informasjon som serveren teknisk sett har tilgang til, men som klienten (angriperen) ikke skal ha direkte tilgang til. Ulike tiltak kan forhindre slike feil, f.eks. ved at serveren validerer at alle forespørsler fra klienter er i henhold til sikkerhetspolicy.

Å holde seg oppdatert på de mest kritiske sikkerhetsrisikoer og sårbarheter er svært viktig for alle som utvikler web-applikasjoner og administrerer et nettsted. OWASP Top 10 er et godt utgangspunkt for å skape bevissthet rundt dette temaet, og bør være obligatorisk kunnskap blant alle applikasjonsutviklere.

For å illustrere typiske risikoer beskrevet i OWASP Top 10 beskriver vi SQL-injeksjon og XSS i avsnitt 11.7.

11.6.4 OWASP ASVS

OWASP ASVS (*Application Security Verification Standard*) er en veileder for teknisk sikkerhetstesting, som også definerer en liste over krav til sikker utvikling. Det primære målet for

OWASP ASVS er å definere beste praksis for sikker utvikling og sikkerhetstesting. Standarden fokuserer på tiltak som beskytter mot sårbarheter beskrevet i OWASP Top 10. Veilederen gir grunnlag for å etablere et nivå av tillit til sikkerheten til web-applikasjoner. ASVS kan brukes til følgende:

- *Målestokk for sikkerhet:* Gi applikasjonsutviklere og applikasjonseiere en målestokk for å vurdere graden av tillit med hensyn til sikkerhet som kan legges til deres webapplikasjoner.
- *Veiledning for sikker utvikling:* Gi veiledning til utviklere om hvordan applikasjoner bør bygges for å tilfredsstille krav om sikkerhet.
- *Kravsetting ved anskaffelse:* Gi grunnlag for å spesifisere krav om sikkerhet ved bestilling og innkjøp av applikasjoner.

11.7 Eksempel på angrep mot applikasjoner

Det fins svært mange ulike angrepsmetoder, og trusselaktører jobber kontinuerlig med å utvikle nye. I dette avsnittet beskriver vi to klassiske angrepsmetoder: SQL-injeksjon og en variant av XSS (Cross Site Scripting).

11.7.1 SQL-injeksjon

SQL (Structured Query Language) er et maskinlesbart språk med kommandoer for interaksjon med et *databasehåndteringssystem*, forkortet som *DBMS (Database Management System)*. Et DBMS er programmet som brukes til å håndtere *databaser*, dvs. tabeller og samlinger av strukturerte data. SQL-injeksjon er et angrep mot et DBMS som består av å manipulere SQL-kommandoer til å utføre operasjoner på en database de ikke var ment å gjøre. Angrepet er mulig hvis SQL-kommandoer bygges med parametere som er input fra brukeren. Dersom en angriper vet eller kan gjette hvordan SQL-kommandoen bygges, er det mulig å sende manipulert input-data som gjør at den opprinnelige SQL-kommandoen endres til å bli en angrepskommando. Dette kan gjøre det mulig for angriperen å hente ut sensitive data fra en database, typisk brukernavn, passord og e-postadresser, endre databasen eller få uautorisert tilgang til systemer.

Se for deg en innloggingsprosess der brukeren spesifiserer bruker-ID og passord. Dette resulterer typisk i at applikasjoner bygger opp en SQL-kommando som sendes til DBMS for å sjekke om brukernavn og passord er korrekt. SQL-kommandoen nedenfor er et eksempel:

```
SELECT * FROM users WHERE userid =
'$userid' AND password = '$password'
```

Kommandoen bygges med bruker-input \$userid og \$password, og gjør et oppslag i databasen med navn users som returnerer data for alle treff med riktig kombinasjon av userid og password. Vi antar også at applikasjonen logger brukeren inn hvis DBMS returnerer et treff fra databasen. DBMS returnerer ingen resultater dersom kombinasjonen av userid og password ikke fins i databasen.

La oss anta at angriper oppgir følgende tekst som bruker-ID, som dermed legges i parameteren \$userid:

```
' OR 1=1--
```

Det første tegnet ' er en apostrof som avslutter innkapslingen med apostrofer ved oppbygging av SQL-kommandoen. Det etterfølgende logiske uttrykket OR 1=1 er alltid TRUE (sant), som dermed tolkes som treff ved oppslaget. De to siste tegnene -- (to bindestreker) er metategn som betyr at etterfølgende data skal tolkes som kommentarer. Dermed blir resten av kommandoen kommentert vekk, uansett hva som står der.

Den manipulererte SQL-kommandoen vil dermed se slik ut:

```
SELECT * FROM users WHERE userid =
'' OR 1=1-- ' AND password = '$password'
```

Forespørselen vil gi TRUE (sant) for hver eneste bruker-ID i databasen, og DBMS vil returnere data for alle. Den første bruker-ID-en i databasen er ofte admin-brukeren, slik at angriperen typisk blir logget inn som administrator.

SQL-injeksjon er et velkjent angrep, og samtidig egentlig et løst problem som lett kan forhindres ved standard tiltak. Likevel fins det fremdeles mange web-applikasjoner som er sårbare for SQL-injeksjon, og mange angrep foregår fremdeles på denne måten.

Den vanligste metoden for å forhindre SQL-injeksjon består av å benytte parametriserte kommandoer. En typisk prosess for å bygge parametriserte SQL-kommandoer går som følger:

1. *Forbered:* Først bygger applikasjonen en mal for SQL-kommandoen som sendes til DBMS. Visse parametere er fremdeles uspesifisert (merket «?» nedenfor):

```
SELECT * FROM users WHERE userid = '?' AND password = '?'
```

2. *Kompiler:* Deretter kompilerer DBMS kommandomalen uten å utføre kommandoen. Strukturen i kommandoen er dermed fastlåst og kan ikke manipuleres med injeksjon.
3. *Utfør:* Til slutt binder applikasjonen verdier for parameterne i malen og lar DBMS utføre SQL-kommandoen.

Parametriserte SQL-kommandoer forhindrer SQL-injeksjon fordi verdiene for parameterne legges til etter at malen er kompilert med en fast struktur. Manipulerte input-verdier, slik som i eksemplet ovenfor, ville resultert i en SQL-kommando med forventet struktur, men med parametere som ikke ville gitt noen treff i databasen.

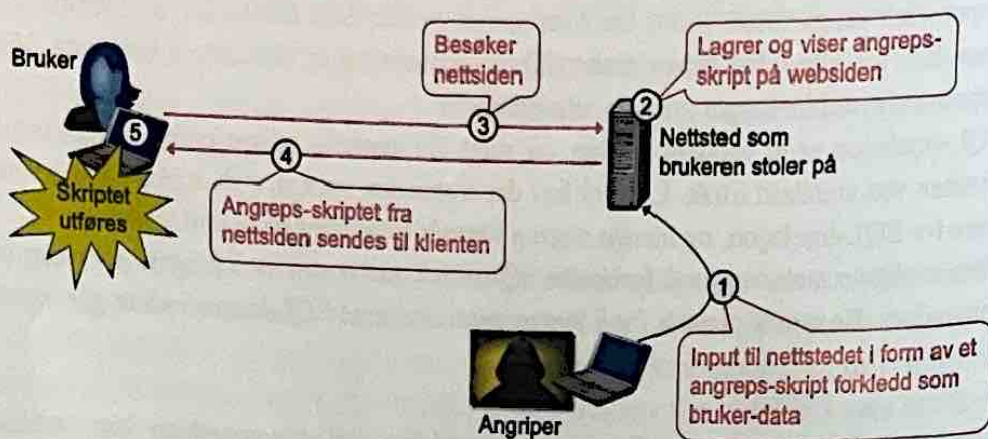
11.7.2 XSS: Cross-Site Scripting

Nettsteder sender ofte JavaScript til klienten for å kunne gi god funksjonalitet på websiden. Det er i utgangspunktet risikabelt fordi JavaScript er aktiv kode som potensielt kan gjøre ugagn på klienten, men det går som regel bra så lenge JavaScript kommer fra nettsteder man kan stole

på. Imidlertid fins det metoder for angripere å lure nettstedet til å sende skadelige JavaScript til klienter, og det er nettopp hva XSS (Cross-site scripting) gjør. Hvis et nettsted (og en nettleser) er sårbare for XSS-angrep, er det mulig for angripere å injisere skadevare i form av JavaScript på klienter bare ved å besøke (sårbare) nettsteder, som kalles drive-by-angrep.

Det fins ulike former for XSS, hvor tre vanlige typer er *persistent (lagret) XSS*, *reflektert XSS* og *DOM-basert XSS*. Som et eksempel beskrives persistent XSS nedenfor.

Se for deg et nettsted der brukere kan gi input som blir lagret synlig for andre brukere. Dette kan for eksempel være et nettsted der brukere kan stille spørsmål og gi svar til hverandre. En angriper kan forsøke å sende et JavaScript som svar på et spørsmål. Hvis nettstedet er sårbart for XSS, vil JavaScriptet bli lagret og gjort synlig for alle som aksesserer nettstedet. Alle klienter/nettlesere som besøker nettstedet, vil dermed motta JavaScriptet. Hvis nettleseren ikke er i stand til å filtrere bort JavaScriptet, vil skriptet bli utført. Dette er illustrert med et enkelt scenario i figur 11.7.



Figur 11.7. Persistent XSS.

Det fins intet enkelt tiltak som forhindrer alle typer XSS-angrep. Generelt gjelder det at både tjener og klient filtrerer input for å beskytte seg mot manipulererte data og skadelige skript. OWASP Top 10 beskriver i detalj metoder for å unngå XSS-sårbarheter.

11.8 Sikkerhet i skyen

Å bruke «skyen» som plattform blir etter hvert den vanligste måten å tilby og bruke digitale tjenester på. Derfor er det viktig å forstå hvilke konsekvenser det har for informasjonssikkerhet å legge tjenester i skyen. Før vi stuper inn i sikkerhetsaspektene, er det nyttig å forklare sentrale begreper rundt skyinfrastrukturer.

11.8.1 Skytjenester

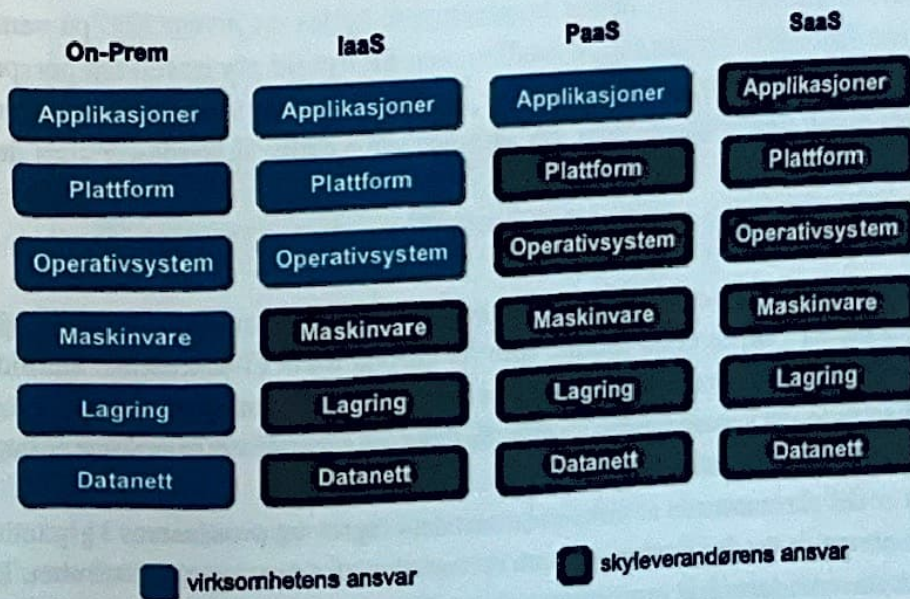
Sourcing er valg av hvem som skal utføre en arbeidsoppgave. *Sourcing-strategi* er altså strategien som ligger til grunn for hvordan virksomheten gjør slike valg. *Outsourcing* betyr at

virksomheter skiller ut arbeidsoppgaver de tidligere selv har utført, til tredjeparter, som for eksempel produksjon av deler til et produkt eller montering av ferdige produkter. Det meste av IT-tjenester kan i prinsippet outsources, som f.eks. systemutvikling, administrasjon, drift og vedlikehold av maskinvare, programvare og applikasjoner. Tradisjonelt ble slike tjenester levert av konsultentselskaper basert på en leveransemodell med spesialtilpassede kontrakter, dedikerte IT-ressurser og en nær forretningsforbindelse mellom kunde og leverandør.

Skytjenester har mange likhetstrekk med tradisjonell outsourcing av IT-tjenester, men skytjenester følger en mer smidig leveransemodell. Det særegne med skytjenester er at kunden har en mindre tett forretningsforbindelse til skyleverandøren, og ressurser hos skyleverandøren (som maskinvare, programvare, datalagring og fysiske bygninger) er delt mellom flere kunder samtidig. En definisjon på skytjenester er gitt av NIST:⁵⁰

«Å tilby skytjenester betyr å muliggjøre en allestedsnærværende, praktisk online tilgang til et felles sett med konfigurerbare databehandlingsressurser (f.eks. nettverk, tjenere, lagring, applikasjoner og tjenester) som raskt kan klargjøres av leverandøren og tas i bruk av kunden med minimal administrasjon og interaksjon med tjenesteleverandøren.»

De tre tjenestemodellene av skytjenester er *IaaS* (Infrastructure-as-a-Service), *PaaS* (Platform-as-a-Service) og *SaaS* (Software-as-a-Service), som er forklart nedenfor. IT-omgivelser uten skyløsninger kalles *On-Prem* (On Premises), som kan oversettes med «i egne lokaler». Hierarkiske lag av elementer i en IT-infrastruktur kalles en *IT-stack*, i betydning «stabel». Den samme stacken kalles en *skystack* når den gjenspeiles i skymodellene *IaaS*, *PaaS* og *SaaS*, som vist i figur 11.8.



Figur 11.8. Delt ansvar for IT-stacken i ulike skymodeller.

50 <https://csrc.nist.gov/publications/detail/sp/800-145/final>.

Hvem som har ansvar for hvert lag i stacken, avhenger av skymodellen. Her er det viktig å skille mellom de to betydningene av ansvarlig, som enten er «å ha som oppgave», eller «å være regnskapelig», det vil si «å stå til regnskap». Skymodellene i figur 11.8 tolker ansvarlig i form av hvem som har som oppgave å utføre de ulike funksjonene i IT-stacken. Betydningene av begrepet ansvar diskuteres i avsnitt 15.1.2.

On-Prem betyr at virksomheten eier og drifter maskinvare og programvare selv, typisk beskrevet som «å ha serveren i kjelleren».

IaaS-modellen tilbyr (virtuelle) maskinressurser og lagringsressurser. IaaS brukes av IT-arkitekter for å designe og sette opp virksomhetens IT-infrastruktur. Virksomheten må selv installere og drifte operativsystemer og utvikle/installere applikasjoner for å kunne drifte tjenester.

PaaS-modellen tilbyr en plattform for utvikling og drift av applikasjoner. Denne plattformen består av verktøy for utvikling, installering og kjøring av applikasjoner. PaaS brukes av virksomheter som selv utvikler/installerer og drifter sine applikasjoner, men som samtidig ikke ønsker å drifte (operativ)systemene der applikasjonene kjører.

SaaS-modellen tilbyr ferdige applikasjoner til kunden. SaaS-produktene er tjenester vi som sluttbrukere kjenner best, som f.eks. Gmail (for e-post), Dropbox (for lagring) og Office 365 for produktivitet og samarbeid. SaaS tilbyr standardiserte tjenester som virksomheten umiddelbart kan ta i bruk.

SaaS-tjenester administreres utelukkende av skyleverandøren, noe som begrenser hvordan en kunde kan skreddersy produktet etter eget behov. Hvis kunden har behov for større fleksibilitet, er alternativet å kjøpe en PaaS- eller IaaS-løsning for å kunne bygge og installere spesialtilpassede applikasjoner på toppen av en utviklingsplattform eller på toppen av en virtuell maskin.

En skyleverandør som tilbyr tjenester på det åpne markedet, kalles *allmenn sky* (også kalt «offentlig sky»), på samme måte som en butikk eller kafé er åpen for alle. En skyleverandør som kun leverer tjenester til en lukket kundegruppe, kalles en *privat sky*, på samme måte som en privat klubb kun gir adgang til medlemmer. En *hybrid sky* er sett fra perspektivet til kunden, og betyr at kunden benytter tjenester fra både allmenne/offentlige og private skyer. En *felles sky* er når flere virksomheter går sammen om å drifte skytjenester som de bruker i fellesskap.

11.8.2 Skysikkerhet

Skysikkerhet er beskyttelsen av data, applikasjoner og infrastrukturer i skyen. Mange aspekter av sikkerhet i skyen er de samme som for enhver lokal IT-arkitektur. Samtidig er det forskjeller det er viktig å være klar over. En viktig forskjell er at også sikkerhetsfunksjoner kan virtualiseres, og at kostnaden for å anskaffe f.eks. en virtualisert brannmur er langt lavere enn å anskaffe en fysisk brannmur.

Intuitivt er det skremmende at virksomhetens data lagres og prosesseres i gigantiske data-sentre som er spredt rundt i verden, og som driftes av andre enn egen virksomhet. Flere, om ikke alle, skyleverandører har segmentert infrastrukturen sin i regioner, slik at kundene lettere kan styre hvor data blir lagret og behandlet. Det er også viktig å merke seg forskjellen på «brukerens data» og «data om brukeren». Selv om brukerens data lagres i et segment som er avgrenset til en bestemt region, vil føderert IAM ofte bety at data *om brukeren* lagres globalt.

Samtidig er det betryggende at skyleverandører faktisk er store profesjonelle aktører med rikelig kompetanse og ressurser for sikker drift og administrasjon, som i de fleste tilfeller kan opprettholde bedre sikkerhet enn egen virksomhet er i stand til. Imidlertid er det viktig å ha bevissthet om at skyleverandører kontinuerlig utsettes for angrep og opplever sikkerhets-hendelser. Slike hendelser gjelder ikke nødvendigvis hele skytjenesten, men for eksempel en eller flere SaaS-tjenester. Skyleverandørene publiserer regelmessig driftsstatistikk, og det er kundens ansvar å følge med.

Sikkerhet i skyen er et delt ansvar mellom leverandør og bruker, der «ansvar» her tolkes som «å ha til oppgave». Se avsnitt 15.1.2 for en forklaring på betydninger av begrepet «ansvarlig». Figur 11.9 viser en forenklet oversikt over ansvarsfordeling av sikkerhetsfunksjoner i ulike modeller. Oversikten er inspirert av Microsoft.⁵¹

For å bedre forstå hva det innebærer at skyleverandøren har ansvar for systemsikkerhet i figur 11.9, er det nyttig å være klar over at systemsikkerheten blant annet er basert på virtuelle maskiner, som illustrert i figur 3.9. Det er skyleverandøren som eier og drifter både maskinvare med hypervisor og operativsystemer, og denne driftsfunksjonen skjer gjerne fra et annet land enn der maskinvaren er fysisk plassert. Samtidig vil personell med fysisk tilgang til maskinvaren teknisk sett også ha tilgang til virtuell maskinvare, systemer og data.

Anvarsområde	On-Prem	IaaS	PaaS	SaaS
Klassifisering og håndtering av data				
Klient- og endepunktsikkerhet				
Identitets- og tilgangshåndtering				
Applikasjonssikkerhet				
Nettverksikkerhet				
Systemsikkerhet				
Fysisk sikkerhet				
Sikkerhet mot korrupsjon og innsidetrusler				
Sikkerhet mot (lovlig) tilgang fra fremmede stater				
virksomhetens ansvar skyleverandørens ansvar irrelevant				

Figur 11.9. Delt ansvar for sikkerhet i ulike skymodeller.

De nederste to ansvarsområdene for informasjonssikkerhet i figur 11.9 er ikke beskrevet i Microsofts modell for delt sikkerhetsansvar i skyen, men tas med her fordi disse sikkerhetsutfordringene er spesielt relatert til skytjenester.

Muligheten for korrupsjon og innsidetrusler hos skyleverandøren økes betraktelig i skyen fordi privilegerte ansatte hos skyleverandøren teknisk sett kan få tilgang til kundenes data og applikasjoner. Sannsynligheten for slike trusler er gjerne korrelert med grad av ustabilitet i land

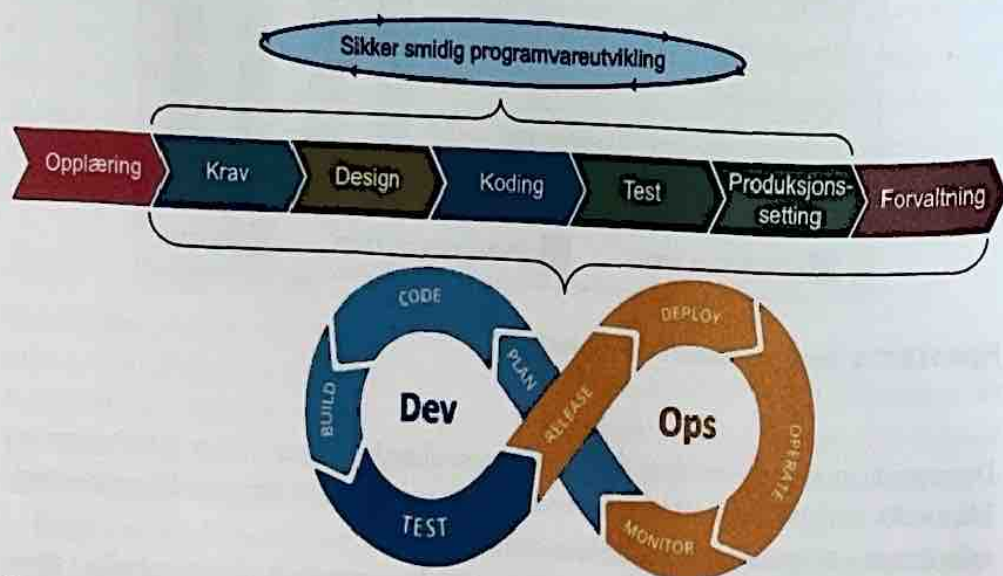
51 <https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility>.

og regioner så vel som (sikkerhets)kulturen innad i skyleverandørens organisasjon. Konkret knytter utfordringene seg til spørsmålet om hvem som teknisk sett kan få tilgang til dataene, og hvordan en skytjeneste kan bidra til å forhindre at teknisk tilgang misbrukes, ved å ha kontroller og retningslinjer på plass som kan forebygge og oppdage uregelmessigheter og avvik.

En annen sikkerhetsutfordring er i hvilken grad en skyleverandør er juridisk forpliktet eller kan tvinges til å gi myndighetene i landet der skyleverandøren er lokalisert, tilgang til kundenes data og applikasjoner når myndighetene etter landets lover krever det. Dette gjelder ikke bare i tilfeller av statlig overvåking, men kan også gjelde i tilfeller av kriminal-etterforskning. Det kan være vanskelig å vite i hvilken grad myndigheter kan kreve tilgang generelt, og kanskje enda vanskeligere å vite om det faktisk har skjedd, fordi den type tilgang foregår i hemmelighet. Hvis en skyleverandør er et amerikansk selskap og kunden er en virksomhet i EU, er det viktig å vite hvilke krav lokale og føderale amerikanske myndigheter kan stille for lovlig tilgang. Denne utfordringen knytter seg til gjennomsiktighet hos skyleverandøren og i landet der leverandøren er lokalisert. I USA har myndighetene varierende grad av lovlig tilgang, som blant annet er årsaken til at Schrems II-dommen basert på GDPR i 2020 kom frem til at overføringsgrunnlaget kjent som *Privacy Shield* ikke lenger er gyldig for overføring og behandling av personopplysninger fra EU til USA.⁵²

11.8.3 DevOps

DevOps, også kalt *DevSecOps*, er som navnet indikerer å kombinere programvareutvikling (Development) og drift (Operations). DevOps tar sikte på å forkorte syklusen rundt utvikling og drift av programvare og gi kontinuerlig levering med høy kvalitet og sikkerhet (Security). DevOps er videreutvikling av sikker smidig programvareutvikling ved at DevOps også inkluderer drift/forvaltning, mens sikker smidig programvareutvikling bare går frem til produksjonssetting, som vist i figur 11.10.



Figur 11.10. Sammenhengen mellom sikker smidig programvareutvikling, innebygd informasjonssikkerhet og DevSecOps.

52 <https://www.datatilsynet.no/regelverk-og-verktoy/internasjonalt/retningslinjer-og-uttalelser-fra-personvernradet/utfyllende-veiledning-om-schrems-ii/>.

Vi kan med visshet si at DevOps + Sky = Sant. Alle verktøy som trengs i hele DevOps-syklusen, ligger i skyen, fra utviklingsverktøy og testverktøy til verktøy for produksjonssetting, drift og monitorering. Skymodeller for DevOps må være enten IaaS eller PaaS, der hver modell har sine fordeler og ulemper.

I kjernen er DevOps en automatisering av sikker smidig utviklingsmetodikk. Ideen er å gi utviklere mulighet til å implementere nye krav og sette den nye versjonen av programvaren i produksjon på meget kort tid. Samtidig tar DevOps hensyn til sikkerhet på en mer automatisert måte og i en tidlig fase av syklusen. Begrepet «*shift-left*» i sammenheng med DevOps betyr at det fokuseres mer på sikkerhet på venstre side av 8-tallet i figur 11.10 (under utvikling og test), med det resultat at det blir færre sikkerhetssårbarheter og -hendelser å håndtere på høyre side av 8-tallet (under drift).

11.8.4 Cloud Security Alliance

*Cloud Security Alliance (CSA)*⁵³ er en organisasjon med over 80 000 medlemmer på verdensbasis dedikert til å definere og øke bevisstheten rundt god praksis for å sikre skytjenester. CSA benytter fagkompetanse til sine bedrifts- og enkeltmedlemmer i privat og offentlig sektor for å tilby forskning, utdanning, sertifisering, seminarer og produkter relatert til sikkerhet for skytjenester. CSA er uavhengig av private enkeltelskaper, noe som skaper et nøytralt kompetansenettverk der ulike parter kan jobbe sammen for å skape og vedlikeholde et bærekraftig økosystem for skytjenester.

Cybersikkerhet nevnes ofte som det største usikkerhetsmomentet for selskaper som ønsker å ta i bruk skytjenester. I Norge jobber CSA med å skape lokale arenaer for dialog og kunnskapsutveksling knyttet spesifikt til skytjenester og sikkerhet. CSA publiserer veiledere og sjekklistor som er nyttige for å øke sin bestillerkompetanse vedrørende sikkerhet hos brukere og kunder av skytjenester, og for at skyleverandører bedre skal kunne tilpasse sine produkter til forventede sikkerhetskrav. En nyttig veileder er f.eks. *Software Defined Perimeter (SDP) and Zero Trust* fra Cloud Security Alliance (CSA 2020).

11.9 Sikkerhet i digitale leveransekjeder

Risikostyring for digitale leveransekjeder (eng. C-SCRM, Cyber Supply Chain Risk Management) er prosessen med å identifisere, vurdere og redusere risikoene knyttet til den distribuerte og sammenkoblede strukturen til IT/OT-produkt- og tjenesteleveransekjeder. En anerkjent veileder for C-SCRM er NISTs *SP 800-161 Rev. 1 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* (2022). Dette dekkes også av NSMs *grunnprinsipp 2.1: Ivareta sikkerhet i anskaffelses- og utviklingsprosesser*, beskrevet i avsnitt 12.4.

Det vil alltid inngå leveranser av komponenter, verktøy og tjenester i utvikling og drift av systemer. C-SCRM dekker derfor hele livssyklusen til et system (inkludert design, utvikling, anskaffelse, testing, idriftsetting og vedlikehold) ettersom trusler og sårbarheter i forsyningskjeden med vilje eller utilsikt kan kompromittere et IT-produkt eller en IT-tjeneste på et hvilket som helst stadium. Relevante aspekter for sikkerhet i leveransekjeden bør inkluderes i kontrakter og tjenestenivåavtaler (eng. Service Level Agreement, SLA), som for eksempel:

53 <https://www.cloudsecurityalliance.no/>.

- Rapportering og varslingsplikt om sikkerhetsrelaterte ting som sikkerhetshendelser, sikkerhetspolicyer og endringer av eierstruktur
- Tilsyn og revisjonsrapporter om sikkerhet
- Nivå for risikoaksept hos underleverandør
- Forventet oppetid av tjenester, og underleverandørens risikoaksept for overholdelse av denne
- Endrings- og exit-klausuler, f.eks. basert på avvik eller endring i eierstruktur

Uavhengig av formelle kontrakter og tjenestenivåavtaler bør virksomheten kartlegge og overvåke underleverandørens eierstruktur. En mulig trussel er at en underleverandør kjøpes opp av et selskap lokalisert i et land Norge ikke har sikkerhetspolitisk samarbeid med. Da er det plausibelt at myndighetene i det landet kan utnytte den nye eierens styringsrett til å angripe virksomheten via leveranse av produkter og tjenester.

En generell tilnærming til sikkerhet i leveransekjeder er å sørge for at risikostyring for digitale leveransekjeder er inkludert i virksomhetens ISMS.

Digitale stykklistor (SBOM) er et virkemiddel for å holde oversikt over programvareleveransekjeder, se avsnitt 3.3. Med digitale stykklistor kan hver enkelt programvaremodul spores til dens utvikler eller leverandør.

Oppgaver til kapittel 11

11.1 Innebygd

- Hva menes med at informasjonssikkerhet og personvern skal være innebygd?
- Hvilke to veiledere/rammeverk fra Microsoft og Datatilsynet definerer en sammenfallende syvtrinns modell for innebygd informasjonssikkerhet (og personvern)?
- Nevn hva som bør gjøres generelt, og hva en virksomhet bør gjøre for å sørge for god opplæring i informasjonssikkerhet (1. fase).

11.2 Sikker smidig systemutvikling

- På hvilken måte er smidig utvikling forskjellig fra systemutvikling med fossefallmetoden?
- Hvordan kan sikkerhet integreres i smidig systemutvikling?

11.3 Sikkerhet i skyen

- Nevn faktorer som kan bidra til bedre sikkerhet ved skyløsninger enn ved On-Prem.
- Nevn faktorer som kan bidra til dårligere sikkerhet ved skyløsninger enn ved On-Prem.
- Forklar meningen med «venstreskift» (Shift-Left) i DevSecOps.

Styring og ledelse av informasjonssikkerhet

Informasjonssikkerhet inngår i styring og ledelse av ethvert foretak. Samtidig er det en rekke unike aspekter ved informasjonssikkerhet som krever særskilte kompetanser, noe som gjør at informasjonssikkerhet på mange måter er et eget område innen styring og ledelse.

I dette kapitlet lærer du om sentrale prinsipper, standarder og rammeverk for styring og ledelse av informasjonssikkerhet. Videre lærer du om hvilke prosesser og arbeidsoppgaver som inngår. Til slutt lærer du om vurdering av et foretaks modenhet med hensyn til styring og organisering av informasjonssikkerhet.

12.1 Styringsnivåer for informasjonssikkerhet

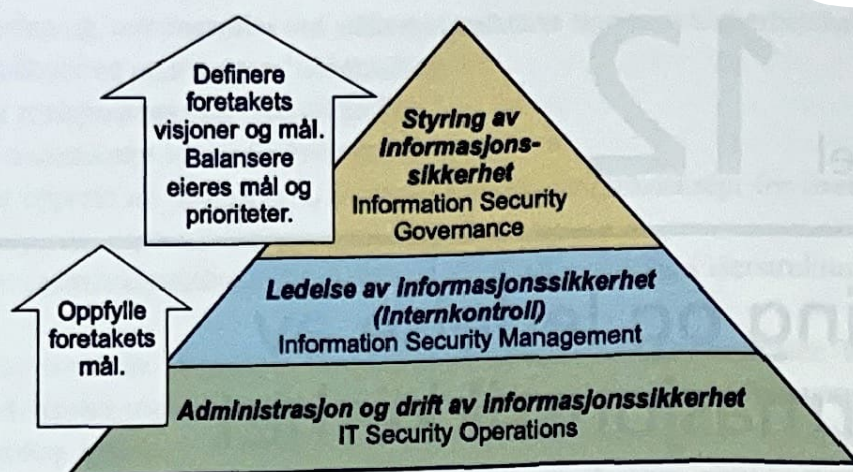
Organisasjonsstrukturer er som regel hierarkiske. Alle nivåer i en organisasjon har på hver sin måte ansvar for å utføre oppgaver relatert til informasjonssikkerhet, men styret og toppledelsen står til regnskap og er juridisk ansvarlig for at informasjonssikkerhet er godt organisert og ivaretatt.

Styringsnivåene for organisering av informasjonssikkerhet kan deles inn på ulike måter. En vanlig oppdeling av styringsnivåer generelt, og som også kan anvendes på informasjonssikkerhet, er vist i figur 12.1.

Det er nyttig å ha en god forståelse av begreper relatert til styringsnivåene i figur 12.1.

Foretaksstyring er det øverste styringsnivået i en organisasjon, som er styrets og toppledelsens ansvarsområde. Risikostyring generelt, og styring av informasjonssikkerhet spesielt, inngår i foretaksstyring.

Det engelske begrepet «Information Security Management» oversettes offisielt til «ledelse av informasjonssikkerhet» av Standard Norge. Frem til 2014 var oversettelsen imidlertid «styring av informasjonssikkerhet», og mange organisasjoner (f.eks. NSM) bruker fortsatt den oversettelsen. Begge oversettelsene er dermed i bruk. Begrepet «internkontroll» er i stor grad overlappende med styring/ledelse av informasjonssikkerhet, men med særlig vekt på etterlevelse av lover og forskrifter.



Figur 12.1. Styringsnivåer for informasjonssikkerhet.

Administrasjon og drift av informasjonssikkerhet består av det daglige arbeidet med å ivareta sikkerhet i drift av systemer og nettverk. Dette arbeidet består for eksempel av monitorering og konfigurering av systemer og nettverk, håndtering av sikkerhetshendelser og rapportering. Det er et voksende marked rundt administrasjon og drift av informasjonssikkerhet, som kalles *MSS (Managed Security Services)*. Det fins en rekke selskaper som er spesialisert på å yte denne typen tjenester, både i Norge og internasjonalt. Disse kalles typisk *MSSP (Managed Security Service Providers)*. De store konsulentselskapene tilbyr også tjenester i dette markedet.

De tre styringsnivåene i figur 12.1 er nærmere beskrevet nedenfor.

12.1.1 Styring av informasjonssikkerhet

Styret og toppledelsen i et foretak har som ansvar å definere foretakets målsettinger, visjoner og verdigrunnlag. I den grad det må gjøres en avveining mellom satsing på ulike målsettinger, er det styrets og toppledelsens ansvar å balansere disse. Dette gjelder også for styring av informasjonssikkerhet.

Virksomheter er under konstant press for å øke effektivitet og kvalitet og for å være konkurransedyktige i markedet. Et vanlig virkemiddel for å oppnå disse tingene er å redusere kostnader og øke effektivitet gjennom digitalisering av forretningsprosesser. Sammen med den stigende avhengigheten av digitale forretningsprosesser øker også trusler mot de samme prosessene gjennom online eksponering. Når digitale forretningsprosesser har sårbarheter som kan utnyttes av trusselaktører, oppstår informasjonssikkerhetsrisikoer. I den grad viktige forretningsprosesser og tjenester kan bli angrepet og falle ut som følge av trusler og sårbarheter, oppstår det risikoer for virksomhetens målsettinger og kanskje for hele dens eksistens. For at digitalisering av forretningsprosesser skal være bærekraftig, må disse sikkerhetsrisikoene håndteres forsvarlig.

Styret og ledelsen har dessuten overordnet ansvar for å påse at lover og forskrifter overholdes til enhver tid. Mange virksomheter har i tillegg krav om å ha *et styringssystem for informasjonssikkerhet*, som enkelt sagt betyr at prosesser og aktiviteter rundt informasjonssikkerhet skal være systematisk strukturert og følge et anerkjent rammeverk. Den engelske

betegnelsen er *ISMS (Information Security Management System)*, som oversettes enten som «styringssystem for informasjonssikkerhet» eller «ledelsessystem for informasjonssikkerhet» (LSIS). Denne boken oversetter ISMS som «styringssystem for informasjonssikkerhet». ISMS beskrives i avsnitt 12.3.2.

Å ivareta kravene beskrevet over kan generelt beskrives som styring av informasjonssikkerhet. En mer konsis definisjon på styring av informasjonssikkerhet er gitt av ISACA:⁵⁴

«Styring av informasjonssikkerhet består av å definere strategiske målsettinger for informasjonssikkerhet, sørge for at disse blir oppnådd, styre sikkerhetsrisiko med effektiv bruk av organisatoriske ressurser, påse at styringssystemet for informasjonssikkerhet fungerer hensiktsmessig og at resultater følger forventninger og målsettinger.»

ISACA (Information Systems Audit and Control Association) er en internasjonal forening for IT-revisorer og fagfolk som jobber med IT-ledelse. ISACA publiserer rammeverk og veiledningsmateriale for styring og ledelse av IT generelt, deriblant for styring og ledelse av informasjonssikkerhet. ISACA forvalter profesjonelle sertifiseringsprogrammer for fagfolk innen IT-revisjon og IT-ledelse, og arrangerer faglige møter for medlemmer, blant annet også i Norge.

I tillegg til definisjonen på styring av informasjonssikkerhet gjengitt ovenfor definerer ISACA følgende fem hovedmålsettinger for styring av informasjonssikkerhet:

- **Strategisk tilpasning av aktiviteter for informasjonssikkerhet.** Nyten av aktiviteter rundt informasjonssikkerhet er uunngåelig knyttet til hvor godt de støtter målene for organisasjonen og med hvilken kostnad. Uten organisatoriske mål som referansepunkt kan andre prinsipper som f.eks. *beste praksis* ofte være for omfattende, utilstrekkelige eller feilrettet på andre måter. Fra et forretningsperspektiv er en *adekvat og tilstrekkelig praksis* som er proporsjonal med kravene, som regel mer kostnadseffektiv og hensiktsmessig enn alltid å følge beste praksis. Noe annet vil i utgangspunktet være vanskelig for styret og toppledelsen å forsvare, særlig i kommersielle selskaper. Fra et styringsperspektiv er informasjonssikkerhet ikke et mål i seg selv – det skal bidra til å nå virksomhetens mål.
- **Risikostyring.** Optimal risikostyring er et grunnleggende mål – ikke bare for aktiviteter rundt informasjonssikkerhet, men egentlig for alle sikkerhetsaktiviteter i en organisasjon. Nytteverdi av risikostyring kan ikke måles direkte, men må måles med indikatorer som på en indirekte måte korrelerer med risikostyringens nytteverdi. Sagt på en relativt abstrakt måte kan risikostyring sies å ha god nytteverdi hvis den på en konsistent og kostnadseffektiv måte oppfyller forventningene om å oppnå definerte sikkerhetsmål.
- **Effektiv bruk av ressurser.** Som med alle andre organisatoriske ressurser må ressurser relatert til informasjonssikkerhet brukes fornuftig og effektivt. Det er for eksempel viktig å kartlegge allerede implementerte løsninger og vurdere om en løsning kan gjenbrukes innenfor andre områder eller avdelinger. Kompetanse og menneskelige ressurser er svært viktig. Kunnskap må fanges opp, tas vare på, bli formidlet og gjort tilgjengelig når det

- trengs. Kompetanse må bygges, brukes og ivaretas på best mulig måte. Styringssystemer og prosesser må standardiseres så langt det er mulig for å redusere administrasjons- og opplæringskostnadene. Alt må være godt dokumentert, referert og tilgjengelig.
- **Verdiskaping.** Det kan virke paradoksalt at arbeid med informasjonssikkerhet skaper verdi, fordi det i første rekke er en stor kostnadspost i organisasjoner. Imidlertid skaper god styring av informasjonssikkerhet verdi på bunnlinjen gjennom reduserte tap, økt om-dømme og tillit i markedet, balansert risikostyring og mer effektiv organisering og bruk av ressurser. Optimal verdiskaping oppstår når strategiske mål for informasjonssikkerhet oppnås, juridiske krav etterleves og sikkerhetstrusler balanseres med en akseptabel risiko, alt til lavest mulig kostnad.
 - **Målbarhet.** En enkel regel for styring kan uttrykkes slik: «Du kan ikke styre det du ikke kan måle.» Måling, monitorering og rapportering av aktiviteter rundt informasjonssikkerhet er derfor en forutsetning for å kunne vurdere om organisatoriske mål oppnås. Metoder for å måle aktiviteter og hendelser relatert til informasjonssikkerhet på tvers av organisasjonen må utvikles, og analysemodeller som gir en indikasjon på effekten av aktiviteter og prosesser rundt informasjonssikkerhet, må defineres. Det vil typisk være et spekter av slike målinger og analysemodeller som ikke direkte kan oversettes til en enkelt metrikk for hvor «sikker» organisasjonen er. Grad av informasjonssikkerhet i en organisasjon må derfor måles indirekte gjennom vurdering av kvalitet i prosesser, og kan til syvende og sist uttrykkes som grad av modenhet i styring av informasjonssikkerhet. En relevant standard og veileder for måling, evaluering og analyse av informasjonssikkerhet er ISO/IEC 27004.⁵⁵

12.1.2 Spørsmål som styret og toppledelsen bør stille seg

For mange styremedlemmer og toppledere kan utfordringer med cybersikkerhet virke overveldende. På den ene siden har de ansvar og står til regnskap for styring av informasjonssikkerhet i organisasjonen, på den andre siden har de kanskje utilstrekkelig kompetanse til å ta dette ansvaret på en god måte. Etter som de fleste forretningsprosesser digitaliseres og eksponeres mot cybertrusler, som ofte resulterer i betydelig cyberrisiko, er kompetanse innen dette området en forutsetning for at styret og toppledelsen skal kunne gjøre en god jobb.

Listen med spørsmål nedenfor kan brukes som en enkel sjekkliste for styremedlemmer og toppledere på om de er oppdatert med hensyn til styring av informasjonssikkerhet i organisasjonen de har ansvar for.

1. Hvordan holder virksomheten seg oppdatert om digitale trusler generelt og for egen sektor og virksomhet spesielt?
2. Har virksomheten god oversikt og forståelse av risiko relatert til informasjonssikkerhet?
3. Hvor godt er risikostyring for informasjonssikkerhet integrert i helhetlig risikostyring?
4. Bør cyberforsikring inkluderes i virksomhetens forsikringspoliser?
5. Hvor modent er virksomhetens ISMS?
6. Hvor godt er ISMS forankret hos ledelsen?
7. Jobbes det med god sikkerhetskultur som del av virksomhetskulturen generelt?
8. Dekker beredskapsplanen også cybersikkerhetshendelser, og er planen testet?

55 <https://www.iso27001security.com/html/27004.html>.

9. Hvor god er virksomhetens etterlevelse av lover og forskrifter relatert til informasjonssikkerhet?
10. I hvilken grad bør virksomheten outsource sikkerhetsfunksjoner, som f.eks. gjennom å kjøpe MSS (sikkerhetstjenester)?
11. Hvor god er beskyttelsen av informasjon som overføres til tredjeparter?
12. Hvor god er virksomhetens etterlevelse av GDPR?

12.1.3 Ledelse av informasjonssikkerhet

Ledelse av informasjonssikkerhet er å opprette, drifte og vedlikeholde et sett med prosesser og aktiviteter som på en fornuftig måte beskytter organisasjonens informasjonsverdier mot sikkerhetstrusler, og som dermed bidrar til å opprettholde KIT-sikkerhetsmålene konfidensialitet, integritet og tilgjengelighet. Et viktig element i ledelse av informasjonssikkerhet er risikostyring, en prosess som involverer vurdering av sikkerhetsrisikoer en organisasjon er eksponert mot, og hvordan disse best kan håndteres og reduseres til et adekvat nivå. Risikostyring er beskrevet i kapittel 14 nedenfor.

Ledelse av informasjonssikkerhet bør være basert på et ISMS (*Information Security Management System*), som vanligvis oversettes til *styringssystem for informasjonssikkerhet*. Et ISMS er et sett med prosesser og aktiviteter rundt informasjonssikkerhet definert gjennom et utvalg av standarder, rammeverk og egendefinerte retningslinjer og policyer. I Norge og Europa er det vanligste rammeverket som danner grunnlag for ISMS, beskrevet i den internasjonale standarden *ISO/IEC 27001 Ledelsessystem for informasjonssikkerhet*.⁵⁶

Elementer i ISMS er nærmere beskrevet i avsnitt 12.3.

12.1.4 Administrasjon og drift av informasjonssikkerhet

Administrasjon og drift av informasjonssikkerhet består av en portefølje med ulike aktiviteter. En virksomhet kan velge å selv ta hånd om disse aktivitetene, eller outsource dem til en MSSP (*Managed Security Service Provider*), kalt *leverandører av informasjonssikkerhetstjenester* på norsk.

Små virksomheter har typisk ingen ansatte som utelukkende jobber med informasjonssikkerhet, mens større virksomheter kan ha et SOC-team for sikkerhetsmonitorering og et CSIRT eller CERT for hendelsesrespons.

Et SOC (*Security Operations Center*), kalt *sikkerhetsoperasjonssenter* på norsk, er et team med eksperter som har kompetanse, verktøy og ressurser til å utføre oppgaver og aktiviteter for informasjonssikkerhet. Disse aktivitetene er for eksempel:

- brannmurer – konfigurering, overvåking og drift
- IDS (Intrusion Detection System), dvs. konfigurering, overvåking og vedlikehold av systemer for inntrengningsdeteksjon i systemer og nettverk
- sårbarhetsskanning og oppdatering av programvare
- forebygging av tap og gjenoppretting av data
- digital trusseletterretning
- deteksjon og rapportering av sikkerhetshendelser

Et CSIRT (*Computer Security Incident Response Team*), eller CERT (*Computer Emergency Response Team*), kalt *hendelsesresponsteam* på norsk, er et team med eksperter som har kompetanse, verktøy og ressurser til å håndtere sikkerhetshendelser når de oppdages. CERT er et varemerke eid av Carnegie Mellon University, mens CSIRT er et begrep som kan brukes fritt. Et CSIRT håndterer hendelser som rapporteres av SOC eller detekteres på andre måter. Trinn i håndtering av sikkerhetshendelser er:

- sortering (triage) for å bekrefte at hendelsen er betydelig og ikke en falsk positiv
- analyse for å samle inn og analysere relevant informasjon for å forstå hendelsen
- skadebegrensning for å forhindre at angrepet sprer seg videre og skaden forverres
- utkastelse for å fjerne årsaken til hendelsen og sårbarheter som ble utnyttet
- gjenoppretting og normalisering, og eventuelt innføring av nye sikkerhetstiltak og rutiner
- lukking av saken for å dokumentere og lære av hendelsen

Nødvendig kompetanse og grad av kompleksitet for utførelse av SOC- og CSIRT-aktiviteter kan medføre betydelige kostnader. Det kan derfor være kostnadseffektivt å kjøpe slike tjenester. Som tidligere nevnt fins det et raskt voksende marked for SOC- og CSIRT-tjenester. Disse temaene er nærmere beskrevet i kapittel 16 og kapittel 17.

12.2 Standarder og rammeverk for styring og ledelse av informasjonssikkerhet

Det fins et stort utvalg av standarder og rammeverk å velge mellom for å bygge opp et ISMS. Blant de mest fremtredende er 27000-serien av standarder publisert av ISO/IEC, som er et samarbeid mellom ISO (International Organization for Standardization) og IEC (International Electrotechnical Commission). Den sentrale standarden i 27000-serien er *ISO/IEC 27001 Ledelsessystem for informasjonssikkerhet – krav*, forkortet til ISMS (Information Security Management System). Dette er ekvivalent med det som vanligvis kalles et styringssystem for informasjonssikkerhet. En viktig egenskap ved ISO/IEC 27001 er at den bygger på samme lest, eller prinsipper, som flere andre av styrings-/ledelsessystemene til ISO/IEC som nevnes i avsnitt 12.3. Dette gir bedre forutsetning for at virksomhetsledelsen kan etablere et helhetlig styringssystem (som favner mer enn bare informasjonssikkerhet). En ulempe med standarder fra ISO/IEC er at de må kjøpes.

Digdir (Digitaliseringsdirektoratet) publiserer *Internkontroll i praksis – informasjonssikkerhet*,⁵⁷ som tar utgangspunkt i ISO/IEC 27001, og er mye brukt i offentlig sektor.

NSM (Nasjonal Sikkerhetsmyndighet) publiserer *Grunnprinsipper for IKT-sikkerhet*,⁵⁸ som hovedsakelig er en tiltaksbank på linje med ISO/IEC 27002, men der kategorier av sikkerhetstiltak er strukturert annerledes. NSMs grunnprinsipper for IKT-sikkerhet er beskrevet i avsnitt 12.4. De er mye brukt i Norge, både fordi de er velstrukturerte og konsise, og fordi de har en norsk språkdrakt.

⁵⁷ <https://internkontroll-infosikkerhet.difi.no/>.

⁵⁸ <https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/>.

I USA publiserer NIST (National Institute of Standards and Technology) *SP 800-serien*⁵⁹ av standarder, rammeverk og veiledere for informasjonssikkerhet som generelt har høy kvalitet. Et av deres prominente rammeverk er NIST CSF (Cybersecurity Framework), som er beskrevet i avsnitt 12.5. NSMs grunnprinsipper for IKT-sikkerhet har likhetstrekk med NIST CSF.

ISACA publiserer *COBIT-rammeverket*,⁶⁰ som er mye brukt i styring og revisjon av IT. CIS (Center for Internet Security) publiserer *The CIS Controls and Resources*,⁶¹ som gir en dekkende beskrivelse av tiltak og tilhørende ressurser for informasjonssikkerhet.

Listen over er langt fra uttømmende, og det kan nesten være for mye av det gode på den måten at det er forvirrende med så mange ulike standarder, veiledere og rammeverk. De mest relevante for norske virksomheter er 27000-serien fra ISO/IEC og *Grunnprinsipper for IKT-sikkerhet* fra NSM, som beskrives i avsnittene nedenfor.

12.3 ISO/IEC 27000-serien med standarder

ISO og IEC samarbeider gjennom JTC1 (Joint Technical Committee 1) om å utarbeide standarder for informasjonssikkerhet. Et sett med standarder som JTC1 har ansvaret for, er 27000-serien, som fokuserer på styring og ledelse av informasjonssikkerhet. Det fins mange ulike standarder i 27000-serien, der de to viktigste av disse er standarden *ISO/IEC 27001 Ledelsessystem for informasjonssikkerhet (ISMS) – Krav*, og standarden *ISO/IEC 27002 Informasjonssikkerhetstiltak*, som beskrives i avsnittene nedenfor. En annen viktig standard er *ISO/IEC 27005 Risikostyring* for informasjonssikkerhet, som beskrives i kapittel 14.

12.3.1 Historien bak ISO/IEC 27001 og 27002

De fleste med interesse for informasjonssikkerhet er kjent med ISO/IEC 27001, den internasjonale standarden som beskriver krav til et ISMS.

Mange er ikke like godt kjent med ISO/IEC 27002, som er en tilleggsstandard til 27001. Enda færre kjenner til at det opprinnelig var omvendt, det vil si at ISO/IEC 27001 var en tilleggsstandard til 27002. Dette må forklares.

På begynnelsen av 1990-tallet begynte informasjonssikkerhet for alvor å bli svært viktig. På den tiden var det et stort problem at fagfolk innen IT som regel hadde liten eller ingen kompetanse innen informasjonssikkerhet. Samtidig manglet en felles forståelse av terminologi, teknologi og tiltak rundt informasjonssikkerhet.

Oljeselskapet Shell var relativt tidlig ute med å systematisere arbeidet med informasjonssikkerhet innen egen organisasjon. De laget en egen veileder for informasjonssikkerhet, som ble gitt til BSI (*British Standards Institution*) tidlig på 1990-tallet. BSI utviklet denne veilederen videre, og den ble i 1995 publisert som en standard for *praksisnormer for informasjonssikkerhet*, kalt *BS 7799: Code of Practice for Information Security Management*. Standarden fokuserte på å beskrive en rekke tiltak for informasjonssikkerhet, og den ble godt mottatt i fagmiljøet – ikke bare i Storbritannia, men også i andre land.

⁵⁹ <https://csrc.nist.gov/publications/sp800>.

⁶⁰ <https://www.isaca.org/resources/cobit>.

⁶¹ <https://www.cisecurity.org/>.

Imidlertid ble det raskt klart at BS 7799 ikke dekket styrings- og ledelsesaspektene av informasjonssikkerhet. Utover på 1990-tallet ble styring av IT etter hvert et viktig fagfelt, og dermed var det også viktig å definere *praksisnormer for styring og ledelse av informasjonssikkerhet*. På den bakgrunn publiserte BSI i 1999 en tilleggsstandard som ble kalt *BS 7799-2: Information Security Management System (ISMS)*. Denne standarden ble også godt mottatt og raskt tatt i bruk, både i Storbritannia og i mange andre land.

ISO og IEC, som publiserer internasjonale standarder, så behovet for å publisere standarder nettopp innenfor styring og ledelse av informasjonssikkerhet. Ettersom dette hastet, besluttet de i 2001 å publisere standardene fra BSI, simpelthen ved å legge til et «1»-tall foran og ellers beholde de samme titlene, slik at standardene fikk nummer ISO/IEC 17799 og ISO/IEC 17799-2.

På 2000-tallet besluttet ISO (og IEC) å definere kategorier av standarder for styrings-/ledelsessystemer innen særskilte fagområder, der listen nedenfor gir noen eksempler:

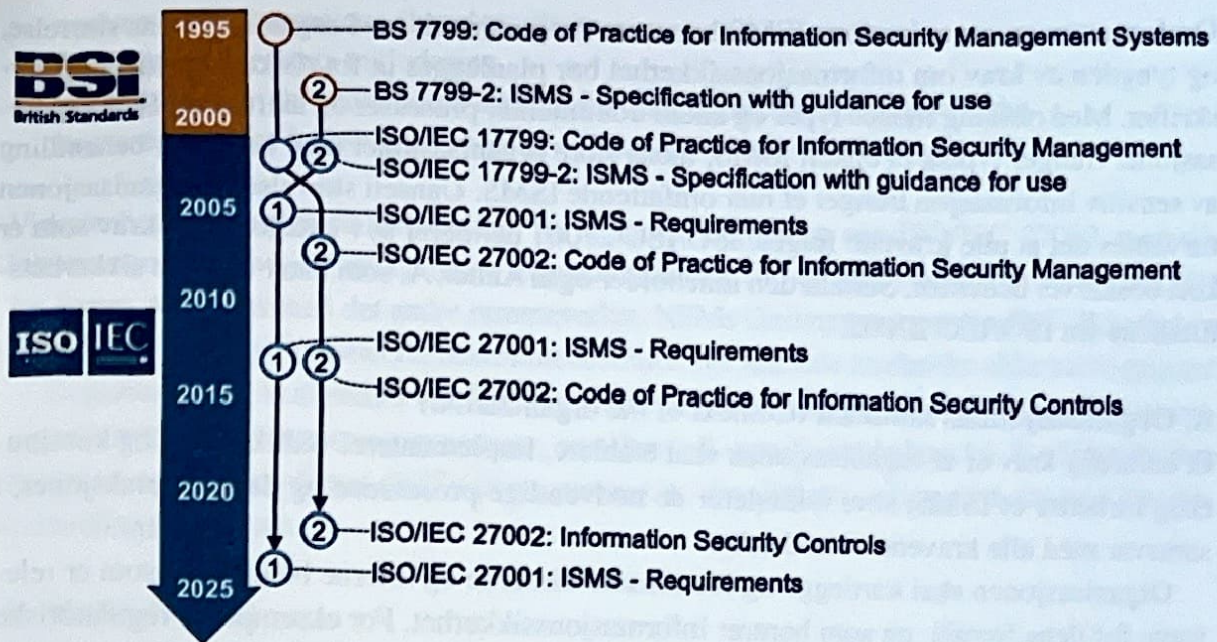
- ISO 9001 Quality Management (Kvalitetsledelse)
- ISO/IEC 20000 Service Management (Tjenesteledelse)
- ISO 22300 Security and Resilience (Samfunnssikkerhet)
- ISO/IEC 27001 ISMS: Information Security Management System – Requirements (Ledelsessystem for informasjonssikkerhet – Krav)
- ISO 31000 Risk management (Risikostyring)
- ISO 39001 Road Safety Management System (Styringssystem for trafikkssikkerhet)
- ISO 22000 Food Safety Management System (Ledelsessystem for næringsmiddeltrygghet)

Fra listen over legger vi merke til at 27000-serien ble definert som en egen serie av standarder for styring og ledelse av informasjonssikkerhet. Dermed var det nødvendig å gi nye nummer til de allerede publiserte standardene for informasjonssikkerhet, og her skjedde det noe interessant: Standarden for ISMS (17799-2), som opprinnelig var en tilleggsstandard, ble vurdert til å være den grunnleggende standarden for styring og ledelse av informasjonssikkerhet, og fikk dermed nummer 27001, altså nummer 1. Standarden for praksisnormer i administrasjon av informasjonssikkerhet (17799), som opprinnelig var ansett å være hovedstandard, ble «degradert» til å få nummer 27002, altså nummer 2. Denne utviklingen er illustrert i figur 12.2.

I tillegg til endring av nummer har ISO/IEC 27002 gjennomgått flere navneendringer. Fra å ha det tunge navnet *Code of Practice for Information Security Management Systems* i 1995 fikk standarden med 2022-utgaven det enkle og intuitive navnet *Information Security Controls*.

Den norske oversettelsen av 27001 var opprinnelig *Styringssystem for informasjonssikkerhet – krav*, men dette ble i 2014 endret til *Ledelsessystem for informasjonssikkerhet – krav*. Ny utgave fra 2023 har beholdt navnet *Ledelsessystem for informasjonssikkerhet – krav*, som refererer til det som i denne boken og i andre sammenhenger kalles et *styringssystem for informasjonssikkerhet*, forkortet til ISMS.

Norske lover og forskrifter benytter som regel betegnelsen «Styringssystem for informasjonssikkerhet», blant annet personopplysningsloven beskrevet i kapittel 10 og sikkerhetslo-



Figur 12.2. Utviklingen av standardene ISO/IEC 27001 og 27002.

ven beskrevet i kapittel 15. Det kan skape forvirring at begge betegnelse «styringssystem» og «ledelsessystem» benyttes med samme betydning, men det må fagfolk i informasjonssikkerhetsmiljøet bare bli vant til. I denne boken oversettes ISMS til «styringssystem for informasjonssikkerhet».

Den norske oversettelsen av ISO/IEC 27002 var opprinnelig *Administrasjon av informasjonssikkerhet*. Samtidig med endringen av den engelske tittelen til ISO/OEC 27002:2022 «Information Security Controls» er den norske tittelen endret til «Informasjonssikkerhetstiltak».

12.3.2 ISO/IEC 27001 Ledelsessystem for informasjonssikkerhet (ISMS) – krav

ISO/IEC 27001:2022 er altså det sentrale rammeverket i ISO/IEC 27000-serien, som er serien med standarder for styring og ledelse av informasjonssikkerhet. ISO/IEC 27001 beskriver kravene for å etablere, implementere, vedlikeholde og kontinuerlig forbedre et ISMS. Det er med andre ord en oversikt over aktiviteter, prosesser og dokumentasjon en virksomhet bør opprettholde for å være i samsvar med typiske regelverk som krever et styringssystem for informasjonssikkerhet.

Et styringssystem for informasjonssikkerhet (ISMS) er samlingen av dokumenterte samvirkende prosesser og aktiviteter for informasjonssikkerhet som en organisasjon har definert basert på anerkjente standarder, rammeverk og retningslinjer, samt på egendefinerte policyer og prosedyrer. Dette kalles «et system» fordi det representerer en *systematisk* tilnærming til informasjonssikkerhet.

Omfanget av en organisasjons ISMS bør være proporsjonalt med organisasjonens størrelse, og tyngden av krav om informasjonssikkerhet bør planlegges ut fra risiko eller lover og forskrifter. Med omfang menes typer og antall dokumenter prosesser og aktiviteter. Små organisasjoner trenger typisk et enkelt ISMS, mens store organisasjoner med betydelig behandling av sensitiv informasjon trenger et mer omfattende ISMS. Uansett størrelse på organisasjonen forventes det at alle kravene følges. ISO/IEC 27001 definerer syv kategorier av krav som er kort beskrevet nedenfor. Standarden inneholder også Annex A, som lister opp alle sikkerhetstiltakene fra ISO/IEC 27002.

A. Organisasjonens kontekst (Context of the organization)

Et helhetlig krav er at organisasjonen skal etablere, implementere, vedlikeholde og kontinuerlig forbedre et ISMS, som inkluderer de nødvendige prosessene og deres interaksjoner, i samsvar med alle kravene i standarden.

Organisasjonen skal kartlegge og identifisere eksterne og interne betingelser som er relevante for dens formål, og som berører informasjonssikkerhet. For eksempel er regulatoriske etterlevelseskrav og bransjenormer viktige eksterne betingelser. Videre må organisasjonen forstå informasjonssikkerhetsbehov og -forventninger til relevante tredjeparter som virksomheten kommer i kontakt med og må forholde seg til.

Omfanget av organisasjonens ISMS skal bestemmes ut ifra behov og organisasjonens størrelse.

B. Lederskap (Leadership)

Toppledelsen skal vise lederskap blant annet ved å sørge for at policyer og målsettinger for informasjonssikkerhet er etablert og er compatible med organisasjonens helhetlige strategi, sørge for tilstrekkelige ressurser til arbeidet med informasjonssikkerhet, kommunisere viktigheten av informasjonssikkerhet til hele organisasjonen og sjekke at ISMS oppnår de forventede resultater.

Toppledelsen skal sørge for at ansvar og myndighet for roller som er relevante for informasjonssikkerhet, er tildelt og kommunisert internt i organisasjonen.

C. Planlegging (Planning)

Organisasjonen skal planlegge for risikostyring ved å velge metode for risikovurdering og definere kriterier for risikoaksept. Videre skal organisasjonen etablere en prosess for å håndtere identifiserte risikoer.

Ved valg av sikkerhetstiltak for å redusere risiko til et akseptabelt nivå, eller for å tilfredsstille regulatoriske krav, skal organisasjonen ta i betraktning listen over sikkerhetstiltak i Annex A (og som er beskrevet i detalj i ISO/IEC 27002). I tillegg kan andre sikkerhetstiltak vurderes.

En relevanserklæring (eng. SoA: Statement of Applicability) er et dokument som lister opp alle sikkerhetstiltakene i Annex A, og som for hvert tiltak kort forklarer om, og hvorfor, tiltaket er implementert eller ikke. Når en risikovurdering utføres (som del av punkt E Drift nedenfor) for å velge sikkerhetstiltak, og virksomheten ønsker å utarbeide dokumentasjon som grunnlag for revisjon eller sertifisering, skal det utarbeides en SoA som minst skal inneholde:

- nødvendige informasjonssikkerhetstiltak
- begrunnelse for deres inkludering
- informasjon om de nødvendige sikkerhetstiltak er implementert eller ikke
- begrunnelsen for å ekskludere noen av sikkerhetstiltakene i Annex A

Virksomheter kan velge sikkerhetstiltak fra et annet rammeverk enn ISO/IEC 27002, men dokumentasjon for revisjon må da ha en relevanserklæring (SoA) som inneholder en kartlegging fra Annex A til tiltakene i det andre rammeverket. NSMs Grunnprinsipper for IKT-sikkerhet og NIST Cybersecurity Framework, beskrevet nedenfor, har allerede utarbeidet slike kartlegginger.

Organisasjonen skal etablere målsettinger for informasjonssikkerhet for relevante domener, funksjoner og forretningsprosesser, som betyr å spesifisere behov for konfidensialitet, integritet og tilgjengelighet (KIT). Hvis praktisk mulig skal det måles og dokumenteres om målsettingene oppnås.

D. Støtte (Support)

Organisasjonen skal tildele tilstrekkelige ressurser som trengs for arbeidet med ISMS.

Organisasjonen skal kartlegge behov for kompetansen og sørge for at relevante medarbeidere faktisk har den kompetansen.

Organisasjonen skal sørge for at ansatte har bevissthet rundt sikkerhetspolicyer, viktigheten av å følge policyer og konsekvenser av å ikke følge policyer.

Organisasjonen skal ha en plan for kommunikasjon vedrørende informasjonssikkerhet, både internt og med ulike eksterne parter.

Dokumentasjon er et grunnleggende krav. Organisasjonens ISMS skal innbefatte dokumentert informasjon som eksplisitt kreves av standarden, og dokumentert informasjon som er nødvendig for effektiviteten i hele ISMS, blant annet om de ulike prosessene som inngår. Omfanget av dokumentasjon kan variere ut ifra størrelsen på organisasjonen og dens type aktiviteter, prosesser, produkter og tjenester, kompleksiteten til prosesser og deres interaksjoner, og kompetansen til personer.

E. Drift (Operation)

Organisasjonen skal planlegge, implementere og forvalte prosesser og sikkerhetstiltak som er nødvendige for å oppfylle kravene i ISMS, og for å drifte aktivitetene relatert til håndtering av risiko og forvaltning av sikkerhetstiltak beskrevet under kategori C. Planlegging.

Organisasjonen skal peke ut relevante domener, funksjoner og forretningsprosesser for vurdering av informasjonssikkerhetsrisiko. Vurdering av risikoer skal bestå av å kartlegge verdier, identifisere trusler og sårbarheter, estimere sannsynlighet og alvorlighetsgrad for de ulike risikoene, som til slutt danner grunnlag for å beregne risikonivåer.

Ut ifra risikovurderingen og kriterier for risikoaksept, samt regulatoriske etterlevelseskrav, skal organisasjonen bestemme og sette i verk håndtering av de ulike risikoene, som kan være å redusere risiko ved å implementere sikkerhetstiltak, overføre risiko for eksempel ved å kjøpe cyberforsikring, akseptere risiko ut ifra nivået for risikoaksept eller unngå risiko ved å stanse forretningsprosessen som medfører risiko.

Organisasjonen skal oppbevare dokumentert informasjon om risikovurderinger og hvordan risikoene er håndtert.

F. Evaluering (Performance evaluation)

For overvåking, måling, analyse og evaluering av ISMS skal organisasjonen bestemme hva som må overvåkes og måles, samt metoder for dette. Metodene som velges, bør gi sammenlignbare og reproducerbare resultater for å anses som gyldige.

Organisasjonen skal gjennomføre internrevisjoner med planlagte intervaller for å gi informasjon om hvorvidt ISMS fungerer som planlagt.

Toppledelsen skal gjennomgå organisasjonens ISMS med planlagte intervaller for å sikre kontinuerlig egnethet, tilstrekkelighet og effektivitet.

Ledelsesgjennomgangen skal omfatte blant annet vurdering av status for aksjonspunkter fra tidligere ledelsesgjennomganger, endringer i eksterne og interne forhold som er relevante for informasjonssikkerhet, trussel- og risikovurderinger, og hvordan risiko er håndtert.

Resultatene av ledelsesgjennomgangen skal omfatte beslutninger knyttet til kontinuerlige forbedringsmuligheter og eventuelle behov for endringer i ISMS. Ledelsesgjennomgangen skal dokumenteres.

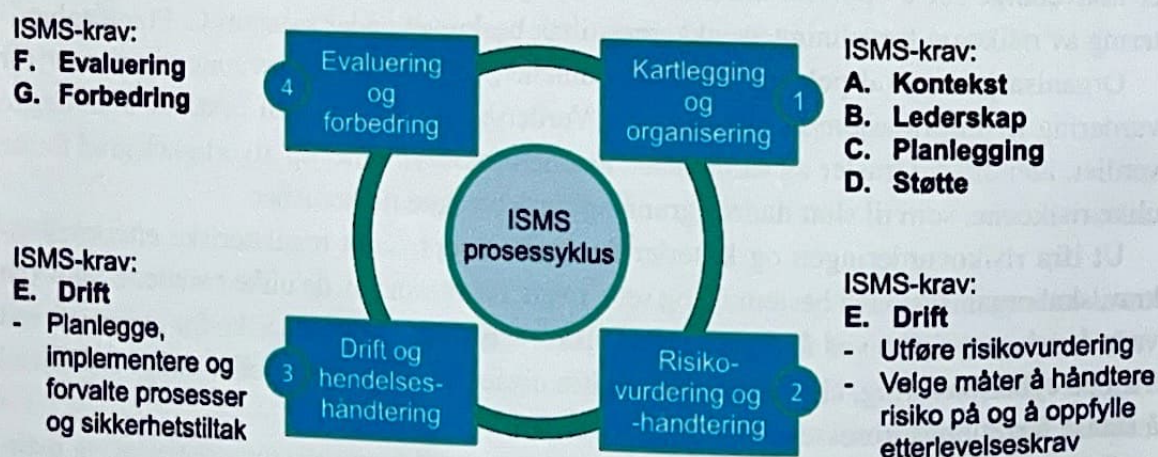
G. Forbedring (Improvement)

Organisasjonen skal kontinuerlig forbedre egnetheten, tilstrekkeligheten og effektiviteten til ISMS.

Når det identifiseres svakheter eller avvik i ISMS, skal organisasjonen iverksette tiltak for å korrigere det, håndtere mulige konsekvenser og vurdere behovet for tiltak for å eliminere årsakene til avvik, slik at det ikke gjentar seg eller oppstår andre steder.

12.3.3 Prosessyklus for ISMS

De syv kategoriene med krav til et styringssystem for informasjonssikkerhet (ISMS) beskrevet i forrige avsnitt følger ikke direkte en prosessyklus som virksomheter vanligvis jobber etter. Derfor kan det være nyttig å plassere kravene til ISMS fra ISO/IEC 27001 i en naturlig prosessyklus for styring av informasjonssikkerhet, der aktiviteter og prosesser for informasjonssikkerhet inngår. Figur 12.3 tilordner ISMS-kravene i fire faser. Figuren er en tolkning av hvor kravene fra ISO/IEC 27001 hører hjemme i ISMS som en prosessyklus, der fasene logisk følger etter hverandre, men der aktiviteter i ulike faser gjerne kan foregå parallelt. I en virksomhet foregår alltid mange prosesser samtidig.



Figur 12.3. ISMS-kravene fra ISO/IEC 27001 tilordnet fasene i en prosessyklus.

Elementene i et ISMS illustrert i figur 12.3 er kort beskrevet nedenfor.

1. *Kartlegging og organisering.* Virksomheten må kartlegge og identifisere eksterne og interne forhold og krav som er relevante for informasjonssikkerhet. Roller og ansvarsområder for arbeid med informasjonssikkerhet må defineres, og organisasjonsstrukturen må tilpasses dette arbeidet. Ansvar for aktiviteter og prosesser rundt informasjonssikkerhet må legges til roller og enheter. Riktig kompetanse må rekrutteres eller bygges opp innenfor organisasjonen. Policyer må utarbeides, først en overordnet informasjonssikkerhetspolicy og deretter underordnede policyer innen områder som sikkerhetsansvar og organisering, informasjonsgradering og -håndtering, identitetshåndtering, personvern, risikostyring, anskaffelse og leverandørstyring, cybersikkerhetsberedskap, personellsikkerhet, sikkerhetsatferd osv.
2. *Risikovurdering og risikohåndtering.* Det fins flere kilder til krav om sikkerhetstiltak, først og fremst risikovurdering:
 - Vurdering av risiko består av å kartlegge verdier, identifisere risikoer basert på trusselmodellering og sårbarhetsanalyse samt å vurdere alvorlighetsgrad for de ulike risikoene. Dette danner grunnlag for valg av metode for risikohåndtering, som typisk er å innføre sikkerhetstiltak.
 - Krav om informasjonssikkerhet kan være begrunnet i juridiske lover og forskrifter. Nødvendige sikkerhetstiltak velges for å være i samsvar med slike krav. Ofte sier lover og forskrifter nettopp at virksomheten skal velge sikkerhetstiltak ut ifra risikovurdering.
 - Sikkerhetstiltak kan velges ut fra hva som er standard praksis, uten å vurdere sikkerhetsrisikoer eller kartlegge regulatoriske sikkerhetskrav. En virksomhet som utelukkende følger dette prinsippet, må anses å ha lav modenhet i styring av informasjonssikkerhet.
3. *Drift og hendelseshåndtering.* Sikkerhetstiltak som er valgt, eller som allerede er i drift, forvaltes etter definerte prosesser. Man må alltid forvente at det skjer sikkerhetshendelser, som må håndteres etter virksomhetens beredskapsplan.
4. *Evaluering og forbedring.* Effektiviteten av sikkerhetsaktiviteter og tiltak bør måles på en måte som er enkel og praktisk og som gir relevante indikatorer. ISO/IEC 27004 beskriver måling, evaluering og analyse av sikkerhetstiltak. Første trinn i arbeidet med måling og analyse er å definere hvilken informasjon som best reflekterer effekten av sikkerhetstiltak på risikoer. Dernest må informasjonen samles inn og analyseres for å danne et bilde av nytteeffekten av ulike sikkerhetstiltak. Dette danner grunnlag for forbedring av ISMS, og rapportering til ledelsen er viktig for styring av informasjonssikkerhet for hele organisasjonen.

Verdien av å arbeide i henhold til et ISMS (styringssystem for informasjonssikkerhet) er at en organisasjon oppnår en mer helhetlig dekkende, konsistent, forutsigbar og målbar informasjonssikkerhet, som i tillegg kan dokumenteres og revideres. Jo mer helhetlig og dekkende, desto mer modenhet har virksomheten i styring av informasjonssikkerhet.

Organisasjoner forvalter mange ulike tiltak for informasjonssikkerhet, som brukerautentisering, brannmur, IDS, kryptering, sikker systemutvikling, sikkerhetskultur osv. Uten et ISMS har tiltakene en tendens til å være usammenhengende, ofte implementert som punkt-løsninger etter hendelser eller bare fordi noen mente at tiltaket var en god idé. For å garantere

et forsvarlig sikkerhetsnivå i henhold til risikovurderinger krever mange lover nettopp at underlagte virksomheter har et ISMS og velger sikkerhetstiltak ut ifra risikovurderinger, som beskrevet i avsnitt 15.1.1.

En organisasjon som oppfyller standardens krav, kan velge å bli revidert av et akkreditert sertifiseringsorgan, som etter vellykket revisjon kan sertifisere organisasjonen i henhold til ISO/IEC 27001. At en organisasjon er 27001-sertifisert, gir en indikasjon på god styring av informasjonssikkerheten, noe som kan gi markedsfordeler eller til og med kan kreves av andre organisasjoner for deltagelse i forretningssamarbeid og anbudskonkurranser.

Merk at en virksomhet som har et modent ISMS, og kanskje til og med er 27001-sertifisert, likevel kan bli utsatt for alvorlige sikkerhetshendelser. Forskjellen er at en virksomhet med høy ISMS-modenhet antageligvis har færre alvorlige sikkerhetshendelser, og at virksomheten er bedre forberedt når en hendelse inntreffer, enn en virksomhet med lav modenhet. Hvis det etter en alvorlig sikkerhetshendelse blir spørsmål om erstatning ved tap, eller sanksjoner på grunn av manglende etterlevelse av lover og forskrifter, vil en virksomhet med høy ISMS-modenhet stå i en bedre posisjon enn en virksomhet med lav modenhet. I ekstreme tilfeller av alvorlige sikkerhetshendelser som følge av mangelfull styring av informasjonssikkerhet kan toppledelsen bli anklaget for uaktsomhet og bli straffet med å betale erstatning eller med fengsel, som beskrevet i avsnitt 15.1.2.

Ledelsen bestemmer omfanget av ISMS for sertifiseringsformål og kan begrense det til for eksempel en enkelt forretningsenhet eller en lokasjon. ISO/IEC 27001-sertifikatet betyr ikke nødvendigvis at resten av organisasjonen, utenfor området, har en tilstrekkelig tilnærming til ISMS.

Målet med et ISMS er at en organisasjon bedre skal være i stand til å beskytte sine informasjonsressurser på en adekvat måte. Merk at ISO/IEC 27001 dekker mer enn bare teknologi. God styring av informasjonssikkerhet er også avhengig av at organisatoriske aspekter av informasjonssikkerhet er ivarettatt.

12.3.4 ISO/IEC 27002 Informasjonssikkerhetstiltak

ISO/IEC 27002:2022 er en tiltaksbank for informasjonssikkerhet, som en virksomhet kan benytte som grunnlag for å velge og implementere sikkerhetstiltak. Standarden forklarer hvordan hvert sikkerhetstiltak fungerer, hva dets mål er, og hvordan det kan implementeres. Standarden er ment å bli brukt i sammenheng med et ISMS basert på ISO/IEC 27001. Ikke alle tiltak er relevante for enhver organisasjon, tiltak velges etter behov og risikovurdering.

Standarden har endret seg opp gjennom årene. ISO/IEC 27002:2022 beskriver 93 sikkerhetstiltak fordelt over fire hovedkategorier: organisatoriske tiltak (37 tiltak), tiltak for personellsikkerhet (8 tiltak), fysiske tiltak (14 tiltak), og teknologiske tiltak (34 tiltak), som vist i figur 12.4. Tidligere utgave fra 2013 hadde en helt annen struktur etter tematiske områder på samme måte som *CIS Security Controls*. Kategoriseringen i den nye utgaven ISO/IEC 27002 ligner for øvrig på kategoriseringen i figur 1.6 i kapittel 1. Forskjellen er at ISO/IEC 27002 har skilt ut tiltak for personellsikkerhet som egen kategori, mens disse regnes som organisatoriske tiltak i figur 1.6.



Figur 12.4. Kategorier av sikkerhetstiltak definert i ISO/IEC 27002:2022.

Tiltakene i ISO/IEC 27002 er beskrevet med en enhetlig struktur. Et nyttig aspekt ved beskrivelsen av hvert tiltak er *attributter*, som gjør det enkelt å søke sikkerhetstiltak ut ifra spesifikke behov. Ved å sortere sikkerhetstiltak etter bestemte attributter kan man lage sin egen kategorisering av tiltakene, som for eksempel kategoriseringen brukt i NSMs grunnprinsipper for IKT-sikkerhet, eller i CIS Security Controls.

Som eksempel vises attributter for sikkerhetstiltak 8.13: *Sikkerhetskopiering av informasjon* fra ISO/IEC 27002. Attributter (markert med #) er spesifisert i en tabell for hvert tiltak. Tabell 12.1 viser attributter for tiltak 8.13. Teksten under gir også en kort forklaring på tiltaket og dets formål.

Tabell 12.1. Attributter for tiltak 8.13: Sikkerhetskopiering av informasjon

Type sikkerhetstiltak	Informasjons-sikkerhets-egenskaper	Cybersikkerhets-konsepter	Operasjonell kapasitet	Sikkerhets-domener
#Korrigerende	#Integritet #Tilgjengelighet	#Gjenopprette	#Kontinuitet	#Beskyttelse

Sikkerhetstiltak

Sikkerhetskopier av informasjon, programvare og systemer bør vedlikeholdes og testes regelmessig i samsvar med de avtalte emnespesifikke policyene for sikkerhetskopiering.

Formål

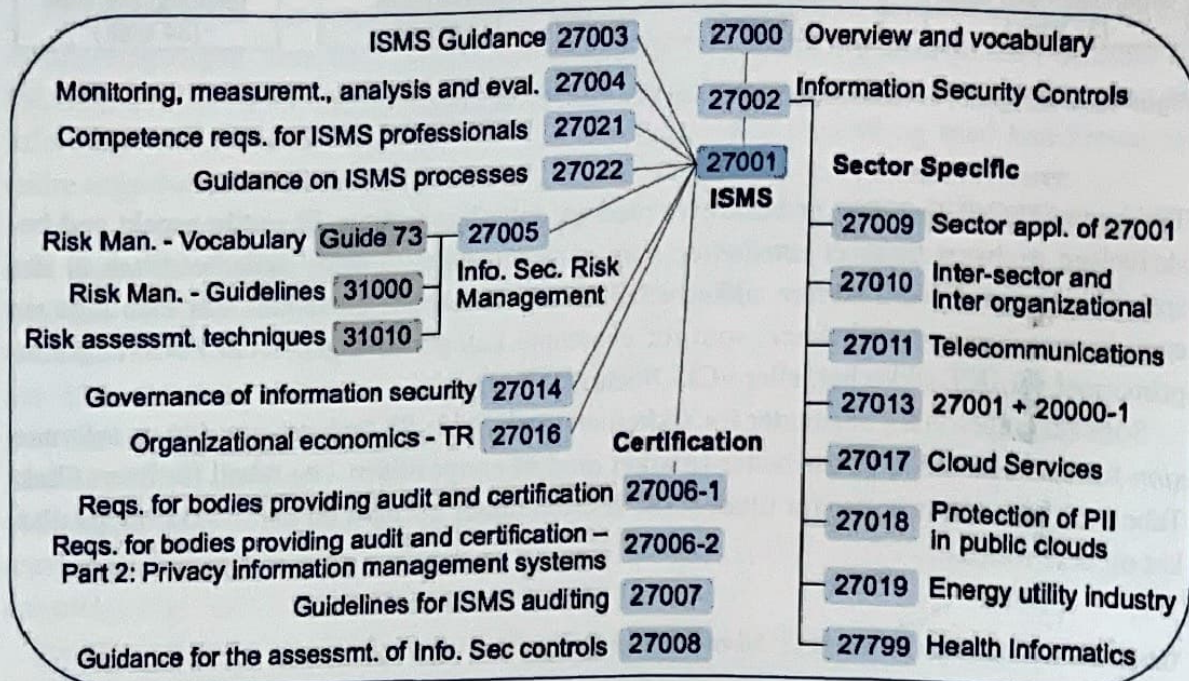
Å muliggjøre gjenoppretting etter tap av data eller systemer.

Tiltakskategoriene i ISO/IEC 27002 følger ikke naturlige faser i administrasjon av informasjonssikkerhet, som typisk er *kartlegging, forebygging, oppdaging og gjenoppretting*. Hensikten med attributtene er nettopp å gjøre det enkelt å finne sikkerhetstiltak som er relatert til disse aspektene. Et rammeverk som følger naturlige faser i administrasjon av informasjonssikkerhet, er NSMs *Grunnprinsipper for IKT-sikkerhet*, som beskrives i avsnitt 12.4.

12.3.5 27000-familien av standarder

27000-serien av ISO/IEC-standarder for informasjonssikkerhet har etter hvert vokst seg stor og variert. Den sterke dynamikken av internasjonal standardisering innenfor informasjonssikkerhet reflekterer viktigheten av fagfeltet informasjonssikkerhet i verden. Figur 12.5 viser

et utvalg av de mest sentrale standardene i 27000-serien per 2023.⁶² Nettsiden *ISO27k information security*⁶³ gir en beskrivelse av alle standardene i 27000-serien.



Figur 12.5. Familien (utvalg) av standarder i 27000-serien.

Rekken av standarder på høyre side i figur 12.5 tar for seg implementering av ISMS og informasjonssikkerhet i ulike industrisektorer. Standardene nederst til venstre i figuren fokuserer på revisjon og sertifisering av virksomheter med hensyn til ISMS og andre sikkerhetsrelaterte aktiviteter. Standarden *ISO/IEC 27005 Risk Management*, som på norsk kalles *Risikostyring for informasjonssikkerhet*, er beskrevet i kapittel 14. I midten av figuren vises også et par standarder for styring og økonomistyring av informasjonssikkerhet.

Det tar typisk flere år å utvikle en internasjonal ISO/IEC-standard, og det er en relativt byråkratisk prosess der representanter fra hele verden deltar. Selv om prosessen er grundig, kan standarder ha svakheter. Ettersom teknologien også endres raskt, er det av og til behov for å revidere standardene. Når en virksomhet velger å inkludere en standard i styring og ledelse av informasjonssikkerhet, er det viktig at virksomheter vurderer i hvilken grad det er fornuftig å følge alle retningslinjene som standarden beskriver. Det kan også være nyttig å vurdere alternativer til 27000-serien, spesielt standarder i SP 800-serien fra NIST.

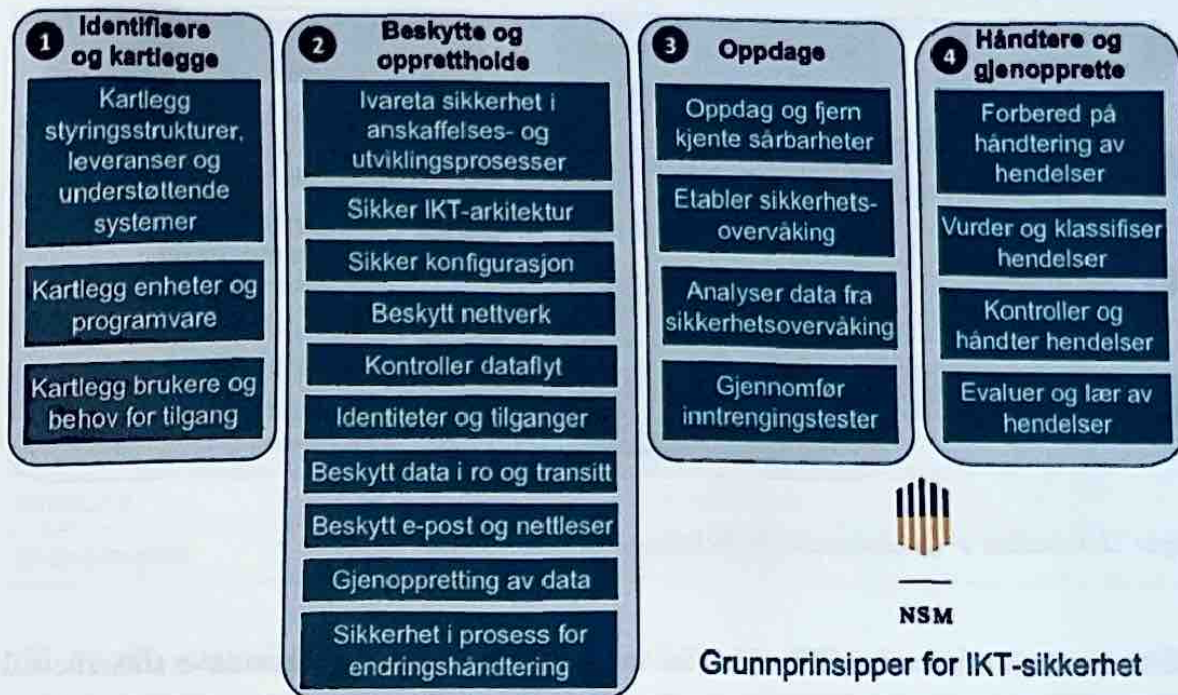
62 Takk til Taewan Park for figuren. Taewan Park er ISO-representant fra Sør-Korea.

63 <https://www.iso27001security.com/>.

12.4 Grunnprinsipper for IKT-sikkerhet

NSMs grunnprinsipper for IKT-sikkerhet er et sett med prinsipper og underliggende tiltak for å beskytte informasjonssystemer, data og tjenestene de tilbyr mot tilsiktede trusler.

NSMs grunnprinsipper for IKT-sikkerhet har som hensikt å hjelpe norske virksomheter med å styrke informasjonssikkerheten, både i offentlig og privat sektor. NSM oppfordrer spesielt virksomheter som er ansvarlige for samfunnskritiske funksjoner, til å benytte prinsippene. Figur 12.6 viser de fire kategoriene av grunnprinsipper og hovedgrupper av prinsipper og tiltak innen hver kategori.

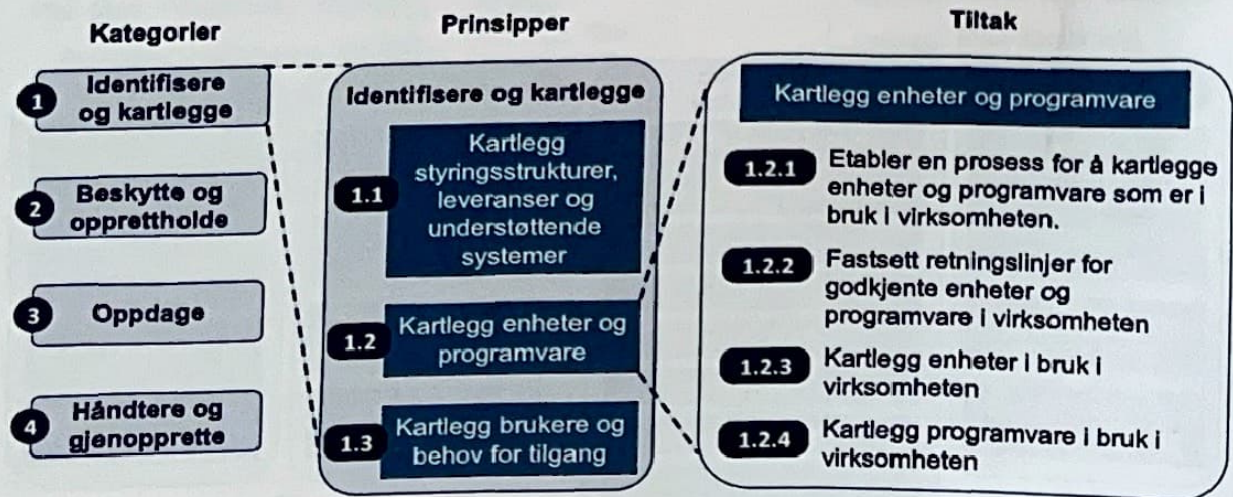


Figur 12.6. Grunnprinsipper for IKT-sikkerhet (NSM).

- 1. Identifisere og kartlegge.** Hensikten med denne kategorien av grunnprinsipper er å forstå virksomhetens leveranser og tjenester, samt å få oversikt over hvilke teknologiske ressurser, forretningsprosesser og tjenester som må sikres, og de roller og brukere virksomheten består av. Denne kategorien av tiltak er grunnlaget for en effektiv implementering av tiltak i de andre kategoriene.
- 2. Beskytte og opprettholde.** Denne kategorien grunnprinsipper inneholder forebyggende sikkerhetstiltak. Hensikten er å ivareta IKT-miljøets evne til å motstå trusler og opprettholde en kontinuerlig sikker tilstand.
- 3. Oppdage.** Denne kategorien av grunnprinsipper inneholder tiltak for å identifisere og fjerne kjente sårbarheter samt etablere sikkerhetsovervåking. Kategorien tar også for seg å oppdage avvik fra ønsket sikkerhetstilstand gjennom analyse av data fra sikkerhetsovervåking.
- 4. Håndtere og gjenopprette.** Denne kategorien av grunnprinsipper inneholder tiltak for å håndtere sikkerhetshendelser på en effektiv måte. For det første er det nødvendig å få på plass tiltak for å håndtere hendelser, som typisk består av å opprette et team for hen-

delseshåndtering (SOC- og CSIRT-kapasiteter). Når sikkerhetshendelser inntreffer under drift, skal denne kapasiteten være i stand til å vurdere, kontrollere og håndtere hendelser, gjenopprette normaltilstand samt kontinuerlig forbedre sikkerheten basert på erfaringer fra hendelseshåndteringen.

Strukturen i NSM sine grunnprinsipper er illustrert i figur 12.7, som viser de fire kategoriene med grunnprinsippene, der hvert grunnprinsipp består av et sett med sikkerhetstiltak.



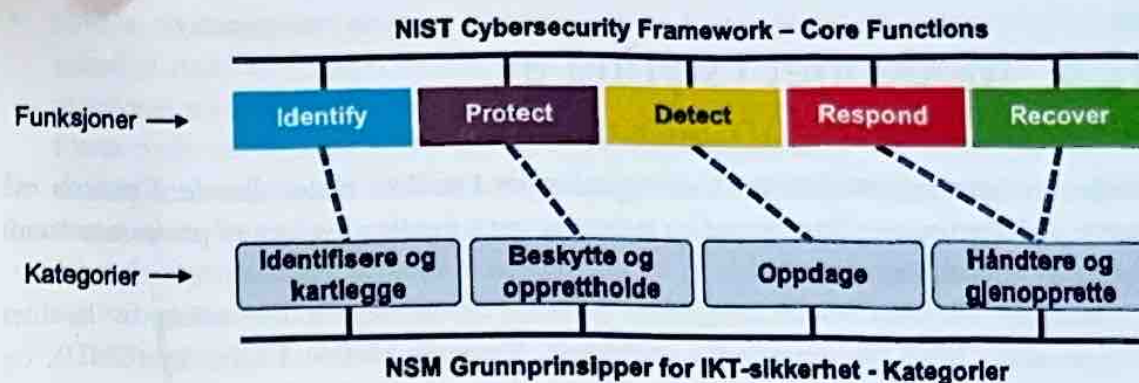
Figur 12.7. Struktur av grunnprinsipper for IKT-sikkerhet.

NSMs grunnprinsipper for IKT-sikkerhet inneholder svært mange spesifikke sikkerhetstiltak, som kan gjøre det vanskelig for en virksomhet å identifisere de viktigste og mest relevant sikkerhetstiltakene de bør investere i. For å gjøre det lettere spesifiserer veilederen en liste med 13 prioriterte sikkerhetstiltak. Virksomheter kan ha stor nytte av å vurdere disse 13 tiltakene først, og deretter hvilke andre tiltak som er relevante.

12.5 NIST Cybersecurity Framework

NIST Cybersecurity Framework (CSF) er et sett med retningslinjer som virksomheter kan bruke for å redusere cybersikkerhetsrisikoer og styrke virksomhetens sikkerhetsprofil. NIST CSF publiseres av det statlige organet NIST (National Institute of Standards and Technology) i USA. CSF er basert på, og kombinerer, eksisterende standarder, retningslinjer og praksis. NIST CSF er delt inn i tre deler, som er «Core», «Profile» og «Tiers».

CSF Core inneholder en rekke aktiviteter og tiltak for cybersikkerhet som ligner på NSMs grunnprinsipper for IKT-sikkerhet beskrevet i avsnitt 12.4. CSF Core er strukturert i fem deler, som vist i figur 12.8. Figuren viser også sammenhengen mellom NIST CSF Core og NSMs grunnprinsipper for IKT-sikkerhet.



Figur 12.8. Sammenheng mellom NIST Cybersecurity Framework og NSMs grunnprinsipper for IKT-sikkerhet.

NIST CSF er hierarkisk strukturert på samme måte som strukturen i NSMs grunnprinsipper vist i figur 12.7, men bruker ulike navn på nivåene i strukturen. Sammenhengen mellom navn i strukturen fra NIST og NSM er vist i tabell 12.2.

Tabell 12.2. Sammenheng mellom begreper i NIST CSF og NSMs grunnprinsipper for IKT-sikkerhet

NIST Cybersecurity Framework	NSMs grunnprinsipper for IKT-sikkerhet
Funksjoner	Kategorier
Kategorier	Grunnprinsipper
Underkategorier	Sikkerhetstiltak

CSF Profile er en tilnærming for virksomheter til å velge kategorier under hver funksjon, og underkategorier under hver kategori. En virksomhet kan lage sin egen profil basert på risikovurderinger, eller følge en profil laget for samme type virksomhet i samme sektor. En virksomhet kan lage en profil som viser nåværende status, og en profil som viser ønsket status for et høyere modenhetsnivå i styring av cybersikkerhet.

CSF Tiers beskriver fire modenhetsnivåer for styring av cybersikkerhet. En lignende modell er CMMI-modellen for modenhet i styring av informasjonssikkerhet, som beskrives i neste avsnitt. En omtrentlig sammenheng mellom modenhetsnivåer definert i NIST CSF og CMMI vises i tabell 12.3.

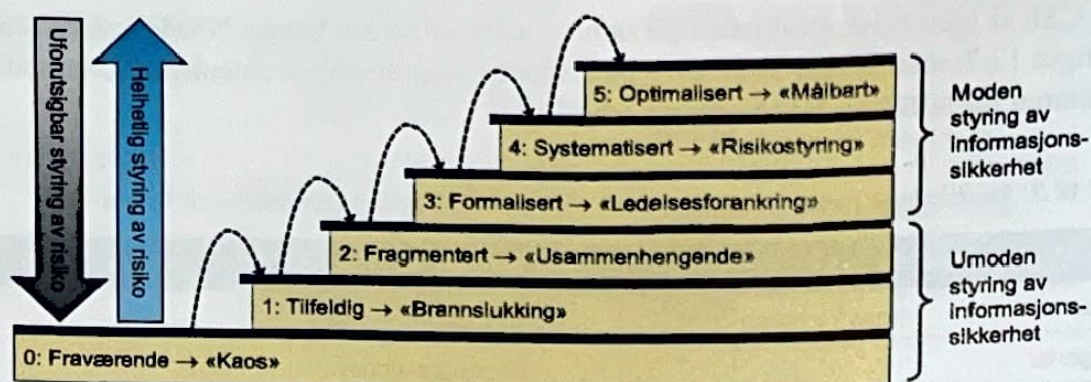
Tabell 12.3. Sammenheng mellom modenhetsnivåer i NIST CSF og CMMI

NIST Cybersecurity Framework	CMMIs modenhetsnivåer
Tier 4 (Adaptive)	Nivå 4: Systematisert prosess og Nivå 5: Optimalisert prosess
Tier 3 (Repeatable)	Nivå 3: Formalisert prosess
Tier 2 (Risk Informed)	Nivå 2: Fragmentert prosess
Tier 1 (Partial)	Nivå 1: Tilfeldig prosess

12.6 Modenhet i styring av informasjonssikkerhet

Graden av informasjonssikkerhet i en organisasjon kan ikke måles direkte. I praksis må graden av informasjonssikkerhet måles indirekte ved å vurdere kvalitet av prosessene rundt styring av informasjonssikkerhet.

Capability Maturity Model Integration (CMMI) er en metode for måling av kvalitet av prosesser. CMMI ble opprinnelig utviklet av Carnegie Mellon University (CMU), og administreres av CMMI Institute, som er et datterselskap av ISACA. En tilpasning av CMMI for styring av informasjonssikkerhet er vist i figur 12.9.



Figur 12.9. Modenhet i styring av informasjonssikkerhet.

Nivåene i modenhetsmodellen i figur 12.9 er forklart nedenfor.

- **Nivå 0: Fraværende prosess for informasjonssikkerhet.** Karakterisert av kaos. Organisasjonen er forsvarsløs mot de fleste sikkerhetstrusler.
- **Nivå 1: Tilfeldig prosess.** Karakterisert av brannslukking i etterkant av hendelser. Organisasjoner med modenhetsnivå 1 kan ha noe informasjonssikkerhetsekspertise, men tilnærmingen er karakterisert som ad hoc, og lite eller intet er planlagt. Det fins ingen dokumentasjon.
- **Nivå 2: Fragmentert prosess.** Karakterisert av å være usammenhengende. Organisasjoner med modenhetsnivå 2 har stort sett en reaktiv tilnærming, men kan ha systematiserte krav om informasjonssikkerhet innenfor isolerte områder og rutiner for hendelseshåndtering. Noe dokumentasjon fins.
- **Nivå 3: Formalisert prosess.** Karakterisert av å ha ledelsesforankring og et styringssystem for informasjonssikkerhet (ISMS). Organisasjoner med modenhetsnivå 3 har engasjerte ledere og tydelig definerte roller og organisasjonsstruktur relatert til informasjonssikkerhet. Krav om informasjonssikkerhet kartlegges relativt godt, hendelseshåndtering er organisert og prosesser dokumenteres.

- **Nivå 4: Systematisert prosess.** Karakterisert av å være basert på risikostyring på den måten at risikovurderinger danner grunnlag for krav om informasjonssikkerhet. Organisasjoner med modenhetsnivå 4 har etablert faste prosesser for å følge trusselbildet og foreta risikovurdering. Prioritering og innføring av sikkerhetstiltak følges opp med tilstrekkelige budsjetter. Beredskap er planlagt og hendelseshåndtering er organisert, inkludert øvelser. Styret og toppledelsen er informert og engasjert.
- **Nivå 5: Optimalisert prosess.** Karakterisert av at virksomheten sørger for kontinuerlig forbedring av styringssystemet for informasjonssikkerhet (ISMS). Nytteeffekten av sikkerhetstiltak kan f.eks. måles med tilnærminger beskrevet i ISO/IEC 27004, og kvaliteten av dokumentasjon og prosesser for informasjonssikkerhet gjøres gjennom internrevisjoner. Nivå 5 karakteriseres også av at virksomheten har en sterk informasjonssikkerhetskultur. Atferd gjenspeiler forståelse for at informasjonssikkerhet er alles ansvar. Organisasjoner på dette nivået tilfredsstiller ISMS-kravene fra ISO/IEC 27001, og har aktiviteter innen alle fasene av ISMS-syklusen vist i figur 12.3.

Naturligvis vil ikke karakteristikene beskrevet ovenfor alltid passe med en gitt organisasjon, slik at nivået må vurderes omtrentlig. Alle organisasjoner bør minst ha ambisjon om å etablere modenhetsnivå 3, aller helst nivå 4, mens nivå 5 kan være et ideal å jobbe mot, selv om målet aldri nås helt.

En viktig grunn for at en virksomhet minst skal ha modenhetsnivå 3, er at virksomhetsleder har det juridiske ansvaret, og da bør ledelsesforankring være et absolutt minimum. Mange lover krever at virksomheter har et styringssystem for informasjonssikkerhet, som beskrevet i kapittel 15 om regelverk for informasjonssikkerhet. For informasjonssikkerhetsleder (CISO) bør det være høy prioritet ved et lederskifte at ny toppleder raskt får revidere og signere de viktigste dokumentene i styringssystemet for informasjonssikkerhet, slik at dette ikke bare er noe som ligger igjen etter den forrige topplederen i måneder og år. Hvis en virksomhet er underlagt lover som krever at sikkerhetstiltak velges ut ifra risikovurderinger, som er tilfellet med personopplysningsloven og sikkerhetsloven, bør virksomheten være på modenhetsnivå 4 eller 5.

Oppgaver til kapittel 12

12.1 Standarder for informasjonssikkerhet

Se på listen over sikkerhetsstandarter i ISO/IEC 27000-serien, for eksempel på Wikipedia (https://en.wikipedia.org/wiki/ISO/IEC_27000-series).

Se på NIST SP800-serien (Special Publications) på <https://csrc.nist.gov/publications/sp>

- Prøv å identifisere lignende standarder i ISO/IEC 27000-serien og i NIST SP800-serien.
- Hva kan grunnen være til at ulike organisasjoner utvikler separate sett med lignende standarder?

Sikkerhetskultur

Kultur og menneskelige faktorer har en avgjørende betydning for informasjonssikkerhet. Ansatte i en organisasjon kan selv bli trusselaktører mot egen organisasjon, og ansatte kan også representere sårbarheter som kan utnyttes av eksterne trusselaktører for å angripe organisasjonen. Det er viktig å forebygge og forhindre at slike ting skjer.

I dette kapitlet lærer du om informasjonssikkerhetskultur generelt, og spesifikt om atferd som støtter sikkerhet i organisasjonen, om innsidetrusselen og om hvordan ansatte kan herdes for å bli motstandsdyktige mot sosial manipulering. Til slutt lærer du om sikkerhetsbrukervennlighet og læringsstadier for informasjonssikkerhet.

13.1 Definisjon av sikkerhetskultur

Organisasjonskultur er felles verdier, normer og virkelighetsoppfatninger som medlemmene i en organisasjon har. Verdier er det som oppfattes som viktig og verdt å streve etter, mens normer er hva som anses som akseptabelt og uakseptabelt når det gjelder holdninger, handlinger og atferd. *Informasjonssikkerhetskultur* er en del av den generelle organisasjonskulturen.

Siden denne boken handler om informasjonssikkerhet, vil vi heretter bruke den avkortede betegnelsen «sikkerhetskultur», med implisitt betydning av «informasjonssikkerhetskultur». Ofte brukes begrepet «digital sikkerhetskultur» i samme betydning. Det fins mange forskjellige definisjoner på sikkerhetskultur, der NSM sin definisjon er gjengitt nedenfor.

«Sikkerhetskultur er summen av de ansattes kunnskap, motivasjon, holdninger og atferd som kommer til uttrykk gjennom virksomhetens totale sikkerhetsatferd.»

NSM

Ettersom definisjonen ovenfor er svært kompakt, er det nyttig å utdype den litt mer. Roer og Petric (2017) identifiserer følgende syv kjernedimensjoner for sikkerhetskultur i organisasjoner:⁶⁴

- **Holdninger:** Ansattes følelser og meninger om de ulike aktivitetene som berører informasjonssikkerhet i organisasjonen. Dette inkluderer følelse av frykt eller mangel på frykt, og holdning til risiko for seg selv, for kollegaer, for organisasjonen og for eksterne.
- **Atferd:** Ansattes faktiske eller tiltenkte aktiviteter og risikotaking som kan ha en direkte eller indirekte innvirkning på informasjonssikkerheten. Dette inkluderer personlig integritet, som er hver enkelt ansattes kompass for etisk og lovlig atferd i henhold til normer og regler.
- **Kognisjon:** Ansattes bevissthet, verifiserbar kunnskap og oppfatning om praksis, aktiviteter og mestringstro relatert til informasjonssikkerhet. Det kan for eksempel være ansattes forståelse av cybertrusler, av sensitivitet ved ulike kategorier informasjon samt eksistensen av og innholdet i policyer.
- **Kommunikasjon:** Måter ansatte kommuniserer med hverandre på, deres tilhørighetsoppfatning og deres aktive støtte for varsling og rapportering av hendelser.
- **Overholdelse:** Ansattes respekt for organisatoriske sikkerhetspolicyer samt bevissthet om eksistensen av og kunnskap om innholdet i slike policyer.
- **Normer:** Oppfatninger om sikkerhetsrelatert organisatorisk oppførsel og praksis som uformelt anses å være normal eller avvikende av ansatte eller andre som er i kontakt med organisasjonen. Dette kan f.eks. være bevisste eller ubevisste forventninger om sikkerhetsatferd og uskrevede regler angående bruk av IKT. Det gjelder også holdninger til kollegaers brudd på sikkerhetspolicyer.
- **Ansvar:** Ansattes forståelse av rollene og hvilke oppgaver og plikter de har for opprettholdelse av informasjonssikkerhet i organisasjonen, og hvordan de kan sette informasjonssikkerheten i fare dersom de ikke oppfyller dette ansvaret. Dette inkluderer sikkerhet i håndtering av egne passord og andre autentikatorer, samt sikker håndtering av organisasjonens IT-utstyr, som datamaskiner og telefoner.

Målsettingen med å forbedre sikkerhetskulturen er å stimulere de ansattes atferd til å støtte digital sikkerhet i organisasjonen.

13.2 Bygging av sikkerhetskultur

God organisasjonsskultur (bl.a. ved at ansatte er motiverte med felles verdier og målsettinger) er en forutsetning for god sikkerhetskultur. NSMs *Grunnprinsipper for personellsikkerhet*⁶⁵ beskriver spesifikke tiltak for å bygge en god sikkerhetskultur i organisasjonen. Anbefalte tiltak er listet nedenfor.

⁶⁴ Roer, K. & Petric, G. (2017). The 2017 Security Culture Report – In depth insights into the human factor. CLTRe North America, s. 42–43.

⁶⁵ <https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-personellsikkerhet/>.

- a. Implementer og oppretthold rutiner for avviksrapportering og sårbarhetsoppfølging.
- b. Skap en aksept og forståelse hos medarbeiderne for hvorfor sikkerhets- og kontrollrutiner eksisterer.
- c. Lær medarbeiderne om viktigheten av rapportering.
- d. Legg til rette for en åpen tilbakemeldingskultur.
- e. Fremhev og belønn positiv sikkerhetsatferd.
- f. Motiver medarbeiderne til å øke egen kompetanse innen sikkerhet.
- g. Gi orienteringer og hold obligatoriske oppfølgingskurs om ulike sikkerhetsutfordringer, eksempelvis sosial manipulasjon, trusselbildet og trusselen fra innsidere.
- h. Lag jevnlige kampanjer for å øke medarbeidernes sikkerhetsmessige bevissthet.
- i. Legg til rette for at den enkelte medarbeider former en kulturell identitet til virksomheten.
- j. Gjennomfør øvelser innen personellsikkerhet.

Tiltakene over har ulik nytteeffekt avhengig av individuelle holdninger til hver ansatt. Nedenfor er en forenklet kategorisering av ansatte i fire kategorier.

1. Motiverte
2. Likegyldige
3. Misfornøyde
4. Hemmelige innsideagenter for fremmede stater

Det er umulig å legge en enhetlig strategi som er egnet til å styrke kunnskap, motivasjon, holdninger og atferd med hensyn til informasjonssikkerhet for alle de ovenfor nevnte kategorier av medarbeidere. Særlig kategori d) er nok uhelbredelig, og samtidig vanskelig å avdekke.

Det er viktig å anerkjenne at selv de beste kan bli lurt, for eksempel med phishing-angrep. Derfor skal organisasjonen aldri tillegge skyld for sikkerhetshendelser når en ansatt har forårsaket en sikkerhetshendelse på grunn av manglende bevissthet, og ingen skal bli beskrevet som naiv. Organisasjonen bør ha en plan for å skjerme ansatte som utilsiktet kan ha forårsaket alvorlige sikkerhetshendelser. Dette vil bidra til punkt c) og d) ovenfor. Psykologisk trygghet er det man ønsker å oppnå, og fryktkultur er det man ønsker å unngå.

Sikkerhetskultur er en integrert del av organisasjonskulturen. Å arbeide med sikkerhetskulturen bør derfor også integreres i arbeidet med å bygge en god organisasjonskultur. Denne tilnærmingen beskrives blant annet i antologien *Informationssäkerhet och organisationskultur* utgitt av Studentlitteratur (2017). Egenarten til organisasjonskulturen bør være førende for egenarten til sikkerhetskulturen. For eksempel ville et forsøk på å etablere en autoritær sikkerhetskultur mest sannsynlig være feilslått dersom organisasjonskulturen er alt annet enn autoritær.

13.3 Innsidetrusselen

En *innsidetrussel* er en ansatt eller annen person med tilgangsrettigheter som misbruker tilgangsrettigheter for å angripe organisasjonen, enten ut fra egne motiver eller på vegne av eksterne aktører, som for eksempel fremmede stater. Innsidetrusler kan være svært potente fordi

angriperen har kjennskap til organisasjonens informasjonsressurser og har autorisert tilgang til mange av disse ressursene. Kjennskap til sikkerhetsprosesser og mekanismer kan i tillegg gjøre det lettere å gjennomføre et angrep samt unngå at angrepet blir oppdaget. Innsidetrusselen kan innebære svindel, tyveri av konfidensiell eller kommersielt verdifull informasjon, tyveri av immateriell eiendom og sabotasje mot datasystemer. En fyldig rapport om innsidetrusselen er publisert av NSM.⁶⁶ En mer konsis beskrivelse av innsidetrusselen fins i kapittel 6 av boken til Paul Martin: *The Rules of Security: Staying Safe in a Risky World* (Oxford University Press, 2019).

Statistikk rundt innsidetrusselen viser at dette er et betydelig sikkerhetsproblem. Store organisasjoner med mange ansatte er ofte utsatt for innsidetrusler, mens dette forekommer sjeldnere i små organisasjoner med få ansatte. Innsidetrusselen er uansett et problem som enhver organisasjon bør ha bevissthet om, og som bør inngå i organisasjonens risikostyring.

Potensielle grupper av personer som kan bli innsidetrusler, er alle ansatte, inkludert toppledere og mellomledere, i tillegg til kunder, besøkende, forretningsforbindelser, underleverandører og konsulenter. Alle disse gruppene har visse tilgangsprivilegier som potensielt kan misbrukes. Kampen mot innsidetrusselen har som mål å sørge for at (autoriserte) tilgangsprivilegier bare blir brukt i henhold til policy, det vil si at privilegiene ikke blir misbrukt.

Tekniske tiltak for å forhindre innsidetrusselen kan for eksempel være mekanismer og prosedyrer som kontrollerer og overvåker at operasjoner som utføres, er i henhold til policy, men vi går ikke nærmere inn på slike tiltak her. Dette avsnittet tar for seg forebygging av innsidetrusler ved å styrke personlig integritet hos ansatte og andre personer som har en eller annen form for tilgang.

13.3.1 Personlig integritet

Under en ansettelsesprosess kan en virksomhet etter behov vurdere personlig integritet som et aspekt hos en jobbsøker. Selv om vurderingen konkluderer med at en jobbsøker har høy personlig integritet der og da, er det alltid uvisshet knyttet til slike vurderinger, og ansattes holdninger vil ofte endres over tid. En ansatt som i utgangspunktet har høy personlig integritet, kan under gitte omstendigheter miste både dømmekraften og integriteten og utvikle seg til å bli en innsidetrussel. Det vil ha stor verdi for en virksomhet å motvirke slike negative endringer av personlig integritet hos ansatte.

Å diskutere innsidetrusler kan være et svært sensitivt tema som organisasjonen må vurdere og behandle med varsomhet og klokskap. Feil tilnærming kan fort gjøre mer ugagn enn nytte. Hvis organisasjonen for eksempel behandler alle ansatte som potensielle innsidetrusler, kan mistenkeliggjøringen paradoksalt skape forhold som forsterker slike trusler.

Målet må være å skape en kultur som stimulerer personlig integritet hos alle ansatte og hos andre som kommer i berøring med organisasjonen. Mange elementer kan brukes for å forebygge innsidetrusler og opprettholde personlig integritet, der noen eksempler er nevnt i punktene nedenfor.

- Alle ansatte bør gjennomgå bevissthetstrening som også omhandler personlig integritet og holdning til overholdelse av policy. Treningen bør også omhandle følger ved (bevisst) brudd på policy.

66 <https://nsm.no/regelverk-og-hjelp/rapporter/temarapport-om-innsidere/>.

- Innsidetrusler har en dynamikk med bakenforliggende årsaker og typiske mønstre, ofte med gjenkjennbare indikatorer. Forvarsel om en innsidetrussel kan være endret oppførsel kjennetegnet av mistriksel og irritabilitet, og at en ansatt begynner å jobbe utenom vanlig arbeidstid. Å sørge for at ansatte forstår denne dynamikken og indikatorer, er avgjørende for å kjenne den igjen hos seg selv og hos andre, og for å styrke den enkeltes moralske dømmekraft og holdninger med hensyn til egne og andres handlinger.
- Det må skapes en kultur der ansatte ikke trenger å frykte for å bli mistenkeliggjort. Å tildele skyld kan være kontraproduktivt og kan motvirke avviksrapporing. Å skape et miljø som ikke tildeler skyld, betyr likevel ikke at enkeltpersoner ikke må stå til regnskap for sine handlinger. Enkeltpersoner må gis mulighet til å erkjenne og stå til regnskap for en hendelse, samtidig som de involveres i å kartlegge de bakenforliggende årsaker og i å takle konsekvensene. En slik tilnærming vil bidra til god håndtering av hendelsen, og til å redusere potensialet for gjentagelse hos den det gjelder, og hos andre ansatte med innsikt i hendelsen. En nærmere beskrivelse av disse aspektene gis i boken til Sidney Dekker: *The Field Guide to Understanding 'Human Error'*, 3. utg. (Ashgate, 2014).
- Påminnelser om policy er viktig. Hvis det er mange år siden en ansatt deltok i en gjennomgang av sikkerhetspolicyer, er lærdommen som sitter igjen, antagelig temmelig falmet. Enkelte ganger skyldes manglende regelmessig gjennomgang at virksomhetens ledelse heller ikke har gjort en tilsvarende gjennomgang – og dersom de ansatte for eksempel ser at virksomhetens policy fortsatt er signert av forrige direktør, som sluttet for flere år siden, kan det ha en uheldig signaleffekt.
- Ansatte med vide tilgangsprivilegier bør få særlig opplæring og oppfølging (og lønn).
- Gi støtte til, og oppfølging av, ansatte i spesielle situasjoner, som f.eks.
 - for ansatte i høyt betrodd stillinger,
 - ved konflikter og situasjoner der en ansatt kan føle seg urettferdig behandlet,
 - når en ansatt har personlige problemer eller problemer i privatlivet,
 - ved endret jobbsituasjon og
 - når en ansatt slutter (se neste avsnitt om ledelsens ansvar).
- Det er svært begrenset hvordan en arbeidsgiver kan eller bør overvåke eller følge med på ansattes privatliv og personlige forhold. Samtidig er dette faktorer som i betydelig grad kan påvirke den ansattes personlige integritet, og dermed sikkerheten i organisasjonen. Det bør legges til rette for, og informeres om, at ansatte kan søke råd hvis de har problemer av en eller annen art som ikke er direkte relatert til arbeidssituasjonen, og som de føler det er nyttig å diskutere med arbeidsgiver. Rammen rundt en slik ordning må være trygg med klare policyer om konfidensialitet og personvern. En veileder om overvåking og personvern på arbeidsplassen er publisert av Datatilsynet.⁶⁷

Det fins en kategori innsidetrusler der tiltakene ovenfor antagelig har liten virkning, nemlig aktører som opptrer på vegne av fremmede stater. Allerede etablerte holdninger og påvirkning fra oppdragsgiver (den fremmede stat) gjør det svært vanskelig å påvirke personlig integritet hos disse. Det er viktig å være klar over at denne typen innsidetrussel kan være påvirket av utpressing fra en fremmed stat. Det kan for eksempel være at en fremmed stat

67 <https://www.datatilsynet.no/personvern-pa-ulike-omrader/personvern-pa-arbeidsplassen/>.

truer med handlinger mot personen (trusselaktøren), eller mot personens familiemedlemmer som bor i den fremmede staten. Ved mistanke om denne typen innsidetrusler kan det være nyttig å søke råd hos PST.

Det kan føles ubehagelig å snakke om personlig integritet på arbeidsplassen fordi det på en måte antyder at noen av tilhørerne kanskje mangler dette. Imidlertid bør det ikke være et tabutema. Det må kunne diskuteres åpent, fordi det er relevant og kan ha stor betydning for informasjonssikkerheten.

13.3.2 Ledelsens ansvar for håndtering av innsidetrusselen

Ledelsen har en viktig rolle for håndteringen av innsidetrusselen. Ledelsen bør gi klare signaler, vise tydelige holdninger og gå foran som et godt eksempel for atferd som viser personlig integritet.

Misfornøyde ansatte har en betydelig høyere sannsynlighet enn fornøyde ansatte for å bli innsideaktører. Selv om det er helt uakseptabelt at misnøye skal føre til innsidetrusler, er det viktig å sørge for at ansatte ikke havner i situasjoner eller roller som frembringer akutt stor misnøye eller generell misnøye over lang tid. Dette er viktig ikke bare for å forebygge innsidetrusler, men også for trivsel og produktivitet i hele organisasjonen. Ledelsen har et særlig ansvar for å legge til rette for at ansatte skal trives og være fornøyde i sin arbeidshverdag.

Statistikk og forskning viser at sannsynligheten for innsidetrusler øker betydelig i forbindelse med at ansatte slutter. De vanligste grunnene til at et ansettelsesforhold opphører, er:

- frivillig oppsigelse
- pensjonering
- oppsigelse ved nedbemanning
- avskjed ved misligheter

Oppsigelse ved nedbemanning, og følelsen av urettferdighet som det ofte medfører, er en betydelig faktor når ansatte som slutter, blir innsidetrusler. Selv om det er helt uakseptabelt at en følelse av urettferdighet skal føre til innsidetrusler, bør ledelsen legge stor vekt på å sørge for «rettferdighet» når nedbemanning er nødvendig.

Det er essensielt å ha en god dialog med ansatte som slutter som følge av en nedbemanningsprosess. Ledere bør være klar over at de oppsagte og de gjenværende ansatte ofte forventer ulik lederatferd under nedbemanningsprosessen.

Det bør utformes policyer for tilgangsrettigheter avhengig av måtene et arbeidsforhold opphører på, og av type organisasjon. Tilnærminger til håndtering av tilgangsrettigheter kan være følgende:

1. Tidligere ansatte beholder begrensede privilegier.
2. Velordnet og avtalt sletting av alle privilegier.
3. Umiddelbar sletting av alle privilegier, sikkerhetsvakt følger vedkommende til utgangen.

Ved avslutning av et ansettelsesforhold kan avtaler gjennomgås med hensyn til hvilken informasjon den tidligere ansatte kan ta med seg og benytte, karantenetid, begrensning i å jobbe for konkurrerende selskap, osv.

13.4 Sosial manipulering

Kevin Mitnick er en kjent ekspert på *sosial manipulering*. Han startet som kriminell hacker rundt 1990, nettopp ved å drive sosial manipulering, ble arrestert og dømt til flere års fengsel, og er nå en prominent konsulent som driver rådgivning og holder foredrag om informasjons-sikkerhet og sosial manipulering. Basert på sin erfaring uttalte han følgende:⁶⁸

Den største trusselen mot sikkerheten til et selskap er ikke et datavirus, en upatchet sårbarhet i et program eller en dårlig installert brannmur. Den største trusselen kan faktisk være deg.

...

Det jeg personlig har erfart, er at det er lettere å manipulere mennesker enn teknologi. Mesteparten av tiden overser organisasjoner det menneskelige elementet.

Kevin Mitnick, BBC online, 2002

Sosial manipulering foregår gjennom mange kanaler, der vi skiller mellom *tekno-sosial manipulering* og *fysisk sosial manipulering*, som foregår fysisk ansikt-til-ansikt, eller gjennom sanntids kommunikasjonskanaler som videokonferanse eller telefon.

13.5 Tekno-sosial manipulering

Tekno-sosial manipulering er typisk basert på teknisk kontakt med ofrene, som e-post, SMS, sosiale nettverk, chat og via nettstedet. Det benyttes ofte en kombinasjon av ulike kanaler. En svært vanlig angrepsvektor som benytter sosial manipulering, er å sende phishing-e-post.

13.5.1 Phishing-angrep

Phishing er et tekno-sosialt angrep der trusselaktører bruker falske e-poster for å lure folk til å dele sensitiv informasjon eller installere skadevare på en datamaskin. Typiske faser av phishing-angrep er:

1. Angriper sender phishing-e-post, kommer gjennom spamfilteret og lander i offerets innboks.
 - Det er stadig vanskeligere å komme gjennom e-postfiltrering som tar i bruk nye metoder for å stoppe spam, f.eks. SPF, DKIM, DMARC. Angripere må hele tiden tilpasse seg for å omgå slike tiltak, og har raskt funnet ut hvordan de kan omgå metodene nevnt ovenfor.
 - Innholdet i e-posten må være tilstrekkelig troverdig for å lure brukeren til å tro at det er en genuin e-post.
2. Offeret blir lurt og utfører den foreslåtte handlingen i meldingen. Eksempler på handlinger er følgende:

⁶⁸ <http://news.bbc.co.uk/2/hi/technology/2320121.stm>.

- Besøke et falskt nettsted og oppgi bruker-ID og autentikator (passord og engangs-PIN).
- Svare på phishing-e-post med sensitiv informasjon.
- Installere skadevare.

3. Angriperen utnytter handlingen, f.eks. for å stjele penger.

Det fins forskjellige kategorier av phishing-angrep:

- **Masse-phishing:** Masseangrep med stort volum av e-poster ment å nå flest mulig mennesker.
- **Spyd-phishing:** Målrettet angrep rettet mot bestemte personer eller selskaper. Med etterretning kan angriper tilpasse meldingen og gjøre svindelen vanskeligere å oppdage.
- **Direktørsvindel (eng.: CEO fraud):** En type spyd-phishing som er rettet mot «stor fisk», inkludert høypofilerte individer eller de som har mye autoritet eller tilgang til å overføre store pengebeløp.
- **Klone-phishing:** Kopi av en legitim og tidligere levert e-post, med originale vedlegg eller lenker som er erstattet med skadelige versjoner. E-posten sendes fra en forfalsket e-postadresse, slik at den ser ut til å komme fra den opprinnelige avsenderen eller en annen legitim kilde.

13.5.2 Deteksjon av phishing-angrep

I de fleste tilfeller er det relativt enkelt å detektere tilfeller av phishing og bare slette den med en gang. Imidlertid er sofistikerte angripere i stand til å konstruere en phishing-e-post som selv eksperter ikke klarer å detektere.

Typiske tegn på phishing er:

- stavefeil (f.eks. «password»), manglende tegnsetting eller dårlig grammatikk
- en internettenke som skiller seg fra den som vises eller er skjult
- truende språk som krever umiddelbar handling
- uberettigede forespørsler om personlig informasjon
- kunngjøring om at du har vunnet en premie eller lotteri
- forespørsler om donasjoner

Generelt er det bra å være skeptisk og bruke sunn fornuft når du mottar en e-post. En nyttig huskeregel er STOPP–TENK–SPØR. Å «stoppe» betyr at du ikke skal klikke på lenker eller åpne vedlegg automatisk. Å «tenke» betyr at du skal vurdere om dette kan være phishing. Å «spørre» betyr at du skal spørre andre hvis du er i tvil.

Vær ekstremt forsiktig med å klikke på lenker i en e-post. Bruk datamusen til å sveve over hver lenke for å bekrefte den faktiske adressen, selv om meldingen ser ut til å være fra en trygg kilde.

Vær oppmerksom på URL-en, og se etter feil stavemåte eller om internettdomenet er et annet enn du forventer (f.eks. datatilsynet.com i stedet for datatilsynet.no).

Vurder å navigere til kjente nettsteder «manuelt» i stedet for å klikke og følge lenker i meldinger.

Undersøk nettsteder for å vurdere om de er ekte. Kriminelle nettsteder kan se helt like ut som legitime nettsteder. Sjekk at nettstedet bruker HTTPS før du fyller inn sensitiv informasjon på en nettside. Husk at HTTPS ikke sier noe om hvorvidt nettstedet er kriminelt eller ikke – det sier bare at forbindelsen er kryptert.

13.5.3 Hvis du er blitt offer for sosial manipulering

Hvis du mistenker at du har utført handlinger i en phishing-e-post eller på en svindelnettside, må du umiddelbart kontakte helpdesk eller en annen relevant enhet.

Hvis du kan ha oppgitt sensitiv, personlig eller økonomisk informasjon til et falskt nettsted, må du umiddelbart endre passord for den berørte kontoen på det ekte nettstedet. Hvis du bruker samme passord for flere kontoer og nettsteder, bør du endre det for hver konto – og aldri bruke samme passord i fremtiden.

Se etter tegn på identitetstyveri ved å gå gjennom bank- og kredittkortutskrifter for mulige uautoriserte betalinger og aktiviteter. Hvis du merker noe uvanlig, må du umiddelbart kontakte banken. Vurder å rapportere angrepet til politiet.

For sosiale nettverk er vi ofte permanent logget inn gjennom flere enheter, som laptop og mobiltelefon. Ved mistanke om at en konto er blitt hacket, dvs. at en angriper har fått tak i passordet, må man umiddelbart endre passord og logge ut av kontoen på alle enheter. Hvis man allerede er låst ute av kontoen, må man prøve å kontakte nettstedet for assistanse, som dessverre kan være frustrerende, men som noen ganger gjør at man får tilbake kontoen.

13.6 Fysisk sosial manipulering

Fysisk sosial manipulering er for eksempel når en angriper går inn i bygningen til en virksomhet og forsøker å manipulere ansatte. Angriperens mål kan være å innhente muntlig informasjon, få personer til å utføre handlinger, stjele dokumenter og materiell, installere spionutstyr som kameraer og mikrofoner eller installere komponenter i datanettet som kan tappe informasjon eller gi uautorisert tilgang. Fysisk ansikt-til-ansikt-kommunikasjon med offeret gir flest muligheter for angriperen, men videokonferanser og telefonsamtaler har også egenskaper som ligner ansikt-til-ansikt-kommunikasjon. Ikke minst har telefon og videosamtaler mulighet for bruk av avansert stemme- eller bildemanipulasjon (deepfake). På den annen side har telefon- og videokommunikasjon andre begrensninger på hva en angriper kan gjøre. I en omgivelse med direkte fysisk kommunikasjon kan angriperen spille på mange ulike strenger for å lure offeret. De to neste avsnittene beskriver strategier for direkte fysisk sosial manipulering og hvordan en organisasjon kan forsvare seg mot slike angrep.

13.6.1 Angrepsstrategier for fysisk sosial manipulering

Fysisk sosial manipulering krever at angriperen har et visst talent som skuespiller for å kunne spille en rolle som virker troverdig overfor offeret. På engelsk kalles en slik svindler *con artist*, noe som uttrykker at det nesten kan regnes som skuespillerkunst. Nedenfor beskrives et sett med teknikker som benyttes for denne typen sosial manipulering.

Nevrolingvistisk programmering (NLP). NLP er en pseudovitenskapelig tilnærming til menneskelig kommunikasjon som går ut på at språk og nevrologiske prosesser kan påvirke

atferdsmønstre (programmering). Dette kan gjøre det mulig for en angriper å påvirke et offer gjennom å speile kroppsspråk, stemmebruk, tonefall og ordbruk hos offeret. I en virksomhetssammenheng er bransje- og bedriftssjargong en viktig del av NLP. Effekten av NLP er å indusere en emosjonell forbindelse med offeret på et underbevisst nivå, noe som gjør det lettere å påvirke offeret. NLP er en teknikk som brukes av selgere for å påvirke kunder.

Bygge tillit. Avhengig av land, region og kultur er folk stort sett naturlig hjelpsomme og tillitsfulle. Denne grunntilliten kan forsterkes og utnyttes for sosial manipulering. En angriper kan starte med å bygge tillit ved å stille tilsynelatende uskyldige spørsmål under normale samtaler, og deretter sakte og umerkelig utnytte tilliten ved å be om stadig viktigere informasjon. På den måten kan angriperen lære seg bedriftssjargong, navn på nøkkelpersonell, navn på prosjekter og avdelinger, navn og lokasjon på servere og applikasjoner. Tenk deg at du er angriperen. Et triks for å få offeret til å stole på deg er at du forårsaker et problem i det skjulte, og deretter tilbyr hjelp til å fikse det. Du kan for eksempel koble om LAN-kabelen når ingen ser det, og være i nærheten når offeret klager over at nettet er nede. Å snakke negativt om fiender/konkurrenter og positivt om venner/partnere får offeret til å tro at dere er på samme side.

Indusere emosjoner. Emosjoner er nært knyttet til atferdsmønstre, noe som innebærer at endring av emosjoner kan avbryte nåværende atferd og frembringe en annen type atferd. Hvis en person vanligvis forsøker å vurdere argumenter rasjonelt, kan plutselige sterke emosjoner gjøre personen mindre årvåken og mindre i stand til å identifisere villedende argumenter. Angriperen kan for eksempel indusere spenning/glede («du har vunnet en pris»), frykt («du kommer til å miste jobben din») eller forvirring («prosjektleder sier X, men avdelingsleder sier det motsatte»).

Informasjonsoverlast. En persons evne til å tolke informasjon og vurdere argumenter kan reduseres ved at angriperen gir for mye informasjon. Angriperens mål er å skape en kognitiv og mental blindhet, eksempelvis ved å beskrive mange relevante og irrelevante aspekter samt å gi argumenter fra uventede vinkler, noe som skaper en høy mental belastning. Når belastningen går over en viss grense, kan offeret til en viss grad slutte å tolke informasjonen og vurdere argumentene.

Gjensidighet. Alle mennesker har et iboende instinkt om å gjengjelde tjenester og favører, noe som kan utnyttes for sosial manipulering. Dette instinktet slår inn selv om den første favøren ikke ble forespurt, og kan gjelde selv om returfavøren er mer verdifull enn den første favøren. Hvis offeret har mottatt en favør av angriperen, vil offeret lettere la seg manipulere av angriperen. *Dobbel uenighet* er en angreps-teknikk der angriperen først ber om to favører som offeret i utgangspunktet ikke er villig til å gi. Hvis angriperen deretter trekker tilbake forespørselen om den ene favøren, vil offeret ubevisst føle en slags forpliktelse til å ettergi den andre favøren. *Forventning* er en teknikk som går ut på at forespørselen om en favør forbindes med (løfte om) at angriperen blir en fremtidig alliert og vil gjengjelde favøren i fremtiden.

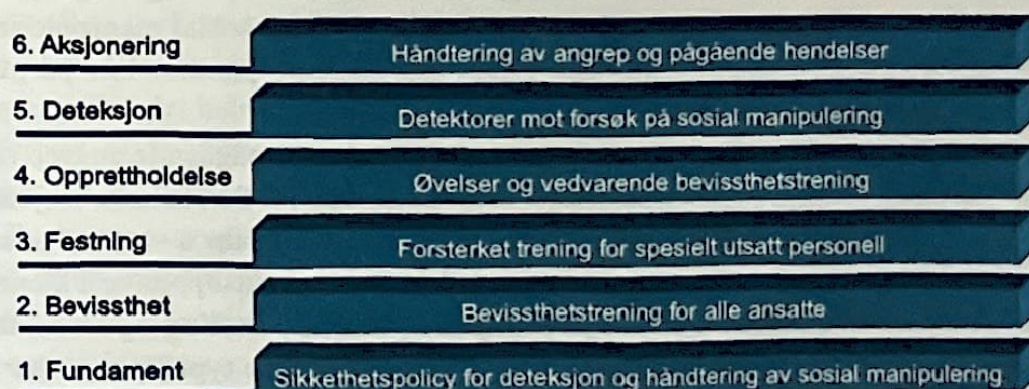
Fordreining av moralsk plikt. Denne angrepsstrategien går ut på å få offeret til å tro at ingen trenger å stå til regnskap for den type handlinger angriperen ber om, og i stedet få offeret til å føle at det er en moralsk plikt å tilfredsstille angriperens forespørsel. Angriperen kan for eksempel vise at sikkerhetspolicyen er ulogisk, har uheldige sider eller er utdatert, noe som er et argument for å ikke følge sikkerhetspolicyen.

Forpliktelseskrp. Folk har en tendens til å følge opp forpliktelser de har tatt på seg, selv når de erkjenner at det kan være uklokt. Å trekke tilbake inngåtte forpliktelser kan tolkes som å ha en svak personlig karakter, noe folk helst vil unngå. En angrepsteknikk som utnytter denne tendensen, er å skape en situasjon der angriperen først gjør en relativt ufarlig forespørsel som offeret utfører, og deretter kommer med en alvorlig forespørsel som logisk ligner på den første slik at offeret føler seg forpliktet til å utføre også den. Angriperen kan for eksempel først spørre om å bruke offerets arbeidsstasjon til en enkel oppgave. Dagen etter spør angriperen om å få bruke offerets passord til å logge på en annen arbeidsstasjon. Hvis offeret kvier seg for å gi fra seg passordet, kan angriperen si at det i praksis er det samme som det de gjorde dagen før, og at det derfor ikke fins noen grunn til å nekte.

Autoritet. Vi har en sterk tendens til å adlyde autoriteter, noe som blant annet det berømte Milgram-eksperimentet dokumenterte.⁶⁹ Det er generelt ansett som frekt å utfordre ektheten av autoriteter. Det er mange måter å ikle seg en falsk autoritet på, for eksempel med falsk legitimasjon eller falsk påstand om å være direktør, overordnet eller ha en rolle i en ekstern organisasjon. Det kreves skuespillertalent for å kunne gjøre dette på en overbevisende måte, og noen mennesker har et slikt talent.

13.6.2 Forsvar mot fysisk sosial manipulering

For å kunne forsvare seg mot fysisk sosial manipulering, som beskrevet i forrige avsnitt, bør virksomheter forstå hva dette er og kjenne typiske angrepsmønstre. En veileder for å etablere et effektivt forsvar mot fysisk sosial manipulering er publisert av SANS.⁷⁰ Modellen som beskrives i veilederen, kalles *Flernivåforsvar mot sosial manipulering*, og er illustrert i figur 13.1. Selv om modellen primært er rettet mot fysisk sosial manipulering, er den også relevant for tekno-sosial manipulering.



Figur 13.1. Flernivåforsvar mot fysisk sosial manipulering.

69 <https://no.wikipedia.org/wiki/Milgram-eksperimentet>.

70 <https://www.sans.org/reading-room/whitepapers/engineering/multi-level-defense-social-engineering-920>.

Hvert nivå av modellen i figur 13.1 er beskrevet nedenfor.

1. **Fundament.** Det må utformes en policy for håndtering av fysisk sosial manipulering. Uten det vil ansatte ikke ha noen retningslinjer å følge. Policyen kan f.eks. gi retningslinjer for verifisering av identitet, tilhørighet og autoritet, både fysisk, over telefon eller gjennom videomøter. Policyen bør forby praksis som ligner på angrepsmønstre i sosial manipulering, som for eksempel å be om passord over telefon. Policyen bør blant annet definere situasjoner der det er obligatorisk å ringe tilbake for å verifisere identitet eller tilhørighet.
2. **Bevissthet.** Alle ansatte må gjennomgå bevissthetstrening for å detektere og håndtere fysisk sosial manipulering. Elementer i treningen er å forstå typiske taktikker og å gjenkjenne angrep, vite når du skal si «nei», vite hvilken type informasjon som er følsom, forstå farer ved uformelle samtaler, lære sunn skepsis og forstå at «uniformer er billige». Begrepet «uniformer er billige» betyr at det er lett å skaffe seg falske rekvisitter som f.eks. refleksvester og arbeidsklær for å spille rollen som montør, eller en elegant dress for å spille rollen som leder. Falske adgangskort er lette å lage, og selv om de ikke virker, vil andre ansatte som regel hjelpe til med å åpne døra. Bevissthet om policyer skal få den ansatte til å føle at det eneste valget er å ikke la seg manipulere.
3. **Festning.** Nøkkelpersonell som er spesielt utsatt for fysisk sosial manipulering, er for eksempel de som sitter i resepsjonen, og de som tar hånd om helpdesk, IT-administrasjon og kundeservice. Disse trenger forsterket trening som skal danne et festningsverk mot sosial manipulering. Tilnærminger kan være oppdatering på hvilke typer angrep de kan forvente å bli utsatt for, herding gjennom å bli utsatt for simulerte angrep og selvinnsikt om hvilke typiske mentale svakheter vi mennesker har som gjør at vi kan bli villedet.
4. **Opprettholdelse.** Selv om ansatte har vært gjennom bevissthetstrening én gang, trenger de vedvarende oppfriskning, ellers vil evnen til å motstå fysisk sosial manipulering avta og bli mindre effektiv. Oppfriskning kan gjøres ved gjentatte påminnelser på plakater, meldinger og øvelser i form av simulerte angrep.
5. **Deteksjon.** Det trengs teknikker for å detektere forsøk på eller pågående angrep med fysisk sosial manipulering. I store organisasjoner er det umulig for den enkelte å kjenne alle kollegaer, som nettopp gjør det mulig for en angriper å gi seg ut for å være en ansatt. Én teknikk er å ha én eller flere ansatte som har som del av sin arbeidsoppgave å kjenne alle, slik at de lettere vil kunne identifisere en angriper. Avviksrapportering og en sentralisert logg over mistenkelige hendelser kan gjøre det lettere å kartlegge typiske mønstre for fysisk sosial manipulering. Ved oppringing kan policy kreve at man ringer tilbake, krav om å stille sentrale spørsmål og krav om «vennligst vent» for å gi mottager av oppringingen tid til å logge og vurdere oppringingen. Utspekulerte deteksjonsmetoder kan være å stille falske spørsmål for å teste hvordan en mistenkt svarer, eller å ha en «alarmkonto» der bruker-ID og passord står på gule klistremerker rundt i kontorlandskapet.
6. **Aksjonering.** I tilfelle et (antatt) angrep er det viktig at ansatte vet hvordan de skal aksjonere og forholde seg. Ettersom det dreier seg om fysisk sosial manipulering, er trygghet første prioritet. Ingen vanlig ansatt skal måtte utsette seg for fysiske farer, så derfor bør sikkerhetspersonell varsles umiddelbart. Likevel bør de ansattes reaksjon være årvåken og bestemt. Ansatte som er i direkte kontakt med den mistenkte personen, kan forsøke å

oppholde personen helt til en sikkerhetsvakt ankommer. Hvis mulig bør andre ansatte i nærheten varsles. Det er naturligvis mulig at det er falsk alarm, og policyen bør beskrive hvordan slike tilfeller håndteres. En ansatt som er blitt mistenkt, bør bli tatt godt vare på når saken er oppklart. Dette er uansett noe alle ansatte skal bli informert om under bevissthetstreningen, slik at de ikke skal være helt uforberedt på å kunne bli mistenkt.

13.7 Sikkerhetsbrukervennlighet og sikkerhetslæring

Brukervennlighet er egenskapen til et system for at en bruker skal kunne utføre en oppgave korrekt, effektivt og trygt. Sikkerhetsbrukervennlighet er noe lignende, bare at systemet er en sikkerhetsfunksjon. Dermed kan vi definere sikkerhetsbrukervennlighet slik:

Sikkerhetsbrukervennlighet er egenskapen til en sikkerhetsfunksjon for at en bruker skal kunne utføre en sikkerhetsoppgave korrekt, effektivt og trygt.

Vi kunne ønsket at sikkerhetsbrukervennlighet ikke var mer enn vanlig brukervennlighet, det vil si at brukeren ikke trengte noen som helst kompetanse i informasjonssikkerhet for å utføre sikkerhetsfunksjoner. Med andre ord – vi kunne ønsket at informasjonssikkerhet var helt transparent (usynlig) for brukeren. Dessverre er det ikke slik – for å kunne utføre sikkerhetsfunksjoner korrekt trenger vi ofte sikkerhetskompetanse.

Forskjellen mellom brukervennlighet og sikkerhetsbrukervennlighet kan illustreres med et eksempel. Hvis et system har dårlig brukervennlighet, vil brukeren typisk ikke klare å utføre oppgaven i det hele tatt, eller i alle fall ikke korrekt, noe som antageligvis blir oppdaget umiddelbart. Hvis systemet har god brukervennlighet, men samtidig har en sikkerhetsfunksjon med dårlig brukervennlighet, vil brukeren kunne utføre oppgaven, men på en usikker måte. Brukeren vil typisk se at oppgaven er utført korrekt, men vil kanskje ikke merke at det er gjort på en usikker måte.

Brukerflater til vanlige applikasjoner har mange sikkerhetslementer vi må forstå og forholde oss til. Nettlesere har ikoner med hengelås som vi må kunne tolke, vi får popup-advarsler om å godta eller forkaste sertifikater, og vi må lære oss å håndtere passord på en sikker måte.

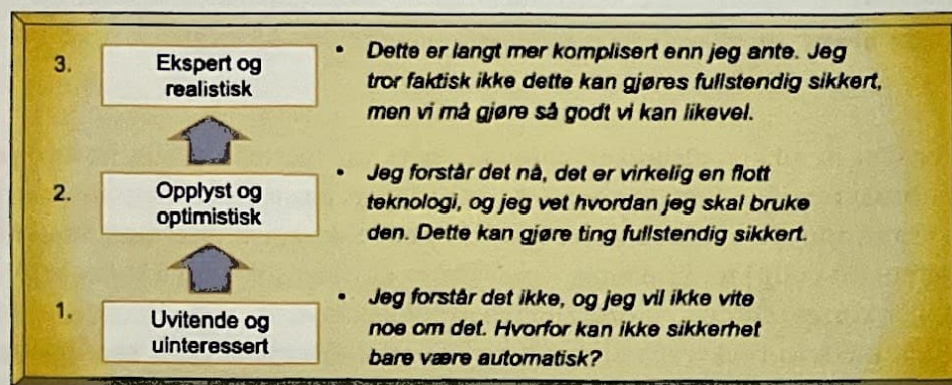
Metaforer er svært vanlig i IT-bransjen, og særlig i IT-sikkerhetsbransjen. Det snakkes om brannmur, virus, trojansk hest, nøkkel, honningkrukke osv. Noen ganger gir metaforene riktige assosiasjoner, slik at brukere intuitivt forstår et sikkerhetskonsept riktig. Andre ganger kan metaforene gi villedende assosiasjoner som gjør at brukere kan misforstå et sikkerhetskonsept. Som eksempel kan begrepet «brannmur» få brukeren til å tro at en brannmur er fullstendig tett og blokkerer alt, mens den i virkeligheten er et trafikkfilter styrt av regler (se avsnitt 6.4). Begrepet «tillit» til nøkkelsertifikater for nettsteder kan få brukeren til å tro at et nettsted som har et sertifikat, av den grunn er tillitsverdig, mens det i virkeligheten kun

betyr at domenenavnet kan autentiseres (avsnitt 5.3.1). Riktig tolkning av disse begrepene må læres, ellers kan brukeren bli villedet.

Et eksempel er et eksperiment om bruk av asymmetrisk kryptografi med offentlige og private nøkler, beskrevet i artikkelen *Why Johnny Can't Encrypt* (1999).⁷¹ I eksperimentet skulle deltagerne velge riktige nøkler for å sende en konfidensiell melding og en autentisert melding. Mange valgte å bruke sin private nøkkel for å sende en konfidensiell melding, fordi de tenkte at «konfidensiell» og «privat» hører sammen. Årsaken til denne feilen lå i misforståtte metaforer.

Gode metaforer er viktige for læring, men det er ikke alltid mulig å lage gode metaforer for avanserte sikkerhetskonsepter. Det kan være bedre å unngå metaforer enn å bruke dårlige. I stedet bør man definere nye sikkerhetskonsepter og gi dem et beskrivende semantisk innhold som må læres. PKI (avsnitt 5.2) og fremoverhemmelighold (avsnitt 4.7.4) er begreper som ikke bygger på metaforer, og som må læres for å forstå hva de betyr.

Sikkerhetslæring er viktig for å kunne bruke sikkerhetsteknologi riktig. Figur 13.2 illustrerer stadier av sikkerhetslæring som folk typisk går gjennom.



Figur 13.2. Stadier av sikkerhetslæring.

Denne boken er ment å støtte sikkerhetslæring på en måte som gjør at du som leser blir ekspert og realistisk med hensyn til hva som er mulig å oppnå med informasjonssikkerhet. Betydningen av ekspertise i informasjonssikkerhet drøftes i boken til Christian Espinosa: *The Smartest Person in the Room: The Root Cause and New Solution for Cybersecurity* (Lioncrest, 2021).

71 https://people.eecs.berkeley.edu/~tygar/papers/Why_Johnny_Cant_Encrypt/OREilly.pdf.

Oppgaver til kapittel 13

13.1 Bygging av sikkerhetskultur

- a. Ta utgangspunkt i aspektene for sikkerhetskultur beskrevet i avsnitt 13.1. Nevn et eksempel på dårlig sikkerhetskultur for hvert aspekt.
- b. Med utgangspunkt i eksemplene fra a: Foreslå tiltak for å forbedre sikkerhetskulturen.
- c. Foreslå mulige strategier som er egnet til å styrke kunnskap, motivasjon, holdninger og atferd med hensyn til informasjonssikkerhet for følgende kategorier av ansatte i en organisasjon:
 - ansvarsfulle
 - likegyldige
 - misfornøyde
 - hemmelige agenter for fremmede stater

Hvordan kan ulike strategier anvendes når det er uvisst hvilken kategori hver ansatt passer inn i, eller bør man forsøke å utforme en strategi som passer for alle kategorier av ansatte?

13.2 Innsidetrusselen

- a. I perioden fra å bli ansatt til å slutte i et selskap, når er det størst sannsynlighet for at en ansatt blir en innsidetrussel?
- b. Tiltak for å bygge holdninger og personlig integritet kan bidra til å forhindre at anstte blir en innsidetrussel. Hva er en type innsidetrussel som er lite påvirkelig for denne typen tiltak?

13.3 Sosial manipulering

- a. Beskriv måter å bruke sosial manipulering på for
 - å installere skadevare på PC-en til administrerende direktør i et selskap
 - å få uautorisert tilgang til bygningen for selskapets hovedkontor
- b. Tenk deg at ansatte utgjør menneskelig «IDS» (Intrusion Detection System) mot sosiale manipuleringsangrep. Hva ville være en «falsk positiv» og en «falsk negativ» deteksjon av sosial manipulering? Vurder potensiell alvorlighet av falsk positiv og falsk negativ deteksjon av sosial manipulering.
- c. Hva bør du gjøre hvis du tror du er blitt lurt av sosial manipulering?

Risikostyring for informasjonssikkerhet

Risikostyring er et sentralt element i styring og ledelse av informasjonssikkerhet. Risikovurdering som inngår i risikostyring, er en av de tre kildene til krav om informasjonssikkerhet, som forklart i avsnitt 1.5. Det betyr at innføring av sikkerhetstiltak blant annet gjøres på grunnlag av risikovurderinger, med det formål å redusere risikoen til et akseptabelt nivå.

I dette kapitlet lærer du at risikostyring for informasjonssikkerhet er en prosess der hovedelementet er risikovurdering som kartlegger relevante risikoer. Du lærer hvordan en virksomhet kan utføre risikovurderinger, og hvordan dette danner grunnlag for håndtering av risikoen slik at den reduseres til et nivå som er akseptabelt for virksomhetens ledelse.

14.1 Tolkning av risiko og risikostyring

Begrepet «risiko» brukes svært ofte i dagligtale, der ordet kan ha ulike meninger. Vi forstår intuitivt de ulike meningene av ordet ved at vi tolker det ut fra sammenhengen. Nedenfor er noe eksempler.

- a) «Det er stor risiko ved å kjøpe bitcoin.»
- b) «Det er liten risiko ved å sette pengene i banken.»
- c) «Det er en risiko for regnvær når vi skal ha hageselskap på lørdag.»
- d) «Løsepengevirus gir en betydelig risiko.»

For å klargjøre betydningen av «risiko» i hvert utsagn over kan utsagnene omskrives ved å bytte ut ordet «risiko» med et mer presist begrep, slik som vist nedenfor.

- a) «Det er stor *uvisshet om fortjeneste eller tap* ved å kjøpe bitcoin.»
- b) «Det er liten *uvisshet om fortjeneste eller tap* ved å sette pengene i banken.»
- c) «Det er en *sannsynlighet* for regnvær når vi skal ha hageselskap på lørdag.»
- d) «Løsepengevirus gir en betydelig *sannsynlighet for negative konsekvenser*.»

Utsagnene over gjenspeiler at «risiko» kan tolkes som *uvisshet (om målsettinger)* eller som *sannsynlighet (for negative konsekvenser)*. Disse to tolkningene gjenfinnes i definisjoner av risiko i internasjonale standarder.

14.1.1 Definisjon av informasjonssikkerhetsrisiko

Den mest generelle standarden for risikostyring er *ISO 31000:2018 Risikostyring*.⁷² Denne internasjonale standarden definerer *risiko* slik:

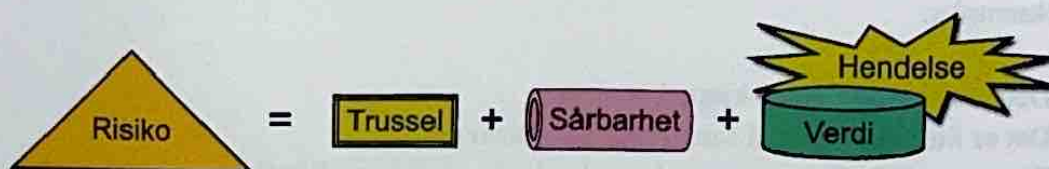
«Risiko er effekten av uvisshet på målsettinger.»

Denne definisjonen er så abstrakt at den nesten kan virke meningsløs. Imidlertid må en generell definisjon av risiko nødvendigvis være tilstrekkelig abstrakt for å dekke alle tolkninger av risiko i ulike sammenhenger. Innenfor finanssektoren er uvisshet om fremtidig fortjeneste eller tap ved investeringer et sentralt aspekt ved risiko, der definisjonen ovenfor passer svært godt.

I sammenheng med informasjonssikkerhet gir standarden *ISO/IEC 27005 Risikostyring for informasjonssikkerhet* flere tolkninger av risiko som er mer presise enn definisjonen over. Tolkningen nedenfor fra ISO/IEC 27005 er en god arbeidsdefinisjon på *informasjonssikkerhetsrisiko*:

«Informasjonssikkerhetsrisiko er assosiert med potensialet for at en gitt trussel vil utnytte sårbarheter rundt verdier og dermed skade organisasjonen.»

Tolkningen av risiko over er illustrert i figur 14.1. Her består risiko av en relevant sammenstilling av en trussel som utnytter en sårbarhet med resultat at en verdi blir skadet.



Figur 14.1. Risiko bestående av en trussel som utnytter en sårbarhet og skader en verdi.

Vær klar over at det fins mange risikoer, der hver enkelt består av en relevant sammenstilling av trussel, sårbarhet(er) og hendelse på verdi(er). En viktig del av risikovurderingen er nettopp å identifisere relevante risikoer på denne måten, som beskrevet i avsnitt 14.4.

72 <https://www.iso.org/iso-31000-risk-management.html>.

Standarden ISO/IEC 27005 gir også en annen tolkning som kan være en god arbeidsdefinisjon av *nivå* for informasjonssikkerhetsrisiko:

«Informasjonssikkerhetsrisiko uttrykkes ofte som en kombinasjon av sannsynligheten for en informasjonssikkerhetshendelse og dens konsekvens.»

Tolkningen av denne definisjonen av risiko er illustrert i figur 14.2. Her beregnes et risikonivå ut fra sannsynlighet for en sikkerhetshendelse og hendelsens konsekvens. Begrepet *risikoeksponering* (eng.: risk exposure) brukes ofte som synonym for risikonivå.



Figur 14.2. Risiko som kombinasjon av sannsynlighet for en hendelse og hendelsens konsekvens.

Denne tolkningen av informasjonssikkerhetsrisiko stemmer godt overens med den amerikanske standarden *NIST SP 800-39 Managing Information Security Risk*,⁷³ som gir følgende definisjon av informasjonssikkerhetsrisiko (oversatt):

«Informasjonssikkerhetsrisiko er et mål på i hvilken grad en entitet er truet av en potensiell omstendighet eller hendelse, og er vanligvis en funksjon av (i) de negative konsekvenser som vil oppstå hvis omstendigheten eller hendelsen inntreffer, og (ii) sannsynligheten for hendelsen.»

Under risikovurderingen er beregning av risikonivå nettopp basert på kombinasjonen av sannsynlighet og konsekvens av en sikkerhetshendelse, der beregningen kan gjøres på en kvalitativ, kvantitativ eller relativ måte, som beskrevet i avsnitt 14.5. Begrepet *risikoeksponering* (eng.: risk exposure) brukes ofte som synonym for risikonivå.

Modeller for tolkningene og definisjonen av informasjonssikkerhetsrisiko over er beskrevet i neste avsnitt.

14.1.2 Modeller for informasjonssikkerhetsrisiko

Modeller for informasjonssikkerhetsrisiko er nyttige for å forklare og visualisere hva risiko betyr, og for å analysere risiko. Figur 14.3 viser en generell og relativt abstrakt modell for sikkerhetsrisiko.

73 <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf>.



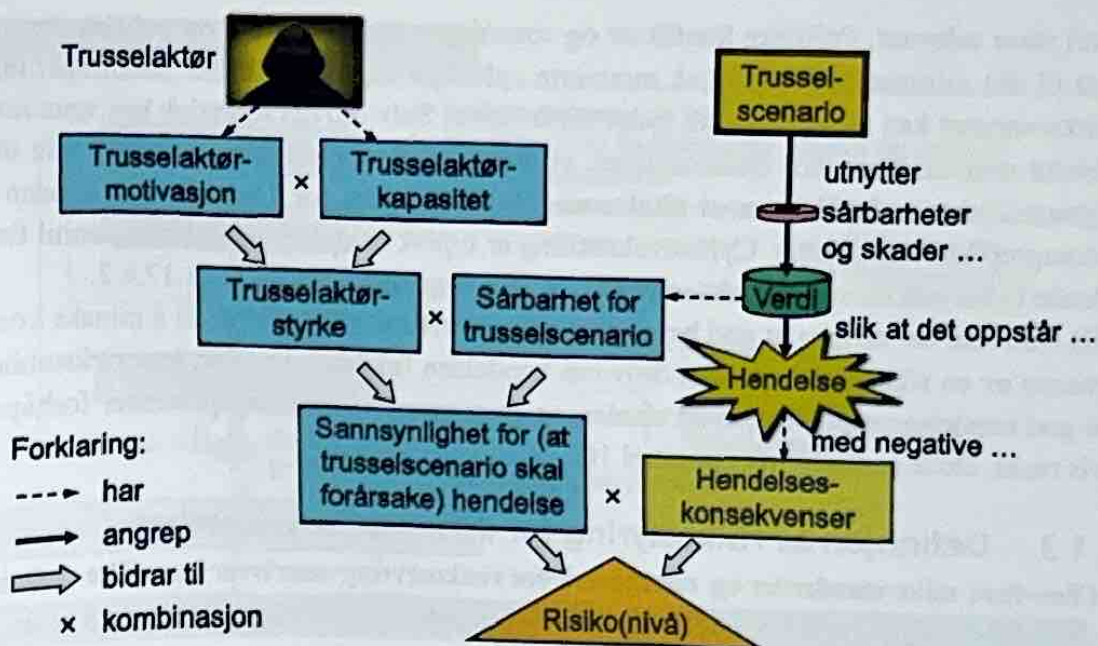
Figur 14.3. Generell modell for sikkerhetsrisiko.

Tolkningen av figur 14.3 går ut på at sikkerhetsrisiko oppstår når det fins sårbarheter som kan utnyttes av trusler og dermed skade verdier. Figuren skal også vise at risikonivået (størrelsen på triangelet) øker proporsjonalt med (i) verdienes mengde/størrelse, (ii) sårbarhetenes alvorlighet og (iii) truslenes antall/styrke. Begrepene «trussel» og «sårbarhet» er beskrevet i avsnitt 1.6.

Begrepet «verdi» har en tvetydighet som kan skape forvirring. På den ene siden kan «verdi» bety en *ressurs* som er viktig for virksomhetens forretningsprosesser og målsettinger. På den andre siden kan «verdi» bety *graden av viktighet* av ressursen. Å benytte begge betydningene sammen kan gi forvirrende utsagn som at «*verdien av verdiene må estimeres som del av risikovurderingen*». I tillegg kan begrepet «verdi» benyttes for å uttrykke strategiske og etiske målsettinger for en virksomhet, som for eksempel «*vårt verdigrunnlag er å være bærekraftig for miljøet*». Vi vil primært styre unna denne tvetydigheten ved at «verdi» tolkes ut fra sammenhengen. Om nødvendig blir ordet omskrevet med «ressurs» eller lignende.

En mer detaljert visualisering av sammenhengen mellom sikkerhetsrisiko og relaterte begreper ser du i figur 14.4. Denne visualiseringen gir en dypere forståelse av dynamikken rundt sikkerhetsrisiko, og er egnet som støtte til praktisk vurdering og analyse for å beregne risikonivå.

Tolkningen av figur 14.4 starter med at det fins en *trusselaktør* som har en viss *motivasjon* og en viss *kapasitet* til å angripe en *verdi* basert på et *trusselscenario*. Vær oppmerksom på at det ikke alltid fins en tydelig trusselaktør med en tilsiktet målsetting. For eksempel kan brann i datasenteret forårsakes av feil og uhell. I kontekst av risikostyring for informasjonssikkerhet legges det imidlertid stor vekt på uønskede hendelser som følge av tilsiktede handlinger, der en trusselaktør spiller en tydelig rolle. Trusselaktørens styrke kan defineres som kombinasjonen av motivasjon og kapasitet. På den andre siden fins det en grad av sårbarhet for trusselscenarioet som gjør det mulig for trusselaktøren å skade verdier og dermed forårsake en sikkerhetshendelse. Sannsynligheten for en sikkerhetshendelse kan defineres som kombinasjonen av trusselaktørens styrke og grad av sårbarheter for trusselscenarioet. På dette stadiet må alvorligheten av konsekvensene som følge av hendelsen estimeres. Til slutt kan sikkerhetsrisikonivået beregnes som en kombinasjon av sannsynlighet for hendelsen og dens konsekvens.



Figur 14.4. Detaljert modell for sikkerhetsrisiko.

Det er interessant å tenke gjennom elementene i figur 14.4. Gjennom digitaliseringen blir flere og flere forretningsprosesser, og samtidig deres iboende sårbarheter, eksponert online, noe som igjen bidrar til å øke trusselaktørenes motivasjon.

Trusselaktørers motivasjon er i stor grad påvirket av en svært god forventet avkastning på investering (ROI: Return On Investment). Cyberangrep har forholdsvis lav kostnad, kan lett utføres utenfor lovens rekkevidde og kan gi stor gevinst. Kapasiteten kan i stor grad baseres på økende tilgjengelighet av ekspertise og avanserte verktøy.

Trusselaktørens fordelaktige ROI ved å utføre angrep gjenspeiles ikke nødvendigvis av en fordelaktig ROI hos virksomheter ved å fjerne sårbarheter for å motvirke angrep. Et eksempel er leverandørkjedeangrep, hvor trusselaktøren er motivert av verdien hos en sluttbruker, mens sårbarheten som utnyttes i angrepet, kan ligge hos en underleverandør som ikke ser verdien hos sluttbrukeren og derfor ikke har tilstrekkelige insentiver til å fjerne sårbarhetene.

Utfordringen her er at underleverandøren gjerne har en dårlig forutsetning, eller manglende interesse, for å vurdere verdien som underleverandørens kunder representerer for en trusselaktør.

En annen motivasjon for en trusselaktør er å bruke virksomhetens verdier eller aktivitet som et middel til å angripe en helt annen part. Et eksempel kan være å angripe navigasjonssystemet til et stort skip slik at det grunnstøter i en smal og viktig farled som for eksempel Suezkanalen.

Figur 14.4 viser hvor tiltak kan settes inn for å redusere risikoer. Den mest vanlige måten å senke risikonivået på er å fjerne sårbarheter for trusselscenarioer. Selv om en trusselaktør er motivert og har betydelig kapasitet, vil angrepsforsøk feile hvis systemer og nettverk ikke har sårbarheter som kan utnyttes.

I prinsippet kan risikonivået senkes hvis det er mulig å redusere trusselaktørers motivasjon. I utgangspunktet virker det vanskelig å styre en trusselaktørs motivasjon, men det kan

likevel være relevant. Politiske konflikter og spenninger mellom stater og politiske grupper bidrar til økt motivasjon for politisk motiverte *cyberoperasjoner*. Uetiske handlinger utført av virksomheter kan fremprovosere *cyberhaktivisme*. Selv om det teoretisk kan være mulig å påvirke motivasjonen hos trusselaktører, vil effekten av slike tiltak som regel være uforutsigbare. *Cyberavskrekking* er et tiltak som faktisk benyttes for å senke motivasjonen for cyberangrep hos opponenter. Cyberavskrekking er typisk en del av cyberstrategien til fremtredende cybermakter som for eksempel USA, noe som beskrives i avsnitt 17.4.2.

Til slutt kan det nevnes at god beredskap og hendelsesrespons bidrar til å minske konsekvensene av en sikkerhetshendelse. Selv om hendelsen faktisk inntreffer, kan virksomheter med god hendelsesrespons reparere skaden og gjenopprette forretningsprosesser forhåpentligvis raskt. Dette er beskrevet i kapittel 16.

14.1.3 Definisjon av risikostyring for informasjonssikkerhet

Det fins flere ulike standarder og rammeverk for risikostyring som hver har ulike definisjoner. Standarden *ISO 31000:2018 Risikostyring* definerer *risikostyring* på følgende måte:

«Risikostyring består av koordinerte aktiviteter for å styre og lede en organisasjon med hensyn til risiko.»

Ettersom ISO 31000 er en generell standard, er definisjonen ovenfor nødvendigvis relativt abstrakt. Standarden *ISO/IEC 27005 Risikostyring for informasjonssikkerhet* gir følgende definisjon, som er mer spesifikk og relevant for informasjonssikkerhet:

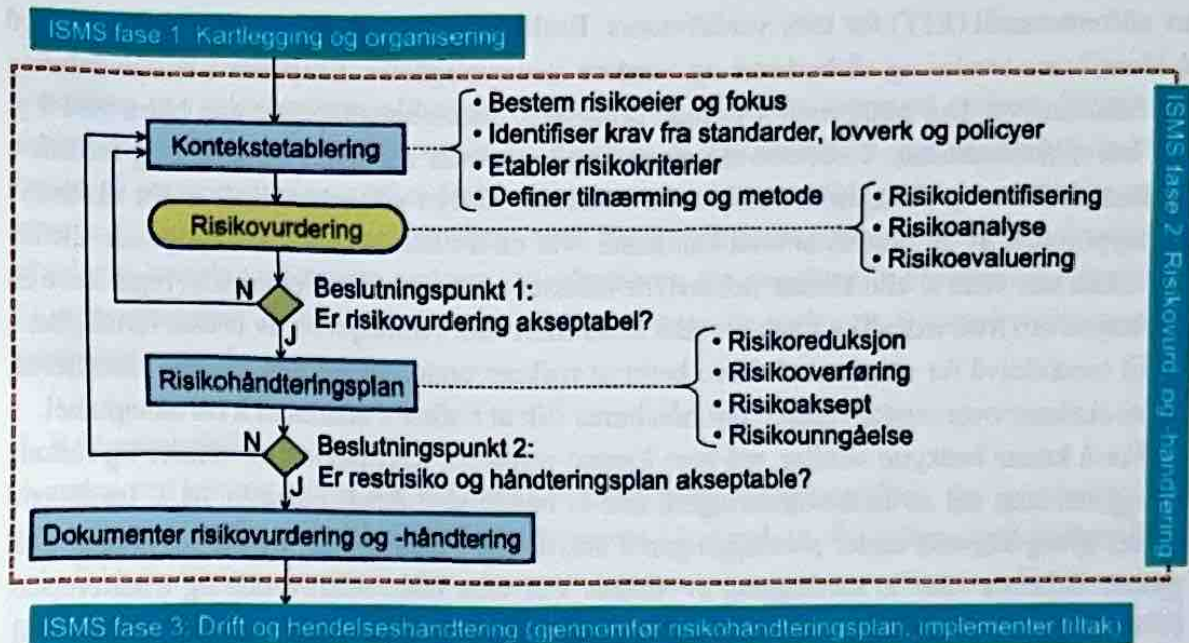
«Risikostyring for informasjonssikkerhet er å analysere hva som kan skje, og hva de mulige konsekvensene kan være, før man bestemmer hva som bør gjøres og når, for å redusere risikoen til et akseptabelt nivå.»

Det hersker en generell konsensus om hva risikostyring er, og hva som bør inngå i prosessen for risikostyring. Hele prosessen for risikostyring er relativt omfattende, som beskrevet i neste avsnitt.

14.2 Prosess for risikostyring

En prosess for risikostyring av informasjonssikkerhet er beskrevet i standarden *ISO/IEC 27005*. Denne prosessen består av faser og beslutningspunkter, som vist i figur 14.5.

Det er ikke alltid nødvendig eller hensiktsmessig for en virksomhet å gjennomføre hele prosessen i figur 14.5. Det kan være tilstrekkelig å gjennomføre deler av prosessen hvis virksomheten f.eks. bare har én, eller et utvalg, av følgende målsettinger:



Figur 14.5. Prosess for risikostyring for informasjonssikkerhet (ISO/IEC 27005).

- Få oversikt over trusler
- Få oversikt over sårbarheter
- Få oversikt over eksisterende risikoer
- Peke ut relevante sikkerhetstiltak
- Vurdere restrisiko etter nye foreslåtte sikkerhetstiltak
- Gi grunnlag for å kjøpe cyberforsikring
- Gi grunnlag for å spesifisere budsjett for håndtering av risiko

Ved å gjennomføre hele prosessen vil alle målsettingene ovenfor oppnås. De forskjellige fasene i risikostyringsprosessen i figur 14.5 er beskrevet i avsnittene under.

14.2.1 Kontekstetablering

Aktiviteter i risikostyringsprosessen må naturligvis planlegges. Elementer i planleggingen er blant annet å

- sette sammen team som har ansvar for utførelse av risikovurdering og andre aktiviteter
- spesifisere hvem som er risikoeier og fokusområde for risikovurdering
- identifisere krav fra standarder, lovverk, sektorspesifikke rammeverk og policyer
- spesifisere et terskelnivå og/eller et sett med kriterier for akseptabel risiko
- velge en metode eller tilnærming for risikovurdering
- velge en modell for risikoanalyse som skal brukes til å beregne risikonivåer
- antyde detaljnivå for kartlegging av verdier og ressurser

Et team for utførelse av risikostyring bør ha en representativ sammensetning. For risikovurderingen kan eiere av verdier og ressurser bidra med å kartlegge disse og spesifisere viktighet

av sikkerhetsmål (KIT) for hver verdi/ressurs. Brukere og sikkerhetsekspertene kan bidra med å identifisere trusler og sårbarheter og vurdere sannsynligheter. Ekspertene i risikovurdering og risikoanalyse kan bidra med å veilede prosessen. Sikkerhetsekspertene kan bidra med å gi råd om sikkerhetstiltak. Ledelsen må gjennomgå rapporter for risikovurdering og foreslåtte sikkerhetstiltak, og godkjenne budsjett for tiltakene. Et dyrt sikkerhetstiltak er for eksempel en toppmodell av en brannmur som kan koste over en million kroner. Et inngripende sikkerhetstiltak kan være at alle ansatte må benytte tofaktor-autentisering. Det vil som regel være en diskusjon om hvorvidt slike tiltak er verdt kostnaden eller reduksjonen av brukervennlighet.

Et terskelnivå for akseptabel risiko betyr at risikoer under terskelverdien kan aksepteres, mens risikoer over terskelverdien bør håndteres slik at risikoen endres til å bli akseptabel.

For å kunne beskytte verdier, må man kjenne verdiene. Kartlegging av verdier og ressurser gjøres som del av risikovurderingen, noe vi beskriver i detalj i avsnitt 14.3. Imidlertid er det nyttig allerede under planleggingen å antyde hvor detaljert denne kartleggingen skal gjøres. Erfaring viser at kartlegging av verdier kan være både tidkrevende og frustrerende. Hvis teamet forsøker å gjøre kartleggingen svært detaljert, risikerer de å aldri komme i mål. Kartlegging av ressurser og verdier bør derfor gjøres relativt grovkornet.

14.2.2 Risikovurdering

Fasen for risikovurdering er hovedelementet i risikostyringsprosessen. Denne fasen er relativt omfattende, og er beskrevet i detalj i avsnitt 14.3. Vi nevner her bare at risikovurdering består av følgende trinn:

- **Risikoidentifisering** – kartlegging av alle relevante risikoer
- **Risikoanalyse** – beregning av nivåer for hver risiko
- **Risikoevaluering** – rangering og prioritering av risikoer i forhold til terskelverdi og kriterier
- **Kommunisering** – rapportering av risikovurderingen

Etter risikovurderingen følger beslutningspunkt 1. Dette beslutningspunktet tar stilling til om resultatet av risikovurderingen er tilfredsstillende. Det er mulig at de beregnede risikonivåene har en svært skjev fordeling, for eksempel at flesteparten av risikoene har samme nivå (f.eks. alle har bare svært lave nivåer eller bare svært høye nivåer), noe som gjør det nokså vanskelig å rangere og prioritere risikoene. Om nødvendig kan kalibrering og estimering av sannsynligheter og konsekvensnivåer endres, eller beregningsmodellen for risikoanalyse endres, for å oppnå en bedre spredning av risikonivåene. Husk at kvalitative eller relative risikonivåer ikke har noen absolutt betydning. De skal kun være et grunnlag for å rangere og prioritere risikoer og for å kunne sammenligne med et terskelnivå.

En annen grunn til å anse rapporten fra risikovurderingen for utilfredsstillende er hvis det er betydelig uvisshet rundt en eller flere høye risikoer. I utgangspunktet skal en høy risiko prioriteres for å bli håndtert, noe som typisk vil medføre en kostnad. Uvisshet rundt en høy risiko betyr dermed at det hersker tvil om hvorvidt håndtering av risikoen er nødvendig. Uvisshet rundt risikoer kan være vanskelig å redusere, men hvis mulig kan det gjøres et forsøk på å gjøre en mer grundig vurdering av enkelte risikoer.

14.2.3 Risikohåndtering

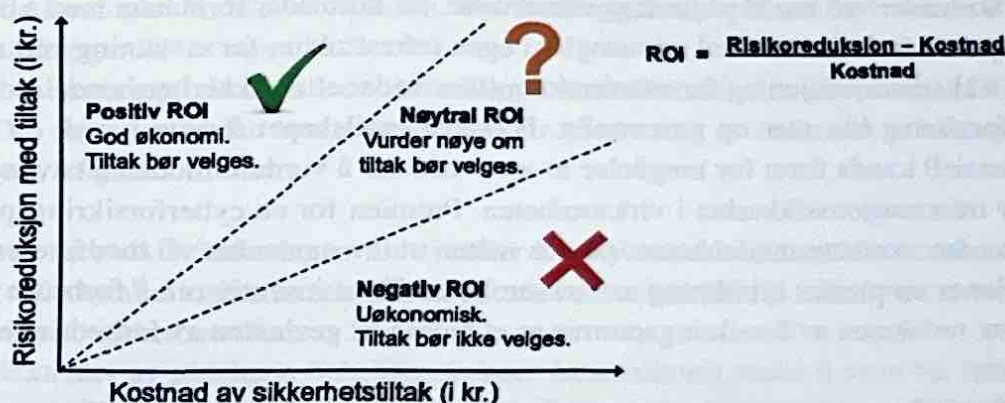
Resultatet av risikovurderingsfasen er en rangert og prioritert liste med risikoer. Prioriterte risikoer er de som anses uakseptable. Hva som er akseptabelt eller uakseptabelt, kan være basert på sammenligning med et forhåndsbestemt terskelnivå eller ut fra en særskilt vurdering av risikoer som har et relativt høyt nivå. Risikohåndteringsfasen består av å foreslå og planlegge hvordan prioriterte risikoer skal håndteres. De fire aktuelle håndteringsmåtene er: 1) redusere risiko, 2) dele eller overføre risiko, 3) beholde risiko og 4) unngå risiko, som er beskrevet nedenfor.

1. Redusere risikoen

Å redusere risikoen gjøres normalt ved å implementere sikkerhetstiltak, der relevante tiltak er beskrevet i ulike veiledere og standarder nevnt i kapittel 12. Å innføre et sikkerhetstiltak vil alltid medføre en kostnad, som i forretningssammenheng er en investering. For å avgjøre om investeringen lønner seg, er det i utgangspunktet nødvendig å estimere gevinsten ved å innføre sikkerhetstiltaket. Hvis vi antar at det er mulig å estimere både kostnaden og gevinsten av å innføre et sikkerhetstiltak, kan vi beregne ROI (*Return On Investment*), kalt *avkastning på investering* på norsk. Formelen for å beregne ROI er gitt nedenfor:

$$ROI = \frac{\text{Gevinst} - \text{Investering}}{\text{Investering}}$$

I vårt tilfelle er investering det samme som kostnad ved å innføre et sikkerhetstiltak, mens gevinst er det samme som risikoreduksjon, der begge er målt i kroner. Figur 14.6 illustrerer hva det betyr at et sikkerhetstiltak har positiv, negativ eller nøytral ROI.



Figur 14.6. ROI (avkastning på investering) ved innføring av sikkerhetstiltak.

ROI-modellen for vurdering av sikkerhetstiltak illustrert i figur 14.6 er relativt teoretisk, og ikke direkte anvendbar i praksis. Denne modellen forutsetter at det er mulig å estimere forventet nominell verdi av en risikoreduksjon målt i et kronebeløp, men i praksis kan det være vanskelig annet enn med svært grove overslag. Figur 14.6 er derfor ment å illustrere grunnprinsippet for å velge sikkerhetstiltak, nemlig at dyre tiltak kan velges hvis det kan antas å

ha en betydelig effekt for å redusere sikkerhetsrisikoen. Hvis det kun forventes en moderat effekt av et sikkerhetstiltak, bør det ikke medføre særlig stor kostnad å implementere. Imidlertid fins det tiltak der estimering av ROI kan gjøres relativt nøyaktig. Tiltak som reduserer tiden det tar å oppdage og håndtere en uønsket hendelse, kan i prinsippet måles, både ved øvelser, red-teaming og faktiske hendelser, og gi grunnlag for gode estimerer.

Tiltak for hver risiko vurderes i utgangspunktet separat, men det er ofte mulig at et enkelt tiltak vil kunne fjerne flere sårbarheter og dermed påvirke flere ulike risikoer samtidig. Oppgradering av underliggende systemkomponenter for å fjerne sårbarheter kan også redusere *teknisk gjeld* i systemer, selv om teknisk gjeld ikke nødvendigvis medfører en sikkerhetsrisiko. Teknisk gjeld er forventede fremtidige ekstrakostnader som følge av å velge lettvinne og kortsiktige løsninger i stedet for gode og langsiktige løsninger.

2. Dele eller overføre risiko til andre

Dette alternativet for risikohåndtering har til hensikt å dele eller flytte risiko over til eksterne enheter eller organisasjoner. Det kan ofte være et fornuftig valg å overføre risiko knyttet til drift av komplekse systemer til en annen organisasjon med større kompetanse på å håndtere disse risikoene. Kjøp av skytjenester er et eksempel der deler av risikoen for informasjonssikkerhet overføres til skyleverandøren. Som regel vil en skyleverandør kunne håndtere risikoen på en langt mer kostnadseffektiv måte enn virksomheten som kjøper skytjenesten.

Alternativt kan organisasjonen kjøpe cyberforsikring mot potensielle tap forårsaket av sikkerhetshendelser. Hensikten med cyberforsikring er å beskytte virksomheten mot risiko knyttet til informasjonssikkerhet og personvern ved drift og forvaltning av IKT-systemer og -tjenester. Risikoer av denne typen er vanligvis ekskludert fra tradisjonelle generelle ansvarspoliser. Dekningen som tilbys gjennom cyberforsikring, kan omfatte direkte tap som følge av ødeleggelse av data, utpressing, tyveri, hacking og tjenestenektangrep. Det tilbys også dekning for bøter og juridiske kostnader ved brudd på juridisk etterlevelse, for kostnader forbundet med å dekke tap hos tredjeparter forårsaket av feil og mangler i egen infrastruktur, for erstatning ved ærekrenkelse, for sikkerhetsrevisjon og for etterforskningskostnader etter sikkerhetshendelser.

Cyberforsikring blir mer og mer vanlig. Forsikringsselskapet foretar typisk en revisjon av en potensiell kunde forut for inngåelse av en avtale for å vurdere modenhet av styring og ledelse av informasjonssikkerhet i virksomheten. Premien for en cyberforsikringspolise vil avhenge av den vurderte modenheten, på den måten at lav modenhet vil medføre en høyere premie. Her er en positiv bivirkning at virksomheten får et insentiv om å forbedre sitt eget ISMS, hvor reduksjon av forsikringspremie er et bidrag til gevinsten av forbedringen.

3. Beholde risiko

Å beholde en spesifikk risiko betyr at virksomheten ikke gjør noe videre for å håndtere risikoen. Å akseptere en risiko slik den er, må være begrunnet i at virksomheten forstår risikoen og bevisst er forberedt på potensielle konsekvenser ved cyberangrep

Dette alternativet er forsvarlig bare når en risiko er under terskelnivået for akseptabel risiko, eller at kostnader ved innføring av tiltak eller håndtering på annen måte ville vært uforholdsmessig høy i forhold til risikonivået.

Her vil det også være tilfeller hvor virksomheten velger å beholde risiko midlertidig, det vil si at det eksisterer en tidsplan. Da blir det viktig å følge opp risikoen knyttet til dens

varighet. Eksempler kan være utfasing av tjenester eller å beholde en risiko i påvente av en planlagt oppgradering som vil redusere kostnaden for etablering av tiltak.

Risikoappetitt beskriver i hvilken grad organisasjonen er villig til å akseptere risiko som en avveining i forhold til kostnadene ved å redusere risikoen eller overføre den til andre.

4. Unngå risiko

Å unngå en spesifikk risiko betyr normalt å stoppe aktiviteten eller forretningsprosessen som forårsaker risikoen. Enhver forretningsaktivitet medfører en viss risiko, men nytten og fortjenesten av aktiviteten oppveier normalt risikoen.

Imidlertid kan det i spesielle situasjoner være nødvendig å stoppe forretningsaktiviteten som medfører risiko. Dette vil være tilfellet hvis risikoen er uforholdsmessig høy sammenlignet med nytten og fortjenesten, og det samtidig ikke er mulig å redusere, mitigere eller overføre risikoen på en kostnadseffektiv måte.

Fra et holistisk perspektiv er det også en risiko forbundet med å ikke drive en forretningsaktivitet, fordi det tar bort all mulighet for nytte og fortjeneste ved aktiviteten. Denne risikoen bør også tas i betraktning før virksomheten velger å stoppe en forretningsaktivitet for å unngå risiko.

Drøftinger av denne typen ligger typisk utenfor det avgrensede området av informasjons-sikkerhetsrisiko, og hører hjemme i det overordnede området virksomhetsrisiko (eng.: enterprise risk management). Dette er vesentlig å være oppmerksom på i dialogen med virksomhetsledelsen hvis spørsmålet om å unngå risiko blir relevant.

14.2.4 Risikohåndteringsplan og akseptert risiko

Det utarbeides en plan for håndtering av identifiserte risikoer som ligger over terskelnivået, eller som på bakgrunn av andre kriterier foreslås å bli håndtert. Denne rapporten vil også inneholde forslag til budsjett for planen. Ved fremleggelse av planen for ledelsen kommer vi til beslutningspunkt 2 i figur 14.5.

Ved beslutningspunkt 2 tar ledelsen stilling til om risikohåndteringsplanen er tilfredsstillende. Det er mulig at den foreslåtte planen for håndtering av risikoene er uakseptabel, for eksempel i følgende tilfeller:

- Planen for risikohåndtering er for dyr eller for ambisiøs. Ledelsen kan bestemme at nivået for akseptabel risiko heves, slik at det vil være tilstrekkelig å innføre færre og mindre ambisiøse sikkerhetstiltak.
- Risikonivået av planlagte beholdte risikoer (restrisikoer) anses å være for høyt til å bli akseptert. Hvis ledelsen vurderer restrisiko til å være for høy, kan flere sikkerhetstiltak bli foreslått som typisk vil kreve et større budsjett.
- Den estimerte kostnaden for risikohåndteringsplanen anses å være misvisende på grunn av feilvurdering av risikonivåer eller feilvurderinger av kostnader ved tiltak slik at risikovurdering og/eller plan for risikohåndtering må revideres.

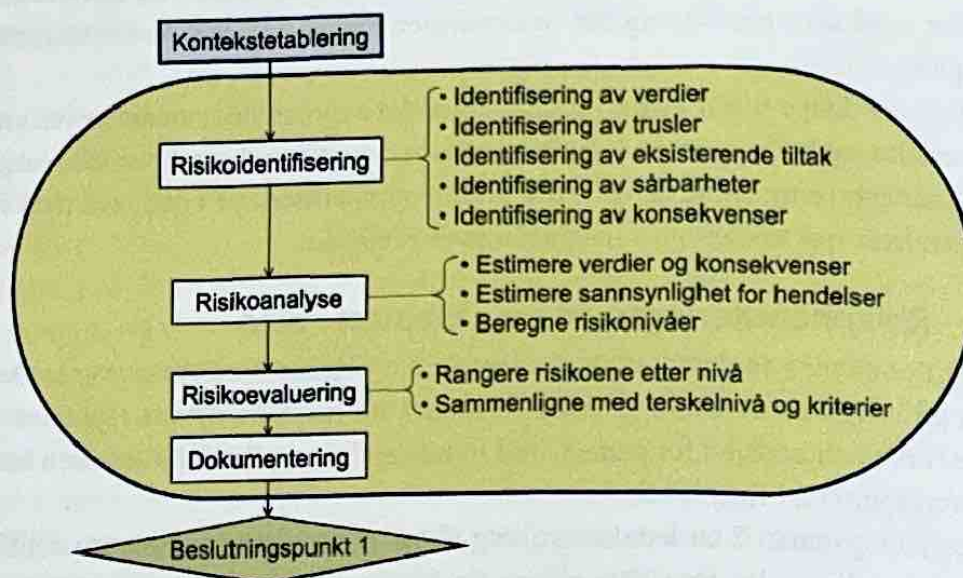
Hvis planen i første omgang ikke kan aksepteres, må ledelsen og ansvarlig representant for risikovurderingen sammen bli enige om måter å forbedre planen på.

Etter at planen for risikohåndtering er akseptert, kan planen settes i verk. *Restrisiko* er de risikoer og nivåer som gjenstår og aksepteres etter håndteringen.

14.3 Prosess for risikovurdering

Risikovurderingen innenfor et fokusområde bør utføres jevnlig (f.eks. en gang i året, ved behov eller forespørsel, osv.). En risikovurdering gir en midlertidig oversikt over identifiserte risikoer, mer eller mindre fylldig beskrevet, inkludert beregnet risikonivå.

Risikovurderingen kan gjennomføres i flere iterasjoner – den første på høyt nivå for å identifisere høy risiko, mens de andre detaljerer analysen av de største risikoene og andre risikoer av spesiell interesse. Prosessen for risikovurdering er illustrert i figur 14.7. Den gule ovalen er en ekspandert versjon av den gule ovalen i figur 14.5.



Figur 14.7. Prosess for risikovurdering.

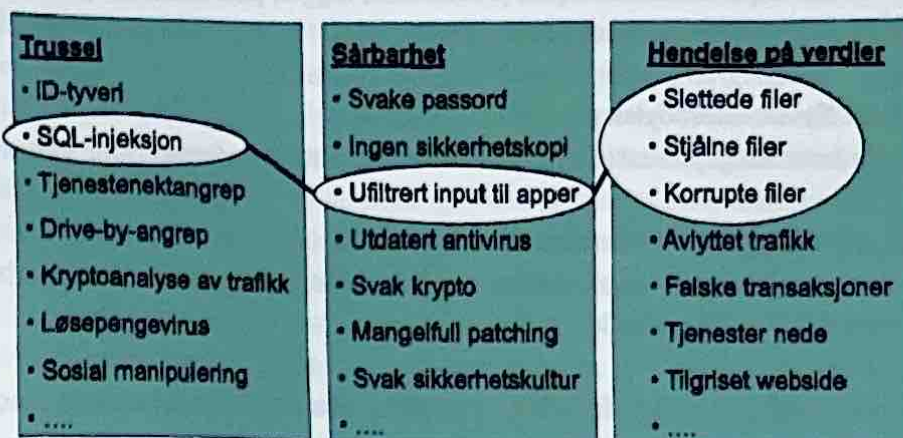
Trinnene i prosessen for risikovurdering beskrives i de tre neste avsnitt.

14.4 Risikoidentifisering

En enkel risiko består av en relevant sammenstilling av en trussel som utnytter en sårbarhet og forårsaker en sikkerhetshendelse på en verdi, som illustrert i figur 14.1. En sikkerhetshendelse kan bestå av brudd på ett eller flere KIT-sikkerhetsmål (konfidensialitet, integritet og tilgjengelighet).

For å identifisere risikoer er det altså nødvendig å kunne identifisere relevante trusler, sårbarheter og verdier som kan skades av truslene. Hvis vi hadde hatt lister over alle relevante trusler, alle relevante sårbarheter og alle relevante verdier som kan skades, kunne vi

identifisert risikoer ved å kartlegge sammenhenger, som illustrert i figur 14.8. Selv om dette er en mulig tilnærming, er det ikke særlig praktisk å lage store lister av trusler, sårbarheter og verdier, og deretter forsøke å finne risikoer i form av passende sammenstillinger.



Figur 14.8. Prinsipp for identifikasjon av risikoer.

Erfaring viser at en effektiv tilnærming for å identifisere risikoer kan være å fokusere på trusselscenarioer først. Dette kan gjøres ved å stille spørsmål som «Hva kan gå galt her?», «Hvordan kan noen angripe eller misbruke denne applikasjonen?» eller «Hvordan kan noen få uautorisert tilgang?». Hvis et relevant trusselscenario kan identifiseres, vil verdiene som skades, naturlig peke seg ut. Satt på spissen kunne vi nesten si at det er unødvendig å kartlegge verdier fordi relevante verdier vil peke seg ut når vi kartlegger trusselscenarioer. Imidlertid er det viktig å ha en oversikt over de viktigste ressurser og verdier som kan skades, fordi det gjør det lettere å identifisere relevante trusselscenarioer der nettopp disse verdiene er utsatt.

Moralen er at det er viktig å identifisere både verdier og trusler. Dette beskrives nedenfor, i tillegg til identifisering av konsekvenser.

14.4.1 Identifisering av verdier

Identifisering av ressurser og verdier i organisasjonen er tradisjonelt definert som første trinn av risikovurderingen. Det kan være utfordrende å sette riktig detaljnivå for registrering av verdier. Det bør ikke være for detaljert, ellers blir arbeidet overveldende. Det bør heller ikke være for generelt, ellers vil registeret ikke ha noen praktisk anvendelse.

Det er ofte en god tilnærming å kartlegge *verdiklasser* i motsetning til spesifikke ting. Hver verdi eller verdiklasse kan beskrives med et sett *attributter*. Her fins standard maler og regneark som kan brukes. Eiere av verdier i en virksomhet er ofte best plassert til å identifisere verdier og deres attributter.

Verdier som kartlegges, bør beskrives systematisk med et felles sett attributter. Listen nedenfor er et eksempel på attributter som kan beskrives for hver verdi.

- Nummer: Hver verdi/ressurs har et entydig nummer/identifikator.
- Type verdi: F.eks. fysisk infrastruktur, data, personinfo, systemer, applikasjoner, tjenester og ansatte (roller).

- **Ting eller klasse:** Hva som registreres. Hvis mulig er det nyttig å registrere en klasse ting under ett i stedet for spesifikke ting.
- **Informasjonstyper:** Ulike informasjonstyper kan defineres, som kan være attributt for en verdi. For eksempel dokumentasjon, prosessdata, logger, personaldata og økonomidata.
- **Eier:** Avdeling/entitet som anses å eie verdien.
- **Forvalter:** Avdeling/entitet som forvalter verdien (ofte eier).
- **Lokasjon:** Fysisk eller logisk plassering av verdien.
- **Funksjon/forretningsprosess:** Funksjoner eller forretningsprosesser som støttes / er avhengig av verdien.
- **Dataklassifisering:** Sensitivitet/klassifisering av data.
- **Konsekvensvurdering:** Det kan være nyttig å definere grad av konsekvens ved brudd på sikkerhetsmål (KIT) for verdien.

Ikke alle attributter er relevante for alle typer verdier. Bare relevante attributter trengs å beskrives for hver identifisert verdi.

14.4.2 Trusselmodellering: Identifisering av trusler

Trusselmodellering består av å identifisere, analysere og beskrive potensielle trusselscenarier, det vil si måter virksomheten kan bli angrepet på. Figur 11.5 illustrerer utfordringen med å holde oversikt over alle grensesnitt et system eller en applikasjon har med omverdenen, med tanke på at disse utgjør mulige angrepskanaler.

Formålet med trusselmodellering er å hjelpe eierne av systemer og applikasjoner til å se hvor potensielle svakheter og sårbarheter ligger, slik at disse kan fjernes. Trusselmodellering svarer på spørsmål som «*Hvor er vi mest utsatt for angrep?*» og «*Hva må vi gjøre for å beskytte oss mot disse truslene?*».

Ut over det å stille spørsmål som de ovenfor, fins det konkrete teknikker der tradisjonelt tre *tilnærminger* ofte nevnes. Disse er kort beskrevet nedenfor.

- **Angriper-sentrisk trusselmodellering:** Denne tilnærmingen tar utgangspunkt i angriperens målsettinger og vurderer alternativer for hvordan angriperen kan oppnå disse. Et nyttig spørsmål å stille er «*Hva er angriperen mest interessert i, og hvordan kan han oppnå det?*». Det er viktig å tenke på hva trusselaktører er interessert i, ikke bare hva som er viktig og verdifullt for egen virksomhet. STRIDE (beskrevet i avsnitt 11.5.4) er et eksempel på en angriper-sentrisk tilnærming. En relatert teknikk er å tegne et *angrepstre*, der roten er angriperens målsetting, og grenene er (alternative) sekvenser med trinn som angriperen må utføre for å nå målet.
- **Arkitektur-sentrisk trusselmodellering:** Denne tilnærmingen tar utgangspunkt i arkitekturen av systemer og nettverk, og prøver å følge arkitekturs dynamikk og logikk på jakt etter relevante angrep som kan utnytte sårbarheter i ulike komponenter i arkitekturen. Et nyttig spørsmål å stille er «*Hvor er vi mest utsatt for angrep?*». Denne tilnærmingen benyttes for eksempel for trusselmodellering i *Microsoft SDL*, beskrevet i avsnitt 11.1, og i *OWASP Top 10*, beskrevet i avsnitt 11.6.3.
- **Verdi-sentrisk trusselmodellering:** Denne tilnærmingen tar utgangspunkt i verdier som anses som spesielt sensitive eller viktige, for å avdekke hvordan disse kan skades. Et nyt-

tig spørsmål er «Hvilke verdier er viktigst for oss, og hvordan kan disse bli angrepet?». Konsekvenser av angrep mot en spesifikk verdi avhenger av hvilket av KIT-sikkerhetsmålene som skades i angrepet.

De tre tilnærmingene over kan og bør kombineres, for ingen av dem anses å være mer effektiv enn en annen, isolert sett.

En generell tilnærming er å definere et sett med kjernetrusselsscenarioer som anses å være mest relevant for virksomheten. Et relativt lite antall, kanskje bare rundt fem, ulike trusselsscenarioer kan gi god dekning for de mest relevante angrepstypene man trenger å vurdere. Angrepsvektorene beskrevet i kapittel 2 representerer generelle trusselsscenarioer. I tillegg kan inspirasjon hentes fra typiske hendelser omtalt i pressen og i rapporter om trusselvurderinger. Mange land, deriblant norske myndigheter representert ved f.eks. PST, E-tjenesten og NSM, lager jevnlig trusselvurderinger, der noen publiseres åpent. PST publiserer hvert år rapporten Nasjonal trusselvurdering. E-tjenesten publiserer hvert år rapporten FOKUS, som er en vurdering av aktuelle sikkerhetsutfordringer for Norge. NSM publiserer to risikorapporter i året – på våren en generell rapport om risiko samtidig med de to andre sikkerhetstjenestene, og på høsten et helhetlig digitalt risikobilde. SRM-er (sektorvise responsmiljøer beskrevet i avsnitt 16.7) rapporterer til virksomheter i sine sektorer. Mange private konsultantselskaper innen cybersikkerhet produserer og publiserer også denne type rapporter, som kan være åpne eller kan kjøpes. Åpne trusselrapporter publiseres også av internasjonale organisasjoner, som ENISA.⁷⁴

Det skjer ofte at en spesifikk sektor blir utsatt for en kampanje av angrep over en tidsperiode. Ettersom trusselbildet endrer seg hele tiden, er det utfordrende å stadig holde seg oppdatert på hva som er de mest relevante truslene for egen virksomhet.

14.4.3 Identifisering av konsekvenser

En hendelse kan føre til brudd på ett eller flere KIT-sikkerhetsmål for verdier, der verdier kan være for eksempel driftsdata, persondata, system, nettverk, applikasjoner, prosesser, tjenester etc.

Konsekvensen av en hendelse kan ha ulike aspekter, der følgende er typiske *konsekvensaspekter*:

- Tapt fortjeneste/profitt
- Svekket ytelse av tjeneste
- Brudd på juridisk etterlevelse
- Skadet omdømme
- Kostnader ved gjenoppretting

Alvorligheten av hvert konsekvensaspekt vil alltid variere. For en gitt hendelse og verdi vil noen konsekvensaspekter være relevante, mens andre er irrelevante. Av de relevante aspekter er noen mer alvorlige enn andre. Ved estimering av konsekvens av en hendelse skal alle konsekvensaspektene vurderes som helhet. Denne estimeringen kan være utfordrende fordi det ikke er åpenbart hvordan ulike aspekter skal kombineres.

74 <https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape>.

14.4.4 Registrering av risikoer

Risikoer som kartlegges, bør registreres på en systematisk måte med et felles sett attributter. Dette kan være en del av et regneark for risikoanalyse. Neste trinn etter risikoidentifisering er nettopp risikoanalyse. Listen nedenfor er et eksempel på attributter som kan beskrives for hver risiko.

- **Nummer:** Hver risiko har en entydig identifikator.
- **Trussel:** Hvordan kan noe skje? Hvilke trinn inngår i scenarioet? Hvem eller hva initierer hendelsen? Hvilken kapasitet og hvilket motiv har trusselaktøren?
- **Sårbarhet:** Hvilken svakhet/feil kan utnyttes? Hva gjør trusselscenarioet gjennomførbart?
- **Sikkerhetshendelse på verdier:** Hvilke verdier er berørt? Hvilke sikkerhetsbrudd oppstår? Er det brudd på ett eller flere av KIT-sikkerhetsmålene for en eller flere verdier?
- **Konsekvenser:** Typiske negative konsekvenser er tapt fortjeneste, utfall/svekkelse av tjenester, juridiske konsekvenser, tapt omdømme, kostnad ved gjenoppretting.
- **Eksisterende sikkerhetstiltak:** Kan hendelsen bli forhindret? Fins det allerede noe som kan stoppe eller bremse trusselen på et av trinnene slik at hendelsen forhindres?
- **Eksisterende kontrolltiltak:** Hvordan kan hendelsen bli oppdaget hvis den inntreffer?
- **Sannsynlighet:** Estimert for hvor sannsynlig det er at hendelsen inntreffer.
- **Konsekvens:** Estimert for hvor alvorlige konsekvensene av hendelsen vil være.
- **Risikonivå:** Beregnet nivå for risikoen.
- **Nye tiltak:** Forslag til hvordan nye tiltak kan bidra til å forhindre hendelsen.
- **Ny sannsynlighet:** Endret estimat for sannsynlighet med antatte nye tiltak.
- **Ny konsekvens:** Endret estimat for konsekvens med antatte nye tiltak.
- **Nytt risikonivå:** Endret risikonivå med antatte nye tiltak.

14.5 Risikoanalyse

Risikoanalysen tar utgangspunkt i at risikoer er blitt identifisert og registrert, der hver risiko er beskrevet med blant annet trussel, sårbarhet(er) og hendelse på verdi(er).

Praktisk risikoanalyse vurderer vanligvis to faktorer for å bestemme nivået på hver risiko. Disse faktorene er estimert *sannsynlighet* (frekvens/odds/hyppeghet) av hver type hendelse og estimerte *konsekvenser* (alvorlighet) for verdier som følge av en hendelse. Figur 14.2 illustrerer dette prinsippet.

Begrepet *ROS* (*risiko- og sårbarhetsanalyse*), som i norsk sammenheng ofte brukes i kontekst av risikostyring, har stort sett samme betydning som «risikovurdering». ROS er et særmorsk begrep som ikke fins i ISO 31000, ISO/IEC 27005 eller andre internasjonale veiledere for risiko. Denne boken benytter begrepet «risikovurdering» i stedet for «ROS».

Det fins mange måter og modeller for å representere sannsynlighet og konsekvens, og for å beregne risikonivå. Nedenfor beskriver vi eksempler på en kvalitativ, en relativ og en kvantitativ modell for risikoanalyse. Enkle regneark for risikoanalyse er tilgjengelig på nettsiden www.nettressurser.no/informasjonssikkerhet.

14.5.1 Kvalitativ risikoanalyse

I *kvalitativ risikoanalyse* er skalaer for sannsynlighet og konsekvens uttrykt med beskrivende ord (og tilhørende tallverdi). Antall nivåer og fortolkning av hvert nivå kan spesifiseres etter behov, eller etter hvilken skala som virksomheten vanligvis benytter. Figur 14.9 viser et eksempel på en kvalitativ sannsynlighetsskala med fem nivåer og fortolkning av hvert nivå.



Sannsynlighet	Beskrivelse
(5) Svært høy	Det fins motiverte trusselaktører som med letthet kan nå sitt angrepsmål ved å gjennomføre det vurderte trusselscenarioet for denne risikoen. En hendelse er antagelig allerede i ferd med å skje, eller vil skje om kort tid.
(4) Høy	Motiverte trusselaktører vil med høy sannsynlighet nå sitt angrepsmål ved å gjennomføre det vurderte trusselscenarioet. En hendelse kan inntreffe noen ganger per måned.
(3) Betydelig	Trusselaktører har en betydelig mulighet til å nå sitt mål ved å bruke det vurderte trusselscenarioet. En hendelse kan inntreffe noen ganger per år.
(2) Lav	Trusselaktører har relativt liten mulighet til å nå sitt angrepsmål ved å bruke det vurderte trusselscenarioet. Det vil antagelig gå flere år mellom hver hendelse.
(1) Usannsynlig	Trusselaktører har svært liten mulighet til å nå sitt angrepsmål ved å bruke det vurderte trusselscenarioet. Det vil kanskje aldri skje en hendelse.

Figur 14.9. Kvalitativ sannsynlighet for hendelser.

På engelsk brukes begrepet *likelihood* om sannsynlighet for hendelser. Vær oppmerksom på forskjellen på engelsk mellom «probability» og «likelihood» som ikke fins på norsk. Begrepet «probability» har hovedsakelig den velkjente statistiske betydning av relativ frekvens. Begrepet «likelihood» kan også ha betydningen sjanse eller «chance», som ikke nødvendigvis tolkes statistisk. Vanskeligheten med å tolke «likelihood» relatert til risikoanalyse diskuteres blant annet i kapittel 6, avsnittet «defining probability» i Douglas Hubbard: *The Failure of Risk Management: Why It's Broken and How To Fix It*, 2. utg. (Wiley, 2020).

Figur 14.10 gir et eksempel på en kvalitativ konsekvensskala med fem nivåer og fortolkning av hvert nivå.



Konsekvensnivå	Beskrivelse
(5) Svært alvorlig	Svært alvorlig skade på verdier, paralyserende tjenestavbrudd, svært stort økonomisk tap og mulig konkurs. Gjenoppretting krever langvarig arbeid med store ressurser. Eksterne funksjoner som avhenger av virksomheten kan falle bort i lang periode.
(4) Alvorlig	Alvorlig skade på verdier som kan medføre alvorlig tjenesteavbrudd og stort økonomisk tap. Det kreves store ressurser for å håndtere hendelsen. Funksjoner utenfor den berørte virksomheten kan bli negativt påvirket, men uten langvarige konsekvenser.
(3) Betydelig	Betydelig skade på verdier som kan medføre betydelig tjenesteavbrudd og betydelig økonomisk tap. Gjenoppretting og tjenestekontinuitet krever betydelig arbeid. Funksjoner utenfor virksomheten blir sannsynligvis lite påvirket.
(2) Liten	Relativt liten skade på verdier som kan true kvalitet av drift, og antagelig lite eller intet tjenesteavbrudd. Bare lite økonomisk tap. Håndteres greit med moderate ressurser.
(1) Ubetydelig	Ubetydelig skade på verdier, uten tjenesteavbrudd. Hendelsen håndteres relativt lett som del av rutinemessig drift. Lite eller intet økonomisk tap.

Figur 14.10. Kvalitativ konsekvensskala.

Kvalitativ risikoanalyse er typisk basert på en todimensjonal matrise der sannsynlighet og konsekvens utgjør hver sin dimensjon, som vist i figur 14.11.

		Kvalitative konsekvensnivåer				
		(1) Ubetydelig	(2) Liten	(3) Betydelig	(4) Alvorlig	(5) Sv. alvorlig
Kvalitativ sannsynlighet	Kvalitative risikonivåer	(5) Svært høy	(3) M	(4) S	(4) S	(5) SS
	(4) Høy	(2) L	(3) M	(4) S	(4) S	(5) SS
	(3) Betydelig	(2) L	(2) L	(3) M	(4) S	(4) S
	(2) Lav	(1) SL	(2) L	(2) L	(3) M	(3) M
	(1) Usannsynlig	(1) SL	(1) SL	(2) L	(2) L	(2) L

Tolkning av risikonivåer:

- (5) SS: Svært stor risiko, må håndteres med høy prioritet
- (4) S: Stor risiko, skal vanligvis håndteres
- (3) M: Moderat risiko, håndtering og tiltak bør vurderes
- (2) L: Liten risiko, kan vanligvis aksepteres
- (1) SL: Svært liten risiko, kan ignoreres

Figur 14.11. Kvalitativ risikoberegning.

Risikomatrisen fungerer som en oppslagstabell, der man peiler inn med estimert sannsynlighet og estimert konsekvens, for å peke ut risikonivået. Hver virksomhet må selv bestemme fordelingen av risikonivåer i risikomatrisen, og figur 14.11 er bare et eksempel. For at risikoanalyser skal være sammenlignbare, er det viktig at virksomheten bestemmer seg for en spesifikk risikomatrise som benyttes for all risikoanalyse.

Risikomatriser som i figur 14.11 er som regel omtrent additive etter følgende formel:

$$\text{Risikonivå} = \frac{\text{Sannsynlighet} + \text{Konsekvens}}{2}$$

Ved å uttrykke sannsynlighet og konsekvens som nivåer på skala 1–5, kan en enkel beregning av risikonivåer gjøres med formelen over, som gir risikonivåer på skala 1–5.

14.5.2 Relativ risikoanalyse

Ved relativ beregning av risikonivåer uttrykkes hvert nivå for sannsynlighet og konsekvens med en relativ verdi i intervallet [0, 1]. For å gjøre det mer forståelig kan hvert relative nivå for sannsynlighet og konsekvens tolkes med beskrivende ord, på samme måte som for kvalitativ risikoanalyse.

En statistisk sannsynlighet er allerede en relativ verdi. I tillegg kan konsekvens uttrykkes som en relativ verdi. Det er naturlig at både sannsynligheter og konsekvensnivåer er logaritmisk fordelt, som betyr at forskjellen mellom hvert nivå utgjør én størrelsesorden, dvs. en 10-gangers forskjell. Tabell 14.1 viser sammenhengen mellom kvalitative og relative nivåer for sannsynlighet og konsekvens.

Tabell 14.1. Relative nivåer for sannsynlighet og konsekvens

Kvalitative nivåer for sannsynlighet og konsekvens	Relative nivåer for sannsynlighet og konsekvens
5	$1,0000 = 1 \cdot 10^0$
4	$0,1000 = 1 \cdot 10^{-1}$
3	$0,0100 = 1 \cdot 10^{-2}$
2	$0,0010 = 1 \cdot 10^{-3}$
1	$0,0001 = 1 \cdot 10^{-4}$

Relativ risikoberegning er multiplikativ og gjøres etter følgende formel:

$$\text{Risikonivå} = \text{Sannsynlighet} \times \text{Konsekvens}$$

Relativ risikoberegning er matematisk mer korrekt enn kvalitativ (additiv) beregning, men kan være vanskelig å tolke intuitivt. Relative risikonivåer kan knyttes til kvalitative beskrivelser av risiko med ord, slik at relativ risikoberegning også kan tolkes kvalitativt. Tabell 14.2 viser hvordan kvalitative risikonivåer kan uttrykkes som relative risikonivåer beregnet med formelen over.

Tabell 14.2. Sammenheng mellom kvalitative og relative risikonivåer

Kvalitative risikonivåer	Relative risikonivåer
5	$1,00000000 = 1 \cdot 10^0$
4	$0,01000000 = 1 \cdot 10^{-2}$
3	$0,00010000 = 1 \cdot 10^{-4}$
2	$0,00000100 = 1 \cdot 10^{-6}$
1	$0,00000001 = 1 \cdot 10^{-8}$

Konsekvens kan ha ulike aspekter, som beskrevet i avsnitt 14.4.3. Hvert konsekvensaspekt kan uttrykkes som en relativ verdi i intervallet $[0, 1]$. I tilfelle en risiko har flere konsekvensaspekter, er det nødvendig å beregne et helhetlig konsekvensnivå. Ulike konsekvensaspekter kan for eksempel være tapt omsetning og skadet omdømme. La K uttrykke helhetlig konsekvensnivå, og k_i uttrykke nivå for et spesifikt konsekvensaspekt i .

Hvis alle konsekvensaspektene anses som uavhengige, kan helhetlig relativ konsekvens beregnes som summen av konsekvensene fra hvert aspekt etter følgende formel:

$$K = k_1 + k_2 + k_3 + \dots$$

Hvis konsekvensaspektene anses mer eller mindre avhengige, kan den helhetlige konsekvensen settes lik den største av de ulike konsekvensene etter følgende formel:

$$K = \max[k_1, k_2, k_3, \dots]$$

For eksempel: Hvis tapt omsetning er et resultat av skadet omdømme, kan disse to aspektene betraktes som gjensidig avhengige, og helhetlig konsekvens kan settes lik den største av de to.

14.5.3 Kvantitativ risikoanalyse

Kvantitativ risikoanalyse går ut på å representere konsekvens i absolutte pengeverdier. Det fins flere ulike modeller for kvantitativ beregning av risiko. Nedenfor beskriver vi en enkel modell.

La sannsynlighet P uttrykkes i intervallet $[0, 1]$, som tolkes som relativ frekvens av en viss type hendelse per år. $P = 0,5$ betyr f.eks. at hendelsen er forventet å inntreffe annethvert år. Konsekvens K uttrykkes som absolutt pengeverdi.

Risikonivå R beregnes som forventet tap (per år) i absolutt pengeverdi. Ved kvantitativ risikovurdering brukes gjerne begrepet *risikoeksponering* (eng.: risk exposure) i denne betydningen av risikonivå.

$$R = P \times K$$

Kvantitativ risikoanalyse er besnærende fordi rapportert risiko lettere kan vurderes i sammenheng med budsjettering av sikkerhetsaktiviteter i en virksomhet. Imidlertid er det typisk betydelig uvisshet knyttet til inputverdiene i en kvantitativ risikoanalyse, slik at de beregnede risikonivåene nødvendigvis også er befengt med stor uvisshet.

Kvantitativ risikoberegning kan knyttes til kvalitativ risikoberegning ved hjelp av relative nivåer for sannsynlighet og konsekvens fra tabell 14.1. Hvis vi definerer en spesifikk frekvens for høyeste sannsynlighet, vil frekvenser for de lavere sannsynlighetene følge naturlig. På samme måte: Ved å velge et spesifikt pengebeløp for høyeste konsekvens vil de lavere konsekvensene følge naturlig.

Som eksempel: La høyeste sannsynlighetsfrekvens (nivå 5) være at en hendelse inntreffer 100 ganger per år, det vil si omtrent to ganger per uke. Ved å multiplisere med relativt sannsynlighetsnivå for nivå 4 fra tabell 14.1 vil sannsynlighetsfrekvens for nivå 4 da være 10 ganger per år, dvs. omtrent én gang per måned. Ut ifra dette eksemplet viser tabell 14.3 hvordan kvantitative sannsynlighetsfrekvenser tilsvarer kvalitative sannsynligheter.

Tabell 14.3. Kvantitative sannsynlighetsfrekvenser

Kvalitativ sannsynlighet	Kvantitative sannsynlighetsfrekvenser ut ifra maks 100 ganger per år
5	$100 \times 1 \cdot 10^0 = 100$ ganger per år
4	$100 \times 1 \cdot 10^{-1} = 10$ ganger per år
3	$100 \times 1 \cdot 10^{-2} = 1$ gang per år
2	$100 \times 1 \cdot 10^{-3} = 0,1$ (1 gang hvert 10. år)
1	$100 \times 1 \cdot 10^{-4} = 0,01$ (1 gang hvert 100. år)

På tilsvarende måte: Anta som eksempel at høyeste konsekvens (nivå 5) vil være NOK 10 millioner. Ved å multiplisere med relativt konsekvensnivå for nivå 4 fra tabell 14.1 vil konsekvens for nivå 4 da være NOK 1 million, osv. Ut ifra dette eksemplet viser tabell 14.4 hvordan kvalitative konsekvensnivåer tilsvarer kvantitative konsekvenser.

Tabell 14.4. Kvantitative konsekvensnivåer

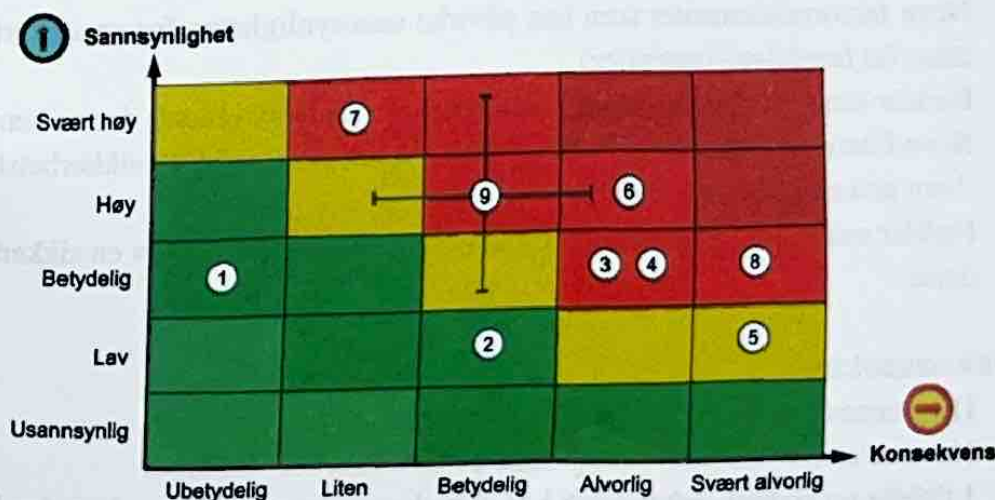
Kvalitative konsekvensnivåer	Kvantitative konsekvenser ut ifra maks NOK 10 millioner
5	$\text{NOK } 10 \text{ millioner} \times 1 \cdot 10^0 = \text{NOK } 10\,000\,000$
4	$\text{NOK } 10 \text{ millioner} \times 1 \cdot 10^{-1} = \text{NOK } 1\,000\,000$
3	$\text{NOK } 10 \text{ millioner} \times 1 \cdot 10^{-2} = \text{NOK } 100\,000$
2	$\text{NOK } 10 \text{ millioner} \times 1 \cdot 10^{-3} = \text{NOK } 10\,000$
1	$\text{NOK } 10 \text{ millioner} \times 1 \cdot 10^{-4} = \text{NOK } 1000$

Hver virksomhet må selv vurdere hva de anser som høyeste konsekvens. For store selskaper kan høyeste konsekvens for eksempel vurderes til å være NOK 100 millioner, som gjør at de lavere konsekvensene følger naturlig med 1 størrelsesorden mindre for hvert nivå. Dette er en praktisk måte for virksomheter å tilpasse risikoanalyse til virksomhetens størrelse på.

14.6 Risikoevaluering og rapportering

Risikoevalueringen tar utgangspunkt i risikoanalyse for å gjøre en prioritering av risikoer for senere håndtering. Evalueringen er primært basert på rangering av beregnede risikonivåer, der de største risikoene naturlig peker seg ut.

Visualisering av risiko er viktig for at beslutningstagere skal kunne forstå og ta stilling til hva som bør prioriteres. Figur 14.12 gir et eksempel på hvordan risiko kan visualiseres i henhold til sannsynlighet og konsekvens, og viser ni hypotetiske risikoer.



Figur 14.12. Visualisering av risiko.

Terskelnivå for akseptabel risiko og eventuelt andre kriterier bør tas med i evalueringen. I figur 14.12 kan terskelnivå trekkes som en diagonal på skrå nedover mot høyre. I figuren har for eksempel risiko 3 og 4 lik sannsynlighet og konsekvens, noe som gjør det logisk at de får samme prioritet. Selv om risiko 3 og 7 har samme nivå, har de ulik sannsynlighet og konsekvens, noe som kan være en grunn til at de får ulik prioritet.

Visualiseringen i figur 14.12 kan tolkes som kvalitativ på den måten at hver risiko er plassert i midten av et «kvalitativt» felt. Hvis risikoanalysen er kvantitativ, er plassering av en risiko i figuren ikke bundet av å ligge i midten av et felt, men vil ha en fri plassering ut fra relativ eller kvantitativ sannsynlighet og konsekvens.

Hvis det er ønskelig å visualisere grad av uvisshet rundt risikoene, kan en risikosirkel i tillegg ha en horisontal strek for å uttrykke uvisshet om konsekvens, eller en vertikal strek for å uttrykke uvisshet om sannsynlighet, slik som vist for risiko 9 i figur 14.12. Lengden på en strek kan representere grad av uvisshet. Det fins mange andre måter å representere uvisshet på, som i varierende grad gjør det intuitivt lett å forstå uvissheten. Selv om representering av uvisshet bringer mer detaljrikdom til visualiseringen, har det liten nytte hvis de som skal lese rapporten, ikke forstår hva det betyr. Det er bedre å benytte en enkel visualisering som folk forstår, enn en avansert visualisering som folk ikke forstår. Kommunikasjon av risiko er viktig for god helhetlig risikostyring. Det er derfor viktig å tenke på hvordan visualiseringen best kan bidra til å kommunisere resultatet av risikovurderingen.

Resultatet av risikoevalueringen kommuniseres typisk med en rapport som beskriver resultatet av risikovurderingen og hvordan identifiserte og analyserte risikoer er prioritert i henhold til terskelverdi og andre kriterier. Beslutningspunkt 1 (beskrevet i avsnitt 14.2.2) tar stilling til om rapporten kan aksepteres, eller om deler av risikovurderingen må revideres.

Oppgaver til kapittel 14

14.1 Risikofaktorer

- Hva er forskjellen på «risiko» og «risikonivå» i kontekst av informasjonssikkerhet?
- Nevn faktorer/elementer som kan påvirke sannsynligheten for en sikkerhetshendelse (at hendelsen inntreffer).
- Forklar om det er lett/meningsfullt å redusere sannsynligheten for en hendelse.
- Nevn faktorer/elementer som kan påvirke konsekvensen av en sikkerhetshendelse (hvor alvorlig en hendelse er).
- Forklar om det er lett/meningsfullt å redusere konsekvensen av en sikkerhetshendelse.

14.2 Risikoaspekter

- Hva menes med at en hendelse medfører et sikkerhetsbrudd?
- Nevn relevante konsekvensaspekter av en sikkerhetshendelse.
- I tilfelle en sikkerhetshendelse har ulike konsekvensaspekter – hvordan bør disse inkluderes i analysen av hendelsens risiko?

14.3 Risikokommunisering

- Hvorfor er det viktig å kommunisere trussel-/risikovurderinger?
- Hvem skal trussel-/risikovurderinger kommuniseres til?
- Nevn faktorer for å kunne kommunisere trussel-/risikovurderinger på en god måte.

Lover og regelverk for informasjonssikkerhet

15.1 Viktigheten av regelverk om informasjonssikkerhet

Lover og regelverk for informasjonssikkerhet

I dette kapitlet skal du først lære hvorfor regelverk for informasjonssikkerhet er viktig, og hva det betyr å være ansvarlig for etterlevelse av regelverk. Deretter lærer du om grunnleggende begreper rund lovgivning og regelverk, som for eksempel hvordan ulike typer regelverk henger sammen, og hvordan man finner ut hvem eller hva som er underlagt en lov eller forskrift. Til slutt lærer du hva som er hovedelementene i et sett med sentrale lover og forskrifter for informasjonssikkerhet.

15.1 Viktigheten av regelverk om informasjonssikkerhet

Lover og regler har alltid vært nødvendig for å opprettholde et velfungerende samfunn. Gjennom digitalisering er samfunnet blitt helt avhengig av digitale systemer for å fungere. Økning i angrep mot digitale systemer med alvorlige konsekvenser utgjør dermed en alvorlig trussel, slik at sikkerheten i digitale systemer må reguleres for å opprettholde et velfungerende samfunn.

15.1.1 Regelverk som kilde til krav om informasjonssikkerhet

Regelverk for informasjonssikkerhet er en essensiell kilde til krav om informasjonssikkerhet, slik som beskrevet i avsnitt 1.5. Noen lover eller forskrifter gir direkte pålegg om sikkerhetstiltak, som f.eks. *forskrift om IT-standarder i offentlig forvaltning*, § 11, som blant annet sier at alle nettsider tilhørende offentlig forvaltning skal sikres med serversertifikater og HTTPS, som beskrevet i avsnitt 6.2.1. Imidlertid er det mer og mer vanlig at lover og forskrifter pålegger virksomheter å implementere sikkerhet ut ifra risikovurderinger, som f.eks. *sikkerhetsloven*, § 4-2, som blant annet sier at risikovurderinger skal danne grunnlag for iverksetting av forebyggende sikkerhetstiltak.

Virksomheter har en plikt til å følge lover og forskrifter, der ledelsen er ansvarlig (eng. accountable) for at virksomheten etterlever disse. For en virksomhet er det betydelig mer utfordrende å etterleve krav om å styre informasjonssikkerhet basert på risikovurderinger, enn

det er å etterleve konkrete krav om å implementere spesifikke sikkerhetstiltak. Virksomheten må ha en viss modenhet og trenger et *styringssystem for informasjonssikkerhet* (ISMS) for å kunne styre informasjonssikkerhet basert på risikovurderinger. En ekvivalent betegnelse for ISMS er «*system for internkontroll*». For at en virksomhet skal kunne styre informasjonssikkerhet på best mulig måte, og gjøre risikobaserte prioriteringer, krever mange lover og forskrifter at virksomheter nettopp skal ha et styringssystem for informasjonssikkerhet, som beskrevet i avsnitt 12.3.3.

Arbeidet med å etterleve krav til informasjonssikkerhet spesifisert i regelverk har naturligvis en kostnad som virksomheter må integrere i sine budsjetter. Å ikke etterleve, eller bare delvis å etterleve, visse krav kan derfor gi en kostnadsbesparelse. På den annen side vil det medføre en risiko for at virksomheten, eller individer, blir ilagt straff, eller får andre negative konsekvenser hvis det avdekkes at virksomheten ikke etterlever lover og forskrifter. Rent økonomisk kan virksomheter se på dette som *etterlevelsrisiko*, som altså er risikoen for at mulige kostnader ved mangel på etterlevelse er større enn besparelser gjennom reduserte kostnader ved redusert etterlevelse. Ansvarsområdet for slike vurderinger ligger hos toppledelsen.

15.1.2 Ansvar

Toppledelsen og eierne av en virksomhet er ansvarlig (eng. *accountable*) for å sørge for at drift av virksomheten skjer i samsvar med gjeldende regelverk. Ved brudd på etterlevelse av gjeldende regelverk kan virksomheten straffes med overtredelsesgebyrer, som er en *virksomhetsstraff*. Alternativt, eller i tillegg, kan individer straffes med bøter eller fengsel, som er en *personlig straff*. Hvem i virksomheten som kan gis en personlig straff ved lovbrudd, avhenger av omstendigheter. I utgangspunktet skal den straffes som har høyest autoritet i virksomheten, og som samtidig burde visst om, og kunne forhindret, bruddet på loven. Det er en misforståelse å tro at den ansatte som klikket på en skadelig lenke i en phishing-e-post, dermed er ansvarlig hvis det fører til et sikkerhetsbrudd med betydelig tap som følge. Selv om alle i virksomheten er «ansvarlige» (eng. *responsible*) for informasjonssikkerhet, ligger «ansvaret» (eng. *accountability*) alltid hos toppledelsen. Den tvetydige språkbruken rund begrepet ansvarlig, som dessverre er vanlig på norsk, kan være forvirrende, og forklares lenger ned i avsnittet.

Sentrale lover for informasjonssikkerhet uttrykker prinsippet om ansvar svært tydelig. Sikkerhetsloven § 4-1 sier at virksomhetens leder har ansvar for det forebyggende sikkerhetsarbeid i virksomheten, og GDPR Art. 5-2 peker på at *den behandlingsansvarlige* (i prinsippet virksomhetens ledelse) nettopp er ansvarlig for å overholde GDPR. Ved brudd på etterlevelse kan virksomheten etter sikkerhetsloven eller GDPR få en virksomhetsstraff.

Som nevnt over kan individer også straffes. Aksjeloven § 17-1 sier for eksempel at daglig leder eller (medlemmer i) styret i et aksjeselskap kan bli erstatningsansvarlig dersom selskapet eller aksjeeierne påføres tap som følge av uaktsomhet fra daglig leder eller styret. Krav om erstatning mot individer kan komme dersom selskapet blir påført betydelige tap som følge av brudd på informasjonssikkerhet, og det blir påvist at ledelsen eller styret over tid bevisst har nedprioritert styring av informasjonssikkerhet i den helhetlige ledelse og styring av selskapet. GDPR Art. 84 sier at hvert medlemsland skal bestemme strafferammen overfor individer i tilfelle det begås grove brudd på GDPR. Som nasjonal tilpasning har Norge for, gjennom personopplysningsloven § 48, satt strafferammen til bøter og/eller fengsel inntil 1 år (3 år ved særdeles skjerpene omstendigheter).

Begrepet «ansvarlig» er tvetydig på norsk. På engelsk skilles det mellom «accountability» og «responsibility». Det kan forklares slik at «accountability» betyr «regnskapelighet» eller «å stå til regnskap», mens «responsibility» betyr å ha som oppgave og plikt å utføre noe. På norsk betyr begrepet ansvarlig begge deler, slik at vi er nødt til å tolke meningen av «ansvarlig» ut fra sammenhengen, men det er ikke alltid like enkelt.

I GDPR (personopplysningsloven) beskrevet i avsnitt 10.5 betyr «den behandlingsansvarlige» den som står til regnskap for behandlingen overfor «de registrerte» og overfor myndighetene. Det står i kontrast til modellen for skyarkitekturer og skysikkerhet beskrevet i avsnitt 11.8, der ansvarlig betyr den som har til oppgave å utføre en type IT-tjeneste eller en type sikkerhetsfunksjon.

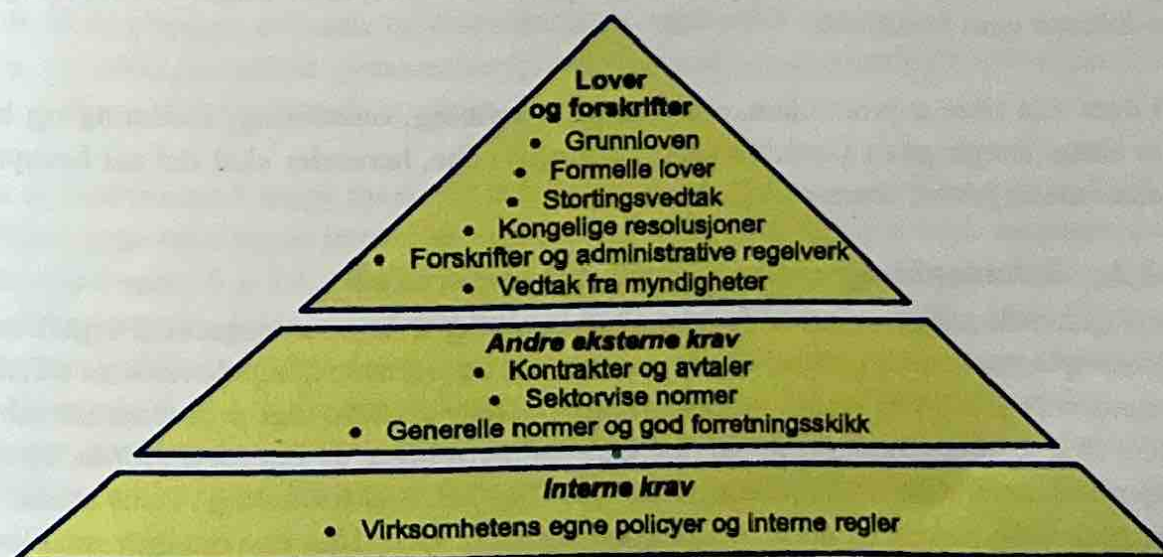
For å unngå misforståelser er det viktig å være bevisst de to betydningene av begrepet ansvarlig. Når begrepet nevnes i lover og forskrifter, og i diskusjoner om etterlevelse av lover og forskrifter, er det alltid betydningen av «den som står til regnskap» (eng. accountable) som gjelder. Når begrepet benyttes i sammenheng med sikkerhetskultur og ansattes roller i arbeid med informasjonssikkerhet i virksomheten, er det som regel betydningen av «den som har til oppgave» (eng. responsibility) som gjelder.

15.2 Grunnleggende begreper om regelverk

Dette avsnittet gir en kort beskrivelse av generelle aspekter ved regelverk. Det fins lærebøker om lov og rett som gir en mer utfyllende oversikt.

15.2.1 Hierarki av regelverk og krav

Regelverk rangeres etter et hierarki, som betyr at regelverk lenger opp i hierarkiet er mer generelle enn regelverk lenger ned. Det betyr også at regelverk lenger opp overkjører regelverk lenger ned hvis de på en eller annen måte skulle motsi hverandre. Figur 15.1 viser hierarkiet av regelverk delt opp i tre kategorier.



Figur 15.1. Hierarki av regelverk.

Den øverste kategorien består av lover og forskrifter bestemt av myndighetene. I denne kategorien ligger naturligvis Grunnloven på topp, etterfulgt av vanlige lover, stortingsvedtak, kongelige resolusjoner, administrative regelverk og andre vedtak fra ulike myndigheter. For en virksomhet utgjør denne kategorien eksterne myndighetskrav.

Den mellomste kategorien består av eksterne krav fra andre enn myndigheter. I første rekke vil kontrakter med eksterne parter sette krav som avtales mellom virksomheten og eksterne parter. I mange sektorer fins det formelle normer som setter krav til virksomheter for å kunne delta innen sektoren. Et eksempel på slike krav er den nasjonale *Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren* (Normen), som setter sikkerhetskrav til alle virksomheter som deltar i, og er koblet til, Norsk helsenett. Et annet eksempel er den internasjonale *Payment Card Industry Data Security Standard* (PCI DSS), som setter sikkerhetskrav til alle virksomheter som deltar i betalingstransaksjoner med betalingskort og kredittkort. Det fins også en rekke mindre formelle normer som virksomheter forventes å følge, uten at det nødvendigvis får noen direkte konsekvenser om de ikke gjør det. For eksempel regnes det som god praksis at virksomheter gir offentlig informasjon når de har vært utsatt for alvorlige cyberangrep.

Den nederste kategorien krav er de som virksomheten setter til seg selv gjennom policyer og interne regler for prosedyrer, forretningsprosesser og saksbehandling. Virksomhetens policyer kan for eksempel sette krav til passordstyrke eller ansattes bruk av personlige enheter.

15.2.2 Formål og virkeområde til lover og forskrifter

Virksomheter må kartlegge hvilke lover og regler de er underlagt. Med utgangspunkt i hver enkelt lov eller forskrift er det forholdsvis enkelt å finne ut om den gjelder for en virksomhet. Lover er typisk delt inn i kapitler, der kapittel 1 alltid har en paragraf som definerer hvem eller hva loven gjelder for. I sikkerhetsloven, som beskrives nedenfor, er det § 1-2 som definerer hvem loven gjelder for. I energiloven er det § 1-1 som definerer *Virkeområde*, det vil si hva loven gjelder for.

En lov har alltid et formål (ellers ville loven være meningsløs). Formålet er ofte eksplisitt uttrykt i loven i en av de første paragrafene (i kapittel 1) av loven. I energiloven er det § 1-2 som definerer dens formål slik:

Loven skal sikre at produksjon, omforming, overføring, omsetning, fordeling og bruk av energi foregår på en samfunnsmessig rasjonell måte, herunder skal det tas hensyn til allmenne og private interesser som blir berørt.

15.2.3 Sammenheng mellom lover og forskrifter

Teknologiutviklingen går i rasende fart, mens utvikling og revisjon av regelverk typisk er en langsom og møysommelig prosess. Det er derfor svært utfordrende å lage lover som effektivt kan regulere bruk av ny IT (informasjonsteknologi). Dette er desto mer problematisk når ny IT fører til dramatiske endringer av samfunnet, som innføringen av internett gjorde, og som nå skjer med innføringen av KI (kunstig intelligens) og ML (maskinlæring) i stor skala.

Det går relativt raskere og det er lettere å lage og endre forskrifter enn det gjør med lover. Dermed er forskrifter ofte bedre egnet til å regulere ny IT. For at det skal være mulig, må lover inneholde paragrafer som nettopp sier at regjeringen (beskrevet som Kongen i statsråd),

et departement eller annen reguleringsmyndighet kan lage forskrifter som gir mer detaljerte regler enn selve loven. Når en forskrift på den måten utfyller en spesifikk lov, sier vi at forskriften har hjemmel i loven. Alle forskrifter må ha hjemmel i minst én lov, og kan ha hjemmel i flere lover.

Lovhjemmelen til en forskrift er alltid oppført helt i begynnelsen av forskriften. Som eksempel er det lett å slå opp i Lovdata.no og se at *virksomhetssikkerhetsforskriften* er hjemlet i sikkerhetsloven, at *kraftberedskapsforskriften* er hjemlet i energiloven, og at *forskrift om IT-standarder i offentlig forvaltning* er hjemlet i forvaltningsloven.

Lover og forskrifter må håndheves av et statlig organ, ellers er de meningsløse. Lover og forskrifter kan nevne et statlig organ som forvaltningsmyndighet for loven, eller kan si at regjeringen (Kongen i statsråd) eller et departement kan utpeke en forvaltningsmyndighet. Som eksempel er NSM (Sikkerhetsmyndigheten) forvalter av sikkerhetsloven, Datatilsynet er forvalter av personopplysningsloven, NVE er forvalter av kraftberedskapsforskriften, og hvert organ for stat eller kommune regnes som forvaltningsorgan for forvaltningsloven.

15.3 Sentrale lover for informasjonssikkerhet

Det eksisterer et stort antall lover og forskrifter som berører informasjonssikkerhet. Avsnittene nedenfor dekker bare de mest sentrale. Personopplysningsloven (GDPR) nevnes ikke her ettersom den allerede er beskrevet i kapittel 10.

15.3.1 Sikkerhetsloven

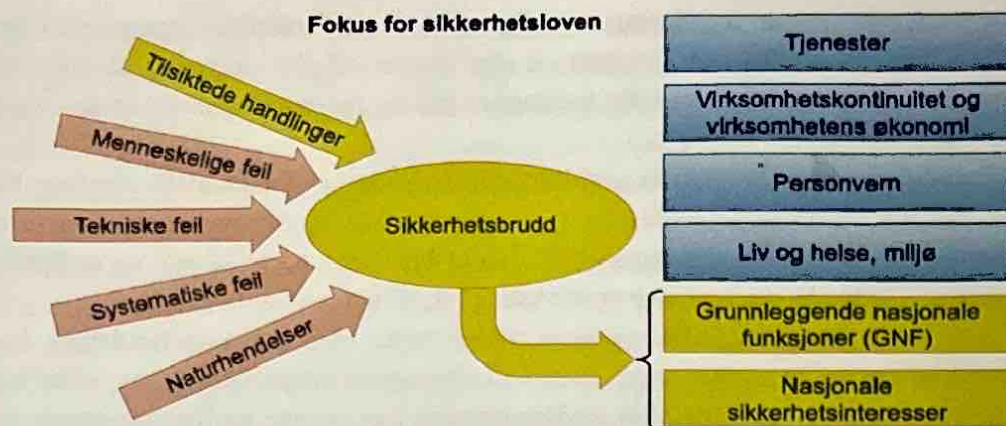
Formålet med sikkerhetsloven av 2019 er særdeles klart uttrykt i § 1-1:

Loven skal bidra til

- a. å trygge Norges suverenitet, territorielle integritet og demokratiske styreform og andre nasjonale sikkerhetsinteresser
- b. å forebygge, avdekke og motvirke sikkerhetstruende virksomhet
- c. at sikkerhetstiltak gjennomføres i samsvar med grunnleggende rettsprinsipper og verdier i et demokratisk samfunn.

Det er interessant å legge merke til at begrepet «sikkerhetstruende virksomhet» i § 1-1.b er definert som «tilsiktete handlinger som direkte eller indirekte kan skade nasjonale sikkerhetsinteresser» i § 1-5.4. Med andre ord fokuserer sikkerhetsloven ikke på å forebygge brudd på sikkerhet som følge av naturhendelser, systemfeil eller menneskelige feil. Sikkerhetslovens smale fokus på både årsak og konsekvens er illustrert med oransje farge i figur 15.2.⁷⁵

I henhold til § 1-2 gjelder sikkerhetsloven for statlige, fylkeskommunale og kommunale organer, for leverandører av varer eller tjenester i forbindelse med sikkerhetsgraderte anskaffelser, og andre områder som regjeringen (Kongen i statsråd) bestemmer.



Figur 15.2. Sikkerhetslovens fokus.

Sikkerhetsloven fokuserer både på beskyttelse av gradert informasjon, og på beskyttelse av informasjonssystemer, infrastruktur og objekter av sentral betydning for nasjonal sikkerhet. Sikkerhetsloven er dynamisk på den måten at den setter krav til at virksomheter har et styringssystem for informasjonssikkerhet og innfører sikkerhetstiltak basert på risikovurderinger for å oppnå et forsvarlig sikkerhetsnivå.

I tillegg til offentlig sektor er flere private selskaper og sektorer underlagt sikkerhetsloven, som f.eks. infrastruktur, elektronisk kommunikasjon, kraftforsyning, vannforsyning, bank, og finans. De private virksomheter, eller deler av disse, som er underlagt sikkerhetsloven, forvalter grunnleggende nasjonale funksjoner (GNF). For disse er det viktig at ansatte, styre og ledelse evner å forstå styring av informasjonssikkerhet.

Virksomhetssikkerhetsforskriften, som er hjemlet i sikkerhetsloven, gir utfyllende regler om hvordan offentlige og private virksomheter som er underlagt sikkerhetsloven, skal utføre forebyggende sikkerhetsarbeid. Forskriften setter blant annet krav til styringssystem for informasjonssikkerhet.

15.3.2 Andre relevante lover og forskrifter for informasjonssikkerhet

Det fins et relativt stort antall lover og forskrifter som setter krav til informasjonssikkerhet. Nedenfor presenteres et lite utvalg.

- **eForvaltningsforskriften**

Forskriftens formål er å legge til rette for sikker og effektiv bruk av elektronisk kommunikasjon med og i forvaltningen. Forskriften gjelder for elektronisk kommunikasjon med forvaltningen og for elektronisk saksbehandling og kommunikasjon i forvaltningen. Forskriften setter krav om at forvaltningsorganer skal ha et styringssystem for informasjonssikkerhet, beskrevet som *Internkontroll på informasjonssikkerhetsområdet* (Kapittel 3. Styring og kontroll med informasjonssikkerheten, § 15)

- **Kraftberedskapsforskriften**

Forskriften skal sikre at kraftforsyningen opprettholdes og at normal forsyning gjenopprettes på en effektiv og sikker måte i og etter ekstraordinære situasjoner for å re-

dusere de samfunnsmessige konsekvensene. Kraftberedskapsforskriften gjelder for alle KBO-enheter, der KBO (Kraftforsyningens beredskapsorganisasjon) omfatter NVE og de virksomheter som står for kraftforsyningen. Dette omfatter alle enheter som eier eller driver kraftproduksjon med tilhørende vassdragsregulering, overføring og distribusjon av elektrisk kraft og fjernvarme. Forskriften har en rekke bestemmelser relatert til informasjonssikkerhet. Disse er:

- Kapittel 5. Klassifisering og sikringstiltak
- Kapittel 6. Informasjonssikkerhet
- Kapittel 7. Beskyttelse av driftskontrollsystem
- **Aksjeloven og allmennaksjeloven**
Et aksjeselskap er en selskapsform hvor eierne ikke er personlig ansvarlige for selskapets forpliktelser eller gjeld. Det betyr at selskapets kreditorer ikke kan kreve at aksjeeierne personlig dekker gjelden til selskapet. Selskapet skal ha et styre med ett eller flere medlemmer. Lovene inneholder bestemmelser om hvordan aksjeselskapet skal organiseres på en forsvarlig måte.
Aksjeloven og allmennaksjeloven tar i liten grad for seg informasjonssikkerhet. Imidlertid er det viktig å legge merke til det implisitte kravet om rapportering til styret ved alvorlige cybersikkerhetshendelser. Dette uttrykkes slik i § 6-14 nr. 2: «*Den daglige ledelse omfatter ikke saker som etter selskapets forhold er av uvanlig art eller stor betydning.*» Hvis en cybersikkerhetshendelse er uvanlig eller har stor betydning, har altså daglig leder plikt til å rapportere hendelsen til styret.

15.3.3 Regelverk fra EU

EU har et omfattende regelverk bestående hovedsaklig av direktiver (eng. directives) og forordninger (eng. acts, regulations).

Et EU-direktiv skal implementeres i en eller flere nasjonale lover med omtrent tilsvarende innhold. Hvis Norge tar inn et nytt direktiv, kan det hende at Norge allerede har lover som dekker direktivet helt eller delvis.

En EU-forordning skal som hovedregel implementeres som nasjonal lov nøyaktig slik den er artikulert av Europakommisjonen, bare oversatt til det nasjonale språk. Den nasjonale loven er da en *henvisningslov*. Imidlertid kan en forordning inneholde bestemmelser som gir den enkelte stat mulighet til å tilpasse deler av en forordning til nasjonal rett. Et typisk eksempel på dette er GDPR, der Norge har gjort en rekke nasjonale tilpasninger i personopplysningsloven som omfatter GDPR.

EØS-landene bestemmer sammen om et EU-direktiv eller en EU-forordning skal gjelde i EØS-landene, som dermed betyr at direktivet eller forordningen blir tatt inn i selve EØS-avtalen. Her gjelder prinsippet om alle eller ingen, det vil si at Norge ikke kan bestemme alene om vi skal eller ikke skal ta inn et EU-direktiv eller en EU-forordning. Norge kan også vedta lover som er i samsvar med et direktiv eller en forordning, uten at disse formelt blir en del av EØS-avtalen.

- **NIS2-direktivet** (Network and Information Security nr. 2), 2023
NIS2-direktivet gjelder fra 2023, og erstatter det tidligere NIS-direktivet fra 2016. Da Norge og EØS-landene allerede har innlemmet det forrige NIS-direktivet, betyr NIS2 at Norge vil tilpasse nasjonale lover og/eller lage en ny lov. Elementer i NIS2 er blant annet:
 - skape samarbeid om en europeisk infrastruktur for håndtering av cyberkrise gjennom EU-CyCLONe (European Cyber Crises Liaison Organisation Network)
 - harmonisere sikkerhetskrav og rapporteringsplikter
 - sørge for at medlemslandenes cybersikkerhetsstrategier dekker sikkerhet i leveransejeder, sårbarhetshåndtering, sikkerhet i kjernenettet og generell digital sikkerhetskultur og cyberhygiene
- **GDPR** (General Data Protection, Regulation), 2018
GDPR heter på norsk *Personvernforordningen*, som er implementert i *personopplysningsloven*. GDPR er beskrevet i kapittel 10.
- **eIDAS-forordningen** (electronic IDentification And trust Services), 2014
eIDAS heter på norsk *lov om elektroniske tillitstjenester*. Forordningen er under revisjon og vil få nytt navn. eIDAS er beskrevet i avsnitt 8.7.
- **PSD2** (betalingstjenestedirektivet), 2019
PSD2 (Payment Services Directive nr. 2) regulerer betalingstjenester i EUs indre marked, og er implementert bl.a. i finansforetaksloven og forskrift om betalingstjenester. Et viktig aspekt er at direktivet åpner for at bankkunder kan benytte andre aktører enn de tradisjonelle bankene for å utføre finansielle operasjoner
- **Ekomdirektivet** (Directive for establishing a European Electronic Communications Code), 2021
Ekomdirektivet er implementert i ekomloven, som har til formål å stimulere investeringer i og utrulling av i høyhastighetsnett i hele EU, styrke det indre marked og styrke forbrukerrettigheter. Den reviderte ekomloven utvider virkeområdet til å dekke nye typer kommunikasjonstjenester som f.eks. Messenger, WhatsApp, Signal osv.
- **Cybersikkerhetsforordningen** (Cybersecurity Act), 2023
Det noe pretensiøse navnet på denne forordningen er ikke lett å tolke intuitivt. Forordningen dreier seg hovedsakelig om ENISA (European Union Agency for Cybersecurity), som gjennom forordningen får en permanent status med spesifikt mandat. ENISA ble opprettet i 2004 som *European Network and Information Security Agency*, men hadde ingen permanent status og var avhengig av årlig budsjettbevilgning fra Europakommisjonen. Cybersikkerhetsforordningen gir ENISA permanent status, et styrket budsjett, flere ansatte og et styrket mandat. ENISA skal etter anmodning kunne bistå medlemslandene med grenseoverskridende hendelseshåndtering, herunder blant annet rådgivning, analyse og tekniske undersøkelser. ENISA skal også særlig bistå og legge til rette for medlemslandenes kapasitetsutbygging, operasjonelt samarbeid og forskning og utvikling.

Forordningen etablerer også et felleseuropeisk rammeverk for frivillig sertifisering av IKT-produkter, tjenester og prosesser. Forordningen er foreløpig ikke vedtatt som norsk lov, men blir det antagelig. Det vil gi Norge og EØS-landene deltagelse og status i ENISA og ECCG (The European Cybersecurity Certification Group), men uten stemmerett.

- **Cyber Resilience Act** (under arbeid)

Forslaget til Cyber Resilience Act fokuserer på å sette sikkerhetskrav til digitale produkter, både maskinvare og programvare. *Cyber resilience* kan oversettes med *cybertåleevne*, eller angelifisert som *cyberresiliens*. Denne forordningen kan knyttes sammen med sertifisering av IKT-produkter som er en del av cybersikkerhetsforordningen beskrevet over.

Oppgaver til kapittel 15

15.1 Ansvar

Se for deg at selskap A og selskap B av samme størrelse blir ofre for cyberangrep, og at begge selskapene får betydelige tap som negativt påvirker kunder og aksjonærer. Begge selskap er underlagt lovkrav om å ha et styringssystem for informasjonssikkerhet. Under etterforskningen av hendelsene blir det funnet at selskap A har implementert et ISMS (styringssystem for informasjonssikkerhet) og har god modenhet for ledelse av informasjonssikkerhet, mens selskap B har mangelfullt ISMS og bare har en ad hoc-ledelse av informasjonssikkerhet. Hvis man antar at tapet for begge selskapene er i samme størrelsesorden, forklar mulige forskjeller mellom selskapene vedrørende reaksjoner og sanksjoner mot selskapene eller deres ledelse.

15.2 Kraftberedskapsforskriften

Skykraft (et fiktivt selskap) ønsker å tilby skybaserte IoT-løsninger for bryterfunksjonalitet i kraftforsyningen, f.eks. for måling av elektrisk energi og begrensnings av energi- og effektuttaket ved det enkelte målepunkt. Tjenestene skal la kraftselskapene utføre bryterfunksjonalitet fra enkle brukerterminaler gjennom internett fra hele verden. Sikkerhet skal ivaretas bl.a. med sterk tofaktor-autentisering med BankID.

Vil en slik løsning være lovlig i henhold til kraftberedskapsforskriften?
Forklar hvorfor / hvorfor ikke.

15.3 EU-regelverk

- a. Direktiver (directives) og forordninger (acts and regulations) er ulike regelverk som utvikles og publiseres av EU. Som EØS-land gjelder mange av disse for Norge. Hvordan bestemmes det om et direktiv eller forordning skal gjelde for Norge?
- b. Hva er et EU-direktiv, og hvordan implementeres et EU-direktiv i Norge?
- c. Hva er en EU-forordning, og hvordan implementeres en EU-forordning i Norge?

Beredskap og hendelseshåndtering

I dette kapitlet lærer du om betydningen av beredskap og hendelseshåndtering, samt de viktigste elementene som inngår i beredskapsplanlegging og i selve håndteringen av sikkerhetshendelser. Du lærer også om digital etterforskning, og hva som kreves for at bevis skal kunne fremlegges i en rettssak. Til slutt lærer du om hvordan håndtering av cyberhendelser er organisert nasjonalt og i ulike sektorer.

16.1 Bakgrunn for beredskap og hendelseshåndtering

Hensikten med beredskap og hendelseshåndtering er å være best mulig forberedt når en sikkerhetshendelse inntreffer, slik at skadeomfanget kan begrenses mest mulig. Uten beredskap og hendelseshåndtering kan en sikkerhetshendelse som i utgangspunktet er relativt ubetydelig, gi uforholdsmessig store og negative konsekvenser. Å sørge for cyberberedskap er et ISMS-krav og en forutsetning for å nå høy modenhet i styring av informasjonssikkerhet, som forklart i avsnitt 12.6.

Frem til nå har denne boken for det meste beskrevet metoder og prinsipper for å sikre verdier mot angrep, og som dermed kan forhindre eller redusere sannsynligheten for at sikkerhetshendelser inntreffer, eller for å oppdage når en slik hendelse inntreffer. Imidlertid er det umulig å stoppe alle trusler og forhindre alle hendelser. Når en sikkerhetshendelse skjer, er det viktig at virksomheten er forberedt, som kalles *beredskap*. Aktivitetene for respons og videre håndtering av sikkerhetshendelser kalles *hendelseshåndtering*.

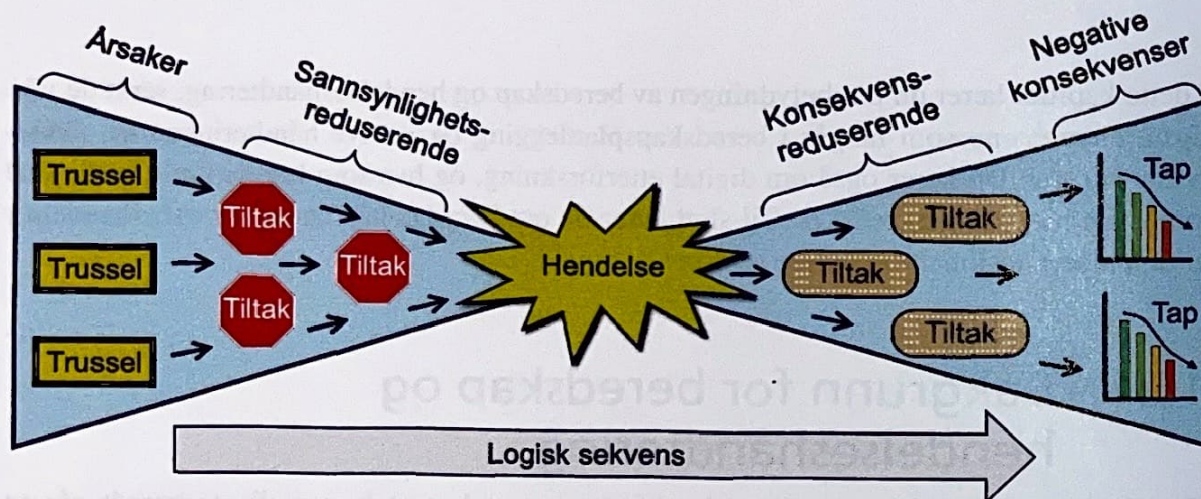
Forrige kapittel tok hovedsakelig for seg vurdering og analyse av risiko basert på følgende prinsipper:

- Identifisering av risikoer som sammenstillinger av trussel, sårbarhet og hendelse på verdier.
- Beregning av risikonivåer som kombinasjon av sannsynlighet og konsekvens av sikkerhetshendelser.

Risikovurdering har til hensikt å identifisere og analysere risikoer som nevnt over, og deretter å sammenligne og vurdere alvorlighetsgrad av de ulike risikoene.

En annen måte å analysere og visualisere risiko på er ved hjelp av sløyfediagrammer (eng.: bow tie diagrams). Et sløyfediagram visualiserer sammenheng og hendelsesforløp mellom årsak og konsekvens av uønskede hendelser. Det benyttes et separat sløyfediagram for å visualisere hver type hendelse.

Hvert sløyfediagram fokuserer på en spesifikk type/klasse av hendelse/risiko, og visualiserer relevante trusler, preventive tiltak (som allerede er eller kan bli implementert), skadebegrensende tiltak (som allerede er eller kan bli implementert) og til slutt de mulige negative konsekvensene som kan følge av hendelsen. Konsekvenser av informasjonssikkerhetshendelser er forskjellige typer tap som beskrevet i avsnitt 14.4.3. Det generelle sløyfediagrammet i figur 16.1 viser en udefinert hendelse som eksempel, og illustrerer det logiske hendelsesforløpet fra venstre mot høyre.



Figur 16.1. Sløyfediagram for å visualisere risiko for en hendelse.

Diagrammets venstre side representerer både årsaker/trusler og mulige tiltak som kan redusere sannsynligheten for at hendelsen inntreffer. Høyre side representerer mulige tiltak som kan redusere konsekvensen og begrense skaden gitt at hendelsen inntreffer likevel.

Sløyfediagram er ofte brukt i samfunnssikkerhet for å analysere uønskede fysiske hendelser som brann, oversvømmelse og ulykker. Diagrammet kan også brukes for å visualisere sammenheng mellom forebygging og håndtering av sikkerhetshendelser.

Aktiviteter rundt informasjonssikkerhet har tradisjonelt fokusert på venstre side av sløyfediagrammet, det vil si på tiltak for å forhindre sikkerhetshendelser. Høyre side av sløyfediagrammet, som representerer beredskap og hendelseshåndtering for informasjonssikkerhet, er også svært viktig for helhetlig informasjonssikkerhet.

I *Nasjonal strategi for digital sikkerhet* fra 2019 uttrykker regjeringen målsetting 1) om at norske virksomheter sørger for egenbeskyttelse og har evne til å håndtere cyberangrep, 2) om å styrke digital sikkerhetskompetanse i tråd med samfunnets behov og 3) om at samfunnet får en bedre evne til å avdekke og håndtere digitale angrep. Målsetting (1) om virksomheters

egenbeskyttelse mot cyberangrep står i kontrast til hva vi forventer av myndighetene med hensyn til å håndtere vold og fysiske innbrudd, der vi forventer at politiet etterforsker og samler bevis til bruk i rettssaker og for å håndheve lov og rett. Innen cybersikkerhet forventes altså at hver virksomhet «er sitt eget politi», som forutsetter at de har en viss cyberberedskap.

NSMs grunnprinsipper for IKT-sikkerhet (beskrevet i avsnitt 12.4) definerer følgende fire hovedprinsipper: 1) Identifisere og kartlegge, 2) Beskytte og opprettholde, 3) Oppdage sårbarheter og skadevare, 4) Håndtere hendelser og gjenopprette.

Hovedprinsipp 4) *Håndtere hendelser og gjenopprette* ligger på høyre side av sløyfediagrammet i figur 16.1, og dekker beredskap og hendelseshåndtering. Hovedprinsipp 4) består av følgende trinn:

- Forbered håndtering av hendelser
- Vurder og klassifiser hendelser
- Kontroller og håndter hendelser
- Evaluer og lær av hendelser

Det første trinnet hører til beredskapsplanlegging, som er beskrevet i neste avsnitt. De tre siste trinnene hører til hendelseshåndtering, som er beskrevet i avsnitt 16.5.

16.2 Beredskapsprinsippene

Terrorangrepene den 22. juli 2011 satte samfunnets beredskap på prøve, noe som førte til at Justis- og beredskapsdepartementet publiserte *Stortingsmelding 29 (2011–2012) Samfunnsikkerhet* i juni 2012. Stortingsmeldingen definerte følgende fire grunnleggende prinsipper for samfunnssikkerhet og beredskap:

1. **Ansvarsprinsippet.** *Den organisasjonen som har ansvar for et fagområde i en normal-situasjon, har også ansvaret for nødvendige beredskapsforberedelser og for å håndtere ekstraordinære hendelser på området.*

For en privat virksomhet tolkes «fagområde» som virksomhetens egne aktiviteter og forretningsprosesser, som dermed betyr at hver virksomhet må ha sin egen beredskapsplan.

2. **Nærhetsprinsippet.** *Kriser skal håndteres på lavest mulig nivå i organisasjonen.*

Dette prinsippet skal gjøre hendelses- og krisehåndteringen mest mulig effektiv, og skal ivareta organisasjonens ressurser. Krisehåndtering kan være svært ressurskrevende, og hvis små hendelser som skjer ofte, skulle bli eskalert til krisehåndtering hver gang, ville det slite på organisasjonens ressurser.

3. **Likhetsprinsippet.** *Den organiseringen man opererer med under kriser skal være mest mulig lik den organisasjonen man har til daglig.*

Dette prinsippet sier at hvis en hendelse inntreffer innen en spesifikk avdeling eller forretningsprosess, så skal hendelsen håndteres av nettopp de som til vanlig jobber i den avdelingen eller som forvalter den forretningsprosessen.

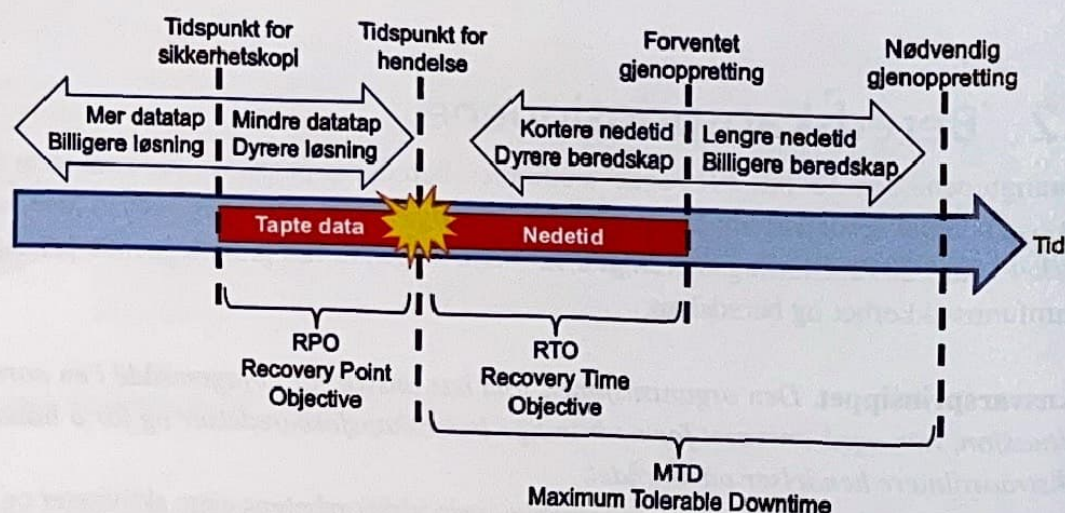
4. **Samvirkeprinsippet.** *Organisasjoner har et selvstendig ansvar for å sikre et best mulig samvirke med relevante aktører og virksomheter i arbeidet med forebygging, beredskap og krisehåndtering.*

Dette prinsippet sier at hver virksomhet må kartlegge relevante eksterne aktører som kan bistå ved hendelser og kriser. Det må etableres kontakt og avtaler med disse aktørene slik at de raskt kan tilkalles ved behov.

Selv om prinsippene over ble definert for nasjonal samfunnssikkerhet, er de også anvendbare for cyberberedskap i virksomheter, slik forklaringen av hvert prinsipp viser. Det er viktig å ha en klar ansvarsfordeling i beredskapsarbeidet, som betyr å vite hvem som har hvilke oppgaver. Samfunnssikkerhetsprinsippene definerer nettopp ytre rammer for ansvarsfordeling.

16.3 Tekniske beredskapsbegreper

Det brukes forskjellige tekniske begreper for å kunne tallfeste tidsmessige målsettinger for beredskap. Figur 16.2 viser sammenhengen mellom disse begrepene, som forklares nedenfor.



Figur 16.2. Tidsaspekter ved beredskap og gjenoppretting.

- **RPO (Recovery Point Objective)** (mål for gjenopprettingspunkt) er den maksimalt akseptable alderen på den siste sikkerhetskopien (eng. backup). Rutiner for sikkerhetskopiering må dimensjoneres for å tilfredsstille RPO. Hvis en lagringsenhet svikter, filer slettes ved et uhell eller som resultat av en tilsiktet ondsinnet handling, kan filer eller databaser med alder gitt av RPO eller eldre gjenopprettes fra sikkerhetskopien. Virksomheten må være forberedt på at yngre data med en lavere alder enn RPO kan bli tapt ved en hendelse. Jo kortere RPO, desto mer kostbar blir løsningen for sikkerhetskopiering.
- **RTO (Recovery Time Objective)** (mål for gjenopprettingstid) er tiden virksomheten tar sikte på å trenge etter en hendelse med sikkerhetsbrudd, for å gjenopprette eller gjenopp- ta sine aktiviteter, produksjon eller tjenesteytelse. Ressurser for beredskap må dimensjo-

neres for å tilfredsstille RTO. Hvis det kun dreier seg om å hente sikkerhetskopi, er det tiden som trengs for å hente og installere sikkerhetskopien. Hvis det dreier seg om feil som medfører at drift og tjenester stopper opp, er det tiden som trengs for å rette feilen. Hvis det dreier seg om cyberangrep med kompromittering der virksomheten selv velger å stanse drift, er det tiden som trengs for å rydde opp og kaste ut inntrenger slik at virksomheten finner det forsvarlig å gjenoppta drift. Jo kortere RTO, desto dyrere blir det å etablere tilstrekkelig beredskap med nødvendig kompetanse.

- **MTD (Maximum Tolerable Downtime)** er den maksimale tiden drift eller tjenester kan være utilgjengelig for brukere før det anses å ha katastrofale konsekvenser. Å fastsette MTD er basert på innvirkningen på forretningsfunksjoner, og analyse av forventet tapt inntekt og andre kostnader som påløper for hver time, dag eller uke en gitt applikasjon eller database kan være utilgjengelig, og er spesifisert av bedriftsledelsen. MTD brukes for å velge strategi for gjenoppretting, der to alternativer er *gjenoppretting*, som på engelsk kalles **DRP (Disaster Recovery Planning)**, og *nødrutiner*, som på engelsk kalles **BCP (Business Continuity Planning)**. **DRP** og **BCP** forklares nedenfor.
- **DRP (Disaster Recovery Planning)** er å planlegge for gjenoppretting av systemer og prosesser som er blitt skadet etter en hendelse, slik at produksjon og tjenester kommer tilbake i normal drift. Hvis for eksempel kassasystemer i en butikkjede ikke virker som følge av et cyberangrep, betyr en beslutning om å følge **DRP** at cyberhendelsen må håndteres og systemene gjenopprettes slik at kassasystemene igjen fungerer. I noen tilfeller kan det ta lengre tid enn MTD, slik at det kan være nødvendig å også planlegge for *nødrutiner*.
- **BCP (Business Continuity Planning)** er å planlegge for *nødrutiner* for å opprettholde drift av produksjon og tjenester mens gjenoppretting av skadede systemer og prosesser foregår. Med *nødrutiner* vil vanligvis kapasitet og kvalitet være redusert, men det kan være et bedre alternativ enn at produksjon og tjenester faller helt ut. Hvis for eksempel kassasystemer i en butikkjede ikke virker som følge av et cyberangrep, kan **BCP** innebære at kunder betaler med kontanter. En beslutning om å sette i verk **BCP** typisk gjøres hvis det antas at gjenoppretting av normale systemer og prosesser med **DRP** vil ta lengre tid enn MTD.

16.4 Beredskapsplanlegging

Beredskapsplanleggingen skal gjøre virksomheten forberedt på å håndtere små og store sikkerhetshendelser, slik at håndteringen kan utføres best og raskest mulig. Dette trinnet er samtidig en del av *innebygd informasjonssikkerhet og personvern*, som er nærmere beskrevet i avsnitt 11.3. NSMs grunnprinsipper for IKT-sikkerhet beskriver *forberedelse på håndtering av hendelser* med følgende punkter:

- *Plan for hendelses- og krisehåndtering.* Planen bør inneholde a) krav (forventet evne) til gjenopprettelse av IKT-funksjoner basert på en **BIA (Business Impact Analysis)**, b) rolle- og ansvarsbeskrivelser, c) krav til opplæring, d) klassifiseringsregime for hendelser og kriterier for å aktivere krisestab samt e) krav til testing og øving av planen. Planen skal oppdateres jevnlig og i etterkant av øvelser og større hendelser.

- **BIA (Business Impact Analysis)**, som kan kalles forretningskonsekvensanalyse. BIA gjøres for å identifisere virksomhetskritiske funksjoner. Denne bør kartlegge a) prioritering av de mest vitale forretningsfunksjoner samt definere MTD og sikkerhetskrav for disse, b) identifisere avhengigheter mellom IKT-funksjoner og c) definere krav til gjenopprettingstid (RTO), evne til å tåle tap av data (RPO) og evne til å tåle redusert tjenestenivå og bruk av BCP. Det er nyttig å definere kategorier av MTD for alle virksomhetskritiske funksjoner, som f.eks.

– Kategori 1: Helt essensielle funksjoner,	MTD = 0–12 timer
– Kategori 2: Svært viktige funksjoner,	MTD = 13–24 timer
– Kategori 3: Viktige funksjoner,	MTD = 1–3 dager
– Kategori 4: Mindre viktige funksjoner,	MTD = mer enn 3 dager
- **Team for hendelsesrespons og andre roller** som skal involveres i hendelseshåndteringen. Dette inkluderer a) roller med ansvar for sentrale driftsoppgaver og for håndtering av hendelser, b) ledere med beslutningsansvar på ulike nivåer, c) beredskapsvakter med krav til tilgjengelighet utenom normal arbeidstid og i ferieperioder og d) opplæring og øving av personell.
- **Avtaler med relevante tredjeparter** slik at disse er klare til å yte støtte dersom det kreves ved en hendelse. Dette kan være SRM (sektorvise responsmiljøer), IT-spesialister innen ulike fagfelt, leverandører av utstyr og programvare og MSSP (Managed Security Service Providers), dvs. leverandører av SOC- og CSIRT-tjenester.
- **Kommunikasjonskanaler** som skal benyttes i forbindelse med hendelser: a) kontaktinformasjon for relevant personell, b) plan for alternative kommunikasjonskanaler og c) plan for intern og eksternt kommunikasjon rundt hendelser.
- **Testing og øvelser.** Det er viktig at planen testes. Øvelser bør inkludere relevante underleverandører, og bør inkludere testing av rutiner for deteksjon av hendelser.

Testing og øving kan gjøres på forskjellige måter, fra abstrakte til praktiske. Noen varianter av testing/øving er for eksempel følgende:

- **Sjekkliste-test:** Planen for beredskap og hendelseshåndtering blir gjennomgått av berørte enheter for kommentarer til forbedring.
- **Strukturert gjennomgang:** Representanter fra berørte enheter kommer sammen for å gå gjennom planen. En slik test trenger liten forberedelse, og kan gjøres i en workshop med varighet av noen timer. En strukturert gjennomgang kan også omfatte øving av ledelse og administrasjon, med tanke på konsekvenshåndtering, koordinering og kommunikasjon.
- **Simuleringstest.** Representanter fra berørte enheter kommer sammen for å øve på håndtering av angrep på systemer og forretningsfunksjoner i en simulert omgivelse. En slik øvelse krever omfattende forberedelse, og øvelsen tar typisk hele dagen.

16.5 Hendelseshåndtering

Hendelseshåndtering er en organisert reaksjon på en sikkerhetshendelse. Målet er å håndtere situasjonen på en måte som begrenser skade og minimerer gjenopprettingstid og tap.

De tekniske aspektene av hendelseshåndtering kalles *hendelsesrespons*, som typisk utføres av et eget team med støtte fra IT-drift og andre støttefunksjoner i organisasjonen. Organisering av hendelsesrespons varierer mye fra virksomhet til virksomhet. I en virksomhet som har et teknisk operasjonssenter, vil hendelsesrespons starte i operasjonssenteret. Et drifts- eller operasjonssenter for en nettoperatør eller et større datasenter håndterer gjerne et stort antall avvik og uønskede hendelser hver eneste dag. Dersom hendelsen er alvorlig, eller eskalerer over et gitt nivå, blir det satt et eget team, og selv da er det gjerne enda en terskel for å beslutte varsling til ledelsen.

For enkelte sektorer er det også definert terskel for når virksomheten skal varsle myndighetene om en pågående hendelse. Da kan det være snakk om sanntid, og ikke f.eks. tre dager etter hendelsen.

I store, alvorlige hendelser vil det eksistere flere team. Virksomheten etablerer typisk en kriseledelse, og ved behov settes det også en krisestab som avlaster kriseledelsen med innhenting av relevant informasjon, lager regelmessige situasjonsrapporter og ekspederer all rutinemessig kommunikasjon. På den måten kan kriseledelsen konsentrere seg om kjerneproblemer, planlegging, koordinering og beslutninger. Dette gjelder alle typer alvorlige hendelser, og ikke bare hendelser på området informasjonssikkerhet. For virksomheter som har dette på plass, er det en selvfølge å inkludere håndtering av informasjonssikkerhetshendelser.

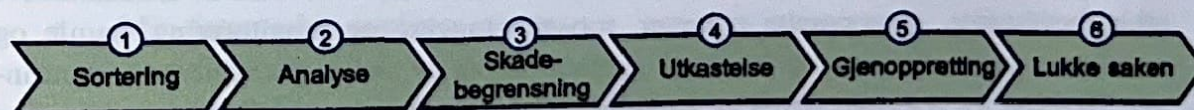
Organisasjonens plan for beredskap og hendelseshåndtering kan utarbeides som del av ISMS, beskrevet i avsnitt 12.3.3, eller som del av virksomhetens helhetlige styringssystem. Hendelseshåndtering er også en del av innebygd informasjonssikkerhet og personvern, som beskrevet i avsnitt 11.3.7.

Hendelseshåndtering dekker hovedsaklig IT-aspekter i form av hendelsesrespons, men også andre aspekter. Hendelseshåndtering er en sammensatt prosess der tekniske IT-funksjoner samarbeider med beslutningstagere, representanter for PR og kommunikasjon, og med juridiske representanter.

Ved utilstrekkelig håndtering av noen av aspektene kan en sikkerhetshendelse få uforholdsmessig uheldige konsekvenser. Ved utilstrekkelig teknisk håndtering kan små hendelser vokse og bli store. Ved svak beslutningstaking kan et ellers kompetent team kaste bort tid og ressurser på unødvendige aktiviteter eller jobbe inkonsistent. Ved svak eller dårlig gjennomtenkt kommunikasjon kan eksterne parter fordreie pressedekningen av hendelsen, som kan skade organisasjonens omdømme. Ved mangelfull håndtering av bevis kan det bli vanskelig å føre en rettsprosess mot angriperne, selv om det kanskje er kjent hvem som sto bak angrepet.

Det er primært viktig å reagere raskt når en hendelse oppdages, men det er også viktig å sørge for god håndtering av de andre aspektene nevnt over.

Den tekniske delen av hendelseshåndtering er hendelsesrespons. Prosessen for hendelsesrespons består av et sett med trinn, der figur 16.3 viser en vanlig måte å inndele prosessen på.



Figur 16.3. Prosess for hendelsesrespons.

Figuren er en forenklet fremstilling som kan gi inntrykk av at det er en fullstendig sekvensiell prosess. I virkeligheten arbeides det typisk med flere av disse trinnene parallelt og i iterasjoner. Trinnene i prosessen fra figur 16.3 er beskrevet nedenfor.

1. *Sortering (Triage)*: Deteksjon av en hendelse kan skje på forskjellige måter, f.eks. basert på (i) IDS (Intrusion Detection System) eller annen monitorering som klassifiserer nettverkstrafikk eller systemhendelser som skadelig eller normal, (ii) intern avviksrapportering eller (iii) rapportering fra eksterne parter. Sortering er den første vurderingen av en detektert hendelse for å luke ut falske positive, kategorisere hendelsen i henhold til type og alvorlighetsgrad, prioritere ressurser og angi retningen for videre håndtering. Dette trinnet utføres som del av vanlig drift. Beslutning om å iverksette beredskapsplaner og sette i gang hendelsesrespons gjøres gjerne her. Med hensyn til effektiv bruk av ressurser har det stor praktisk betydning at sortering gjøres riktig.
2. *Analyse*: Det må søkes og samles inn dokumentasjon, som så analyseres for å opparbeide størst mulig forståelse av hva som har skjedd, og hva som bør gjøres videre. For innsamling anvendes prinsippet om *flyktighetsrekkefølge*, dvs. at det mest flyktige bevismaterialet samles inn først, deretter bevismaterialet som har mer varig karakter. Bevismaterialet må hele tiden håndteres korrekt for å opprettholde dets juridiske *notoritet* i tilfelle det blir nødvendig å legge frem materialet i en rettssak. Analysen kan også støtte seg på CTI (digital trusseletterretning), som er beskrevet i avsnitt 17.2. Digital etterforskning inngår i dette trinnet, se avsnitt 16.6.
3. *Skadebegrensning (Containment)*: For å unngå forverring av hendelsen er det viktig å sørge for at angrepet ikke sprer seg videre. Bruk skjønn for å avgjøre hvorvidt servere, applikasjoner og systemer bør stoppes eller isoleres (settes offline) eller fortsette å kjøre og være online. Det kan være nødvendig å la infiserte systemer fortsette å kjøre for å opprettholde kritiske og viktige forretningsapplikasjoner. Her kan virtuelle plattformer ha visse fordeler. Ideelt sett kan virtuelle maskiner stoppes og lagres for analyse, og nye virtuelle maskiner kan raskt spinnes opp for å opprettholde kritiske tjenester.
4. *Utkastelse (Eradication)*: Årsaken til hendelsen må fjernes, som typisk beskrives med å kaste trusselaktøren ut av virksomhetens nett. Denne aktiviteten kan bestå av å identifisere og fjerne sårbarhet, oppgradere/patche systemet, fjerne skadevare og korrigere systemkonfigurasjoner. Ofte vil denne årsaken være en trusselaktør som har uautorisert tilgang og som har installert skadevare eller endret konfigurasjoner. Målet med utkastelsen er å fjerne alt dette. Kunnskapen som opparbeides i analysen, er svært viktig input til denne fasen. For å kaste ut trusselaktøren må man være helt viss på (i) å ha full kontroll på hva aktøren har gjort for å sikre kunnskap om eventuelle bakdører, og (ii) å ha en forsvarbar infrastruktur med gode deteksjonsskapabiliteter som gjør at gjentatte inntrengningsforsøk blir oppdaget.
5. *Gjenoppretting (Restoring) og normalisering*: Dette trinnet kan bestå av å reinstallere sikkerhetskopier, gjenopprette tjenester, fortsette logging og monitorering, samle og overlevere bevis, *herding* og eventuell gjennomføring av andre, permanente forbedringer. Herding av systemer består av å redusere sårbarhetsflaten ved å fjerne unødvendige programmer og funksjoner.
6. *Lukke saken (Closing)*: Lukking av saken besluttet normalt av systemeier. Team for hendelsesrespons og andre involverte overleverer sluttrapport med samlet og avsluttende

informasjon. Organisasjonen bør legge vekt på å lære av hendelsen, for om mulig å forbedre prosessen og dokumentasjonen for hendelseshåndteringen.

Myndighetsrapportering er tilleggstrinn som vurderes etter type og alvorlighet av hendelse. Et trinn for myndighetsrapportering kan omfatte følgende:

- Politiet bringes inn i etterforskningen når hendelsen har preg av alvorlig kriminalitet. En utfordring ved anmeldelse til politiet kan være å miste kontroll over etterforskningen og beslag av utstyr. På den annen side kan politiets tilgang til ulike lukkede nettverk for utveksling av CTI være meget nyttig for analysefasen av en hendelse.
- Datatilsynet skal informeres innen 72 timer etter en hendelse med personvernkonsekvens.

Ved en hendelse er virksomheten i utgangspunktet godt rustet hvis den har etablert og innøvd en beredskapsplan for hendelseshåndtering. Beredskapsplaner må være tilgjengelige på fysiske dokumenter, som også må være øvd i bruk. Det kan være kostbart å bygge opp og opprettholde et eget team for hendelsesrespons. Som alternativ kan virksomheten kjøpe MSS (Managed Security Services), som er kommersiell *administrasjon av sikkerhetstjenester*. Det fins ulike typer sikkerhetstjenester, der de vanligste er SOC (Security Operations Centre) og CSIRT (Computer Security Incident Response Team). Et SOC sørger for monitorering av infrastruktur og varsling av hendelser. Et CSIRT håndterer varslede hendelser. Disse begrepene blandes til en viss grad, slik at en SOC også kan drive hendelsesrespons. Det er et voksende marked for slike tjenester med et økende antall tilbydere, både i Norge og internasjonalt.

16.6 Digital etterforskning

Digital etterforskning omfatter analyse av materiale som fins i digitale enheter og nettverkslogger, vanligvis i sammenheng med sikkerhetshendelser og datakriminalitet. Etterforskningen kan være oppdagende for å finne ut hva som har skjedd, eller rettet mot å bevise eller motbevise en hypotese. Digital etterforskning kan inngå som en del av hendelseshåndtering.

Digital etterforskning kan deles inn i flere undergrener, avhengig av hvilken type teknologi og digitale enheter som er berørt. Det kan være digital etterforskning av systemer, datanett og mobile enheter eller ren dataanalyse. Prosessen for digital etterforskning består hovedsakelig av følgende trinn:

1. Identifisering

Dette trinnet består av å oppdage hendelsen, f.eks.:

- «Min datamaskin oppfører seg rart.»
- «Noen har lagt ut hele vår database på WikiLeaks.»

2. Sikring

Pass på at bevisene ikke blir ødelagt ved uaktsom håndtering. Det kan være nødvendig å si: «Ikke slå av datamaskinen!»

3. Innsamling

Innsamling av alt potensielt bevismateriale må gjøres etter flyktighetsrekkefølgen – først flyktige data som RAM, deretter harddisker. Bruk skriveblokkering, og lag flere kopier av disker der én kopi defineres som «masterkopi». Det er viktig å sørge for å ha en *beviskjede*, som betyr at innsamling og håndtering av bevis gjøres på en rettslig forsvarlig måte som forhindrer at bevis kan bli kompromittert. Beviskjeden må dokumenteres, som er nødvendig for at bevisene skal ha *notoritet* i en eventuell rettssak, se avsnitt 16.6.

4. Undersøkelse

Innsamlet data undersøkes for å avdekke relevante elementer, som kan være å finne skjulte filer og partisjoner på en disk.

5. Analyse

Gjennom analyse av innsamlet materiale og logisk resonnering forsøker etterforskeren å komme frem til fakta som kan bevise eller motbevise hypoteser. Det kan settes krav til å bruke to ulike verktøy for å gjøre samme analyse for å bekrefte resultatene av analysen. Trinnene i analysen må være repeterbare. Lag en kronologisk oversikt over antatte hendelser.

6. Fremlegging

Dette trinnet består av å presentere bevis og konklusjoner av analysen til systemeier, til politienheter eller til domstolen.

I tilfelle av «live» innsamling hentes bevismateriale fra et system der mikroprosessen kjører. I tilfelle «post mortem»-innsamling av bevismateriale hentes det fra et lagringsmedium der systemet er slått av. «Post mortem» gir bedre bevaring av integritet og påvirker ikke dataene. Flyktige data kan imidlertid gå tapt i prosessen med å slå av et system. «Live» innsamling gjør innsamling av flyktige data mulig, men påvirker også dataene. I tilfelle harddisken er kryptert, er det bedre å hente informasjonen fra disken mens systemet kjører, fordi nøkkelen for kryptering/dekryptering ligger i RAM.

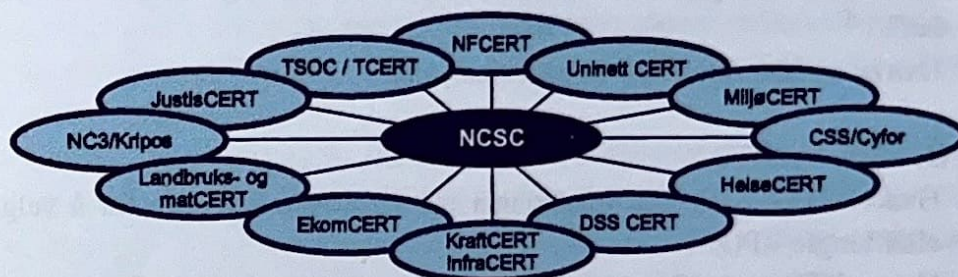
Notoritet i juridisk sammenheng betyr at det fins en beviskjede som er etterviselige og kontrollerbare. En beviskjede i digital etterforskning kan oppnås ved at det lages en kronologisk dokumentasjon som viser beslag, oppbevaring, håndtering, transport, analyse og disponering av bevismateriale, enten det er fysisk eller elektronisk. Fordi bevis kan brukes i retten til å dømme personer for å ha begått forbrytelser, må det håndteres på en særdeles betryggende måte for å unngå mulig feilaktige påstander om forfalskning eller uredelighet. Hvis slike påstander kan underbygges med argumenter om manglende notoritet, vil det kunne skade påtalemyndighetens sak og føre til frifinnelse, selv om påtalemyndigheten ellers er overbevist om at tiltalte er skyldig.

16.7 NCSC og sektorvise responsmiljøer

For å kunne stå sterkere i forsvar mot cyberangrep er det essensielt at virksomheter deler informasjon og koordinerer sine aktiviteter. I Norge er organiseringen av denne typen samarbeid blitt relativt moden. Dette er ikke bare viktig for virksomheter og næringslivet, men utgjør en del av Norges defensive cyberoperasjoner, som forklart i avsnitt 17.4.

NCSC (*Nasjonalt cybersikkerhetssenter*), som er en del av NSM, er nasjonal koordinerende enhet for sikkerhetshendelser med hensyn til deteksjon, hendelsesrespons og koordinering.⁷⁶ NCSC gir også anbefalinger om cybersikkerhet til offentlige myndigheter og næringsliv. NCSC spiller rollen med å samle nasjonal cybersikkerhetskompetanse, der ulike aktører samarbeider basert på felles risikobilde og situasjonsforståelse, både i felles lokaler og over nett. NCSC publiserer fortløpende varslinger om kjente sårbarheter.

I tillegg til NCSC er det opprettet en rekke *sektorvise responsmiljøer* (SRM), som er selvstendige enheter som koordinerer sine aktiviteter med NCSC, som vist i figur 16.4.



Figur 16.4. Sektorvise responsmiljøer og organisering av hendelsesrespons på nasjonalt nivå.

Det er etter hvert blitt opprettet relativt mange SRM-er. De som er opprettet så langt, er NFCERT (Nordic Finacial CERT), Uninett CERT (utdanningssektoren), MiljøCERT (klima- og miljøsektoren), CSS/Cyfor (Forsvarets cybersikkerhetssenter i Cyberforsvaret), HelseCERT (helsesektoren), DSS CERT (Departementenes sikkerhets- og serviceorganisasjon), KraftCERT/InfraCERT (kraft og energisektoren), EkomCERT (post- og telekomsektoren), Landbruks- og matCERT, NC3/Kripos (Nasjonalt cyberkrimsenter), JustisCERT (politi og justissektoren), og TSOC (Telenor Security Operations Center) sammen med TCERT (Telenor CERT). Det vil antagelig komme flere SRM-er i årene som kommer. Begrepet *CERT* (*Computer Emergency Response Team*) er et alternativt navn på CSIRT. De første SRM-ene, som NFCERT og KraftCERT, ble opprettet av sektorene selv, med NSM som pådriver. For nye SRM-er er departementene ansvarlige for å oppnevne SRM-er i sine respektive sektorer, og sette krav og forventninger til denne funksjonen. Hvert departement kan vurdere om det er hensiktsmessig med et spesifikt SRM for en sektor, eller om relaterte sektorer kan være bedre tjent med et tverrsektorielt SRM.

Det er svært nyttig for virksomheter innen en sektor å ha et SRM å støtte seg til. Cyberangrep foregår ofte i kampanjer mot en sektor. I slike situasjoner spiller et SRM en viktig

76 <https://nsm.no/regelverk-og-hjelp/andre-publikasjoner/rammeverk-for-handtering-av-ikt-hendelser/>.

rolle for å koordinere deling av etterretning og gi råd om sikkerhetstiltak til virksomheter i sektoren. Noen sektorer har spesialiserte systemer og infrastrukturkomponenter. Særsilt håndtering og kunnskap om sikkerhet i disse er et spesielt viktig bidrag fra SRM-ene.

I tillegg til NCSC ble FCKS (Felles cyberkoordineringssenter) etablert i 2017. FCKS er et koordineringssamarbeid mellom PST, NSM, Kripos og E-tjenesten. Hensikten er raskest mulig å kunne avklare hovedansvarlig for håndtering og oppfølging av alvorlige cyberhendelser og cyberkriminalitet. FCKS tilrettelegger også analyseprodukter til støtte for etterretning, analyse og håndtering.

Oppgaver til kapittel 16

16.1 Beredskap

- Med utgangspunkt i sløyfediagrammet – hvilke(t) element(er) utgjør beredskap?
- Hva er den vanligste form for beredskap i sammenheng med informasjonssikkerhet?
- Hva er en BIA (Business Impact Analysis)?

16.2 RPO, RTO og MTD

- Hva er RPO, og hvilke vurderinger må virksomheten gjøre for å velge kortere eller lengre RPO?
- Hva er RTO, og hvilke vurderinger må virksomheten gjøre for å velge kortere eller lengre RTO?
- Hva er MTD, og hvordan bestemmes MTD for spesifikke funksjoner og prosesser?

16.3 Responsmiljøer

- Hvilken rolle har et SRM (sektorsvise responsmiljø)?
- Hva er rollen til NCSC (Nasjonalt cybersikkerhetssenter)?
- Hvorfor er koordinering og samarbeid mellom responsmiljøer viktig?

Cyberoperasjoner

Cyberoperasjoner er et nokså vagt begrep som blir brukt i litt varierende betydninger i kontekst av angrep og forsvar innen digitale infrastrukturer. Det kan bety aktiviteter for å koordinere og styrke evnen til å motstå cyberangrep, som inkluderer *digital trusseletterretning*. Begrepet cyberoperasjoner kan også ha betydningen av offensive taktiske og strategiske cyberaktiviteter utført eller sponset av stater.

I dette kapitlet lærer du om de vanligste angrepsvektorene, vanlige typer skadevare og hvordan typiske cyberangrep foregår. Du lærer hva digital trusseletterretning er, hvilke teknikker som brukes, og hvilke utfordringer det har. Du lærer også hva som menes med cyberkrigføring og ulike aspekter ved denne typen aktiviteter.

17.1 Avanserte cybertrusler

Avanserte cyberangrep utføres av ressurssterke trusselaktører. De to neste avsnittene beskriver hva som menes med begrepene APT (Advanced Persistent Threat), eller avansert vedvarende trussel på norsk, og *cyber kill chain*, som er en modell for typisk målrettede cyberangrep og hvordan de kan stoppes.

17.1.1 APT: Avansert vedvarende trussel

En APT (avansert vedvarende trussel, eng.: Advanced Persistent Threat) er en trusselaktør eller gruppering som ofte tilhører en nasjonalstat eller er sponset av en nasjonalstat. Imidlertid fins det også APT-er som kun er kriminelle og ikke har noen tilknytning til en stat ut over at personene oppholder seg i et land. Slike APT-er kan være like avanserte og vedvarende som statlige APT-er, og kan være beskyttet av staten på den måten at de får operere fritt så lenge de ikke angriper mål i eget land. I tillegg kan en del politisk motiverte aktører kunne betegnes som APT-er. De er da ikke knyttet til en stat, men en ideologisk overbevisning med betydelige ressurser i en organisert form.

En APT er ikke beskrevet med et organisasjonsnavn og adresse, men som en gruppering med en observert *aktivitetsprofil*. Begrepet APT ble først brukt av det amerikanske luftforsvaret i 2006, og er etter hvert blitt en generell typebetegnelse på de mest ressurssterke trus-

selaktørene. Den er *avansert* fordi den har til rådighet rikelig med ressurser for etterretning, kompetanse og verktøy til å utvikle exploits, til å kontrollere infrastrukturer og til å utføre angrep.

En APT er *vedvarende* fordi en slik aktør har langsiktige målsettinger, i motsetning til å opportunistisk bare søke kortvarig gevinst for seg selv. Målsettingene blir som regel fastlagt av overordnede politiske eller strategiske enheter. Langsiktigheten gjør at en APT ikke gir opp hvis den møter motstand, men at den har utholdenhet til å utføre angrep i sakte tempo, noe som gjør at slike angrep ofte «går under radaren» og forblir uoppdaget. En målsetting er typisk å oppnå vedvarende tilgang over flere år til infiltrerte systemer og nettverk, der tilgangen kan ligge ubrukt i påvente av at det oppstår behov for å utnytte den.

En APT er en *alvorlig trussel* nettopp fordi en slik aktør både har motivasjon gjennom langsiktige målsettinger og kapasitet gjennom statlige ressurser, og har profesjonelle medarbeidere som har det som fulltidsjobb å drive offensive cyberoperasjoner.

Angrep fra en APT er typisk rettet mot spesifikke land og sektorer, som departementer, forsvar, finans, industri, telekommunikasjon, helse og energi.

Gjennomsnittlig varighet av en APTs uautoriserte tilganger, dvs. tiden det tar før et APT-angrep blir oppdaget og stoppet, er over 100 dager. Med så lang tilgang har angriperen som regel tid til å fullføre hele angrepssyklusen og oppnå hele eller store deler av målsettingen.

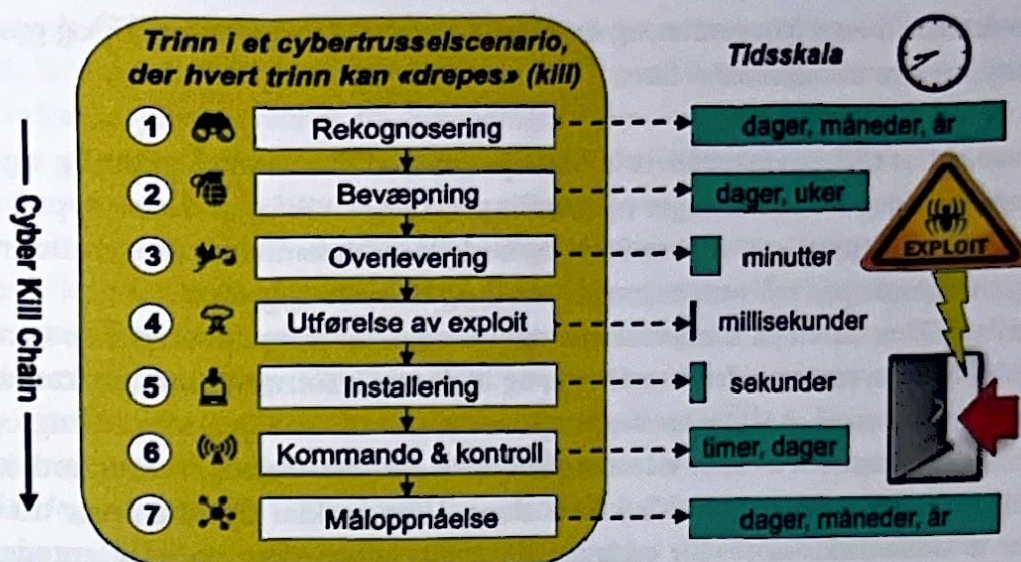
Flere organisasjoner vedlikeholder lister over de mest aktive APT-grupperingene, der en relativt fyldig oversikt vedlikeholdes av MITRE ATT&CK beskrevet i avsnitt 17.2.2 nedenfor.

17.1.2 Cyber Kill Chain – en modell for APT-angrep

En *cyber kill chain* beskriver trinnene i et typisk cyberangrep fra en APT, som faktisk kan gå over flere år. Begrepet «kill» (eng. å drepe) refererer til det faktum at denne typen angrep kan bli «drept» (stoppet) på ethvert trinn i kjeden – jo tidligere, desto bedre, naturligvis. Hvis angriperen ikke er i stand til å utføre tilstrekkelig rekognosering for å identifisere en organisasjon som et angrepsmål eller finne ut hvordan organisasjonen kan angripes, vil denne organisasjonen i utgangspunktet heller ikke bli angrepet. Figur 17.1 viser trinnene i CKC (Cyber Kill Chain), med omtrentlig tid det tar for gjennomføring av hvert trinn.

CKC er en nyttig hjelp for analyse av et angrep fra en APT. Alle stegene er i teorien mulige å detektere, men de to første er nok de vanskeligste. Et slikt APT-angrep er målrettet, som betyr at det starter med rekognosering mot spesifikke utpekte virksomheter, som senere blir angrepet med eksempelvis spydphishing og skadevare. Å kunne danne et fullstendig bilde av aktørens handlinger i de ulike fasene av et målrettet angrep er svært viktig for å kunne gjøre en trygg utkastelse og gjøre tiltak for å motstå nye angrep. Trinnene i CKC er følgende:

1. *Rekognosering* (Reconnaissance): Trusselaktøren samler informasjon om det potensielle offeret, for å finne sårbarheter og muligheter for angrep. OSINT er ofte brukt for rekognosering (se avsnitt 17.3.2)
2. *Bevæpning* (Weaponization): Trusselaktøren konstruerer exploit-skadevare basert på f.eks. «zero days», pakket i et egnet format som kan leveres til offeret. Formatet kan være et PDF-dokument eller en mediefil. Dette er vanligvis trinnet hvor angriperens første interaksjon med offeret kan observeres i offerets infrastruktur, og hvor deteksjonsmulighetene vil øke.



Figur 17.1. Trinnene i «cyber kill chain», med tilhørende tidsskala.

3. *Overlevering* (Delivery): Skadevaren kan f.eks. sendes som vedlegg med en phishing-e-post (villedende) som har til hensikt å lure mottageren til å åpne vedlegget eller å installere skadevaren.
4. *Utførelse av exploit*: Ved å anta at mottageren er blitt lurt til å åpne/installere skadevaren, vil exploiten starte å utføre skade.
5. *Installering* (Installation): Den direkte effekten av exploiten er vanligvis å laste ned en bakdør i form av et C&C-program fra en ekstern server. Etter dette trinnet har angriperne ekstern tilgang til det infiserte systemet.
6. *Kommando og kontroll* (K2) (Command & Control): Angriperne kan utforske nettverket rundt det infiserte systemet, forplante seg videre til andre systemer, skjule spor og identifisere ressurser som kan stjeles eller saboteres.
7. *Måloppnåelse* (Objectives): Data samles inn, klargjøres og sendes ut av nettverket til servere som kontrolleres av angriperne. Hvis sabotasje er angriperens mål, blir det iverksatt ødeleggende aksjoner.

Et viktig ledd i å forebygge målrettede cyberangrep som følger mønsteret til CKC, er gjennom digital trusseletterretning, som beskrives i neste avsnitt.

17.2 CTI: Digital trusseletterretning

Digital trusseletterretning, også kalt CTI (Cyber Threat Intelligence), er trusseletterretning innen cybersikkerhet. Nedenfor er en definisjon på trusseletterretning⁷⁷ som ofte brukes.

Trusseletterretning er faktabasert kunnskap, inkludert kontekst, mekanismer, indikatorer, resonnementer og råd, som har praktisk nytte i forbindelse med en eksisterende eller

77 <https://www.gartner.com/en/documents/2487216>.

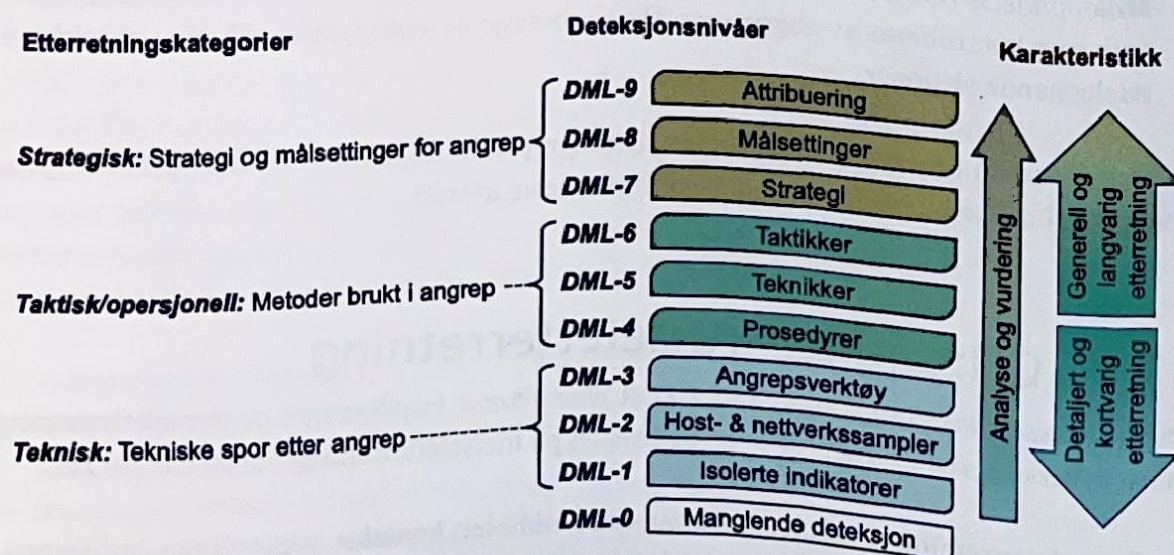
fremvoksende trussel mot verdier, og som kan brukes til å ta beslutninger og gjennomføre operasjoner mot trusselen eller faren.

Betydningen av at CTI er «faktabasert kunnskap», er at CTI må være pålitelig og troverdig for å danne grunnlag for beslutninger og handlinger. Det er viktig at denne typen kunnskap faktisk har «praktisk nytte» for å identifisere og beskytte virksomheten mot reelle trusler, noe som betyr at kunnskapen må være relevant, presis og tilstrekkelig fersk.

Nytten av CTI er basert på at informasjon om trusselaktører og cyberangrep kan produseres og deles mellom samarbeidende entiteter, og at denne informasjonen lett kan analyseres og integreres i prosesser og sikkerhetsløsninger hos hver entitet. Gjennom deling og berikelse av detaljer og kontekst av CTI vil samarbeidende entiteter forstå trussellandskapet mye klarere og raskere enn om hver hadde jobbet alene. Uten en klar og til enhver tid oppdatert forståelse av trussellandskapet ville entiteter ofte måtte gjøre gjetninger og antagelser i stedet for å kunne ta faktabaserte beslutninger om forsvar mot cybertrusler og håndtering av hendelser.

17.2.1 Kategorier og nivåer av digital trusseletterretning

CTI kan deles opp i forskjellige kategorier, der figur 17.2 illustrerer en vanlig modell med de tre hierarkiske kategoriene *strategisk*, *taktisk/operasjonell* og *teknisk CTI*. Samtidig viser figuren at de tre etterretningskategoriene representerer ulike nivåer av hva virksomheten klarer å detektere, som er beskrevet i DML-modellen (Detection Maturity Level) til Stillions.⁷⁸ DML-modellen sier at det er relativt enkelt å detektere tekniske spor som IP-adresser, domener og filnavn på skadevare, fordi det kan leses direkte ut av loggene, det vil si at det kun krever lav modenhet i hendelsesrespons og digital trusseletterretning. Det kreves større modenhet av en virksomhet å kunne detektere hvilke taktikker, teknikker og prosedyrer en trusselaktør har benyttet i et angrep, fordi disse aspektene kan ikke leses direkte ut av loggene. Det kreves enda større modenhet for å kunne tilskrive angrep til en spesifikk gruppering.



Figur 17.2. Kategorier av CTI.

- **Strategisk CTI:** Dette er generell informasjon om en trusselaktør/APT eller om en type trussel. Strategisk CTI produseres over en viss tid ved å sammenstille og analysere mange ulike informasjonselementer fra forskjellige kilder. Fokuset for strategisk CTI er å kunne beskrive en trusselaktør/APT basert på observerte aktiviteter og annen etterretning, samt å forstå overordnede målsettinger og strategier hos trusselaktøren. *Attribusjon* betyr at en CTI-entitet er i stand til å identifisere hvilken gruppering som står bak et angrep. Strategisk CTI er viktig for bedre å posisjonere og prioritere ressurser i forsvar mot truslene, og for å kunne gjøre langsiktig planlegging. I tillegg kan strategisk CTI danne grunnlag for politisk reaksjon på cyberangrep. Det skjer regelmessig at regjeringen i en stat som er blitt angrepet, går ut offentlig for å tilskrive angrepet til en spesifikk APT/stat. Dette skjedde blant annet da regjeringen beskyldte Russland for å stå bak et angrep mot Stortinget i 2020.⁷⁹
- **Taktisk/operasjonell CTI:** Dette er spesifikk informasjon om *taktikker, teknikker og prosedyrer* (TTP-er) som brukes av en trusselaktør i et angrep. En taktikk er en operasjonell målsetting, som f.eks. å få initiell tilgang til et system. En teknikk er en metode som benyttes for å oppnå den taktiske målsettingen. En prosedyre er en *angrepsoppskrift* som består av et sett og sekvens med teknikker som trusselaktøren benytter for å nå den taktiske målsettingen. En trusselaktør har som regel et utvalg av TTP-er som de mestrer og er vant til å bruke. Å utveksle taktisk/operasjonell CTI mellom entiteter blir mer og mer vanlig og er ansett som viktig for å styrke forsvaret mot cybertrusler. MITRE ATT&CK, som beskrives i neste avsnitt, er en katalog over ulike TTP-er som er observert og som brukes i virkelige cyberangrep. Taktisk/operasjonell CTI kan være spesifikk for en organisasjon eller en sektor. Ettersom angripere ofte gjennomfører kampanjer mot en spesifikk sektor, kan entiteter innen samme sektor ha stor fordel av å utveksle CTI om kampanjer som kan brukes til å advare hverandre om et sannsynlig forestående angrep. SRM (sektorvis responsmiljøer) (beskrevet i avsnitt 16.7) har nettopp som del av sin rolle å koordinere utveksling av operasjonell CTI innen en sektor.
- **Teknisk CTI:** Denne typen CTI består av tekniske indikatorer (eng.: indicators of compromise) om angrep og infisering, som typisk samles inn gjennom monitorering og logging av aktiviteter i systemer og nettverk. Angrepsindikatorer består f.eks. av IP-adresser, domenenavn, signaturer (hash-verdier) av observert skadevare samt observert bruk av spesifikke verktøy. Det er svært vanlig å utveksle teknisk CTI mellom samarbeidende entiteter. Teknisk CTI kalles noen ganger «taktisk CTI», noe som er ulogisk fordi CTI om TTP-er hører til operasjonell CTI.

Det samles inn store mengder data av teknisk natur, som logger fra systemer, nettverk og brannmurer eller alarmer fra IDS (Intrusion Detection System). Figur 17.2 viser at tekniske CTI-data kan brukes i analyse og berikelse for å produsere operasjonell og strategisk CTI.

Når en spesifikk type angrep observeres og blir kjent, iverksettes det typisk tiltak for å stoppe denne typen angrep. Det betyr at trusselaktører hele tiden er tvunget til å endre angrepsmetode for å lykkes med sine angrep. Visse ting kan lett endres, mens andre ting krever mer arbeid og omstilling, noe som indikerer hvorvidt relatert CTI er kortvarig eller langvarig, det vil si om den har kort eller lang gyldighet.

79 https://www.nrk.no/norge/stortinget-ikke-alene_-massivt-hackerangrep-mot-norge-1.15277734.

Modellen i figur 17.2 illustrerer at teknisk CTI er *detaljert*. Det er fordi IP-adresser, domenenavn og signaturer kan beskrives på en presis måte. CTI om TTP-er er litt mer generell, fordi det er utfordrende å lage en presis beskrivelse av en TTP.

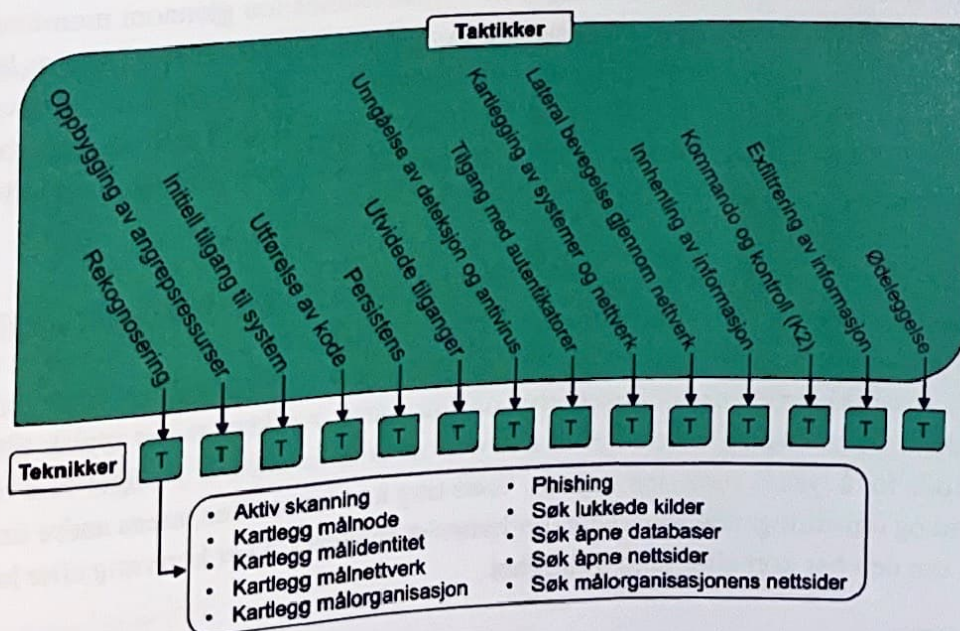
Figuren illustrerer også at strategisk CTI er *generell*. Dette må forstås på den måten at denne typen CTI ikke direkte kan brukes til å lage regler i en brannmur eller en IDS for å stanse en viss type angrep. Verdien av denne typen CTI ligger i å kunne være generelt bedre forberedt på angrep fra visse grupperinger og kunne tilpasse beredskapsnivået deretter.

Modellen i figur 17.2 illustrerer at teknisk CTI er *kortvarig*. Dette er fordi en trusselaktør relativt enkelt kan endre IP-adresser, domenenavn og skadevare. Da denne typen CTI er kortvarig, har den også begrenset verdi over tid. Det er relativt enkelt å innhente denne typen CTI, men samtidig har den en begrenset holdbarhet som ligger relativt kort frem i tid.

Figuren illustrerer også at taktisk/operasjonell og strategisk CTI er mer *langvarig*. Dette er fordi en trusselaktør eller APT ikke enkelt kan endre på sine TTP-er, da det tar tid å etablere ekspertise og å utvikle verktøy for å utføre visse typer angrep. Trusselaktører kan enda mindre endre på «hva den er», eller hvilke overordnede målsettinger den har. Det er relativt utfordrende å produsere denne typen CTI, men fordi den er langvarig, kan den ha stor verdi over relativt lang tid.

17.2.2 MITRE ATT&CK

MITRE ATT&CK er et rammeverk og en kunnskapsbase over TTP-er (taktikker, teknikker og prosedyrer) som trusselaktører bruker gjennom livssyklusen til cyberangrep. Rammeverket er ment å være et verktøy for å forstå hvordan trusselaktører opererer, for dermed å styrke virksomhetens beredskap mot cyberangrep. Som beskrevet ovenfor er en taktikk en operasjonell målsetting, som kan være å utføre rekognosering. For hver taktikk kan en trusselaktør velge å utføre et sett med teknikker, der figur 17.3 viser at taktikken *rekognosering* omfatter 10 forskjellige teknikker. Den generelle MITRE ATT&CK-kunnskapsbasen beskriver 14 taktikker, der hver taktikk omfatter et større eller mindre antall teknikker.



Figur 17.3. MITRE ATT&CK.

MITRE ATT&CK beskriver ulike typer cyberangrep fra trusselaktørens perspektiv. Ved å detektere en sekvens med bestemte angrepsteknikker i egne systemer og nettverk kan virksomheten avlede hvilken taktisk målsetting trusselaktøren har. Dette er svært nyttig for at virksomheter skal kunne være forberedt på å stoppe de neste trinn som trusselaktøren planlegger som del av angrepsprosedyren.

MITRE vedlikeholder og oppdaterer ATT&CK-kunnskapsbasen kontinuerlig ved å inkludere angrepstaktikker og teknikker fra offentlig tilgjengelig trussetetterretning og rapportering av cyberangrep, samt fra forskning på nye angrepsteknikker.

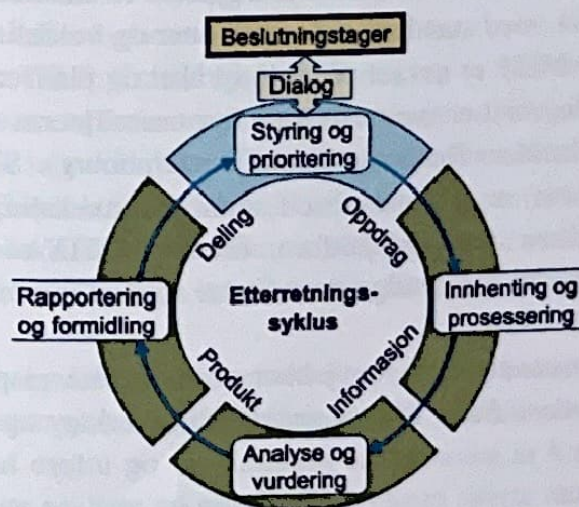
MITRE er en ideell organisasjon opprettet for å gi teknisk veiledning til myndighetene i USA, men gir også verdifull støtte til private virksomheter. Organisasjonen utviklet opprinnelig rammeverket for bruk i et MITRE-forskningsprosjekt i 2013 og ble oppkalt etter dataene den samler inn, som er Adversarial Tactics, Techniques & Common Knowledge – eller, i akronymform, ATT&CK. I dag brukes MITRE ATT&CK av organisasjoner i hele verden som del av cyberberedskap og trussetetterretning.

Under en parallell aktivitet vedlikeholder MITRE en oversikt over ulike trusselgrupperinger, såkalte APT-er (Advanced Persistent Threats). Per 2023 har MITRE informasjon om 129 APT-er, som blant annet er beskrevet med hvilke TTP-er i ATT&CK-matrisen de er observert å bruke. Når en type TTP som er typisk for en ATP, observeres under et angrep, kan det bidra til attribuering av angrepet til nettopp den ATP-en. I tillegg til ATT&CK-kunnskapsbase og kartlegging av ATP-er, driver MITRE flere tilhørende prosjekter som blant annet brukes som basis for trusselmodellering.

Merk at MITRE ATT&CK og kartlegging av ATP-er har et amerikansk/vestlig perspektiv, slik at det ikke beskriver det amerikanske NSA, som nettopp er svært aktiv innenfor offensive cyberoperasjoner. Mange virksomheter kunne ønske en nøytral (politikk-agnostisk) kartlegging av TTP-er og ATP-er, ettersom de i utgangspunktet ikke kan vite hvilken gruppering som står bak angrep eller spionering mot egne systemer.

17.2.3 Syklus for CTI

Etterretningssyklus er en modell som opprinnelig ble definert i sammenheng med militær etterretning, men grunnprinsippene gjelder også for CTI. Hovedfasene i en CTI-syklus er illustrert i figur 17.4.



Figur 17.4. Syklus for CTI.

Fasene av CTI-syklusen i figur 17.4 er beskrevet nedenfor.

- **Styring og prioritering:** Trusler kan bli vurdert fra ulike perspektiver avhengig av om det er en virksomhet, en sektor eller en hel stat. Hvilke verdier som er viktig å beskytte, avhenger også av perspektivet. Denne fasen definerer fokus for arbeidet med CTI med henblikk på å kartlegge generelle trusselkategorier og antatte trusselaktører som er relevante, samt hvilke verdier de typisk er ute etter å skade.
- **Innhenting og prosessering:** Det fins mange ulike kilder for innsamling av data for CTI. Kilder kan f.eks. være manuelle eller automatiserte, og de kan komme fra egen organisasjon eller fra eksterne kilder. Det må implementeres prosesser for effektiv innsamling og lagring av data for CTI. Data som er innsamlet, må kvalitetssikres før de kan danne grunnlag for analyse. Det er tre hovedhensyn å ta: (i) kildens pålitelig, (ii) om dataene er relevante for virksomhetens formål og (iii) om dataene har tilstrekkelig kvalitet. Data av dårlig kvalitet eller som er upålitelige eller irrelevante, kan forkastes. Å rense dataene gjør analysen lettere fordi det fjerner støy og reduserer arbeidsmengden. Etter som det samles inn større og større mengder data, blir CTI etter hvert «big data», og må prosesseres deretter.
- **Analyse og vurdering:** Analyse av innsamlede data er nødvendig for å gjøre CTI til et produkt som er nyttig for både egen virksomhet og eksterne parter. Berikelse består av å identifisere semantiske sammenhenger mellom data av ulike typer og fra ulike kilder. Berikelse av data har stort potensial for å se sammenhenger mellom indikatorer og gir dermed større situasjonsforståelse. Analysen og vurderingen kan produsere informasjon om generelle trusler, trusler mot en sektor, mot spesifikke applikasjoner eller informasjon om nært forestående eller pågående angrep. Analyse kan gjøres med AI (kunstig intelligens) eller logisk-semantiske teknologier.
- **Rapportering og formidling:** Det er enklere sagt enn gjort å si at CTI skal deles mellom de ulike entitetene nevnt over. Tradisjonelt artikuleres CTI som vanlig tekst, og deles som pdf-dokumenter med andre entiteter. Denne måten å dele CTI på er opplagt ineffektiv, og den skalerer dårlig i forhold til den raske økningen i både antall og hastighet av cyberangrep. Den eneste måten å oppnå tilstrekkelig skalerbarhet og hastighet på er ved automatisert deling basert på maskinlesbar CTI. For å gjøre CTI maskinlesbar må den uttrykkes i et formelt språk, dvs. med standardiserte attributter og veldefinert semantikk. Det fins flere slike språk, der MISP er navnet på både språket og plattformen for digital trussel. STIX (Structured Threat Information eXpression) er et standardisert språk for utveksling av trusselinformasjon (Computer Incident Response Center Luxembourg). STIX er standardisert, kan ulike verktøy og plattformer fra forskjellige produsenter snakke sammen og utveksle CTI.

CTI kan brukes manuelt av analytikere som jobber med hendelsesrespons eller av *SIEM-verktøy* (*Security Information and Event Management*). Slike verktøy og produkter kan integrere CTI for helt eller delvis å ta automatiske beslutninger og utføre handlinger. Automatisert deling og bruk av CTI kan styrke evnen til deteksjon og analyse av angrep før og mens de inntreffer, noe som dermed reduserer sannsynligheten for at det resulterer i en hendelse med

skade. Som nevnt tidligere er det begrenset i hvilken grad SIEM-verktøy er i stand til å prosessere operasjonell og strategisk CTI i henhold til figur 17.2.

CTI kan klargjøres for ulikt publikum. Ren teknisk, operasjonell og strategisk CTI benyttes oftest for hendelseshåndtering og for deling med andre entiteter, men en type CTI kan også lages for ledelse og beslutningstagere for vurdering av prioritering av håndtering, innføring av sikkerhetstiltak m.m.

17.2.4 Deling av CTI

NCSC og SRM-er (beskrevet i avsnitt 16.7) spiller en viktig rolle ikke bare for hendelsesrespons innenfor sine sektorer, men også for å samle inn, produsere, analysere og dele CTI. De deler CTI seg imellom, med virksomheter innenfor sine respektive sektorer og med entiteter i andre land. Det fins også en rekke kommersielle tilbydere av sikkerhetstjenester, som beskrevet i avsnitt 16.5. Dette kan være tilbydere av SOC- eller CSIRT-tjenester. I tillegg til å drive hendelsesrespons er disse entitetene også aktive med innsamling, produksjon, analyse og utveksling av CTI.

ISAC (Information Sharing and Analysis Centre) er betegnelsen på en entitet som hovedsakelig fokuserer på innsamling, produksjon, analyse og deling av CTI. På europeisk nivå er det blitt opprettet ulike ISAC-er innen spesifikke sektorer, som f.eks. EE-ISAC⁸⁰ innen energisektoren. Etablering av ISAC-er er et område i dynamisk utvikling innen EU, ettersom EU satser på *digital suverenitet*, det vil si at Europa skal være uavhengig av andre stater, særlig USA, med hensyn til digital teknologi og økonomi. Cybersikkerhet er en hjørnestein i denne strategien, og med det følger opprettelsen av europeiske ISAC-er. Samtidig kan det nevnes at USA har lengre erfaring med etablering av ISAC-er enn EU. Den ISAC-en som kanskje flest innen sikkerhetsmiljøet har hørt om, er FS-ISAC (Financial Services ISAC).⁸¹

Kilder til CTI kan være gratis eller betalte, noe som ikke alltid betyr åpne eller lukkede. For å få tilgang til CTI er en entitet prisgitt kunnskap om åpne kilder, penger til å betale for lukkede kilder og rolle/posisjon for å få lov til å delta i gratis, men samtidig lukkede fora/kilder til CTI. For en analytiker er forståelse av CTI-landskapet viktig for å kunne vite hvilken CTI det er praktisk mulig å få tak i. *Frikildeetterretning* (OSINT: Open Source Intelligence) er en type etterretning der informasjon samles inn fra kilder som er tilgjengelige for offentligheten. Dette står i kontrast til skjult etterretning, der informasjon hentes fra kilder som ikke er tilgjengelige for offentligheten.

Trafikklysprotokollen (TLP: Traffic Light Protocol) er en merking av CTI som indikerer hvor bredt avsender ønsker at informasjonen kan sirkuleres ut over den nærmeste mottageren. Det er viktig at alle som håndterer TLP-merket kommunikasjon, forstår og overholder reglene i protokollen. Først da kan tillit etableres og fordelene med informasjonsdeling realiseres. Mottageren må konsultere kilden til informasjonen hvis det er behov for bredere formidling. De fire nivåene i TLP-protokollen er beskrevet nedenfor.

- **RØD (RED):** *personlig, kun for navngitte mottagere.* Under møter mellom fagfolk er for eksempel RØD informasjon begrenset til de som er til stede på møtet. Distribusjonen av

80 <https://www.ee-isac.eu/>.

81 <https://www.fsisac.com/>.

RØD informasjon vil vanligvis foregå via en definert liste, og under ekstreme omstendigheter kan den bare sendes muntlig eller personlig.

- **GUL (AMBER): begrenset distribusjon.** Mottageren kan dele AMBER-informasjon med andre i organisasjonen, men bare på «behov-for-å-vite»-basis (eng.: need-to-know). Avsenderen kan spesifisere de tiltenkte mottagerne på en detaljert måte.
- **GRØNN (GREEN): innen miljøet.** Informasjon i denne kategorien kan sirkuleres bredt innenfor et bestemt miljø. Imidlertid kan ikke informasjonen publiseres eller legges ut offentlig på internett, og kan heller ikke videresendes utenfor miljøet.
- **HVIT (WHITE): ubegrenset.** I henhold til standard praksis kan HVIT informasjon distribueres fritt, uten begrensning.

I praksis vil man indikere et dokumentets klassifisering med forkortelsen «TLP», etterfulgt av et kolon og klassifikasjonsnivå, for eksempel «TLP: RED».

Proessen for hendelsesrespons (beskrevet i avsnitt 16.5) har stor nytte av CTI for lettere å kunne analysere hva som har skjedd i forbindelse med en sikkerhetshendelse, og for å kunne ta raskere og bedre beslutninger om hvilke handlinger som bør foretas som del av hendeshåndteringen.

17.2.5 Representasjon og bruk av CTI

Det er utfordrende å beskrive TTP-er enhetlig, selv med MITRE ATT&CK. Det betyr at to CTI-spesialister typisk vil beskrive samme angrep på litt ulike måter. Dermed er det vanskelig å sammenligne og analysere forekomster av samme TTP fra ulike CTI-kilder med automatiserte verktøy. Ettersom like aspekter ved en TTP kan beskrives på ulike måter, vil vi ikke kunne identifisere og analysere likheter i tilstrekkelig grad, noe som gjør det vanskelig å oppnå automatisk utveksling og prosessering av denne type CTI. Å beskrive operasjonell CTI i form av TTP-er betyr å beskrive generell oppførsel i motsetning til rent tekniske aspekter. Som analogi kan operasjonell CTI for kontroll av smugling være en beskrivelse som sier følgende: «*De kjører først en liten bil over grensen, så en stor bil over grensen, deretter stopper begge bilene på en rasteplass, møter en tredje bil og bytter sjåfører.*» Dette står i kontrast til teknisk CTI, som sier følgende: «*Dette registreringsnummeret ble brukt av smuglerne forrige gang.*» Over tid er det relativt vanskelig for smuglere å unngå å bli oppdaget basert på operasjonell CTI, fordi de må endre rutiner, mens en bil med et registreringsnummer lett kan skiftes ut.

For å kunne innføre tiltak mot et spesifikt angrep er det samtidig en fordel å ha detaljert teknisk informasjon. Det gjør en forsvarer i stand til å blokkere spesifikke IP-adresser eller lage signaturer som kan identifisere og stoppe trinn i utførelsen av et angrep.

17.3 Sikkerhetstesting av systemer, nettverk og virksomheter

Den beste måten å finne ut om en virksomhet har tilstrekkelig robust beskyttelse mot angrep på, er å utsette virksomheten for simulerte angrep. Slike angrep kan være cyberangrep eller angrep på fysiske bygninger eller andre sikkerhetsbarrierer. Det fins flere ulike metoder, noen av dem er beskrevet i avsnittene nedenfor.

17.3.1 Pentesting

En penetrasjonstest, vanligvis bare kalt inntrengningstest, pentest eller etisk hacking, er et simulert angrep mot en virksomhet, autorisert av virksomheten og utført for å evaluere sikkerheten til virksomhetens nettverk og øvrige sikkerhetssystemer. Vanligvis er systemeier og IT-drift informert om at pentesten gjennomføres. Som første trinn i pentesting gjøres vanligvis en kartlegging av virksomhetens systemer gjennom eksponerte grensesnitt. Etter dette vil man ofte gjennomføre en sårbarhetsskanning av virksomhetens systemer. Sårbarhetsskanning kan gjennomføres manuelt, eller ved hjelp av delvis automatiserte programmer som kan identifisere om en server er sårbar og potensielt kan utnyttes i et angrep. Sårbarheten kan for eksempel være at serveren mangler sikkerhetsoppdateringer, eller benytter utdatert operativsystem eller annen programvare.

Neste trinn i pentesting er nettopp å utnytte identifiserte sårbarheter for å utforske potensialet for uautorisert tilgang til systemets funksjoner og data. I dette trinnet legges det en plan for hvilke sårbarheter som skal angripes, og det kan defineres en målsetting for angrepet. Målsettingen kan for eksempel være å få uautorisert tilgang til informasjonen som måtte være på systemet (altså et angrep på KIT-begrepet konfidensialitet). Planen inneholder risikovurdering av sårbarhetenes potensielle angrepsflate, målt opp mot alvorligheten av konsekvenser og driftsproblemer som angrepet kan medføre i den aktuelle tjenesten/serveren.

Det er vanlig å definere pentest som white-box-testing eller black-box-testing, avhengig av hvor mye informasjon pentesterne får utlevert. White-box-testing betyr at pentesterne på forhånd mottar all relevant informasjon om systemene som skal testes, som kan være fullstendige nettverkstegninger. Black-box-testing betyr at pentesterne ikke har tilgjengelig noen beskrivelse av nettverk og systemer, slik at de selv må utforske dette så langt det lar seg gjøre. Både white- og black-box-testing vil uansett normalt inneholde en prosess med å undersøke systemet, da nettverkstegninger og annen dokumentasjon ofte viser seg å være utdaterte. Svakheter som pentesten avdekker, skal rapporteres til systemeieren. Rapporter kan også vurdere potensielle konsekvenser for organisasjonen og foreslå mottiltak for å redusere risikoen.

17.3.2 Red-teaming og blue-teaming

En person, eller en gruppe personer, som utfører pentesting mot et mål, kalles et *red-team*. På den annen side er *blue-team* gruppen, med personer i virksomheten som har rollen å forsvare mot angrep og stoppe red-team. I praksis består blue-team av de som vanligvis håndterer sikkerhetshendelser i en virksomhet. På samme måte som for pentesting må virksomheten autorisere simulerte angrep fra red-team før testen starter. Forskjellen på pentesting og red-teaming er at ved red-teaming er blue team ikke informert om at det kommer simulerte

angrep. På den måten vil red-teaming teste virksomhetens cyberberedskap, i tillegg til å teste teknisk, prosessuell og menneskelig sikkerhet i virksomheten. Ettersom blue-team ikke er informert om testen på forhånd, er *white-team* nettopp de i virksomheten som er informert om at den vil bli utsatt for simulerte cyberangrep. Red-teaming er mer realistiske enn bare pentesting, nettopp fordi IT-drift og blue-team ikke er informert på forhånd. Ulempen med red-teaming er at red-teams behov for å ikke bli oppdaget gjør at red-teaming typisk avdekker færre sårbarheter enn pentesting. Hvis man antar at et system inneholder 100 sårbarheter som kan utnyttes i et cyberangrep, vil et red-team normalt bare søke å finne én vei, mens en pentester ønsker å finne alle 100.

På samme måte som med pentesting vil red-team benytte sårbarhetskartlegging for å vurdere mulige angrepsmetoder. I tillegg kan både red-team og pentestere foreta innledende rekognosering, som betyr å samle all mulig relevant informasjon om angrepsmålet. Rekognosering er 1. trinn i CKC (Cyber Kill Chain) som beskrevet i avsnitt 17.1.2.

OSINT (Open Source Intelligence), ofte kalt frikildeetterretning eller åpen kildeetterretning, er typisk en del av rekognosering. OSINT brukes typisk av trusselaktører for å identifisere mål, for å finne ut hvordan mål kan angripes, og for å bli brukt som en del av et angrep. For å hindre eller vanskeliggjøre 1. trinn i CKC bør virksomheter og enkeltpersoner vurdere å begrense eller redusere mengden informasjon som kan produseres med OSINT, for eksempel ved å begrense informasjon som legges ut på nettsider og sosiale nettverk. Det fins automatiserte verktøy for OSINT, bl.a. SHODAN⁸² for å finne IoT-enheter, Maltego⁸³ for kartlegging og visualisering av data fra åpne kilder, og The Harvester, som er et verktøy som benyttes for å samle e-postadresser og domenenavn relatert til et (angreps)mål. Verdens største søkemotor Google er også et utmerket OSINT-verktøy, der begrepet *Google-hacking* betyr å benytte Google for OSINT. En fysisk form for OSINT er søppeldykking, som består av å lete etter papirdokumenter fra en virksomhet eller privatperson i søppelkasse og søppelkonteinere. Tiltak mot søppeldykking er sikker makulering.

En variant av red-teaming og blue-teaming er å øve på cyberangrep og -forsvar i en *cyber range*, som er en syntetisk IT-omgivelse med nettverk, servere og applikasjoner. Red-team forsøker å trenge inn i nettverket, og ta ned servere og applikasjoner, mens blue-team forsøker å detektere red-teams aktiviteter, kaste dem ut og holde servere og applikasjoner i drift. Fordelen med cyber range er at det ikke berører ekte forretningsapplikasjoner i en virksomhet. Imidlertid er det ikke en sikkerhetstest, det er bare en øvelse i cyberoperasjoner.

17.3.3 TIBER

TIBER (Threat Intelligence-Based Ethical Red-Teaming) er den mest avanserte formen for pentesting. TIBER-EU er et rammeverk utviklet av Den europeiske sentralbanken (ECB) for å teste finansinstitusjoners evne til å oppdage og forsvare seg mot avanserte cyberangrep. TIBER-NO er den norske implementeringen av TIBER-EU, og praktiseres i utgangspunktet innen finanssektoren. Etter hvert blir TIBER også benyttet i andre sektorer.

I tillegg til å være en form for red-teaming som beskrevet i forrige avsnitt, er det spesielle med TIBER-testing at det også benytter målrettet trusseletterretning som beskrevet i avsnitt

82 <https://www.shodan.io/>.

83 <https://www.maltego.com/>.

17.2, for at red-team skal kunne etterligne reelle APT-er på en mest mulig realistisk måte. Ettersom TIBER er en svært omfattende metode for sikkerhetstesting, er det også svært dyrt å gjennomføre. Virksomheter må vurdere om nytten ved TIBER veier opp for kostnaden. TIBER er et relativt nytt rammeverk, der virksomheter foreløpig ikke har like mye erfaring som med pentesting og red-teaming.

17.4 Cyberkrigføring

Begrepet *cyberkrigføring* er et relativt upresist begrep med varierende betydninger. Nedenfor er en enkel definisjon som brukes i denne boken:

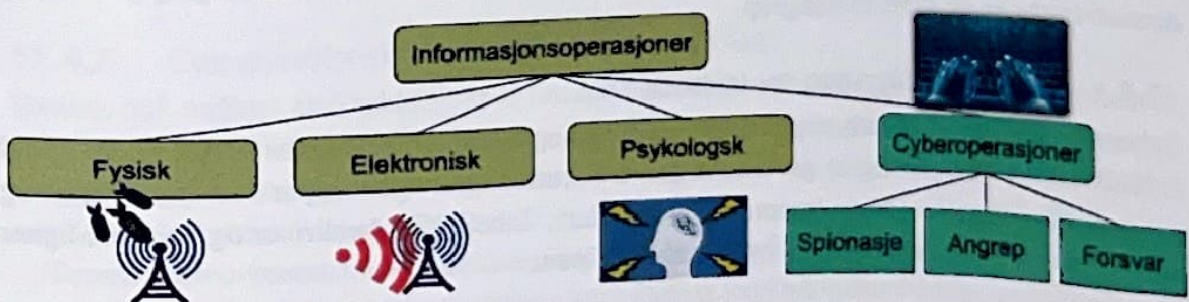
«Cyberkrigføring er alle former for cyberoperasjoner mellom stater for å utføre sabotasje og spionasje, og forsvar mot disse.»

Cyberoperasjoner er en underkategori av *informasjonsoperasjoner* (NATO-begrep), også kalt *informasjonskrigføring* (amerikansk begrep).

Informasjonsoperasjoner består blant annet av fysisk bombing av kommunikasjonsinfrastruktur, elektronisk jamming av radiokommunikasjon, påvirkningsoperasjoner (PsyOps: psykologiske operasjoner) som f.eks. propaganda, og sist, men ikke minst, *cyberoperasjoner* (NATO-begrep: Computer Network Operations; amerikansk begrep: Cyber Operations). Kategorien cyberoperasjoner består igjen av følgende tre underkategorier:

- *Cyberspionasje* (NATO-begrep: CNE, Computer Network Espionage)
- *Cyberangrep* (NATO-begrep: CNA, Computer Network Attack), også kalt *cybersabotasje*
- *Cyberforsvar* (NATO-begrep: CND, Computer Network Defense)

Sammenhengen mellom disse begrepene er vist i figur 17.5.



Figur 17.5. Informasjonsoperasjoner og underkategorier.

De fleste land, og særlig de industrialiserte land, praktiserer alle tre typer cyberoperasjoner. Av disse tre er cyberspionasje det mest nyttige og potente. Sammenlignet med å sende en

person til et fremmed land for å utføre spionasje, med alle kostnadene og risikoer det medfører, er cyberspionasje billig og effektivt.

Å ha et godt forsvar mot cyberangrep med defensive cyberoperasjoner er naturligvis helt essensielt for stater. I kontrast til tradisjonelt militært forsvar der forsvarssektoren har hovedansvaret i tilfelle krig, er alle sektorer i prinsippet involvert i cyberforsvar og har en rolle i defensive cyberoperasjoner, som forklart i avsnitt 16.7.

At et land praktiserer offensive cyberoperasjoner i fredstid, kan være kontroversielt, og svært få land snakker åpent om det. Et unntak er USA, som har en offisiell politikk rundt offensive cyberoperasjoner, med en separat forsvarsavdeling kalt *US Cyber Command*. Det hvite hus sender regelmessig ut pressemeldinger om at presidenten har beordret Cyber Command til å utføre offensive cyberoperasjoner, f.eks. i 2016 for å utføre cyberangrep mot IS,⁸⁴ og i 2019 for å installere bakdører i den russiske kraftsektoren.⁸⁵ Sistnevnte ble opplagt utført som cyberavskrekking, som beskrevet i avsnitt 17.4.2.

Offensive cyberoperasjoner har isolert sett en begrenset effekt fordi virksomheter etter hvert får bedre cyberberedskap slik at de relativt raskt får kastet ut trusselaktøren og gjenopprettet systemer og prosesser etter skaden. Man antar at offensive cyberoperasjoner har sitt største potensial i kombinasjon med tradisjonelle militære angrep. Hvis offensive cyberoperasjoner kan lamme IT-systemer hos fienden i en kort periode, samtidig som det gjennomføres tradisjonelle angrep, kan fienden miste evnen til å koordinere sitt forsvar akkurat når det gjelder. På den måten kan offensive cyberoperasjoner forsterke effekten av tradisjonelle militæroperasjoner. Dette var opplagt hensikten med russiske cyberangrep mot Ukraina i den innledende fasen av invasjonen 24. februar 2022. Imidlertid uteble effekten av disse cyberangrepene fordi Ukraina hadde relativt god cyberberedskap, og i tillegg fikk hjelp fra blant annet Microsoft, for å eliminere skadevare ved raskt å fjerne sårbarheter, som beskrevet i avsnitt 17.4.3.

Etter den russiske invasjonen i Ukraina 24. februar 2022 har Norge og andre vestlige land merket en nedgang i antall cyberangrep fra Russland. Mulige forklaringer på dette er for det første at russiske APT-aktører er opptatt med å angripe mål direkte relatert til Ukraina, og dermed ikke har tid til å angripe for eksempel Norge. En annen mulig forklaring er at Russland er redd for at cyberangrep mot et NATO-land skal utløse Artikkel 5 i NATO-traktaten, som sier at angrep på ett eller flere av medlemslandene skal betraktes som angrep på alle, og dermed trigge et militært motangrep.

17.4.1 Sammenligning av våpen

Cybervåpen består av de ulike typer skadevare og angrepsvektorer som er beskrevet i kapittel 2. Med tanke på krigføring er det interessant å sammenligne egenskaper ved cybervåpen og tradisjonelle kinetiske våpen (granater og missiler). Tabell 17.1 beskriver og sammenligner noen egenskaper ved cybervåpen og kinetiske våpen.

⁸⁴ ISIS Targeted by Cyberattacks in a New U.S. Line of Combat. New York Times, 24. april 2016.

⁸⁵ U.S. Escalates Online Attacks on Russia's Power Grid. New York Times, 15. juni 2019.

Tabell 17.1. Sammenligning av cybervåpen og kinetiske våpen

	Cybervåpen	Kinetiske våpen
Skadeeffekt	Forårsaker brudd på KIT i IT-systemer, og rammer prosesser som er avhengig av IT-systemene. Kan ramme langt flere aktører og sektorer enn angrepet var rettet mot. Kan forårsake indirekte fysisk skade på cyberfysiske systemer.	Kinetiske våpen forårsaker direkte ødeleggende fysisk skade på infrastruktur. Rammer bare området der våpenet treffer.
Gjenbruk	Kan gjenbrukes/gjenvinnes med <i>reversing</i> av skadevare, slik at den som først blir rammet, kan bruke cybervåpenet til å angripe andre.	Kinetisk ammunisjon blir ødelagt i angrepet, kan bare brukes én gang.
Åpenhet	Cybervåpen er immaterielle, og dermed lett å skjule. Cybervåpen holdes vanligvis skjult fordi åpenhet gjør det mulig å utvikle mottiltak som gjør våpenet ubrukelig.	Kinetiske våpen er ofte fysisk store, og dermed synlige, f.eks. fra satellitter. Åpenhet svekker ikke nødvendigvis våpenet.
Attribusjon	Det er ofte utfordrende å identifisere hvilken gruppe eller stat som står bak cyberangrep. Trusselaktøren kan etterlate villedende spor for å frustrere attribuering.	Det er vanligvis relativt lett å se hvor et kinetisk angrep kommer ifra, og dermed tilskrive til en aktør.
Holdbarhet	Cybervåpen er ofte basert på nulldagssårbarheter som har begrenset holdbarhet, ofte mindre enn ett år. Aktører trenger derfor kontinuerlig forsyning av nye cybervåpen, se nedenfor.	Kinetiske våpen har lang holdbarhet, typisk flere tiår. Store våpenarsenal kan lagres i lang tid.

Nulldagssårbarheter er hovedingrediensen i utvikling av cybervåpen som består av utnyttelseskode (eng. exploits), som nettopp utnytter sårbarheten. For å finne nulldagssårbarheter benytter mange aktører automatiserte verktøy og teknikker, som fuzzing (se avsnitt 11.3.5). Nulldagssårbarheter og tilhørende utnyttelseskode kjøpes og selges i lukkede markeder, der både statlige og private aktører deltar. Hvis vi antar at en statlig cyberaktør har fått tak i en svært potent nulldagssårbarhet med tilhørende utnyttelseskode, står myndighetene i landet overfor følgende avveining: På den ene side kan de beskytte landets IT-infrastruktur ved å rapportere sårbarheter til programvareprodusenten og MITRE CVE, som beskrevet i avsnitt 3.3, men på den andre siden kan de benytte nulldagssårbarheten og utnyttelseskoden til å spionere på fiender som truer landets IT-infrastruktur, som dermed vil bidra til å beskytte landets IT-infrastruktur.

17.4.2 Cyberavskrekking og cyberkaperfart

Teorien bak militær avskrekking er at det må baseres på utveksling av signaler om troverdig evne og hensikt til å gjengjelde angrep. Det forutsetter at partene kjenner hverandres vurderinger og prioriteringer, kjenner hverandres kapasiteter og politiske vilje til ødeleggelse, samt faktisk frykter ødeleggelse.

Terrorbalanse basert på avskrekking har til hensikt å forhindre krig ved å gjøre det meningsløst å føre krig. Det antas at avskrekking faktisk har forhindret bruk av atomvåpen etter andre verdenskrig.

Avskrekking har allerede spredt seg over til cyberrommet. Gjennom faktiske hendelser, blant annet sabotasje mot Ukraina i desember 2015, er det kjent at Russland har kompromittert kraftnett i vestlige land siden 2014. Rapporter om kompromittering og spionering indikerer at Russland aktivt kompromitterer kraftnett i USA.

Til gjengjeld har USA siden 2018 begynt å kompromittere kraftnett i Russland. Disse faktaene er ikke basert på etterretningsrapporter, men på pressemeldinger fra den amerikanske regjeringen.⁸⁶ Hensikten med slike pressemeldinger er åpenbar: Dette er cyberavskrekking. Logikken er at hvis Russland forsøker å sabotere amerikanske kraftnett, vil USA gjengjelde med å sabotere russiske kraftnett.

Selv om det fins likhetstrekk mellom atomavskrekking og cyberavskrekking, er det også fundamentale forskjeller. For det første er et cyberangrep langt mindre ødeleggende enn et atomangrep, som betyr at terskelen for å utføre et cyberangrep er mye lavere. For det andre blir cyberangrep ofte utført av ikke-statlige grupperinger, mens vi må anta at kun stater kan stå bak et mulig atomangrep.

Når en ikke-statlig gruppering utfører cyberangrep, er det essensielt for dem å vite om de kan bli rettslig forfulgt i landet der de er bosatt. I den sammenheng har Russlands president Putin uttalt at russiske grupperinger som utfører cyberangrep mot andre land, ikke anses å være kriminelle, «fordi de ikke bryter russisk lov».⁸⁷ Dette er i praksis en moderne form for kaperfart, som kan kalles *cyberkaperfart*.

Kaperfart i perioden 1600–1850 var sjørøveri drevet av private grupperinger med tillatelse fra landets myndigheter, og ble brukt som et virkemiddel i krigføring til sjøs. Målet for kaperfarten var å ta kontroll over fiendens handelsskip og føre dem og deres last til egen havn som *prise*. Piratene ble typisk belønnet med halvparten av verdien til prisen. Mens kaperfarten pågikk, hersket en slags balanse ved at alle land anerkjente denne virksomheten som legitim.

Cyberkaperfart, på den annen side, er asymmetrisk ved at visse stater, som f.eks. Russland, tillater private grupperinger å utføre cyberangrep mot andre land, mens stater i den vestlige verden typisk ikke gjør det. Ved å la private grupperinger angripe mål i andre land for profitt kan en stat oppnå en strategisk fordel i cyberkrigføring. I mai 2021 ble det amerikanske selskapet Colonial Pipeline utsatt for et cyberangrep med løsepengevirus som lammet bensinforsyningen i sørøstlige deler av USA. Etterforskningen pekte på at angrepet var utført av den russiske grupperingen DarkSide, som krevde 4,4 millioner dollar for å dekryptere dataene. Etter dette angrepet startet for alvor en diskusjon i USA (og i andre vestlige land) om gjengjeldelse.⁸⁸

Det ville bryte med rettsstatsprinsipper om vestlige land skulle tillate cyberkaperfart, det vil si å la private grupperinger angripe mål i andre land for profitt uten straffeforfølgelse i eget land. Å anerkjenne cyberkaperfart som et virkemiddel i internasjonale relasjoner ville mest sannsynlig destabilisere hele verdensøkonomien, og virker derfor temmelig utenkelig. Det logiske alternativet for vestlige land er at gjengjeldelse gjøres i form av statlige cyberoperasjoner. Imidlertid fins det faktorer som setter begrensninger for hvilke typer cyberoperasjoner som kan utføres. For eksempel er det antageligvis juridisk og etisk uakseptabelt for vestlige land at statlige cyberoperasjoner skal finansieres gjennom utpressing med løsepengevirus, noe som kan bety at utgiftene ved å utføre cyberoperasjoner belaster statsbudsjettene i vestlige land forholdsvis mer enn i Russland. Dette fordi private og statlige grupperinger

⁸⁶ <https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html>.

⁸⁷ <https://www.nytimes.com/2021/05/29/world/europe/ransomware-russia-darkside.html>.

⁸⁸ <https://edition.cnn.com/2021/06/07/politics/president-joe-biden-cyber-attacks-russia-putin-trump-economy/index.html>.

i Russland faktisk tjener penger på det og dermed kanskje ikke trenger statlig finansiering. Andre land, som Nord-Korea, er også kjent for å tjene store pengebeløp på offensive cyberoperasjoner. Mangelen på internasjonalt anerkjente spilleregler for cyberoperasjoner mellom stater er svært uheldig for hele verdenssamfunnet, fordi den gir insentiver til økende grad av lovløshet i cyberrommet.

Genèvekonvensjonene definerer hva som er lovlige angrepsmål i krigføring. Det skilles klart mellom soldater og sivile, der sivile er definert som ulovlige mål. Men hvis private aktører utfører offensive cyberoperasjoner mot en krigførende part, blir de å betrakte som lovlige mål for den krigførende parten. Offensive cyberoperasjoner utført av private kan legitimere cyberkrigføring mot sivile mål, som vi ikke ønsker at skal skje. Et viktig prinsipp er derfor at offensive cyberoperasjoner kun skal utføres av staters myndigheter under en veldefinert policy.

*Paris Call for Trust and Security in Cyberspace*⁸⁹ (2018) var et forsøk på å få til en internasjonal konvensjon om cyberoperasjoner og bruk av cybervåpen. Små land støttet initiativet, men stormaktene var imot. For det første ser stormaktene at de har stor nytte av cyberoperasjoner, og for det andre mener de, kanskje med rette, at det ville være nesten umulig å overvåke overholdelsen av en slik avtale. I ordspråket som sier at «i krig og kjærlighet er alt tillatt», kan vi legge til at dette også gjelder i cyberkrig.

17.4.3 IT-sektorens rolle i cyberkrigføring

Onsdag 23. februar 2022, noen timer før russiske stridsvogner begynte å rulle inn i Ukraina morgenen etter, fant Microsofts Threat Intelligence Center (MSTIC) indikatorer på en aldri tidligere sett «wiper»-skadevare som i Windows-servere ble observert brukt i forsøk på å angripe Ukrainas regjeringsdepartementer og finansinstitusjoner.

MSTIC plukket raskt fra hverandre skadevaren, kalte den «FoxBlade», og varslet Ukrainas øverste cyberforsvarsmyndighet. FoxBlade-skadevaren var programmert til å slette – «wipe» – alle data på datamaskiner som er tilgjengelige i et datanett. I løpet av tre timer hadde Microsofts virusdeteksjonssystemer på Windows-servere, både i Ukraina og ellers rundt i verden, blitt oppdatert for å blokkere FoxBlade. Dette eksemplet viser hvordan aktører i IT-industrien, særlig Big Tech, har et enormt potensial for å gjennomføre tiltak med øyeblikkelig effekt i store deler av den globale IT-infrastrukturen. Dette og andre lignende tiltak med støtte av vestlige IT-selskaper og myndigheter gjorde at IT-systemene i Ukrainas regjeringsdepartementer fortsatte å fungere mens invasjonen pågikk, slik at de kunne koordinere sine forsvarsoperasjoner. Dette frarøvet Russland den planlagte effekten av å lamme Ukrainas IT-systemer i en kort periode samtidig som invasjonen pågikk.

En enkel gjennomgang av tilsvarende scenarioer avslører at samarbeid med Big Tech kan gi betydelige fordeler i cyberkrigføring. For eksempel kobles hvert Windows-operativsystem til en Microsoft-server minst ukentlig for å se etter programvare- og konfigurasjonsoppdateringer. Fra et teknisk perspektiv gir dette Microsoft full kontroll over alle datamaskiner i hele verden som kjører Windows og som er koblet til internett. Det ville være relativt enkelt å identifisere datamaskinene til enkeltpersoner, så vel som datamaskiner til en bestemt organisasjon eller i en bestemt geografisk region. Teknisk sett er Microsoft i stand til

å fjernstyre hver datamaskin for eksempel for spionasje eller for sabotasje. Lignende typer kontroll vil også være mulig for andre Big Tech-selskaper. Det er plausibelt at et lite utvalg av Big Tech-selskaper har teknisk mulighet for å «slå av» internett i hele eller deler av verden. Som Snowden-avsløringene har vist oss, er private selskaper villige til, eller er juridisk forpliktet til, å samarbeide med sine nasjonale myndigheter, så muligheten for global styring av kjernefunksjoner i systemer, applikasjoner og hele internett gjennom samarbeid med Big Tech-selskaper er realistisk. En naturlig konklusjon på slike refleksjoner er at styrkeforholdet i cyberkrigføring avhenger av å ha Big Tech på sin side. Ettersom Big Tech for det meste er basert i USA, vil det for Norges del si at vår styrke i cyberkrigføring i stor grad avhenger av å ha USA som alliert.

Når store IT-produsenter blir samarbeidspartnere i cyberoperasjoner, er en naturlig konsekvens at markedsandelen til deres produkter og tjenester vil bli påvirket av globale politiske skillelinjer. For eksempel, hvis det var tilfelle at en USA-basert leverandør implementerer en bakdør for NSA i sine produkter, og dette ble offentlig kjent, så er et sannsynlig resultat at markeder i land som stort sett er USA-antagonistiske, ville slutte å bruke disse produktene av frykt for å bli underlagt kontroll og overvåking. Frykten for at det kinesiske Huawei kunne installere bakdører i 5G-nettet, var nettopp årsaken til at regjeringen ikke tillot teleoperatørene i Norge å bygge ut 5G-nettet med teknologi fra Huawei. Disse hendelsene er sannsynligvis bare toppen av isfjellet i den globale politikken for IKT og cyberkrigføring, og reflekterer en trend mot fragmentering av teknologimarkedet etter geopolitiske skillelinjer.

Oppgaver til kapittel 17

17.1 Digital trusseletterretning

- Hvorfor er deling av CTI viktig?
- Hva menes med at CTI kan være kortvarig eller langvarig?
- Hvorfor er det viktig å kunne (del)automatisere CTI?
- Nevn utfordringer med å (del)automatisere CTI.

17.2 Cyberkrigføring

- Hva er sammenhengen/forskjellen mellom informasjonsoperasjoner og cyberoperasjoner i militær sammenheng?
- Beskriv nytten av ulike former for militære cyberoperasjoner.
- Beskriv aspekter og egenskaper ved cybervåpen.
- Hva er cyberavskrekking, og hvorfor kan det være nyttig?
- Hvorfor er det vanskelig å få til en internasjonal konvensjon om cyberkrigføring?

17.3 MITRE ATT&CK

- Hva er likheten mellom DML-modellen (Detection Maturity Model) og MITRE ATT&CK?
- Se på figur 17.3 eller på *ATT&CK Matrix for Enterprise* på <http://attack.mitre.org>. For hver taktikk, si hvilket trinn i Cyber Kill Chain den passer til.