Executive Summary: Cybersecurity and Information Security Management by Jørgen Leiros

Jørgen Maurstad Leiros, as part of his MSc in Business Administration and Data Science, conducted an **in-depth study on cybersecurity threats, risk mitigation, and information security management**, with a particular focus on **phishing, ransomware, and access control mechanisms**. His research integrates **technical defenses, digital security culture, and regulatory compliance** to strengthen **enterprise cybersecurity resilience**.

Key Focus Areas:

1. **Cyber Threats and Attack Vectors** –
    - Analyzed various **cyberattack methods**, including **phishing, smishing (SMS phishing), CEO fraud, and ransomware**, detailing how these tactics exploit **social engineering and system vulnerabilities**.
    - Examined real-world case studies, such as **bank phishing scams and data breaches**, highlighting the **economic and reputational risks** for businesses and individuals.
2. **Risk Management and Defensive Strategies** –
    - Advocated for **multi-layered security strategies**, including **encryption, two-factor authentication (2FA), and real-time phishing detection**.
    - Explored **technical safeguards**, such as **firewalls, intrusion detection systems (IDS), and machine learning-based anomaly detection** for threat prevention.
3. **Information Security Governance and Compliance** –
    - Discussed the **role of GDPR and Norwegian data protection laws** in shaping **cybersecurity policies** for organizations.
    - Addressed **access control frameworks**, including **role-based access control (RBAC)** and **least privilege principles**, ensuring **data confidentiality and integrity**.
4. **Digital Security Culture and Human Factors** –
    - Emphasized the importance of **cyber awareness training and phishing simulations** to reduce **human error and social engineering risks**.
    - Proposed a **superuser system** within organizations to enhance **internal security monitoring and rapid threat response**.

Key Takeaways:

- **Social engineering remains the most effective cyberattack method**, requiring **continuous user education and vigilance**.
- **Advanced threat detection and encryption protocols** significantly reduce **ransomware and phishing risks**.
- **Security culture within organizations is as critical as technical defenses**, making **policy enforcement and training essential**.

Through this research, Jørgen has demonstrated expertise in **cybersecurity management, risk mitigation, and regulatory compliance**, providing actionable insights for **enterprise security strategies and resilience-building**.

Øving 1 – Sikkerhet og sikkerhetskultur

Gjør rede for ulike slike svindelteknikker. Hvordan er svindelen ment å fungere? Hva er svindlerne ute etter? Hvordan kan vi som «vanlige» mennesker kjenne igjen disse? Kom med eksempler, gjerne fra media eller andre kilder.

Nettsvindel er noe de aller fleste har et forhold til, enten direkte eller indirekte. Aviser trykker artikler på ukentlig basis hvor de forteller om alt fra enkeltpersoner til større virksomheter som har blitt utsatt for ulike former for angrep. Svindelaktørene benytter seg av en rekke ulike metoder i sine angrep, hvor motivet er varierende. Denne besvarelsen redegjør for noen av de ulike svindelteknikkene og hva vi som enkeltpersoner og samfunn gjør – og kan gjøre for å redusere sannsynligheten for at slike aktører lykkes.

Nettsvindel er en type bedrageri som blir utført ved bruk av internett, og kan også omtales som cyberangrep. Vedkommende som utfører svindelen kalles en trusselaktør og har som mål å utnytte IKT-systemer til en gitt hensikt (Bergsjø & Windvik, 2020, s. 20). Trusselaktører kan utnytte IKT-systemer med hjelp av mange ulike teknikker, avhengig av hva aktøren ønsker å oppnå. Ofte er hensikten å tilegne seg en form for verdifull informasjon som trusselaktøren ikke er tiltenkt å ha tilgang til. Hva aktøren velger å gjøre med informasjonen kan variere stort, og henger ofte sammen med hva målet med svindelen er. I mange tilfeller er handlingen økonomisk motivert, mens i andre tilfeller kan motivet også være å få tilgang til sensitiv informasjon og benytte denne som et pressmiddel mot enkeltpersoner eller virksomheter. Fellesnevneren for svindelmetodene er at de alle benytter seg av sosial manipulering som det viktigste verktøyet for angriperen (Telenor, 2020). Det innebærer at aktøren spiller på grunnleggende psykologiske følelser som frykt, tillit og opplevelsen av følt tidspress for å få oss til å handle irrasjonelt.

Phishing

Et av de mest kjente begrepene innenfor nettsvindel er phishing, og kommer gjerne i form av e-poster fra mistenkelige kontoer eller ukjente telefonnummer. Phishing er kort fortalt når

Gruppe 1
Kristian Bygland
Jørgen Leiros
Filip Bergli
Jakob Erdal
Bendik Johansson

noen vil lure deg til å gå inn på en falsk side, og oppgi informasjon (Nettvett.no, 2021).

22.05.2022

Aktøren bak e-posten utgir seg ofte for å være en legitim aktør, som for eksempel en stor nasjonal bank, og ber deg gjerne om å klikke på en vedlagt link i e-posten. Offeret blir deretter sendt videre til en nettside som svindelaktøren har kontroll over, og ber deg om å oppgi personlig informasjon.

SpareBank 1 SMN opplevde blant annet høsten 2021 at trusselaktører utnyttet deres arbeid med å innhente kundeinformasjon på store deler av kundeporteføljen (Sparebank1, 2021). Arbeidet med oppdatering av kundeinformasjon genererte store mengder e-post, og SMS-korrespondanse fra banken til kunder. Budskapet var at kundene måtte oppdatere kundeinformasjon, enten fysisk eller via deres nettsider. I mange tilfeller førte manglende respons fra kunder til at banken så seg nødt til å sperre kort og kontoer for å gi kunden insentiv til å agere. Banken legitimerte denne prosessen gjennom hvitvaskingslovens og tilhørende forskrifter som pålegger finansielle aktører å kjenne deres kunder gjennom kundetiltak og løpende oppfølging (Hvitvaskingsloven, 2018, § 9-24). Den omfattende korrespondansen i kombinasjon med sperring av kontoer og legitimering gjennom lovverket, ga trusselaktører en mal for hvordan de skulle få tak i informasjon de kunne utnytte til egen fordel. Svindlerne utga seg for å være SpareBank 1 SMN og ba kunden om å trykke på en link som sendte kunden videre til en side som tilsynelatende skulle verifisere kundens data. Informasjonen kunden oppga her ble umiddelbart brukt av trusselaktørene til å få tilgang til kundens kort eller nettbank. Denne metoden kalles *real-time phishing* og kjennetegnes ved en mellomside som utgir seg for å være legitim, hvor trusselaktøren bruker informasjon hentet her på den faktiske legitime siden (Boodaei, 2010).

Tradisjonelt sett er phishing noe som for en oppmerksom kunde ville vært forholdsvis enkelt å gjenkjenne ved hjelp av tips og triks kommunisert fra sikkerhetsaktører eller andre kompetansebærende individer. Eksempelvis kan det være lurt å se på avsenderadressen, som ofte enten vil være noe helt annet enn hva avsender utgir seg for å være, eller eventuelt ha detaljer man kan skille fra en legitim avsender. At avsenderadresse bruker SpareBankene 1, i stedet for SpareBank 1 SMN kan eksempelvis være en nyanse som gjør at man kan skille legitim- fra ikke legitim avsender. I mange tilfeller er også ordlyden i phishingen dårlig eller annerledes fra en legitim aktør, noe som ikke krever inngående kunnskap for å avdekke. Dersom man trykker på lenken man får tilsendt, vil det også være muligheter for å identifisere siden som ikke-legitim ved å se på domenenavn, logo og andre trekk ved nettsiden. Likevel ser man i løpet av de siste årene at slike forsøk stadig blir mer sofistikerte. Ordlyden blir bedre, ofte så god at selv individer med høy digital sikkerhetskompetanse vil slite med å identifisere teksten som phishing basert på ordlyden alene. I den sammenheng vil det være viktig å ha andre sjekkpunkter å lene seg på. Avsenderadresse vil her være et nyttig sjekkpunkt, hvor det er viktig at man ser på faktisk avsenderadresse, noe som ikke nødvendigvis er det som fremkommer i e-posten. Landingssidene for de vedlagte lenkene er også blitt av vesentlig bedre kvalitet, noe som kan gjøre det vanskelig å avdekke siden som ikke-legitim. Når svindlerne blir mer sofistikerte er det viktig at mottakerne har nok kunnskap til å kunne ta vurderinger basert på flere kriterier. Når det er vanskelig å identifisere phishing gjennom ordlyd, avsenderadresse eller landingsside alene, må man kombinere elementene for å kunne stå imot slike forsøk.

Smishing

Smishing, eller «SMS-phishing» er SMS-meldinger som har som formål å få mottakeren til å gi fra seg personlig informasjon, gjerne i form av linker til nettsteder som svindlerne har kontroll på (Telenor, 2020). Slike svindelforsøk er like vanlig, og foregår på omtrent samme måte som ved bruk av e-post. Svindelaktøren utgir seg ofte for å være en legitim aktør, for eksempel en kjent merkevare, med håp om å øke sannsynligheten for at offeret ikke skal anse meldingen som et svindelforsøk. Som ved phishing er motivet for å gjennomføre slike svindelforsøk forskjellige. Motivet kan være av økonomisk art, men personlige informasjon kan også utnyttes til å svindle andre eller benyttes som et pressmiddel (Telenor, 2022).

Et av gruppens medlemmer ble utsatt for dette selv for noen måneder siden, da medlemmets telefonnummer ble brukt til å spre falske SMSer. Ukjente aktører hadde da benyttet telefonnummeret til å sende meldinger til en rekke personer hvor de ba ofrene om å verifisere BankID gjennom en vedlagt lenke til en nettside. Vi ser derfor at aktørene blir stadig mer sofistikerte i sine svindelforsøk. Hvor det tidligere var mer vanlig å få falske SMSer fra utenlandske numre, kan det nå hende at de benytter private numre eller utgir seg for å være en større organisasjon.

Telefonsvindel

Selv om phishing via internett er blitt veldig vanlig og omfattende, eksisterer det også andre og mindre sofistikerte svindelmetoder. Svindelforsøk gjennom telefonoppringninger fra ukjente telefonnummer utgjør en overraskende stor andel av dagens svindelforsøk. Telenor alene stopper over 1 million svindel-samtaler i uken (Telenor, 2022). Det typiske eksempelet er når du mottar en telefon fra noen som utgir seg for å være en ansatt i Microsoft, som ber deg om å rette opp en feil på datamaskinen din. Fellesnevneren i disse tilfellene er ofte en gebrokken engelskuttale, et ukjent og utenlandsk telefonnummer og et problem du i utgangspunktet ikke kjenner deg igjen i. Selv om dette er svindelforsøk i sin enkleste form, har aktørene bak blitt mer sofistikert i sine metoder gjennom årene, hvor de nå eksempelvis kan kamuflere det utenlandske telefonnummeret bak et tilsynelatende norsk telefonnummer, som gjør det mye lettere for deg som mottaker å plukke opp telefonen når det ringer. Andre former for telefonsvindel innebærer også at aktørene ringer deg opp og umiddelbart legger på, hvor målet deres er at du skal ringe de tilbake, omtalt som «wangiri» (Nettvett.no, 2021). Disse numrene er såkalte høykostnummer, hvor aktørene tjener store penger på at noen ringer de tilbake.

Et annet eksempel på telefonsvindelen er det som ofte omtales som «Olga-svindel», og var svært utbredt høsten 2019 (Din Side, 2019). Svindlere gikk på denne tiden etter kvinner med navn som var populære for 80 år siden, som for eksempel Ola, Kari og Sigrid. De utga seg ofte for å være fra en kjent bank og fikk ofrene til å oppgi BankID-en sin. Herfra og ut har svindelaktøren et stort mulighetsrom. Ved at ofrene utleverer konto- og bankinformasjon, kan svindelaktørene forsøke å ta opp lån i vedkommendes navn, overføre penger til andre kontoer eller gjennomføre kjøp på nettsteder. En slik svindelteknikk er med andre ord svært ofte økonomisk motivert. Dette er et eksempel på bruk av digitale verktøy av brukere som ikke har god nok digital kompetanse til å forstå hvordan verktøyet fungerer, og ikke er klar

over konsekvensen av misbruket. Her ser vi hvordan kompetanse er en viktig del av forståelse for digital sikkerhet, slik som NorSIS påpeker (Bergsjø & Windvik, 2020, s. 40).

Olga-svindelen fikk etter hvert såpass mye oppmerksomhet at de fleste utviklet et skepsis som i stor grad bidro til at svindelmetoden mistet sin effektivitet. Her har man i det siste sett en ny type telefonsvindel med samme fremgangsmåte og hensikt, men rettet mot russisktalende menn (Personlig opplæringsmodul, SpareBank 1 SMN, 2022). Dette er et eksempel på hvordan svindlerne tilpasser seg og utvikler nye metoder raskt etter den foregående tilnærmingen mistet sitt inntektspotensial.

Tjenestenekt

Andre former for cyberangrep er også aktuelle å studere når det kommer til svindelteknikker. Denial-of-service (DoS) attacks er en metode hvor en ondsinnet aktør med intensjon går inn for å paralysere en datamaskin eller et større nettverk gjennom å sende flere dataforespørsler enn datamaskinen eller nettverket er i stand til å håndtere (Nettvett, 2020). Motivasjonen for å gjennomføre et slikt angrep kan variere, men det kan tvinge brukeren til å gå over på andre medier, og hvis aktøren bak kombinerer et slikt angrep med å tilby brukerne en form for «hjelp» gjennom å trykke på en link eller tilsvarende, vil brukeren være mottakelig for å klikke på denne for å oppnå den hjelpen brukeren har behov for. For en bruker vil det ikke alltid være like enkelt å fange opp en slik svindelmetode, da angrepet ofte er rettet mot en organisasjon, og ikke et enkeltmenneske. Likevel er det verdt å være oppmerksom på at nettverket kan oppfattes tregere enn normalt, ved for eksempel åpning av filer eller nettsider. Enkelte nettsteder kan også bli utilgjengelige, som gjør at man kanskje må ta i bruk en annen for å oppnå det opprinnelige målet med å bruke nettsiden. Dersom man ikke har mulighet til å aksessere noen nettsider i det hele tatt, og tilgangen til Internett er intakt, er dette et sikkert tegn på at noe er utenom normalen (Wikipedia, 2022).

Poenget med å nevne en slik form svindelteknikk, er at spekteret innenfor domenet er så bredt, og utvikles i takt med dagens teknologi. For brukeren blir det stadig vanskeligere å helgardere seg mot slike forsøk, til og med umulig. Ved å øke bevisstheten hos den enkelte, og vise til konkrete eksempler på hvordan slike forsøk er gjennomført tidligere, vil vi være bedre i stand til å håndtere disse hendelsene når de først oppstår.

Hybride metoder

Hybride metoder er ikke en anerkjent definisjon innen teorien om svindelteknikker, men et egendefinert begrep hvor svindelaktøren kombinerer ulike metoder i sine svindelforsøk. Svindelaktørene blir stadig mer sofistikerte i sine svindelmetoder og -angrep, og vil hele tiden søke å utnytte nye sårbarheter og svakheter. En kombinasjon av telefonoppringninger og SMS-svindel er et eksempel på at aktørene utvikler sine metoder i takt med samfunnets bevissthet og mottiltak. Det foregår gjerne ved at svindlerne først ringer opp offeret og utgir seg for å eksempelvis være en bank. De forteller hvordan det er mistenkelig aktivitet på kontoen din, eller at kontoen er sperret fordi noen forsøker å svindle deg. De følger deretter opp med en SMS med lenke til en falsk nettsiden hvor du blir bedt om å oppgi sensitiv informasjon (Sparebank1, 2021).

Ved å ta forholdsregler som å være skeptiske til utenlandske telefonnummer og ukjente telefonnummer generelt, kommer man langt. Er man i tvil på hvem som ringer, har vi i 2022 enkel tilgang til telefonlister på nett, hvor man enkelt kan undersøke hvem nummeret tilhører. I tillegg jobber telefonoperatører aktivt med å sperre telefonnummer som assosieres med nettsvindel. Telenor registrerte ved starten av koronakrisen en markant økning i svindelanrop, og sperret en stor andel telefonnummer (Digi, 2020).

Ransomware

Selv om ulike former for phishing eller andre svindelmetoder som sikter seg inn mot enkeltbrukere er noe som både skjer med stor hyppighet og med et forholdsvis omfattende potensielt skadeomfang, er det for bedrifter andre sikkerhetstrusler som utgjør det største potensielle skadeomfanget. En metode som i denne forbindelse trekkes frem med svært stor aktuell risiko er Ransomware, også omtalt som løsepengevirus (Eneroth et. al, 2022, s. 28). Ransomware eller løsepengevirus er en klassisk svindelmetode hvor angriperne krypterer enkeltpersoners harddisk eller større organisasjoners systemer, slik at de kan kreve store pengesummer for å gi opp kontrollen av systemet eller maskinen. En slik metode kan være veldig lønnsomt for profesjonelle aktører som angriper større bedrifter. Her kan pengekravene være store, og det er som regel ingen enkel vei utenom å betale pengekravet. Trusselaktørene som gjennomfører slike svindelforsøk er godt organiserte. De holder seg godt oppdaterte om nye svakheter og leter kontinuerlig etter nye sårbarheter de kan utnytte for å få tilgang til offerets informasjon.

Svindelen kan også starte med phishing mot enkeltindivider, som får ofrene til å trykke på en lenke eller laste ned en fil. Når aktøren har fått tilgang til klienter, servere og hele systemer, søker de å installere skadelig programvare og sette i gang krypteringsprosessen på alle maskinene for å lage mest mulig kaos. Telenor oppgir også at de i økende grad ser at trusselaktørene, i tillegg til å kreve penger for å tilgjengeliggjøre systemene, truer med å offentliggjøre sensitiv informasjon dersom betalingen ikke blir gjennomført. SpareBank 1 SMN peker på denne formen for svindel som med spesielt høy risiko basert på nylige angrep på Nortura, Nordic choice og Stortinget (SpareBank 1 SMN, 2022). For Nordic Choice har angrepene medført kostnader for minst 10 millioner kroner, mens Nortura måtte endre regler for import eller en full stans i slakt og transport. Datatilsynet har også hatt omfattende kostnader i forbindelse med angrepet på Stortinget, som anslås til minst 2 millioner kroner. Dette er kostnader som påløper selv om man ikke betaler løsepengene og illustrerer hvor stor finansiell risiko slike angrep utgjør for virksomheter.

Direktørsvindel

Direktørsvindel, eller CEO-fraud, kan defineres som svindel utført ved hjelp av e-post eller SMS fra personer som utgir seg for å være i ledelsen i bedriften (Nettvett, 2019). Svindelaktørene oppretter ofte domene med bedriftens navn for å kunne opprette e-postadresser som ligner de bedriften har. I tillegg gjør aktørene grundige forberedelser, og velger seg ut nøkkelpersoner i bedriften de mener kan være et passende offer. Målet med en slik svindelmetode er ofte økonomisk motivert, hvor de forsøker å lure en ansatt til å betale en faktura eller overføre et beløp til en konto. En slik henvendelse utnytter maktforholdet

mellom ledere og ansatte, i tillegg til å spille på de ansatte travle hverdag. Overføringen må i mange tilfeller skje raskt, hvor offeret ved gjentatte tilfeller får lite betenkningstid.

Hva tror dere er årsaken til at vanlige, relativt oppegående mennesker går på slike svindelforsøk?

I dagens digitale samfunn bruker de aller fleste av oss store mengder digitale verktøy både i jobb- og privat sammenheng. Dette legger til rette for at vi har utviklet er forholdsvis høy generell grad av digital kompetanse. Likevel er det mange som går på ulike former for svindelforsøk som vi har redegjort for i forrige oppgave. Dette kan i mange sammenhenger være helt oppegående og aktive deltakere i samfunnet, som er vant til bruk av digitale verktøy.

Sosialpsykolog Robert Beno Cialdini publiserte i 1984 en omfattende studie om psykologien bak overtalelse, hvor han skisserer enkle konsepter som personer som ønsker å påvirke andre aktivt benytter (Thudium, 2022). Disse tror vi kan benyttes for å forstå hvorfor vanlige mennesker biter på slike svindelforsøk, i kontekst av psykologien. I tillegg til disse faktorene er det relevant å trekke inn digital kompetanse hos den enkelte, og mangelen på erfaring vedrørende tidligere svindelforsøk.

Det første Cialdini trekker frem er at personer har en tendens til å gjøre det de observerer at andre gjør. Man kan tenke seg at en e-post fra din egen mobiloperatør er helt ufarlig, og du overhørte senest i lunsjen at en annen kollega var nødt til å logge seg inn og verifisere kontaktinformasjon hos deres egen operatør for et par dager siden. Dermed tenker man ikke så nøye over hva denne e-posten egentlig ber deg om, og får deg kanskje til å neglisjere indikatorer som falske domenenavn og skrivefeil. Mennesker er generelt mer påvirkelig av andre personer, grupper eller virksomheter, spesielt de personene eller gruppene vedkommende har et godt øye til. Derfor vil det være fordelaktig for en ondsinnet aktør å utgi seg for å være en legitim aktør som de fleste har et godt forhold til. Sannsynligheten for å utføre det man blir bedt om blir dermed større om vi i utgangspunktet har et godt forhold til den tilsynelatende legitime aktøren. I tillegg vil effekten forsterkes dersom man ser personer rundt seg oppfatter en slik henvendelse som troverdig.

Dette er sterkt koblet til et av de åtte kjerneområdene NorSIS har definert som viktig i forståelsen av digital sikkerhetskultur, tillit (Bergsjø & Windvik, 2020, s. 38). I Norge har vi et velfungerende demokrati hvor tilliten til styrende organer er på et generelt høyt nivå. Dette forplanter seg videre i andre samfunnslag hvor viktige aktører slik som eksempelvis store banker har forholdsvis høy tillit fra befolkningen. At slike aktører har stor tillit, gjør at de opplever å ha god legitimitet for sin drift, og for behandling av kundeinformasjon. Dette er noe svindlere kan utnytte. Det er naturligvis en styrke i samfunnet vårt at det eksisterer tillit mellom enkeltindivider og organisasjoner/myndigheter som forvalter verdier og har direkte påvirkningskraft på livene våre. Likevel vil et helt ukritisk forhold mellom aktører legge til rette for at man ikke ser kritisk nok på tilnærminger fra potensielle trusselaktører. Tilliten gjør med andre ord at man stoler blindt på de henvendelser man får fra de som utgir seg for å være en legitim aktør. Det nevnte eksemplet med svindlere som utnytter bankers innhenting av kundeinformasjon er et godt bilde på dette. Her er det viktig, slik vi vil belyse i neste

oppgave, at virksomheter og regulatoriske myndigheter tar ansvar og sprer kompetanse om hvordan man kan skille mellom henvendelser fra legitime aktører og trusselaktører.

En persons beslutninger vil kunne føre til at man blir offer for svindel, og er etter vårt synspunkt også påvirket av generelle holdninger til teknologi og sikkerhet. Våre holdninger til teknologi påvirkes av mange faktorer slik som kompetanse, interesse- og optimisme for teknologi i tillegg til risikooppfattelse (Bergsjø & Windvik, 2020, s. 36). Hvis vi starter med interessen vi har for teknologi, vil en lav interesse medføre at man omgir seg med individer med samme utgangspunkt. Disse relasjonene bidrar til en gjensidig adopsjon av hverandres holdninger og vil forsterke den manglende interessen for teknologi. Dette vil igjen føre til lavere kompetanse. Lav kompetanse kan både være årsaken til at man blir utsatt for svindel, men også hvordan noen unngår det. Dette bygger på risikooppfattelse. Dersom man har høy kompetanse vil man ofte i større grad utsette seg for risiko, da man har en oppfatning av at kompetansen gjør en i stand til å håndtere risiko. Dette er selvfølgelig i mange tilfeller helt riktig, men kan også slå motsatt vei. Hvis vi tar skikjøring som et eksempel, viser statistikk at de mest kompetente skikjørerne med mest inngående kunnskap om trygg ferdsel i terrenget og best utstyr, er de med høyest ulykkesrate og antall dødsfall (Skaiia & Thomassen, 2016, s. 430). Dette er fordi den inngående kompetansen legger til rette for at man tar høyere risiko enn hva man hadde gjort med en lavere grad av kompetanse. I dette eksemplet er det snakk om kunnskap som i stor grad er konstant, det vil si at den ikke endrer seg over korte tidsperioder. For håndtering av digitale verktøy og sikkerhet er dette helt feil. Ofte kan det som for 15 år siden var ansett som riktig, ikke bare være justert, det kan være direkte feil grunnet den digitale utviklingen og nye svindelmetoder (Bergsjø og Windvik, 2020, s. 42). Dette forutsetter at man holder seg oppdatert på hva som er sikker atferd. I den forbindelse mener vi at eldre mennesker som på et tidspunkt har hatt god forståelse for digital sikkerhet, i møte med svindelforsøk kan overvurdere egen evne. Dette kan resultere i at oppegående mennesker med en overdreven oppfatning av egen kompetanse utsetter seg for unødvendig risiko og blir offer for sikkerhetshendelser.

I forrige oppgave nevnte vi med Telenor som kilde at de fleste svindelforsøk spiller på en eller annen emosjonell faktor. Dette kan være en faktor som kan forklare hvorfor oppegående mennesker går på svindelforsøk. Norge er et velstående land med generell høy levestandard. Dette gir svindlere mulighet til å spille på følelser hvor man eksempelvis blir svindlet til å sende penger til noen som er i vanskeligstilte situasjoner. Disse individene som brukes i svindelforsøkene vil ikke være ekte personer, men kun persona med hensikt å bidra til sosial manipulering. Dette er noe gruppens medlemmer har blitt utsatt for personlig gjennom henvendelser fra personer som tilsynelatende er i nød, og vi har forståelse for at man i slike situasjoner kan la seg lure selv om vi anser oss selv som forholdsvis oppegående.

Direktørsvindel understreker den neste faktoren, hvor Cialdini sier at personer har lett for å føye seg etter autoriteter selv om de i utgangspunktet er uenig i det de blir bedt om. Dette utnyttes i såkalt direktørsvindel, hvor aktøren kan utgi seg for å være en høytstående sjef i virksomheten du jobber i. I e-posten som sendes blir du bedt om å gjøre en handling, som du også velger å gjøre fordi du ser at e-posten kommer fra en høytstående sjef. Dette er ikke noe

gruppens har personlige erfaringer med, men de av oss med faste jobber kan se for oss en slik situasjon, og hvilken utfordring man potensielt står overfor.

En siste faktor er knapphet, og i mange tilfeller mangelen på ressurser og mennesket iboende behov for å få tilgang på disse knappe ressursene. Dette kan eksemplifiseres med falske konkurranser hvor du som deltaker kan vinne et begrenset opplag med telefoner, hvor du dermed tenker at dette er et tilbud som er for godt til å gå glipp av. Frykten for å ikke få tilgang på noe som er begrenset i mengde eller størrelse, tar overhånd og gjør at du utfører irrasjonelle handlinger man vanligvis ville holdt seg for god for. Ett av gruppens medlemmer har i forlengelsen av dette erfaring med følelsen av knapphet, riktignok en nokså dårlig erfaring. Han kom over et usedvanlig godt tilbud på en brukt mobiltelefon på Finn, og tenkte det var for godt til å være sant. Følelsen av å kunne gjøre et kupp ble for stor, og visstnok endte han med å få rett. Tilbudet var for godt til å være sant, noe han innså når pakken ble åpnet og han fant en brukt hårvoks.

Uoppmerksomhet og en travel hverdag preget av forhastede beslutninger kan, i tillegg til de grunnleggende psykologiske faktorene som Cialdini beskriver og NorSIS kjerneområder, påvirke en persons handlinger. Dagens samfunn er omgitt av teknologi, og en ekkel følelse av å hele tiden være tilgjengelig kan gjøre seg gjeldende. Personer går fra møter til møter, skummer gjennom e-poster samtidig som man lander en avtale med en fremtidig kunde over telefonen. Avtalen og mailboksen måtte gjennomgås innen det neste kvarteret, for da var det duket for et Teams-møte med virksomhetens øverste ledelse. Slike hverdager kjenner mange seg igjen i, noe vi mener også kan være en forklaring på hvorfor ondsinnede aktører lykkes med sine svindelforsøk. Hadde vi lest gjennom e-posten med et litt skarpere blikk, hadde vi kanskje ikke trykket på den vedlagte lenken, men heller slettet e-posten.

Det er mange andre aspekter vi kunne trukket inn i besvarelsen av denne oppgaven, men vi har valgt å fokusere på de områdene vi mener har størst betydning for at tilsynelatende oppegående mennesker går på svindelforsøk.

Hvordan kan vi som samfunn eller virksomhet/bedrift/organisasjon stoppe eller forhindre slike svindelforsøk?

Digital sikkerhetskultur

Ved at vi i vårt samfunn eller innenfor vår egen virksomhet har fokus på å utvikle en god digital sikkerhetskultur, vil vi kunne minske sannsynligheten for at slike svindelforsøk får fatale konsekvenser. Digital sikkerhetskultur kan forstås som de verdier, holdninger, antakelser, normer og kunnskaper som mennesker bruker når de forholder seg til digitale verdier (Bergsjø & Windvik, 2020, s. 36). Ved å fokusere på verdier og holdninger, vil man kunne drive forebyggende sikkerhetsarbeid, og ikke brannslukking. Ved å rette fokuset mot verdiene og holdningene, vil dette kunne påvirke normene og kunnskapsnivået hos den enkelte, som til slutt vil kunne rokke ved de grunnleggende antakelsene. Har man derimot et utelukkende fokus på atferd, hvor man oppmuntrer til ønsket atferd ved interaksjon med digitale verdier, vil dette sannsynligvis ikke være nok for å gi menneskene de tilstrekkelige forutsetningene for å ta gode vurderinger og beslutninger når de havner i ulike situasjoner. NorSIS har pekt ut åtte kjerneområder som de mener beskriver digital sikkerhetskultur på en

helhetlig og relevant måte (Bergsjø & Windvik, 2020, s. 36), hvor vi ønsker å trekke fram **kompetanse**, **fellesskap** og **tillit** som de viktigste faktorene man aktivt kan arbeide med for å bedre den digitale sikkerhetskulturen.

For det første må det legges til rette for at man skal øke den digitale kompetansen hos den enkelte i samfunnet, gjennom å tilby opplæring og bevisstgjøring. Dette mener vi er et ansvar som hviler på samfunnet og de større aktørene innen forebyggende sikkerhetsarbeid. Organisasjoner som NSM og NorSIS forvalter et ansvar innenfor opplæring og bevisstgjøring av samfunnet, som kan løses på mange ulike måter. Virksomheter bør tilbys kompetanseheving, og må kunne ta ansvar for deler av kompetansebyggingen selv. Dette må tilbys og gjennomføres jevnlig, da mye av kunnskapen fort blir utdatert som resultat av den teknologiske utviklingen i dagens samfunn. Som tidligere nevnt kan det man lærte for et par år siden kan være utdatert eller direkte feil i lys av dagens teknologi og kunnskap.

I tillegg til det kollektive ansvaret de større aktørene forvalter innen kompetanseheving, bør virksomheter også legge til rette for intern opplæring. Tradisjonell klasseromsundervisning er en måte å løse dette på, men er ofte ikke nok. Kompetansen må som nevnt holdes oppdatert og må gjennomføres jevnlig. Dette kan gjøres ved at virksomheten etablerer det vi kaller for "superbrukere" med et eksplisitt ansvar for å vedlikeholde kunnskap og være ressurspersoner for andre ansatte ved implementering og bruk av nye systemer eller endring i arbeidsrutiner. Disse funksjonene får dypere kompetanse innen sikkerhetsarbeid, og har derfor kunnskaper og ferdigheter til å gjennomføre opplæring av andre. Superbrukere har ikke nødvendigvis ansvar for selve opplæringen av de ansatte i virksomheten, men å følge opp at opplæringen faktisk blir praktisert. De vil være tett på det operative da de gjerne jobber der selv, og i den forbindelse være ressurspersoner å trekke på i hverdagen. Det er viktig at disse funksjonene er kjent blant de ansatte i organisasjonen, slik at de kan utnyttes effektivt og bidra med korrekt kunnskap og forståelse av hva som er riktig og ikke. Dette har Sparebank 1 SMN hatt god erfaring med de siste to årene, noe et av gruppens medlemmer selv har erfart.

Ved å bygge en god digital sikkerhetskultur vil denne kulturen danne et fellesskap som mennesker identifiserer seg med. Når mennesker identifiserer seg med et fellesskap, vil de ha lettere for å akseptere og adoptere den oppførselen fellesskapet mener er «korrekt», som i dette tilfellet betyr korrekt opptreden ved bruk av digitale verdier (Bergsjø & Windvik, 2020, s. 41). Hva man definerer som korrekt er opp til de ansvarlige og fellesskapet selv. Et fellesskap er også viktig for å bedre sikkerhetsarbeidet i alle ledd. Det arbeidet hver enkelt aktør gjør for å bekjempe cyberkriminalitet er viktig, men et samarbeid vil være avgjørende for utvikling og beskyttelse av den digitale infrastrukturen i samfunnet (Telenor, 2020). Det handler om erfaringsutveksling og kompetansedeling, hvor betydningen av nettverk vil være viktig. Nettverk med aktører som bedriver forebyggende sikkerhetsarbeid på et daglig basis har slike fordeler, hvor aktører som NSM, Nordic Financial CERT og Kripos er viktige legitime aktører.

Med en helhetlig og samlende digital sikkerhetskultur vil det gradvis bygges tillit mellom de ulike individene, og videre opp til myndigheter og ledelse. Denne tilliten er avgjørende for at kulturen skal fungere i praksis, og at myndigheter og ledelse skal kunne styre effektivt – som

videre skal resultere i ønsket atferd hos den enkelte. I dette ligger det også at ledelsen må kunne styre selv om noen er uenige i regler og tiltak, eller om noen av disse tiltakene virker fremmede. Har man en grunnleggende tillit til systemer, ledelse og digitale verdier generelt, vil det være lettere å akseptere kontinuerlig bruk av digitale systemer og eventuelle endringer som blir iverksatt. Økt tillit til legitime aktører og myndigheter, kombinert med økt kunnskap hos den enkelte, vil bidra til å minske sannsynligheten for trusselaktørens suksess. Som et eksempel vil en bruker med høy tillit til sin egen bank, kombinert med økt kompetanse gjennom opplæring, kanskje la være å trykke på tilsendte lenker via e-poster.

Som ansvarlig for å utvikle god digital sikkerhetskultur, peker læreboken på konkrete tips for å bygge en helhetlig digital sikkerhetskultur (Bergsjø & Windvik, 2020, s. 45). Målet med å utvikle en slik kultur må defineres tydelig og kommuniseres til alle involverte slik at alle gjør seg forstått med hensikt og ønsket måloppnåelse. Det blir dermed mye lettere for den enkelte å identifisere seg med kulturen og identifisere seg med denne. Det understrekes at arbeidet med å utvikle og påvirke kulturen hos en virksomhet krever en helhetlig tankegang og innsats på mange områder samtidig, som følge av at det er så mange aspekter som inngår i den digitale sikkerhetskulturen. Gjennom å sørge for at alle involverte har den riktige og tilstrekkelige kompetansen, sikrer man at den enkelte har en verktøykasse som kan benyttes i tilfeller hvor det kreves. Økt kompetanse og kunnskap leder videre til bevisstgjøring og økt bevissthet, og understreker viktigheten av å bygge gode holdninger og verdier knyttet til bruk av digitale verdier. Et praktisk eksempel på hvordan dette kan forsterkes, er gjennom bruk av artefakter for å fremme sikkerhetskulturen. Kanskje plakater i fellesområdene som får deg til å stoppe opp og tenke over dine vaner og atferd på nettet er det som skal til for å øke bevisstheten og til slutt lede til en helhetlig god digital sikkerhetskultur?

Tekniske og taktiske sikkerhetstiltak

Økende kompleksitet og ny teknologi stiller krav til ny kompetanse og arbeidsmetodikk. Stadig mer komplekse verdikjeder stiller større krav til hvordan organisasjoner og myndigheter samhandler for å mitigere den økende trusselen (Telenor, 2020). Trusselaktørene vil hele tiden se etter nye sårbarheter og vil søke å benytte nye metoder og mer ressurser for å oppnå sine intensjoner. Innenfor verdikjeden finnes det sårbarheter innen teknologien, hos menneskene og i prosesser (Telenor, 2020). Den digitale sikkerhetskulturen vil være viktig for å redusere sårbarhetene knyttet til menneskene, men tiltak for å redusere sårbarheter knyttet til teknologi og prosesser vil også være viktige. Slike tekniske og taktiske sikkerhetstiltak som kryptering, tofaktorautentisering, innebygde spamfilter i e-post-applikasjoner og dedikerte responsteam er eksempler på slike tiltak.

Secure Practice har utviklet et slikt spamfilter, og er innebygd funksjonalitet i e-posttjenere for å hindre at mistenkelige e-poster havner i de ansattes innbokser (Secure Practice, u.d.). Ved å benytte slike sikkerhetstiltak vil man redusere virksomhetens sårbarheter, og dermed gjøre det mindre sannsynlig å bli utsatt for svindelforsøk eller rettede cyberangrep. Her er et eksempel på hvordan virksomheter kan benytte eksterne aktører som et ledd i deres forebyggende sikkerhetsarbeid. Ved å utnytte nettverket med aktører som jobber med - og tilbyr tjenester innenfor sikkerhetsarbeid, slipper virksomheter å gjøre hele jobben selv og kan utnytte den samlede kompetansen som finnes i slike nettverk.

Dedikerte responsteam som jobber med å avdekke svindelforsøk og håndtering av de situasjonene som oppstår vil være et effektivt tiltak i en virksomhets sikkerhetsarbeid. Et slikt team har både fokus på det forebyggende arbeidet, i tillegg til det brannslukkende. Teamet kan bidra med verdifull rådgivning til virksomhetens ledelse, og kan levere beslutningsgrunnlag inn mot utarbeidelse av sikkerhetspolicy så vel som ved konkrete sikkerhetshendelser og håndtering av disse. Sentrale aktører som NSM har også egne responsteam med et overordnet ansvar for å overvåke det digitale risikobildet (NSM, 2020). Disse kan bidra med kompetanse innen deteksjon, håndtering, analyse og rådgivning knyttet til digital sikkerhet, og er nok et eksempel på hvordan virksomheter kan benytte ekstern kompetanse i deres sikkerhetsarbeid.

Referanser

Bergsjø, H., & Windvik, R. (2020). I *Digital sikkerhet - En innføring.* Universitetsforlaget.

Digi. (2020, Mars 26). *Telenor melder om rekordhøy svindeltrafikk*. https://www.digi.no/artikler/telenor-melder-om-rekordhoy-svindeltrafikk/488591

Din Side. (2019, Oktober 25). *Disse damene er ekstra svindelutsatt*. https://dinside.dagbladet.no/okonomi/disse-damene-er-ekstra-svindelutsatt/71747598

Eneroth, C., Nilsen, H. T., Furberg, P. (2021) Digital sikkerhet 2021. *Telenor.* *https://www.telenor.no/binaries/om/digital-sikkerhet/digitalsikkerhet2021.pdf*

Nettvett. (2020, Januar 13). *DDoS-angrep*. https://nettvett.no/ddos-angrep/

Nettvett. (2021, Oktober 11). *Vanlige typer svindel i omløp*. https://nettvett.no/aktuell-svindel/

Nettvett. (2019, Oktober 16). *Direktørsvindel (CEO-fraud)*. https://nettvett.no/direktor-svindel/

NSM. (2020, Juni 24). *Nasjonalt Cybersikkerhetssenter (NCSC)*. https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/

Secure Practice. (u.d.). *Engage*. https://securepractice.co/engage

Skaiia, S.C, Thomassen, T. (2016, 18. februar). Skredulykker og behandling av skredtatte. *Tidsskrift for Norsk Legeforening. Skredulykker og behandling av skredtatte | Tidsskrift for Den norske legeforening (tidsskriftet.no)*

Sparebank1. (2021, 22. januar). *Unngå å bli lurt av svindlerne*. https://www.sparebank1.no/nb/bv/om-oss/nyheter/sparebank-1-advarer--unnga-a-bli-lurt-av-svindlerne-2021.html

Telenor. (2020, Juni 23). *Digital Sikkerhet 2020 - De lange linjene*. https://www.telenor.no/binaries/om/digital-sikkerhet/Telenor_Digital_Sikkerhet_2020_1.pdf

Telenor. (2022). *Samfunnssikkerhet*. https://www.telenor.no/sikkerhet/samfunnssikkerhet/

Thudium, T. (2022). *Practical Psychology. Robert Cialdini (Psychologist Biography)*. Practical Pie. https://practicalpie.com/robert-cialdini/#t-1595719625816

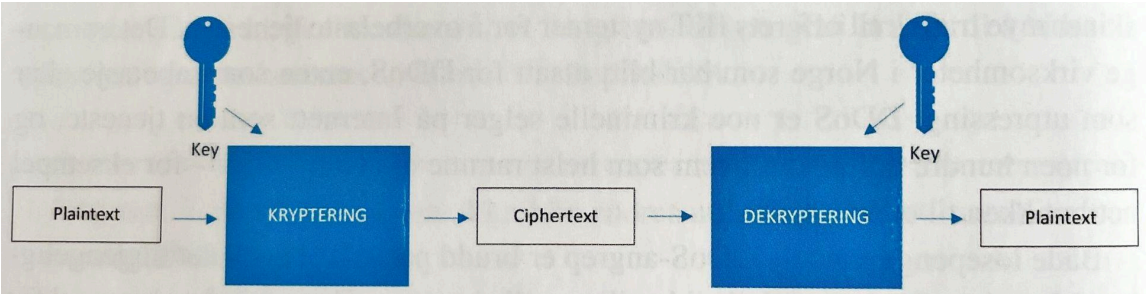
Wikipedia. (2022, April 23). *Denial-of-service attack*. https://en.wikipedia.org/wiki/Denial-of-service_attack#Symptoms

Øving 2 – Identifikasjon, autentisering og aksesskontroll

Gjør rede for grunnprinsippene ved symmetriske og asymmetriske nøkler, og hvordan og hvorfor disse gjerne brukes i kombinasjon. Bruk opprettelsen av 'sikker tilstand' som eksempel.

Sikkerhet innen digitale medier og teknologi generelt handler i stor grad om å etablere tillit mellom brukerne, og de informasjonssystemene som skal brukes. Sikkerhet kan i en slik kontekst fungere som et fundament for tillit, hvor autentisering ofte ses på som et nødvendig steg på veien for å oppnå dette (Bergsjø & Windvik, 2020, s. 75). Autentisering er prosessen hvor man avgjør om en påstått identitet er ekte eller ikke. Denne prosessen kan utføres ved hjelp av flere typer mekanismer og protokoller (Bergsjø & Windvik, 2020, s. 67). Felles for autentiseringsprotokollene er at de verifiserer hvorvidt brukerens *identifikatorer* tilhører den personen de utgir seg for å være. Dette er slik at vi har mulighet til å identifisere en person eller en *entitet* på nettet, og utføres ved hjelp av passord eller nøkler. I denne besvarelsen tar vi for oss grunnprinsippene ved symmetrisk og asymmetrisk kryptering. Vi redegjør først for prinsippene hver for seg, og ser på hvordan de kan kombineres for å utnytte fordelene med hver metode.

Som et teknisk tiltak for å ivareta sikkerhetsmålet konfidensialitet, er det svært utbredt å benytte krypteringsnøkler for å skjule innholdet for utilsiktede aktører. Kryptering kan på denne måten brukes for å autentisere entiteter. Informasjonen «låses» med en nøkkel og kan således ikke «låses opp» uten den korrekte nøkkelen. Innen kryptografi er det vanlig å angi teksten som skal krypteres for *plaintext* (klartekst), krypteringsnøkkelen for *key* og den krypterte teksten for *ciphertext* (chiffertekst), slik vist i figur 1 (Bergsjø & Windvik, 2020, s. 24).



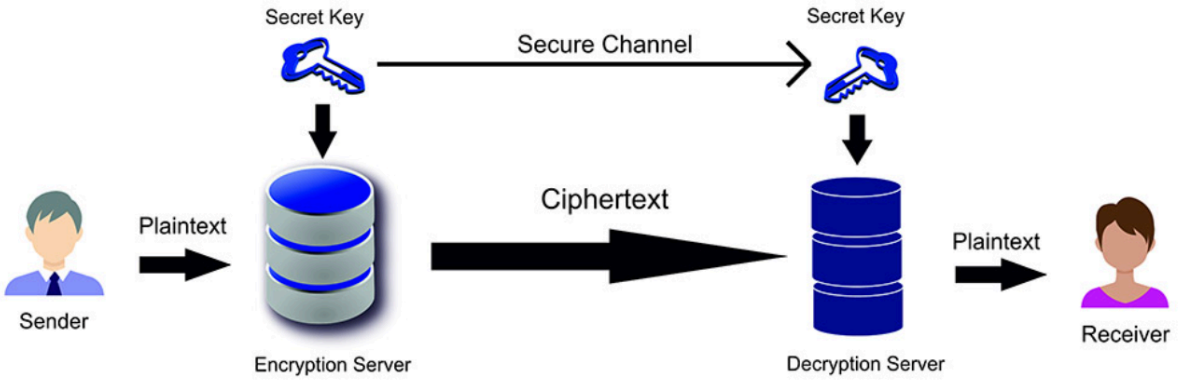
Figur 1.1. Kryptering og dekryptering.

Figur 1 Krypteringsprosessen.

Kryptering kan hindre en trusselaktør i å få tak i informasjon som er lagret på en server eller som overføres mellom to medier. Kryptografi gjør at vi kan kommunisere trygt på nett med personer hvis identitet vi kan være sikre på, samt at vi kan være sikre på at meldingene vi mottar ikke er endret av utilsiktede parter. Vi ser derfor at kryptering ivaretar sikkerhetsmålet *integritet*, noe vi vil komme tilbake til senere i besvarelsen. Av flere autentiseringsprotokoller finnes det to grunnprinsipper innen bruk av kryptografiske nøkler: *symmetrisk kryptering* og *asymmetrisk kryptering*.

Symmetrisk kryptering

Ved symmetriske kryptering bruker sender og mottaker den samme nøkkelen for kryptering og dekryptering. Én nøkkel benyttes med andre ord til både å kryptere og dekryptere informasjonen, og må utveksles mellom avsender og mottaker på en sikker måte (Datatilsynet, 2012). Figur 2 viser hvordan symmetrisk kryptering fungerer, og er et eksempel på hvordan en melding kan overføres fra avsender til mottaker på en trygg måte ved bruk av symmetrisk kryptering (Daniel, 2021). Aktørene har blitt enige om og utvekslet en hemmelig nøkkelen, slik at begge kan kryptere og dekryptere meldinger. Ved hjelp av den symmetriske nøkkelen er det mulig å opprette en kryptert kanal for kommunikasjon, hvor uvedkommende ikke har tilgang, med mindre de finner ut hva den symmetriske nøkkelen er.



Figur 2 Symmetrisk kryptering og dekryptering av en melding ved bruk av samme symmetriske nøkkel.

Symmetrisk kryptografi bidrar til sikkerhetsmålet konfidensialitet, både for informasjon som overføres og informasjon som er lagret (Bergsjø & Windvik, 2020, s. 27). Det finnes to former for symmetrisk kryptografi - *block cipher* og *stream cipher* (Visma, 2020). Ved block cipher deles dataen som skal krypteres inn i like blokkstørrelser på 64 bits eller mer. Deretter kjøres en algoritme som krypterer hver blokk med krypteringsnøkkelen. Da krypteringen ikke skjer før man har nok data (bits) til å fylle en hel blokk, må data lagres i minnet før det kan krypteres. Stream cipher krypterer derimot byte for byte og er raskere enn den tidligere nevnte teknikken. Til forskjell fra block cipher trenger man ikke å lagre data i minnet før det krypteres.

Standardalgoritmen innenfor symmetrisk kryptering kalles for AES (Advanced Encryption Standard), og benyttes eksempelvis til kryptering av enkeltfiler eller harddisker. Denne algoritmen tar hele enheter med plaintext og omgjør til block ciphers bestående av en forhåndsbestemt mengde bits. Denne krypteringsalgoritmen kan brukes til å kryptere banktransaksjoner og personinformasjon som benyttes i helsevesenet, og er estimert å ta milliarder av år å knekke (Daniel, 2021). Årsaken til at det her benyttes symmetrisk kryptering er at denne typen krypteringsalgoritme er i stand til å kryptere svært store mengder data på kort tid, og de er noen av de tryggeste krypteringsalternativene som er tilgjengelig i dag. Som

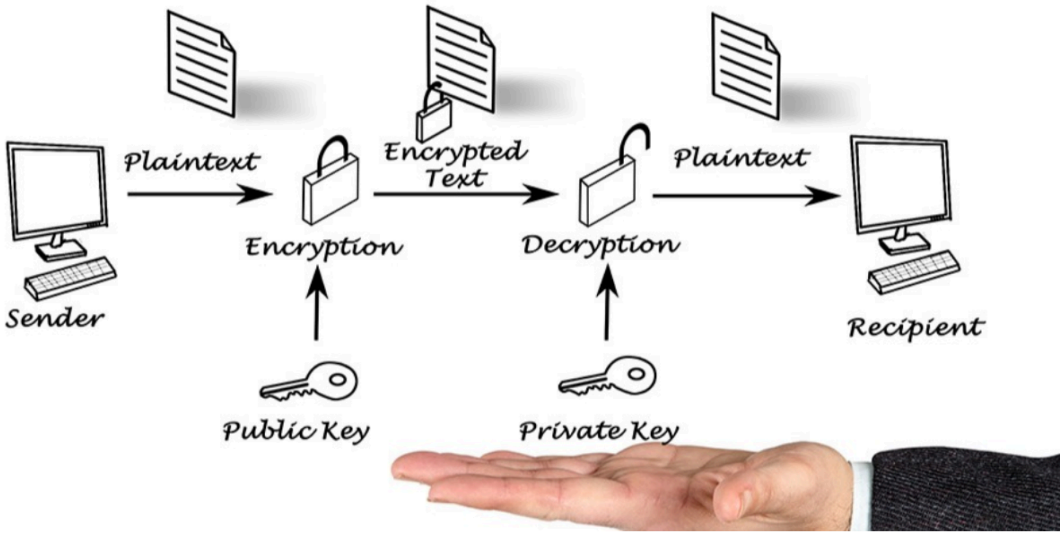
tidligere nevnt er det likevel en svakhet dersom uvedkommende får tilgang til nøkkelen, hvor informasjonen vil bli tilgjengelig for dem. Det er derfor viktig at nøkkelen distribueres og lagres på en trygg måte. Av andre symmetriske krypteringsalgoritmer finner vi Data Encryption Standard (DES), Enigma, RC4 og Cæsar.

Fordelen med symmetrisk kryptering er at det er veldig raskt og effektivt, og kan gjerne benyttes der kapasitet og effektivitet vurderes som et viktigere kriterium enn sikkerhet (Visma, 2020). Symmetriske krypteringsnøkler er som regel minst 128 bits lange og skal være praktisk umulig å gjette seg fram til. En symmetrisk kryptering er kun trygg så lenge ingen uvedkommende kjenner til den symmetriske krypteringsnøkkelen. Dette introduserer problemet med hvordan krypteringsnøkkelen skal distribueres med de relevante partene. Dersom denne nøkkelen distribueres uten kryptert forbindelse, kan uvedkommende få tak i nøkkelen og dermed få tilgang til den krypterte informasjonen. Tidligere brukte de ulike partene en liste over nøkler og når de skulle brukes. Disse listene ble distribuert fysisk og erstattet månedlig, men dersom uvedkommende fikk tilgang til listene ville kommunikasjonen ikke lenger være trygg. Symmetrisk kryptering sørger derfor ikke for autentisering av de involverte partene, og innebærer at partene må stole på at det kun er de tiltenkte partene som har tilgang til nøkkelen. I dag brukes asymmetriske krypteringsalgoritmer for å svare på denne problematikken (Bergsjø & Windvik, 2020, s. 27).

Asymmetrisk kryptering

Asymmetrisk kryptering, også kjent som Public Key kryptografi, innebærer at man benytter et nøkkelpar: én nøkkel for kryptering og en nøkkel for dekryptering. De blir omtalt som en privat nøkkel og en offentlig nøkkel, som har en gjensidig matematisk avhengighet (Datatilsynet, 2012). Den offentlige nøkkelen kan tilgjengeliggjøres for hvem som helst, og reduserer på denne måten problemet rundt nøkkeldistribusjon, som ofte er en utfordring ved bruk av symmetriske nøkler (Bergsjø & Windvik, 2020, s. 27). Den private nøkkelen er kun kjent av nøkkelens eier og må holdes hemmelig.

Asymmetrisk kryptering fungerer ved at både mottaker og avsender har hvert sitt nøkkelpar. Avsender benytter mottakers offentlige nøkkel til å kryptere en melding. Den krypterte meldingen sendes deretter til mottaker, som kan dekryptere meldingen med sin private nøkkel. Noe som krypteres med en offentlig nøkkel, kun kan dekrypteres med den tilhørende private nøkkelen, og vice versa. Figur 3 illustrerer hvordan asymmetrisk kryptering fungerer i praksis.



Figur 3 Asymmetrisk kryptering og dekryptering av en melding ved bruk av en offentlig og en privat nøkkel.

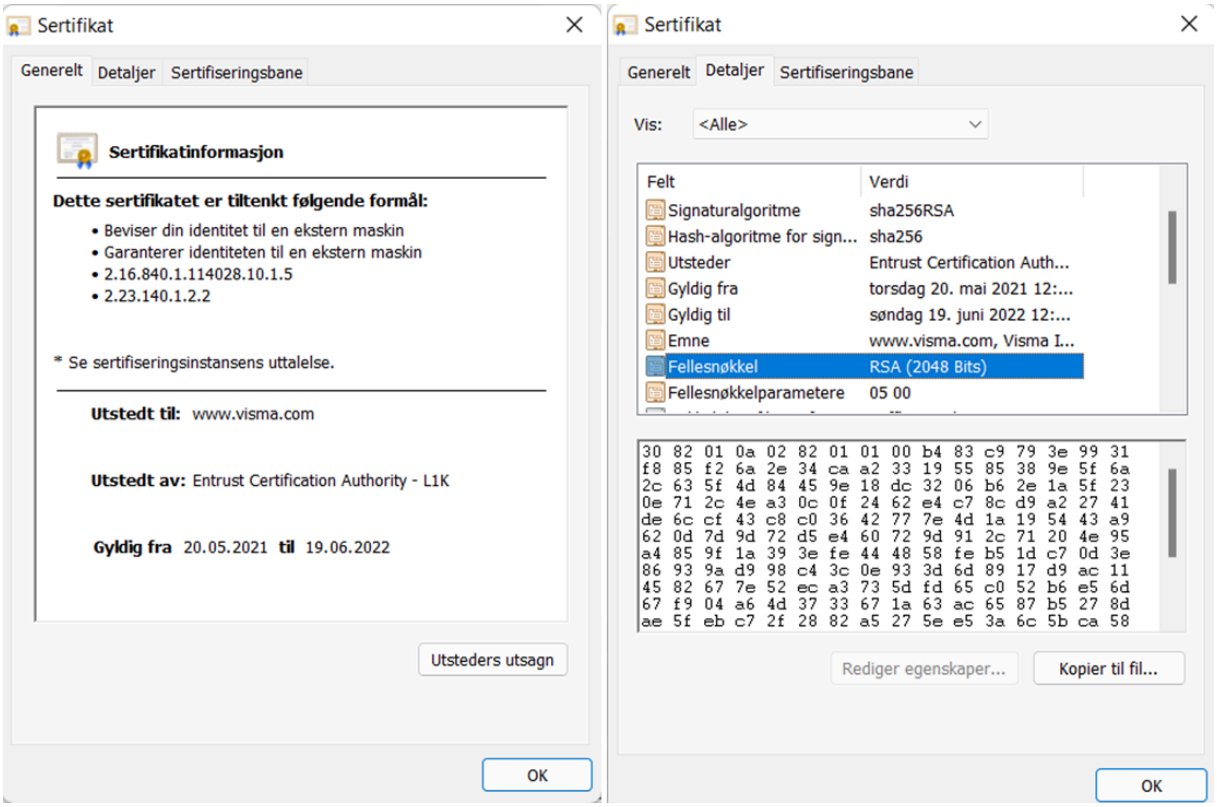
I tillegg til å bidra til informasjonens konfidensialitet, bidrar asymmetrisk kryptering til å autentisere de involverte partene gjennom digitale signaturer. Asymmetrisk kryptering brukes ved digitale signaturer, hvor målet er at brukere på Internett skal kunne signere en melding, noe som skal forsikre mottaker om identiteten til avsender og at meldingen ikke har blitt endret av uvedkommende (Visma, 2020). På denne måten bidrar asymmetrisk kryptering til sikkerhetsmålet integritet i tillegg til konfidensialitet og muliggjør autentisering mellom parter på Internett. Dette skjer ved at avsender bruker sin private nøkkel til å signere meldingen. Mottaker kan deretter bruke avsenders offentlige nøkkel for å bekrefte at meldingen er som den ble utformet av avsender og kommer fra personen avsenderen gir seg ut for å være.

Et eksempel på en slik algoritme er RSA (Rivest Shamir Adleman), der en offentlig nøkkel genereres ved å multiplisere to store primtall og ved å bruke de samme primtallene genereres en privat nøkkel (Daniel, 2021).

Den store utfordringen med bruk av asymmetriske nøkler er hastighet. Det kreves vesentlig større datakraft å kryptere store mengder data, og er i mange tilfeller for tidkrevende som resultat av lengre nøkler og mer komplekse matematiske utregninger. Årsaken til at nøklene krever mer komplekse beregninger, er fordi det skal være umulig å regne seg frem til den private nøkkelen basert på den offentlige nøkkelen til tross for at det er en matematisk sammenheng mellom de to (Daniel, 2021). Asymmetrisk kryptering vil derfor ikke være effektiv nok til å håndtere hyppige transaksjoner eller kryptering av større datamengder. Vi ser dermed at det er nødvendig å benytte de to grunnprinsippene i kombinasjon for å oppnå sikker tilstand.

Asymmetrisk kryptering har en rekke fordeler med tanke på økt funksjonalitet og sikkerhet, men har mindre kapasitet enn symmetrisk kryptering med hensyn til volum og hastighet. Det er derfor utbredt å benytte en kombinasjon av symmetriske- og asymmetriske nøkler ved kryptering av informasjon, noe vi kommer tilbake til senere i besvarelsen. I praksis er det

utbredt å kryptere meldinger og filer med symmetriske nøkler, mens nøkkelen for det symmetriske systemet blir beskyttet med et asymmetrisk system (SNL, 2021). Et eksempel på et slikt system er når man klikker seg inn på en nettside hvor URLen begynner med *https*. HTTPs angir at man ønsker kryptert kommunikasjon, her krever nettleseren at nettsiden har et SSL/TLS-sertifikat for sesjonen. Et slikt sertifikat er et dokument som utstedes av en virksomhet nettleseren din er satt opp til å stole på, og inneholder nøkler og annen informasjon som utsteder går god for ved å signere sertifikatet (Bergsjø & Windvik, 2020, s. 28). Figur 4 viser sertifikatet Visma har utstedt for et av gruppens medlemmer under en sesjon. Under fanen *Detaljer* finner du blant annet informasjon om den offentlige nøkkelen, her omtalt som *fellesnøkkel*, nøklenes varighet og krypteringsalgoritme. Nettsidens offentlige nøkkel blir deretter brukt til å bli enige om en symmetrisk nøkkel som benyttes for videre kryptert kommunikasjon.



Figur 4 Digital sertifikat.

Symmetrisk- og asymmetrisk kryptering i kombinasjon

Hybrid kryptering er en tilnærming til kryptering og dekryptering av data som fusjonerer anvendeligheten og sikkerheten ved asymmetrisk kryptering med effektiviteten og kapasiteten ved symmetrisk kryptering (Techopedia, 2022). For å løse utfordringene relatert til de to krypteringsmetodene er det vanlig å kombinere disse metodene ved transaksjoner over Internett. Vi vil først definere begrepet *sikker tilstand* og gi et eksempel på hvordan symmetrisk- og asymmetrisk kryptering kan benyttes i kombinasjon for å oppnå sikker tilstand.

Som vi nevnte i introduksjonen av denne øvingsoppgaven, handler sikkerhetsarbeidet i stor grad om tillit mellom ulike aktører som behandler digitale verktøy. For å oppnå tillit mellom partene, kan sikkerhet fungere som et fundament. For å utføre sikre transaksjoner på Internett, kreves det at de involverte partene autentiserer seg overfor hverandre og at det opprettes en sikker forbindelse mellom partene. Slike transaksjoner kan være innlogging på en nettbutikk, men kan også være transaksjoner i nettbanken. I slike tilfeller blir det derfor viktig å vite hvem den andre aktøren er, forsikre seg om deres identitet og videre opprette en sikker forbindelse før utveksling av informasjon skjer. En sikker forbindelse er en tilstand som kan endre seg, og for at den skal holdes sikker kreves en rekke sikkerhetstiltak. Denne tilstanden omtales som *sikker tilstand,* og innebærer typisk (Bergsjø & Windvik, 2020, s. 76):

1. At alle parter autentiseres ved hjelp av identifikatorer
2. Hovednøkkel for en sesjon – og nøkler utledet fra hovednøkkel
3. Nøklenes gyldighet er definert
4. Avtaler om hvilke kryptografiske algoritmer som benyttes

For å utnytte effektiviteten ved symmetrisk kryptering og sikkerheten til asymmetrisk kryptering, benyttes disse i kombinasjon ved etablering av sikker tilstand. På denne måten ivaretas sikkerhetsmålene konfidensialitet og integritet. Asymmetrisk kryptering benyttes i begynnelsen av transaksjonen for å etablere en sikker tilstand, og innebærer at partene autentiseres overfor hverandre som tidligere forklart. Når en sikker tilstand er etablert, utnyttes effektiviteten ved symmetriske nøkler. En symmetrisk krypteringsnøkkel blir opprettet og brukes til å kryptere informasjonen mellom partene.

Et eksempel på en slik kombinasjon er med bruk av VPN (Virtual Personal Network), hvor kommunikasjon mellom personlig datamaskin og VPN-tjeneren initieres ved bruk av asymmetrisk kryptering. Asymmetrisk kryptering brukes for å bli enige om en symmetrisk nøkkel som skal brukes til videre kommunikasjon. Sesjonsnøkkelen blir regenerert ofte for å øke kommunikasjonssikkerheten, uten at det gir forsinkelse i dataoverføringen. Det benyttes også en asymmetrisk krypteringsprotokoll kalt IKE (Internet Key Exchange) for å generere og administrere nøklene, og sørger for at brukerne i hver ende er enige om hvilke typer kryptering og autentiseringsprotokoller som skal benyttes (Itigic, 2021).

Som et eksempel på hvordan de to metodene kan benyttes for å oppnå sikker tilstand, tar vi for oss to aktører. **A** og **B** ønsker å kommunisere kryptert med hverandre over nettet. Aktørene ønsker ikke at en uvedkommende aktør **C**, skal ha mulighet til å 1) se innholdet i meldingene som utveksles, og 2) endre innholdet i meldingene som utveksles. For å få til dette benyttes både asymmetrisk- og symmetrisk kryptering.

- Begge aktørene produserer et asymmetrisk nøkkelpar. En offentlig nøkkel som kan distribueres til alle, inkludert aktør **C**, og en privat nøkkel som bare er kjent for aktøren selv.
- Aktør **A** og **B** blir enige om å benytte en felles symmetrisk nøkkel for videre kommunikasjon.

- **A** skriver en melding til **B** som inneholder den symmetriske nøkkelen, og krypterer denne med **B**´s offentlige nøkkel. I tillegg signerer **A** meldingen med en utregning som krypteres med **A**´s private nøkkel.
- **B** mottar meldingen og dekrypterer denne med egen private nøkkel, videre dekrypteres **A**´s signatur med **A**´s offentlige nøkkel, som er kjent for **B**.
- **B** kan signere neste melding med egen private nøkkel for at **A** skal få autorisert vedkommendes identitet i tillegg.
- Aktør **A** skriver en melding (plaintext) og krypterer denne (ciphertext) ved bruk av den symmetriske nøkkelen.
- Aktør **B** dekrypterer meldingen (ciphertext) med den symmetriske nøkkelen, og står igjen med en lesbar melding (plaintext) fra aktør **A**.

I dette tilfellet vil ikke aktør **C** ha mulighet til å dekryptere den første pakken, selv om han har tilgang på den offentlige nøkkelen til aktør **B**. Årsaken er at aktør **C** ikke har den riktige private nøkkelen, som kreves for å låse opp den første datapakken.

Her er sikker tilstand etablert mellom aktør **A** og **B**. Partene er autentisert og integriteten til meldingen som inneholdt den symmetriske nøkkelen ble sjekket ved hjelp av digital signatur. Kommunikasjonen kan deretter fortsette trygt med symmetrisk kryptering. De har på forhånd bestemt seg for hvilken krypteringsalgoritme som skal benyttes, og ut fra den blir nøklenes gyldighet utledet. Jo lenger slik kommunikasjon foregår ved bruk av samme symmetriske nøkkel, jo større skade kan det gjøre dersom uvedkommende finner ut hva nøkkelen er. Det vil derfor være et behov for et system som sikrer at nøklene endres regelmessig for å sikre konfidensialiteten til informasjonen. Når nøklene skal byttes ut vil variere mellom protokollene som benyttes for kryptering (Bergsjø & Windvik, 2020, s. 76).

Referanser

Bergsjø, H., & Windvik, R. (2020). I *Digital sikkerhet - En innføring.* Universitetsforlaget.

Datatilsynet. (2012, Januar 24). *Kryptering*. https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/kryptering/

Itigic. (2021, Januar 15). *Hva er IPSec, en protokoll for VPN med bedre sikkerhet og hvordan det fungerer*. https://itigic.com/no/ipsec-protocol-for-vpn-with-better-security-how-it-works/

SNL. (2021, Mars 5). *Asymmetrisk kryptografi*. https://snl.no/asymmetrisk_kryptografi

Techopedia. (2022, Januar 20). *Hybrid Encryption*. https://www.techopedia.com/definition/1779/hybrid-encryption

Visma. (2020, Oktober 19). *Krypto 101: Hva er det og eksempler på gode kryptoløsninger*. https://www.visma.no/blogg/krypto-og-eksempler-kryptolosninger/

Daniel, B. (2021, Mai 4). *Symmetric vs. Asymmetric Encryption: What's the Difference?*. https://www.trentonsystems.com/blog/symmetric-vs-asymmetric-encryption

Øving 3 - Overvåking og personvern

Denne besvarelsen tar for seg overvåking og personvern. Overvåking er et omfattende begrep i dagens digitale samfunn, hvor borgere blir sporet ved hjelp av ulik teknologi av aktører fra individ- til myndighetsnivå. Denne overvåkingen har skapt stor debatt, hvor mange ikke har noe imot at informasjon samles inn og ser det som et tryggende tiltak. Den andre siden av debatten mener den omfattende overvåkingen er inngripende og går ut over privatlivets fred. Vi vil i denne besvarelsen trekke inn relevante lover og forskrifter samt belyse hvordan disse er utviklet for å regulere den digitale utviklingen, både for å beskytte individets rettigheter og samfunnets trygghet.

Gjør rede for hvordan norske borgere overvåkes nå i år 2020/2021. Hva slags teknologi finnes? Hvordan kan den brukes? Hvem står bak?

I denne delen av oppgaven skal vi se på hvordan norske borgere overvåkes med bruk av ulike teknologier og hvilke aktører som gjennomfører innsamling av informasjon. Vi vil innlede med å belyse hvordan overvåkingen foregår på et overordnet nivå, før vi ser nærmere på hvilken teknologi som benyttes. Til slutt vil vi redegjøre for hvilke aktører som overvåker på ulike måter.

Overvåking

Som vi vil komme frem til senere i oppgaven er det blitt opparbeidet en høy grad av tillit mellom myndigheter og befolkning i Norge. Denne tilliten vil spre seg gjennom flere lag i samfunnet, og i form av et fungerende demokratisk system vil tillit mellom ulike samfunnslag også være høy. Vi har mange legitime aktører som oppbevarer store mengder personopplysninger og som følger med på hva vi foretar oss både fysisk og digitalt. Personopplysningsvern er derfor essensielt, og handler om vern av vår personlige integritet gjennom behandling av opplysninger om oss, både autorisert og uautorisert (Bergsjø & Windvik, 2020, s. 113).

Samfunnet overvåkes i mange ulike kanaler, og det vil i dagens samfunn være svært vanskelig å bevege seg anonymt, enten man snakker om det offentlige, private eller det digitale rom. Den høye graden av overvåking legger til rette for misbruk av informasjon, som stiller høye krav til reguleringer. Reguleringene skal ivareta individets rettigheter når det kommer til innhenting og behandling av personopplysninger. I tillegg vil en viss grad av overvåking være nødvendig for å beskytte samfunnets verdier. I den sammenheng vil personvernloven, personvernforordningen og sikkerhetsloven ivareta disse interessene, og ansvarliggjør de virksomheter, myndigheter eller andre organer som behandler personinformasjon eller driver andre former for overvåking (Bergsjø & Windvik, 2020, s. 111). Vi kommer videre i denne besvarelsen til å jobbe oss nedover fra overvåking på myndighetsnivå til overvåking i private hjem.

Borgere i det norske samfunnet overvåkes av myndighetene og de organene som skal sikre nasjonal sikkerhet og drive forebyggende sikkerhetsarbeid mot trusler som ekstremistiske miljøer og terror. Denne overvåkingen foregår gjerne i flere kanaler. Søkehistorikk er kanskje det de fleste av oss assosierer med slik overvåking. Internett inneholder enorme mengder informasjon og kommunikasjonskanaler, som gjør at man kan kommunisere med tilnærmet

hvem som helst, hvor som helst. Det store informasjonstilfanget muliggjør også innhenting av informasjon av den enkelte, hvor regjeringen oppgir at over halvparten av barn og unge mellom 9 og 18 bruker Internett daglig til å søke opp informasjon (Regjeringen, u.å.).

Den økte digitaliseringen og det enorme informasjonstilfanget dette medfører har lagt grunnlaget for ny lov om digital overvåking, som åpner for at myndighetene kan overvåke all grenseoverskridende kommunikasjon og lagre metadata i opptil 18 måneder (Døvik, 2020). Metadata er «data om data, informasjon som beskriver annen informasjon», og omhandler ikke selve innholdet i kommunikasjonen (Gjersdal & Heine Natt, 2022). Informasjon om hvem som kommuniserer til hvilken tid og geolokalisering er eksempler på data som overvåkes og lagres. Det innebærer i praksis mesteparten av det som foregår på sosiale medier og nettbasert kommunikasjon, da informasjonen ofte lagres i utlandet. Den nye loven byr på nye utfordringer, da det i praksis innebærer en potensiell masseovervåking av norske borgere. I tillegg er det på myndighetsnivå mulig for politiet å ta seg inn på personlige digitale verktøy for kommunikasjon for total overvåking så lenge de har skjellig grunn til mistanke (Straffeprosessloven, 2021, §16).

Det foregår også overvåking under myndighetsnivå basert på regulatoriske krav pålagt private aktører. Overvåking av regulatoriske hensyn, som ikke foregår på myndighetsnivå, foregår eksempelvis blant finansielle aktører. Alle banker, kredittforetak eller juridiske personer spesifisert i lovverket er i Norge underlagt lov om hvitvasking og terrorfinansiering. Dette omfatter blant annet kapittel om løpende kundeoppfølging, hvilket stiller krav til at rapporteringspliktig må ha en risikobasert løpende kundekontroll (Hvitvaskingsloven, 2021, § 9-28). Loven plikter med andre ord disse aktørene til å overvåke sine kunder basert på egen forståelse av risiko for hvitvasking og terrorfinansiering. I praksis betyr det at alle transaksjoner potensielt overvåkes, noe som kan fortelle både om hva man bruker penger på og hvor man befinner seg på transaksjonstidspunktet. Disse aktørene må naturligvis i tillegg forholde seg til sikkerhetsloven og personvernforordningen, noe som stiller høye krav til god risikoforståelse og balansegang mellom å ivareta hensyn regulert i hvitvaskingsloven samtidig som man skal ta hensyn til kunders personvern og nasjonale sikkerhetshensyn.

Selv om overvåking som diskutert i foregående avsnitt ikke nødvendigvis er et nytt fenomen, er kravene til behandlingsansvarlige skjerpet betraktelig. Tidligere lovgivning knyttet til personvern har vært svært detaljert med beskrivelser over hvordan de behandlingsansvarlige skulle gå frem for å ivareta kundenes personvern. Den nye personvernforordningen som trådte i kraft i 2018 gir mer overordnede og generelle retningslinjer og legger dermed ansvaret mer over på den enkelte aktør (Bergsjø & Windvik, 2020, s. 110).

Et av de mest grunnleggende kravene til digital sikkerhet er kravet til risikostyring, eller proporsjonal sikring av opplysninger. Opplysningene eller systemet skal sikres i tråd med de verdier som forvaltes (Bergsjø & Windvik, 2020, s. 121). Samtidig skal den sørge for at man ikke gjennomfører mer inngripende tiltak hos den private person enn hva som er nødvendig for å innfri formålet (Personopplysningsloven, 2022, art. 5.1.b/c). Det innebærer eksempelvis at finansielle aktører må vurdere egne verdier, samt hvilke tiltak de anser som nødvendig for å trygge disse verdiene. Virksomhetens ledelse og styre vil i henhold til den nye lovgivningen kunne holdes personlig ansvarlig dersom man ikke behandler opplysninger på en forsvarlig

måte, noe som forutsetter at ledelsen er involvert i sikkerhetsarbeidet fra beslutning til implementering og revidering (Bergsjø & Windvik, 2020, s. 113).

Ofte oppstår det vanskelige problemstillinger knyttet til digital overvåking og reguleringene. Det vil hele tiden være en balansegang mellom å trygge verdier og ivaretakelse av individers personvern. Det er i dag svært lite kostbart å lagre informasjon så lenge man måtte ønsker, og det finnes svært mange informasjonskilder å hente slik informasjon fra (Bergsjø & Windvik, 2020, s. 87). Teknologi invaderer ikke personvernet i seg selv, men det er bruken av teknologien som gjør at personvernet kan være truet. Det er her lovgivningen kommer inn og regulerer bruken, eksempelvis hvor lenge informasjon kan lagres.

Overvåking som ikke er pålagt juridiske personer, men som foregår basert på inntjeningspotensial er en annen overvåking norske borgere utsettes for. Slik overvåking går ut på å kartlegge en målgruppes aktivitet på kommersielle nettsteder for å kunne tilpasse markedsføringen. Denne overvåkingen er noe vi godtar fortløpende ved å godta bruk av *informasjonskapsler*, noe vi kommer tilbake til senere i oppgaven. Denne type overvåking legger til rette for at informasjon om vår bruks- og kjøpsatferd innhentes, lagres og spres mellom aktører. Selv om enkeltstående personopplysninger ikke oppfattes som særlig inngripende i vårt privatliv, vil det kunne defineres som mer inngripende jo mer opplysninger som lagres, kombineres og distribueres.

Til slutt vil vi trekke frem overvåking som skjer i det offentlige og private rom i form av kameraer eller sensorer. Både offentlige myndigheter, private virksomheter og individer har overvåkingskameraer i ulike former. Slik overvåking muliggjør en kartlegging av personers bevegelsesmønster og kan lagres i en gitt tidsperiode. Denne tidsperioden avhenger av hva man kan dokumentere som nødvendig. Selv om tommelfingerregelen er syv dager lagring før sletting, kan man oppbevare opptak lengre enn dette dersom gyldig årsak dokumenteres (Datatilsynet, 2022).

Bruk av ulike typer teknologier

Informasjonskapsler

First-party cookies

Informasjonskapsler er noe nesten alle i dagens samfunn er kjent med, og er et mye debattert tema grunnet sin tilknytning til digitalt personvern. Informasjonskapsler er identifikatorer, med andre ord personopplysninger, som en bruker legger igjen i nettleseren når en surfer på nettet (Bergsjø & Windvik, 2020, s. 88). Denne informasjonen kan hentes igjen på et senere tidspunkt av nettstedet du har besøkt, og muliggjør en bedre kundeopplevelse. Denne formen for informasjonskapsler anses som *first-party cookies,* da disse informasjonskapslene benyttes på et domene og ikke deles med andre nettsider eller annonsepartnere (Mcguane, 2022).

Informasjonen kan i mange tilfeller benyttes til et slikt formål som er hensiktsmessig for brukeren. *First-Party cookies* bedrer blant annet kundeopplevelsen gjennom lagring av passord slik at en bruker ikke trenger å logge inn på nytt hver gang den besøker nettsiden. Informasjonskapslene brukes også til andre formål enn å bedre kundeopplevelsen, da en

aktør gjennom å kartlegge en brukers atferd på sin nettside vil tilegne seg nyttig informasjon. Informasjon som hvor ofte brukeren besøker nettsiden, hvordan brukeren navigerer på nettsiden og hvilken informasjon brukeren er mest interessert i, er data som kan ha stor nytteverdi for nettsiden i deres markedsføring. Ved å utnytte denne informasjonen kan nettsiden skreddersy visning av informasjon og tilpasse innhold for å øke sannsynligheten for klikk eller kjøp av produkter aktøren tilbyr.

Tredjepartscookies

Den største utfordringen med informasjonskapsler og personvern er med såkalte *tredjepartscookies*. Tredjepartscookies muliggjør sporing av en bruker på tvers av nettsider (Bergsjø & Windvik, 2020, s. 89). Dataene som genereres, kan i langt større grad si noe om en brukers atferd på Internett, og ikke bare på en spesifikk nettside. Denne informasjonen er ikke nødvendigvis mer sensitiv enn informasjonskapsler man legger igjen på én enkelt nettside, men muligheten for misbruk er større når opplysningene kombineres. Når man besøker en tilfeldig norsk nettavis har datatilsynet funnet ut det gjennomsnittlig vil være 43 selskaper med ulike sporingsverktøy på siden (Datatilsynet, 2015). Virksomheter kan ha stor interesse av å samle inn så mye data som mulig om forbrukere, da de bruker dataen til å bygge personprofiler som igjen forbedrer egne evner knyttet til salg og markedsføring. Virksomheter konkurrerer om å lage de mest omfattende profilene på forbrukerne sine og det er dette Datatilsynet kaller for “Det store datakappløpet” (Datatilsynet, 2015).

Aktører som benytter seg av tredjepartscookies plasserer annonser på ulike nettsider og samler inn informasjon som sier noe om et individs digitale brukeratferd (Bergsjø & Windvik, 2020, s. 89). Rent praktisk fungerer det slik at en annonsør plasserer en annonse på en annen aktørs nettside. I det forbrukeren går inn på nettsiden hvor annonsen ligger, og forutsatt at brukeren har godtatt bruk av cookies, får tredjeparten tilgang til informasjon på lik linje med eieren av nettsiden hva angår brukeratferd. Dette muliggjør en bredere innhenting av informasjon som gjør kommersielle aktører i stand til å tilpasse markedsføringen til det neste nettstedet brukeren besøker. Denne prosessen fortsetter og gir en forklaring på hvorfor man får opp annonser for produkter man har vist interesse for på et nettsted, i helt andre sammenhenger på internettet.

Biometrisk informasjon

Biometrisk informasjon er en annen kilde til personopplysninger som veldig mange er berørt av. Denne dataen kan brukes til identifisering og kobling av data mot et spesifikt individ (Bergsjø & Windvik, 2020, s. 91). Slike personopplysninger faller under *særlige kategorier personopplysninger*, og er opplysninger som kan si så mye om oss som individer at de i utgangspunktet ikke er tillatt å behandle (Bergsjø & Windvik, 2020, s. 113). Det fins imidlertid unntak fra denne regelen.

Ansiktsgjenkjenning og fingeravtrykk er teknologi som er innebygd i mange av smartenhetene vi bruker, slik som PC og mobil. Ansiktsgjenkjenning vil medføre at personer gjenkjennes i videoovervåkede områder, hvor man kan kartlegge hvilke aktiviteter man bedriver. Finger- og øyeavtrykk er informasjon som tradisjonelt har blitt brukt til identifisering av personer i forbindelse med passkontroll og lignende. I dagens digitaliserte

samfunn brukes denne informasjonen stadig mindre kritisk, eksempelvis ved innlogging på elektroniske enheter slik som telefon, datamaskin, nettbrett etc. Denne utviklingen medfører at store deler av vår biometrisk informasjon er lagret hos kommersielle aktører, noe som stiller høyere krav til dere behandling av personinformasjon.

Overvåking via kamera

Overvåking via kamera er en teknologi som har vært i bruk over en lengre periode, og er ikke et nytt fenomen. I Norge lagres denne informasjonen i en kortere periode, ofte bare opp til syv dager (Bergsjø & Windvik, 2020, s. 92). Slik informasjon tar også opp betydelig større lagringsplass enn eksempelvis informasjonskapsler, og er også en faktor for hvor mye data det vil være hensiktsmessig å lagre. Kjøpesentre, bedrifter med skjermingsverdig informasjon og objekter man ønsker å sikre, er eksempler på aktører som benytter seg av overvåking via kamera. Det er også de siste årene blitt mer vanlig for den enkelte husstand og gå til innkjøp av slik teknologi, og kan benyttes både til hjemmet og i form av et dashbordkamera til biler. Dette belyser nye utfordringer, når enkeltpersoner potensielt kan forvalte personopplysninger om andre, ofte helt uvitende om hvilken informasjon man egentlig har samlet inn. Kravene for å følge lover og regler må i slike tilfeller også følges av enkeltpersoner, og ikke bare større organisasjoner som bevisst samler inn personopplysninger om individer. Dette medfører i våre øyne en økt risiko for misbruk, da de færreste er godt kjent med de ulike regelverkene.

Smarttelefon

Mye av informasjonen som blir samlet inn gjennom ovennevnte teknologiene, har blitt enda mer knyttet til enkeltindivider grunnet utviklingen av smarttelefoner (Bergsjø & Windvik, 2020, s. 94). Smarttelefoner inneholder informasjon om hvilke apper vi bruker, hvor mye vi bruker appene, hvilke interesser vi har, posisjonsdata, biometrisk informasjon etc. Smarttelefonen knytter de aller fleste teknologier sammen, og muliggjør massiv innhenting av personlig informasjon. I tillegg til å være et verktøy som kan samle mye personlig data, er vi som forbrukere for naive knyttet vår personlig data. Vi har ofte et ukritisk syn på de ulike appene vi laster ned, og godkjenner bruksvilkår uten å egentlig tenke over hva vi har sagt ja til. Vi som forbrukere har vane for å tenke at informasjonen vi gir fra oss ikke er så verdifull, og heller ikke farlig å gi fra seg, noe som ikke stemmer i realiteten. Datatilsynet advarer mot dette, ved at man gir appansvarlig tilgang til alt du har på telefonen din, inkludert kontaktliste, sensorer, kamera osv. (Datatilsynet, 2018). Det er viktig at forbrukere i den forbindelse setter seg inn i hvilke rettigheter man gir applikasjoner, i tillegg til at gjeldende lovverk regulerer applikasjonen bruk av personinformasjon.

Personvern tilknyttet informasjonskapsler

Den digitale utviklingen i samfunnet tilrettelegger for massiv innhenting av personlig data gjennom blant annet informasjonskapsler og biometrisk informasjon som beskrevet tidligere, og for å håndtere denne utviklingen er det kommet på plass diverse regulatoriske krav for å sikre personvern og anonymitet. Bruken av informasjonskapsler kan være inngripende på personvernet og det er sentralt å forstå viktigheten av hvilke regler som gjelder for bruk av denne dataen for å forstå hvilke rettigheter man har. Bruken skal være i tråd med §102 i

grunnloven, som sier *«Alle har rett til respekt for privatlivet og familielivet sitt, for heimen sin og kommunikasjonen sin. Det må ikkje utførast husransakingar, så nær som i kriminelle tilfelle.»* (Kongeriket Noregs Grunnlov, 2020, §102).

Dagens lovverk er som tidligere nevnt generelt og overordnet for å veie opp for at man ikke er i stand til å utvikle reguleringer i samme tempo som den digitale utviklingen. Denne ansvarliggjøringen forutsetter en bevisstgjøring og ledelsesforankring blant de som behandler personopplysninger, men risiko for misbruk og mistolkning vil også oppstå. Når det er opp til hver enkelt aktør å tolke lovverket, vil det kunne oppstå situasjoner hvor man ikke behandler opplysningene ideelt, og risiko for sikkerhetshendelser øker. Manglende ressurser hos mindre aktører kan medføre at risikovurderingen som gjennomføres ikke er tilstrekkelig. Det foreligger også fortsatt en risiko for å finne og utnytte eventuelle smutthull med implementering av ny teknologi. Informasjonskapsler var et eksempel på dette. For å øke brukerforståelsen om lagring av informasjon på Internett, ble det i 2019 vedtatt lov vedrørende aktiv samtykke til informasjonskapsler i EU-Land, gjennom den såkalte Planet 49-dommen (Datatilsynet, 2019). Før denne loven trådte i kraft var det en innstilling i nettleseren som bestemte om man samtykket til informasjonskapsler eller ikke, hvor det i dag er krav om aktiv samtykke for hver nettside man besøker.

Aktører som lagrer informasjon om forbrukere, må også i henhold til nytt lovverk være mer transparent enn tidligere. Prinsipp om lovlighet, rettferdighet og åpenhet fastsetter at behandlingsansvarlige skal kommunisere at det behandles data om et individ, hvordan denne behandles i tillegg til hva den brukes til (Bergsjø & Windvik, 2020, s. 115). Personvernforordningen trekker også denne transparente modellen enda lengre ved å gi forbrukerne rett til å bli glemt (Personopplysningsloven, 2022, art. 17). Dette stiller høye krav til lagringspolicy hos behandlingsansvarlig. Forordningen stiller også krav til at behandlingsansvarlig gjennomfører *"egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med denne forordning"* (artikkel 24 nr. 1). Det må med andre ord etableres systemer hvor personopplysninger kan forvaltes sikkert. Dersom en kunde ønsker å få alle opplysninger lagret om seg slettet, forutsetter det at virksomheten har kontroll over hvor informasjonen er lagret. Et stort problem her er lokal lagring hos virksomhetens ansatte, hvor det vil være tilnærmet umulig å spore lagringsstedet. For å unngå denne problemstillingen tas løsninger for mer global lagring i bruk. Dette kan eksempelvis være skyløsninger eller samarbeidsplattformer slik som SharePoint, noe som skaper nye problemstillinger. For skyløsninger er det viktig at sikkerheten ivaretas godt nok hos tilbyder, noe som er vanskelig å kontrollere og som virksomheten må følge godt med på. For samarbeidsplattformer slik som SharePoint stiller det høye krav til tilgangsstyring slik at ansatte som ikke har tjenstlig behov for tilgang til informasjonen, ikke får innsyn samtidig som informasjonen er tilgjengelig for de som trenger det. Her ser vi hvordan disse problemstillingene fører til utfordringer med tanke på å ivareta sikkerhetsmål om konfidensialitet, integritet og tilgjengelighet.

Dette er et steg i riktig retning hva gjelder personvern. De største selskapene i verden, som for eksempel Google og Facebook, har mye personlig informasjon om forbrukere. Uten regulerende lovverk kunne denne bruken fortsatt å eskalere ut av alle proporsjoner. Data

gjennom tredjepartscookies gjør de i stand til å eksempelvis danne et bilde over hvilke politisk parti du støtter, eller hvilken legning du har (Hill, 2015). Slik data faller under særlige kategorier i personvernlovgivningen, noe som viser viktigheten av å kunne slette sin personlige data knyttet til tredjepartscookies (Datatilsynet, 2019).

Enkelte hevder at man kan avverge og oppklare flere alvorlige kriminelle handlinger gjennom økt offentlig overvåking, og at dette er en pris vi som samfunn bør være villige til å betale. De hevder så at dersom man ikke har noe å skjule, så har man heller ikke noe å frykte. Gjør rede for deres synspunkter og argumenter.

Argumenter for overvåking

Det fins en rekke lover og regler som skal verne om ulike verdier, alt fra individets sikkerhets og integritet til samfunnets suverenitet og sikkerhet. Utfordringen oppstår når man skal balansere disse verdiene opp mot hverandre, hvor det ofte vil oppstå spenninger mellom de ulike behovene (Bergsjø & Windvik, 2020, s. 110-111). Hva veier tyngst av individets integritet og samfunnets sikkerhet? I dette avsnittet skal vi se på de som mener det sistnevnte – hvor samfunnets sikkerhet og fellesskapet er det viktigste.

Offentlig overvåking for samfunnets beste

Offentlig overvåking knyttes ofte opp mot temaer som terrorisme og kriminalitet. Terrorhendelser har tidligere vært en akselerator for debatt og lovgiving rundt offentlig overvåking, og er noe som ofte trer frem i mediebildet ved slike hendelser. Datatilsynet skriver blant annet på sine nettsider "*Det har vært en klar fremvekst av internasjonal og nasjonal lovgivning som har til formål å bekjempe og avdekke terrorhandlinger.*" (Datatilsynet, 7. mars 2018). Forkjempere for omfattende overvåking argumenterer for at økt mengde data gir bedre mulighet for å avdekke individer som utgjør en trussel, og at man i større grad kan forebygge uønskede hendelser. I tillegg argumenteres det for at overvåking er den beste og enkleste metoden å beskytte innbyggerne på. Andre metoder som avhør og infiltrering av målgrupper er ikke effektive nok.

Et annet argument som trekkes frem handler om at målet helliger middelet. Her argumenteres det for å oppgi en del av privatlivet gjennom overvåking, og at det rettferdiggjøres dersom det bidrar til å opprettholde et trygt samfunn og forebygge farlige hendelser. Overvåkingen i denne konteksten handler som regel om digital overvåking av personlige telefoner og nettrafikk. I etterkant av skytingen i San Bernardino som drepte 14 personer i 2016, ville FBI at Apple skulle lage en bakdør til IPhone (Nakashima, 2016). Argumentasjonen fra FBI var at dette ville gjøre dem i stand til å hente ut avgjørende bevis fra telefonen. Apple avslo forespørselen på grunnlaget av sikkerheten til alle andre IPhone brukere.

I tillegg til argumenter om økt overvåking med hensikt om å trygge samfunnets verdier, argumenteres det for at teknologi kan redde liv på andre måter. I denne sammenheng argumenteres det for hvordan teknologi kan bidra til tryggere omgivelser i hverdagen, hvor man fokuserer på de positive gevinstene ved implementering av ny teknologi. Volvo

planlegger eksempelvis å installere kupékameraer og andre sensorer som overvåker sjåføren under kjøring for å forhindre ulykker (Tørdal, 2019).

Grunnlag for personlig inngripen

I juni 2016 ble det for Politiet mulig å ta seg inn på personlige datamaskiner, telefoner og nettbrett for å kunne lese alt som blir og skrevet (Straffeprosessloven, 2021, §16). Forutsetningen for en slik personlig inngripen, er at det foreligger grunnlag for å gjennomføre overvåkingen, basert på bevis som tilsier at vedkommende har noe å skjule. Dette er i henhold til det første prinsippet innenfor personvernforordningen, og et eksempel på hvordan Politiet forholder seg til de regulative lovverkene. En slik handling er å anse som en alvorlig inngripen i et individs privatliv, og regnes av flere som en *nødvendighet* for samfunnets sikkerhet. Dette er et eksempel på en situasjon hvor man setter samfunnets sikkerhet foran individets rett til frihet, og er et av mange eksempler. Aktørene man ofte tenker på i slike tilfeller er Politiet og Forsvaret, som er de fremste organisasjonene som skal sørge for rikets sikkerhet, og har derfor ulike behov enn andre aktører. Det er likevel flere aktører som har behov for overvåking relatert til sikkerhetsarbeid, hvor fellesnevneren synes å være et økt fokus på det forebyggende arbeidet.

Ved å overvåke individer og grupper av personer, vil sannsynligheten for å avdekke avvik og unormal oppførsel være større, og det vil dermed være enklere å kunne avverge en potensiell sikkerhetstrussel før den oppstår. Et eksempel på dette som vi tidligere har trukket frem, er hvordan juridiske aktører i det finansielle markedet som i henhold til hvitvaskingsloven er pliktig til å drive en viss grad av overvåking, samtidig som man skal forholde seg til personvernhensyn. Overvåking som et tiltak for å opprettholde sikkerhet, avverge og oppklare flere alvorlige kriminelle handlinger, anses også som ressursbesparende da det i stor grad er mulig å automatisere gjennomgangen av data. I stedet for å benytte dedikert personell til å oppnå den samme situasjonsforståelsen, benyttes teknologi, algoritmer og kunstig intelligens for å avdekke såkalte røde flagg. Ved kombinasjon av ulike former for overvåking, som for eksempel overvåking via kamera og en database for ansiktsgjenkjenning, vil man effektivt kunne sette opp et system som sender ut et varsel ved treff på mistenksomme og kjente personer.

Overvåking

Som tidligere nevnt er kameraovervåking på offentlige plasser et hett tema i debatten om digital overvåking. Argumentasjonen taler for at kameraovervåking skaper mer trygghet for alle innbyggere, og fungerer både forebyggende og operativt (Li, 2021). Kameraovervåkingen hjelper ved at man har enklere tilgang på konkrete bevis ved hendelser, og at det dermed blir enklere og få kriminelle handlinger dømt. I tillegg hevdes det at synlige overvåkingskameraer i seg selv har en forebyggende effekt, og at det er mindre sannsynligheten for at en kriminell handling skjer i det aktuelle området kun fordi det er et kamera til stede.

Hvor det tidligere var mulig å patruljere gatene og ha kjennskap til visse miljøer gjennom innsideinformasjon, er det ikke lengre like enkelt å oppnå denne situasjonsforståelsen. Teknologisk utvikling med informasjonsutveksling i digitale medier i sanntid, ofte på tvers av landegrenser, har ikke de sikkerhetsansvarlige mulighet til å forstå dagens sikkerhetssituasjon

med mindre de tilpasser metodene sine. Slik som en tjenesteytende bedrift må tilpasse sine verktøy og virkemidler for å få solgt sine tjenester, må også en aktør som skal sørge for samfunnets sikkerhet tilpasse seg dagens situasjon. Det er derfor et helt naturlig tiltak å øke den offentlige overvåkingen.

Oppsummering

Det er bred enighet om at overvåking er viktig, og at tanken i seg selv er god. Vi ønsker alle et fredelig land, og økt overvåking er et tiltak flere mener kan bidra til dette målet og dermed prisen vi må betale. De aller fleste i et samfunn utviser atferd i tråd med samfunnets lover, normer og generelle oppfatninger om hva som er riktig å gjøre. Disse individene og gruppene har ikke informasjon, som potensielt kan utgjøre en sikkerhetstrussel, å skjule - og er dermed ikke en aktør det vil være interessant å drive spesifikk innhenting mot. Det er derimot individene og gruppene som ikke handler i tråd med disse lovene, normene og generelle oppfatningene, som utgjør en potensiell risiko og som derfor vil være aktuelle å holde et ekstra øye med.

En rekke individer og interesseorganisasjoner ønsker å begrense slik overvåking (som beskrevet i deloppgave a) av personvernhensyn. Gjør rede for deres synspunkter og argumenter.

Argumenter mot overvåking

En generell mening blant aktører som ønsker å begrense overvåking av personvernhensyn, er at man i stor grad gir avkall på vår frihet ved økt overvåking. I den europeiske menneskerettskonvensjonen står det «Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse» (ECHR, 2021, s. 7). For personer med lavere grad av tillit til myndighetene, vil overvåking av enkeltpersoner anses som en stor inngripen i ens personlige privat- og familieliv. Personvernet er et av de mest grunnleggende prinsippene i rettsstaten, noe som har kommet tydelig frem gjennom den nye personopplysningsloven som ble vedtatt i 2018. Loven regulerer behandling av personvernopplysninger og er ment for å beskytte individets sikkerhet og integritet gjennom å gi føringer for hvordan disse opplysningene kan og skal behandles (Bergsjø & Windvik, 2020, s. 112).

Ifølge professor Alexander Cappelen ved Norges Handelshøyskole ligger Norge på topp i verden når det gjelder tillit, og han fremhever at vi som samfunn sparer enorme summer på grunn av det (Brenna, 2015). Det norske samfunnet er altså tuftet på en gjensidig tillit mellom borgere og myndighet, og anses vil kunne føre til bedre samarbeid og redusere behovet for dyre kontrolltiltak. Overvåking anses som en av de største truslene mot den tilliten vi gjennom flerfoldige år har bygget opp, og er et ressurskrevende kontrolltiltak. Det er en generell oppfatning blant de som ønsker å begrense overvåking at myndighetene ikke stoler på innbyggerne sine, hvor de ser seg nødt til å overvåke alle og enhver i tilfelle de på et senere tidspunkt gjør noe galt (Mathisen, 2020). Det grunnleggende rettsprinsippet om at man er uskyldig inntil det motsatte er bevist, blir utfordret av den digitale overvåkingen, hvor man nå blir behandlet som mistenkt.

Dette fører oss videre til den neste utfordringen. Ethvert tiltak fører til et mottiltak, som i dette tilfellet vil være å beskytte seg bedre. Den enkelte innbygger som føler en invasjon av sitt privatliv vil forsøke å sikre seg bedre gjennom bedre sikkerhetstiltak, som vil kreve enda mer avanserte metoder fra myndighetenes side. Dette fører til en ond sirkel hvor man over tid gradvis vil bryte ned den tilliten som en gang var så god mellom stat og innbygger. Denne utfordringen gjelder også for andre aktører, hvor selskapet Cambridge Analytica (CA) ble beskyldt for å påvirke valgkampanjer ved bruk av data mining og dataanalyse med strategisk kommunikasjon (Wikipedia, 2021). Overvåking og innsamling av personopplysninger uten deres samtykke var for mange deres største overtramp, og en slik offentliggjøring vil kunne skade folks tillit til noe så grunnleggende i et demokratisk samfunn, som et fritt valg.

En slik overvåking vil føre til at folk legger bånd på seg selv og blir mer forsiktige i sin opptreden i det offentlige rom. Meninger blir fort undertrykt fordi man ikke vet hvem som lytter på, og kan virke som en trussel mot ytringsfriheten i vårt demokratiske samfunn. Som vi også har vært inne på, vil en slik overvåking kunne få økonomiske konsekvenser for et samfunn. Overvåking i seg selv er en ressurskrevende prosess, og den misbrukte tilliten til offentlige myndigheter og private tjenesteleverandører vil kunne føre til økt skepsis i handel med disse. Hvem har vel ikke tenkt seg om en gang eller to før man går til innkjøp av en kinesisk produsert mobiltelefon, etter det er blitt kjent at den kinesiske stat samler inn informasjon fra alle kinesisk eide selskaper? Hvor forkjempere for økt overvåking mener dette kan bidra til økt sikkerhet, er det en helt annen oppfatning blant de som ønsker å begrense den. Et slikt *våpenkappløp,* som de kaller det, med ytterligere mottiltak fra de som føler seg urettmessig overvåket, vil kunne bidra til at det vil være enklere for kriminelle og gjemme seg blant mengden (Brenna, 2015). Å gjemme seg blant mengden i det digitale domenet vil øke graden av digital anonymitet (Bergsjø & Windvik, 2020, s. 100). Å være anonym i den digitale verden er ikke det samme som å være anonym i den virkelige verden, og dermed ikke en absolutt verdi. Man kan ikke være hundre 100 prosent anonym eller 100 prosent identifisert. Dermed vil mottiltakene som følger av økt overvåking føre til at det vil være lettere å oppnå en høyere grad av digital anonymitet, og dermed gjøre det vanskeligere å avdekke avvik.

Vurder argumentene dere har identifisert i deloppgavene b) og c). Hvilke argumenter mener dere bør veie tyngst her i Norge i år 2021? Hvorfor? Er det situasjoner eller hendelser dere kan se for dere som gjør at dere vil skifte mening?

Overvåking i større eller mindre grad?

Som tidligere nevnt, vil det alltid være en balansegang mellom individets sikkerhet og integritet og samfunnets sikkerhet. Etter de ovennevnte argumentene å dømme, er det i praksis en avveining mellom *tillit* og *situasjonsforståelse* som råder når det snakkes om overvåking av innbyggere. I et samfunn hvor digital utvikling er i sterkt fokus, vil det i våre øyne være et utstrakt behov for å fortsette overvåking og monitorering av organisasjoners interne systemer, men også innbyggere i staten. NSM skriver følgende i sin trusselvurdering fra 2020:

> *«Trusselaktørene i det digitale rom vil alltid utnytte mulighetene som oppstår på grunn av ny teknologi og nye bruksmønster, og gjerne sammensatt bruk av virkemidler. (…) økningen av datainnbrudd vi har sett i 2020 må forventes å fortsette i 2021. Digital sikkerhet er et felles ansvar, og det må tas på alvor. Vi har alle et felles mål om å skape robusthet gjennom forebygging, og ha deteksjonsevne og beredskap.»*
>
> *(Hoff, 2021).*

Sikkerhetsvurderingen understreker viktigheten av sikkerhetsarbeid for den enkelte virksomhet, men også at digital sikkerhet er et felles ansvar, hvor vi alle har et felles mål om å skape robusthet gjennom forebygging. Dette går blant annet ut på å ha deteksjonsevne og beredskap. Overvåking listes ikke eksplisitt som et anbefalt tiltak, men vår tolkning av budskapet er at det ligger implisitt i det å skape robusthet gjennom forebygging og ha deteksjonsevne og beredskap. Informasjonen som samles inn vil danne beslutningsgrunnlaget for eventuelle tiltak for å avverge eller oppklare kriminelle handlinger, og uten denne informasjonen vil man i mange tilfeller være blinde.

Basert på argumentene fremlagt i deloppgave a og b mener vi det mest hensiktsmessige er å ha en relativt sterk grad av overvåking gitt at man kan begrunne hvorfor denne graden av overvåking er sentral for samfunnets beste. Forutsetningene for en slik tilnærming er et demokratisk verdisett og høy samfunnstillit. Uten en redegjørelse av fordeler og ulemper tilknyttet overvåkingen vil tillit brytes og påvirke hvordan vi forholder oss til regulatoriske myndigheter. Noen situasjoner vil medføre at det er nødvendig med strengere grad av overvåking enn andre, noe som situasjonen relatert Covid 19 ble et godt bilde for. Myndighetene vurderte det som fordelaktig å spore lokasjonen til enkeltindivider for å kunne gi beskjed om mulig smitte av viruset. Selv om dette var en relativt sterk grad av overvåking, mistet ikke Norges befolkning tilliten til myndighetene siden de var så transparente med hva de overvåket, hvorfor det var nødvendig, og hvordan dette skulle gjøres sikkert. Dette er helt i tråd med personvernforordningens første prinsipp om at personopplysninger skal behandles lovlig, rettferdig og åpent (Bergsjø & Windvik, 2020, s. 115). En slik transparent kommunikasjon med noe strengere overvåking mener vi er en hensiktsmessig måte å løse balansegangen mellom tillit og situasjonsforståelse (Hoff, 2021).

Referanser

Brenna, A. (2015, Januar 6). Overvåking er ikke løsningen på problemet. Overvåking er problemet. *Teknisk Ukeblad (TU)*. https://www.tu.no/artikler/kommentar-overvåking-er-ikke-losningen-pa-problemet-overvåking-er-problemet/223594

Datatilsynet. (2015, November 3). *Personprofilering på det digitale annonsemarkedet*. https://www.datatilsynet.no/regelverk-og-verktoy/rapporter-og-utredninger/personopplysninger-og-det-digitale-annonsemarkedet/

Datatilsynet. (2016, September 23). *Sjekk av hjemmetester avslører manglende informasjon om personvern*. https://www.datatilsynet.no/regelverk-og-verktoy/rapporter-og-utredninger/sjekk-av-helseapper-for-helse-avslorer-darlig-personverninformasjon/

Datatilsynet. (2018, Juni 20). *Råd til deg som brukar mobilappar*. https://www.datatilsynet.no/personvern-pa-ulike-omrader/internett-og-apper/rad-til-deg-som-bruker-apper/

Datatilsynet. (2018, Juni 22). *Terrorbekjempelse og personvern*. https://www.datatilsynet.no/personvern-pa-ulike-omrader/politi-justis/terrorbekjempelse-og-regelverksutvikling/

Datatilsynet. (2019, Juli 17). *Hva er en personopplysning?*. https://www.datatilsynet.no/rettigheter-og-plikter/personopplysninger/

Datatilsynet. (2022, Januar 19). *Kameraovervåking - hva er lov?*. https://www.datatilsynet.no/personvern-pa-ulike-omrader/overvaking-og-sporing/kameraovervaking/

Døvik, O. (2020, Juni 8). Ny lov for e-tjenesten blir vedtatt. *NRK*. https://www.nrk.no/norge/flertall-pa-stortinget-for-ny-etterretningstjenestelov-1.15045224

ECHR. (2021, August 1). *Den Europeisk Menneskerettighetskonvensjonen*. https://www.echr.coe.int/Documents/Convention_NOR.pdf

Gjersdal, A., & Heine Natt, T. (2022, Mars 15). Metadata. *Store Norske Leksikon (SNL).* https://snl.no/metadata

Hill, S. (2015, Mars 29). Are cookies crumbling out privacy?. *Digital Trends.* https://www.digitaltrends.com/computing/history-of-cookies-and-effect-on-privacy/

Hoff, B. (2021, Januar 18). Digitale trusler i 2021. *NSM.* https://nsm.no/hold-deg-oppdatert/meninger/digitale-trusler-i-2021

Li, A. (2021, Desember 20). Top 8 Pros and Cons of Surveillance Cameras in Public Places. *Reolink*. https://reolink.com/pros-cons-of-surveillance-cameras-in-public-places/.

Lovdata. (2021). *Lov om hvitvasking og terrorfinansiering (hvitvaskingsloven)*. https://lovdata.no/dokument/NL/lov/2018-06-01-23/KAPITTEL_1#%C2%A74

Lovdata. (2021). *Lov om behandling av personopplysninger (personopplysningsloven)*. https://lovdata.no/dokument/NL/lov/2018-06-15-38/

Lovdata. (2021, Juli 1). *Lov om rettergangsmåten i straffesaker (Straffeprosessloven)*. https://lovdata.no/dokument/NL/lov/1981-05-22-25?q=straffeprosessloven

Lovdata. (2021, Juli 1). *Kongeriket Noregs grunnlov*. https://lovdata.no/dokument/NL/lov/1814-05-17-nn

Mathisen, H. L. (2020, Mai 13). Den nye loven om digital overvåking vil gjøre Norge mer autoritært. *Aftenposten.* https://www.aftenposten.no/meninger/sid/i/4qwgdg/den-nye-loven-om-digital-overvaaking-vil-gjoere-norge-mer-autoritaert-hanna-lein-mathisen

McGuane, M. (2022, Februar 4). First-Party Cookies vs. Third-Party Cookies (Biggest Differences). *Terakeet*: https://terakeet.com/blog/first-party-cookies-vs-third-party-cookies/

Nakashima, E. (2016, Februar 17). Apple vows to resist FBI demand to crack iPhone linked to San Bernandino attacks. *Washington Post.* https://www.washingtonpost.com/world/national-security/us-wants-apple-to-help-unlock-iphone-used-by-san-bernardino-shooter/2016/02/16/69b903ee-d4d9-11e5-9823-02b905009f99_story.html?itid=lk_inline_manual_8

Regjeringen. (u.d.). *Rett på nett*. https://www.regjeringen.no/no/dokumenter/rett-pa-nett/id2870086/?ch=5

Team, T. R. (2020, Februar 3). The pros and cons of a digital surveillance state. *Tradesmith Daily.* https://tradesmithdaily.com/educational/the-pros-and-cons-of-a-digital-surveillance-state/

Tekna. (2020, Juni 11). *Advarer mot ny etterretningstjenestelov*. https://www.tekna.no/aktuelt/advarer-mot-ny-e-lov/

Tørdal, R. M. (2021, Oktober 18). Overvåking og personvern i det digitale samfunnet. *NDLA.* https://ndla.no/subject:1:576cc40f-cc74-4418-9721-9b15ffd29cff/topic:2:0c9ce0dc-3863-4e03-a2df-a1480a4e929c/topic:26863d4d-97c4-4bac-b486-932dcdfd03fc/resource:f19efe60-c4ed-42f9-923f-770b5fd24362

Wikipedia. (2021, April 14). *Cambridge Analytica*. https://no.wikipedia.org/wiki/Cambridge_Analytica

Øving 4 – Sårbarheter mot tidligere pensum

Gi en kort beskrivelse av de ulike typene sårbarheter: fysiske, menneskelige, organisatoriske og tekniske. Kan du finne minst ett eksempel for hver av dem som ikke står i boka?

Hva er sårbarheter?

Sårbarheter defineres som svakheter som kan lede til brudd på sikkerheten i et IT-system (Bergsjø & Windvik, 2020, s. 130). I praksis kan det være slik at hva en sårbarhet er, avhenger av hvem som ønsker å utnytte den. En definisjon som bedre fanger opp dette, definerer en sårbarhet som

> *«Sannsynligheten for at en trusselkapabilitet overgår motstandskapabiliteten» (Bergsjø & Windvik, 2020, s. 130).*

Derfor er det viktig å kartlegge relevante trusselaktørers kapabilitet for å avgjøre hvilken reell risiko man står overfor. Dette kalles trusselkapabiliteten. Motstandskapabilitet derimot sier noe om hvor godt forsvaret til systemet er, eller hvor sterke angrep systemet evner å motstå. Derfor er kjennskap til virksomhetens sårbarheter og systemer veldig viktig, ettersom at dette øker muligheten for at de mest hensiktsmessige tiltakene med reell risikoreduserende effekt blir valgt (NSM, u.å.).

Sårbarheter kan kategoriseres i flere kategorier avhengig av hvor sårbarheten foreligger. Kategoriene vi skal se nærmere på videre i denne besvarelsen er fysiske, menneskelig, organisatoriske og tekniske sårbarheter.

Fysiske sårbarheter

Fysiske sårbarheter er sårbarheter som ligger på fysiske objekter eller infrastruktur som trusselaktører kan utnytte (Bergsjø & Windvik, 2020, s. 134). Slike sårbarheter er ofte et resultat av mangelfull adgangskontroll eller manglende fysiske sikkerhetstiltak og kan medføre at uvedkommende får tilgang til fysiske komponenter. Trusselaktøren havner da i en posisjon hvor de kan utnytte denne tilgjengeligheten til å endre informasjon de opprinnelig ikke hadde tilgang og/eller eventuelt utføre sabotasje eller hærverk på disse gjenstandene. Vi ser derfor at sikkerhetshendelser som resultat av fysiske sårbarheter potensielt kan kompromittere både konfidensialitet, tilgjengelighet og integritet.

Fysiske sårbarheter kan ramme alt fra datamaskiner og mobiltelefoner til kjøleanlegg i serverrom eller tekniske anlegg. Eksempelvis er det for de fleste virksomheter svært viktig med fungerende alarmsystemer og vakthold slik at man kan sikre informasjon og andre eventuelle verdier. Ofte leveres slike tjenester av en ekstern leverandør. Det vil i den forbindelse være viktig å kartlegge hvor godt sikret alarmsystemet er og hvor godt vaktholdet fungerer. I tillegg er det hensiktsmessig å undersøke leverandøren for å kartlegge hvilke standardiserte løsninger, sikkerhetsrutiner og metoder de benytter. Dersom det eksempelvis skulle oppstå sikkerhetshendelser hvor personvernet brytes, vil det være virksomheten som bestemmer formålet med behandling av personopplysninger som vil være ansvarlig. Eksterne leverandører, som i dette eksemplet er innleid for å ivareta sikkerheten, kan ikke holdes

ansvarlig for slike brudd. Dette understreker viktigheten av å kartlegge og sørge for at eksterne leverandører lever opp til de sikkerhetskravene man stiller for å sikre nødvendige verdier. Dette er noe vi vil komme nærmere tilbake til under organisatoriske sårbarheter i forbindelse med eksponering av leverandørs sårbarheter.

For å vise til et virkelig eksempel på en utnyttelse av fysiske sårbarheter kan vi se til Equinors hovedkvarter i Stavanger i 2019, hvor totalt åtte av selskapets bærbare datamaskiner ble stjålet (Mullis, 2019). Siden Equinor bruker en ekstern leverandør for utfasing av gammelt utstyr, var ikke de klar over at deres pc-er hadde funnet veien til privatmarkedet før de ble varslet av leverandøren som hadde avdekket at de aktuelle pc-ene ikke var registrert hos dem. Det er vanskelig for Equinor å si noe om skadeomfanget ettersom de ikke har oversikt over innholdet på maskinene utover at innholdet skal ha vært kryptert. Equinor har ikke uttalt noe mer om hvordan denne sikkerhetshendelsen utartet, men spesifiserer at de har satt inn ressurser for å oversikt over hva som har skjedd.

Et lignende eksempel som bedre illustrerer dårlig fysisk sikring av områder er PC-ranene av kommunale bygninger i 2019 (Pedersen, 2019). Sent på våren i 2019 ble flere kommunale bygninger på Østlandet frastjålet bærbare datamaskiner av en organisert gruppe. Til sammen ble over 100 maskiner stjålet, bannet annet i Lier, Moss og Oppegård. I alle tilfellene var innbruddene et resultat av dårlig sikrede bygg. Tyvene tok seg inn i bygningene via sidedører og derfra videre inn i bygningen. Ifølge artikkelen skrevet av NRK hadde flere av byggene avskrudde alarmsystem, eller manglet alarmsystem fullstendig.

I øving 2 er autorisasjon og aksesskontroll noen av temaene som belyses og er områder hvor vi tror vi de aktuelle norske rådhusene har mye de kan lære. Autorisasjon er et begrep som sier noe om hvilke rettigheter man er tildelt (Bergsjø & Windvik, 2020, s. 79). En mye brukt metode for å enkelt håndtere autorisasjoner er bruk av klareringsnivåer. Klareringsnivåer er forhåndsdefinerte nivåer som gir personer gitte tilganger i henhold til nivået personen er klarert for. Dette kan gjelde både for fysiske objekter eller for informasjon. Det virker som om de aktuelle rådhusene ikke hadde noen form for aksesskontroll, noe som i stor grad kunne gjort de aktuelle innbruddene vanskeligere å gjennomføre.

Det å låse inn alle datamaskinene i et sentralisert rom fremstår for oss som noe tungvint og lite hensiktsmessig, og man kan i den forbindelse innføre et annet sikkerhetssystem. Mange virksomheter benytter seg eksempelvis av adgangskort man må bruke i de fleste dører, både inne i selve bygning, men også ved bevegelse mellom avdelinger. Et slikt system kan settes opp på mange måter, med ulik grad av sikkerhet, avhengig av hvordan man vurderer verdiene man skal sikre. Eksempelvis er det mulig å kun gi adgang til den avdelingen man selv tilhører, noe som gjør at eventuelt tap av nøkkelkort til en trusselaktør ikke tilgjengeliggjør hele bygningen uten tyngre skyts som vil utløse en alarm. Dette vil være i henhold til hovedprinsippet innen aksesskontroll *"principle of least privilege"*, det vil si at man begrenser rettighetene til et minimum (Bergsjø & Windvik, 2020, s. 78). Man kan også ganske enkelt øke sikkerheten ytterligere ved å innføre personlige pin-koder som må skrives inn i tillegg til skanning av adgangskort, enten hele døgnet, eller etter et gitt tidspunkt. Dette enkle tiltaket stiller krav til at eventuelle trusselaktører i tillegg til å få tak i et adgangskort, også må ha riktig pin-kode tilknyttet adgangskortet. Her legger man også til rette for at man kan spore

hvilke adgangskort som har blitt brukt på hvilken dør til et gitt tidspunkt, og sikkerhetshendelser kan i større grad ettergås.

Sikring av fysiske objekter slik som pc-er i eksemplet over forutsetter også en bevisstgjøring hos de ansatte. Adgangskontroll fungerer bare dersom individer med autorisert adgang sørger for at uvedkommende ikke kan bruke deres autorisasjon uautorisert. Det vil si at ansatte må være oppmerksomme på eventuelle uvedkommende som går i gangene eller som går etter deg i en dør som er åpnet med den ansattes adgangskort. Dette bør understøttes av en digital sikkerhetskultur eksempelvis gjennom artefakter som ber de ansatte vært årvåkne på kontoret og ha lav takhøyde for å spørre om å se adgangskort fra individer man ikke kjenner igjen.

Menneskelige sårbarheter

Menneskelige sårbarheter innebærer alle de sikkerhetsbruddene som kan oppstå som et resultat av menneskelige feil (Bergsjø og Windvik, 2020, s. 134). Ofte går dette på manglende forståelse eller sikkerhetsbevissthet hos brukeren eller driftspersonell, som kan medføre at disse lettere lar seg lure. Eksempler på menneskelige sårbarheter illustreres fint gjennom ulike svindelteknikker som diskuteres i øving 1. Mange av disse teknikkene ønsker å utnytte menneskelige svakheter, særlig teknikker som phishing, real-time phishing eller Olga/Russer-svindel. Her blir det dagligdagse stresset, usikkerheten eller mangelen på kompetanse og kunnskap utnyttet av trusselaktører. I tillegg kan manglende sikkerhetsfokus i en virksomhet være en kilde til sårbarhet trusselaktører kan nye godt av.

Menneskelige sårbarheter er noe man alltid vil stå overfor i en organisasjon med menneskelige ansatte, og det vil derfor være avgjørende for systemenes sikkerhet å ta disse på alvor ved å iverksette tiltak for å redusere sannsynligheten for at hendelser inntreffer. Menneskelige sikkerhetstiltak er ment å påvirke vurderingsevne, kunnskap, atferd og reell evne til å bruke øvrige sikkerhetstiltak (NSM, u.å.). Uten gode sikkerhetstiltak for å håndtere de menneskelige sårbarhetene, vil de resterende tiltakene som angår de fysiske-, organisatoriske og tekniske sårbarhetene være mye mindre effektive. Et godt eksempel på menneskelige sårbarheter knyttet til bruken av teknologi, i lys av dagens situasjon i Ukraina, er annekteringen av Krim, Ukraina i 2014. I en lengre periode hadde president Vladimir Putin påstått at russiske soldater ikke hadde krysset grensen til Ukraina, før en soldat visstnok skal ha oppgitt sin posisjon gjennom bruk av en usikret mobilapplikasjon (Fjellstad, 2014). Slike tilfeller viser hvor viktig det er å utvise god sikkerhetskultur ved interaksjon med teknologien.

Et begrep som kan knyttes tett opp til menneskelige sårbarheter er risikooppfattelse. Risikooppfattelse henger sammen med kompetanse og læring, og er noe som kreves for å kunne vurdere hva som utgjør en risiko (Bergsjø & Windvik, 2020, s. 39). Én av faktorene som binder disse sammen, er at risikooppfattelse varierer fra person til person og avhenger av mer enn bare kvantifiserbar kunnskap. En persons risikooppfattelse påvirkes ikke bare av personens kunnskaper, men også av subjektive erfaringer som opplevelser eller teknologioptimisme. En person som har som har mye kunnskap om teknologi, kanskje også kombinert med tidligere erfaringer med sikkerhetshendelser, vil ha en annen risikooppfattelse i forhold til en person med et mindre kunnskapsnivå og ingen erfaring med hendelser. Disse to personene vil begge utgjøre en menneskelig sårbarhet, men på hver sin

måte. Førstnevnte er mer tilbøyelig til å ta risikoer og eksponerer seg selv dermed i mye større grad gjennom uforsiktig atferd, sistnevnte er kanskje mer tilbøyelig til å falle for klassiske svindelmetoder.

Organisatoriske og prosedyremessige sårbarheter

Organisatoriske og prosedyremessige sårbarheter er sårbarheter som ofte oppstår på grunn av prosedural- eller rutinemessig svikt (Bergsjø & Windvik, 2020, s. 135). Rutiner for sikkerhetsmessig drift av systemet, herunder metoder for å ivareta sikkerhetsaspektenes ønsket grad av konfidensialitet, integritet og tilgjengelighet, anses som et av de mest grunnleggende tiltakene en virksomhet kan implementeres. I tilfeller hvor dette ikke gjøres tilstrekkelig kan svakheter i rutiner eller prosedyrer være en sårbarhet.

Virksomheter som vurderer at etablering av interne funksjoner vil være mer kostbart enn outsourcing leier ofte inn tredjepartsleverandører. Dette vil på en måte redusere potensielle sårbarheter, spesielt når det kommer til tilgjengelighet da sårbarheter i det outsourcede systemet ikke har innvirkning på de resterende systemene internt. På denne måten vil man eksempelvis sikre virksomhetens kjerneaktiviteter for tjenestenekt (Bergsjø & Windvik, 2020. s. 135). Problemet med outsourcing med tanke på sårbarheter er at virksomheten i noen grad kan bli utsatt for sårbarheter i prosedyrer og prosesser tilhørende leverandøren da argumentasjonen over ikke tar hensyn til de to andre sikkerhetsmålene virksomheter må forholde seg til. For det første må virksomheten som leier inn en tredjepart sørge for at informasjon som faller innenfor personvernforordningens virkeområde blir behandlet med tilstrekkelig sikkerhet. Virksomheten som leier inn en tredjepart er her å anse som behandlingsansvarlig og vil derfor holdes ansvarlig dersom personvernet brytes (Bergsjø & Windvik, 2020. s. 113). Leverandøren er i dette tilfellet ansett som databehandler som leverer en tjeneste til behandlingsansvarlig. Derfor er det helt essensielt at behandlingsansvarlig sørger for at konfidensialitet og integritet bevares selv om databehandler får tilgang til nødvendig informasjon. Med nødvendig informasjon er det her viktig at behandlingsansvarlig forholder seg til prinsipp om *dataminimering*, hvor de ikke gir tilgang til mer data enn hva som er tjenstlig berettiget og nødvendig å tilgjengeliggjøre (Bergsjø & Windvik, 2020, s. 116).

Denne problemstillingen har i løpet av de siste årene gjort seg svært aktuell eksempelvis i helsesektoren. I 2017 innrømmet Helse Sør-Øst etter noe tids mediedekning at IT-arbeidere i utlandet, både innenfor og utenfor EU hadde hatt tilgang til pasientdata med personopplysninger som faller innenfor særlige kategorier (Tomter & Remen, 2017). Bruddet på personvernet omfattet ifølge NRK sin artikkel så mye som 2,8 millioner norske borgere som følge av outsourcing av IT-oppgaver. Datatilsynet gjennomførte så sin saksbehandling og publiserte senere samme år en rapport som fastsatte at personvernet var brutt gjennom flere lovbrudd. Deres oppsummering understreker blant annet at Helse Sør-Øst som behandlingsansvarlig ikke hadde hatt tilstrekkelig eierskap til endringen i tillegg til at ansvaret delvis eller helt hadde blitt plassert på databehandler eller individer lengre ned i organisasjonen (Alhaug & Thon, 2017, s. 3). Videre påpekes mangelen på risiko- og sårbarhetsanalyser før beslutning om outsourcing ble tatt, hvorav ovennevnte analyser heller ikke ble gjennomført når valget spesifikt falt på underleverandør i Bulgaria. I rapporten

bruker datatilsynet gjennomgående personvernforordningen som grunnlag når de understreker hvordan outsourcingen har ført til betydelige sårbarheter og sikkerhetshendelser som har gått ut over konfidensialitet, integritet og tilgjengelighet. Helsesektoren ble i forbindelse med outsourcingen pålagt et gebyr på 800 000 kroner per sykehus av datatilsynet (Alhaug & Thon, 2017, s. 4). Dette utgjør med andre ord en kostnad på 7,2 millioner, i tillegg til de kostnader i forbindelse med avvikshåndteringen. Dette eksemplet viser derfor hvor store konsekvenser manglende analyser og forankring kan gi både for enkeltindivider og for organisasjoner og er et godt bilde på skadeomfanget hva gjelder organisatoriske sårbarheter.

Organisatoriske sårbarheter trenger ikke bare omhandle enkeltsystemer eller prosedyrer, men kan også beskrive overordnede sårbarheter i virksomhetens kultur. Sikkerhetskultur er et begrep vi snakker vi om i øving 1, og som spiller en fundamental rolle for å motvirke organisatoriske sårbarheter. Når det kommer til sikkerhetskultur, er det ikke alltid nok å fokusere på hvordan man skal handle i møte med gitte situasjoner eller hendelser. For at menneskene i organisasjonen skal være best mulig rustet for å håndtere en hendelse som truer informasjonssikkerheten, må virksomheten legge vekt på verdier og holdninger som er forenlige med sikkerhetskulturen som ønskes i organisasjon. Slik vil man forhåpentligvis påvirke kunnskapen og normene som gjennomsyrer hele virksomheten. Ved å jobbe på denne preventive måten vil man oppnå en dypere forståelse av informasjonssikkerhet, som gir organisasjonen et sterkt fundament for å håndtere uønskede hendelser. Dette står i stor kontrast til en sikkerhetskultur som i realiteten ikke er eksisterende, hvor man heller løser problemer som de oppstår på stående fot uten at man nødvendigvis har den tilstrekkelige kunnskapen.

Hvis vi skal spille videre på ovennevnte eksempel fra helsesektoren, kan man argumentere for at sikkerhetskulturen var et avgjørende problem for at outsourcing og brudd på personvernet ble et faktum. Rapporten til datatilsynet oppsummerer som nevnt at det ikke ble gjennomført risiko eller sårbarhetsanalyser i tillegg til at manglende forankring i ledelsen førte til at ansvaret ble delegert ned i organisasjonen. Dette vitner om liten grad av forståelse for både hvilke verdier man omsetter i form av personopplysninger i særlige kategorier i tillegg til hva som er en sikker forvaltning av slike personopplysninger. Denne manglende forståelsen kan bunne ut i både for dårlig kompetanse eller lav interesse for sikkerhet, noe som igjen vitner om en altfor dårlig sikkerhetskultur.

Tekniske sårbarheter

Tekniske sårbarheter angir sårbarheter ofte funnet i hardware og software (Bergsjø & Windvik, 2020, s. 136). Slike kan beskrives som feil eller mangler ved programvare som potensielt kan utnyttes av uvedkommende aktører. Sikkerhetshull i software er en vanlig måte for en trusselaktør å utnytte i dagens teknologiske samfunn, hvor ny programvare utvikles hver eneste dag.

Et eksempel på en organisatorisk- og teknisk sårbarhet som ble utnyttet i 2010, var viruset Stuxnet. Viruset skal ha blitt satt inn mot det iranske atomprogrammet og medførte betydelig skade (Rossen, 2011). Viruset var en dataorm spesifikt skrevet for å spionere på og

omprogrammere industrielle systemer som mange mener ble utviklet og implementert av Israel og USA. Hvordan viruset utnyttet sårbarheter i systemet, skal vi ikke beskrive i detalj, men er vurdert som et resultat av organisatorisk- og teknisk svikt. Viruset ble visstnok spredt via USB-enheter, som utnyttet en identifisert teknisk svakhet, og muliggjør fjernstyring av atomkraftanlegget.

Et eksempel på en teknisk sårbarhet som ble oppdaget hos et stort selskap tech-selskap er 0 dags-sårbarheten oppdaget i forbindelse med Microsofts Internet Explorer (IE) nettleser (Winder, 2020). Sårbarheten ble kategorisert som kritisk og ble funnet i skriptmotoren til IE-nettleseren. Sårbarheten lar en angriper kjøre fiendtlig kode på maskinen til brukeren dersom brukeren besøker en spesiallaget nettside på IE-nettleseren. En angriper som utnytter sårbarheten korrekt, vil kunne få tilgang til alle rettigheter den aktuelle brukeren innehar.

Er det forskjell på hvordan man møter kjente trusler og ukjente trusler?

Kjente og ukjente trusler

Så langt i denne oppgaven har vi sett hvordan det i de stadig mer komplekse virksomhetene eksisterer menneskelige, tekniske, fysiske og organisatoriske komponenter hvor det kan foreligge sårbarheter. Disse sårbarhetene står i fare for å bli utnyttet av en trusselaktør hvor et eller flere sikkerhetsmål brytes og medfører store konsekvenser for organisasjonen og eventuelt tilknyttede aktører. Disse sårbarhetene bør forvaltes blant annet gjennom en god sikkerhetskultur slik vi har diskutert og eksemplifisert tidligere. Likevel er det ulike måter å tilnærme seg sårbarheter, både proaktivt og reaktivt basert på forebyggende arbeid og avvikshåndtering- og oppfølging. I den forbindelse er det hensiktsmessig å dele inn sårbarheter i ulike kategorier for å si hvordan man skal tilnærme seg dette arbeidet.

Kjente sårbarheter er sårbarheter som både er kjent for virksomheten og for offentligheten (Bergsjø og Windvik, 2020. s. 131). Slike sårbarheter har både høy risiko for å bli utsatt for angrep fra trusselaktører, men har sannsynligvis i form av å være kjent, en lavere responstid hvor man kan forhindre at slike angrep medfører omfattende konsekvenser. Ukjente sårbarheter derimot, har flere underkategorier. For det første har vi de sårbarheter som eksisterer, men som ikke er kjent for virksomheten. Disse sårbarhetene vil, dersom en trusselaktør avdekker de, kunne være kilde til omfattende tap i et eller flere sikkerhetsmål. For virksomheten vil responstiden være høyere og mer krevende å komme med en sikkerhetsfiks umiddelbart. I det en trusselaktør iverksetter et eventuelt angrep og virksomheten blir gjort oppmerksom på sårbarheten, kalles sårbarheten en dag-0-sårbarhet og refererer til det tidspunktet man kunne iverksette arbeidet med en sikkerhetsfiks (Bergsjø & Windvik, 2020. s. 132). Disse ukjente sårbarhetene kan igjen deles inn i ukjente sårbarheter virksomheten vet at de ikke vet om, og ukjente sårbarheter de ikke vet at de ikke vet om. Dette stiller krav til hvordan man kan jobbe forebyggende for å unngå sikkerhetshendelser. Videre har vi sårbarheter som er kjent for virksomheten, men ikke for offentligheten. Disse kan også omtales som dag-0-sårbarheter da virksomheten kan igangsette arbeidet med sikkerhetsfikser.

Kjente og ukjente trusler bør møtes med ulike tilnærminger og sikkerhetstiltak. Som et grunnlag bør virksomheten kartlegge de relevante trusselaktørers kapabilitet, for å avgjøre hvilken reell risiko man står overfor. Først da har de mulighet til å definere hvilke trusler som er kjent – og hvilke som er ukjent.

Ved ukjente trusler vil det være fordelaktig å kombinere sikkerhetstiltak, både for å unngå at sårbarhetene blir utnyttet og for å redusere konsekvensene av at de blir utnyttet. Gjennom et godt grunnarbeid med strategier og planer, hvor virksomheten definerer standarder og prinsipper for gjennomføring av sikkerhetsarbeidet, vil man ha et grunnlag for å gjennomføre effektive tiltak for å unngå utnyttelse. Disse tiltakene skal være i tråd med virksomhetens vurderte trusselaktører, de interne faktorene og systemenes omgivelser. Først når dette oppnås vil sikkerhetstiltakene være i sin mest effektive form.

Den generiske tidslinjen

Den generiske tidslinjen for en gitt sårbarhet beskriver hendelsesforløpet fra en sårbarhet har oppstått til den er fjernet eller håndtert (Bergsjø & Windvik, 2020, s. 131). Den viser at enhver sårbarhet har et tidsrom hvor sårbarheten er ukjent for virksomheten. Dette tidsrommet er svært attraktivt for trusselaktører da en ukjent sårbarhet sannsynligvis vil ha en lengre responstid. I denne perioden er med andre ord trusselkapabiliteten ofte større enn motstandskapabiliteten, og sårbarheten vil ha et stort potensial til å bli utnyttet av en trusselaktør med riktig tilgang og kompetanse. En ukjent trussel vil i dette tidsrommet ha stort potensiale for å påføre skade. Dermed er det stor sannsynlighet for at tidsperioden hvor leverandør ikke kjenner til sårbarheten er mindre ved håndtering av kjente trusler, dermed er det også nærliggende at konsekvensene reduseres og at mottiltakene blir mer effektive.

Fra det tidspunktet sårbarheten blir kjent for leverandøren har de mulighet til å iverksette situasjonsspesifikke tiltak for å minimere sannsynligheten for nye utnyttelser, samt minimere konsekvensen av utnyttelsene som potensielt har skjedd. Det vil i dette tidsrommet være vanskeligere for en trusselaktør å utnytte den gitte sårbarheten, da motstandskapabiliteten er i ferd med å øke. Dette gjelder både for kjente trusler og tidligere ukjente trusler som nå er blitt kjente. Sikkerhetstiltak som vil være mest aktuelt fra det tidspunktet sårbarheten blir kjent vil være reaktive tiltak som går ut på sikkerhetsfikser for å fjerne eller håndtere sårbarheten. En virksomhet må forsøke å redde det de kan, samtidig som de forsøker å tette sikkerhetshullene før sårbarheten blir offentlig kjent. Fra den dagen sårbarheten blir offentlig kjent øker sannsynligheten drastisk for at sårbarheten utnyttes av flere trusselaktører. Tiden frem til sårbarheten er fjernet eller håndtert er med andre ord særdeles kritisk.

Unngå utnyttelse vs. reduksjon av konsekvens

Læreboken skiller mellom to komplementære tilnærminger for å redusere sårbarheten i egne systemer. Den første søker etter å unngå at sårbarheter blir utnyttet, herunder å redusere antallet sårbarheter. Man forutsetter her at det alltid vil være gjenværende sårbarheter med mulighet for utnyttelse. Den andre tilnærmingen ønsker å redusere konsekvensene utnyttelsen dersom utnyttelsen av en sårbarhet først skjer (Bergsjø & Windvik, 2020, s. 140). I praksis vil det være hensiktsmessig å benytte sikkerhetstiltak for å adressere begge tilnærminger.

Kun gjennom aktiv testing og analyser av de implementerte sikkerhetstiltakene kan vi finne ut om tiltakene er effektive eller ikke. På denne måten kan vi også oppdage manglende sikkerhetstiltak som burde implementeres. Ulike faktorer bør vektlegges i vurderingen om et tiltak er godt nok eller ikke. Dette kan være hvordan systemet benyttes, systemets omgivelser og sikkerhetskompetansen hos brukerne av systemet.

For å unngå at sårbarheter blir utnyttet listes det opp en rekke aktive tiltak man som virksomhet kan gjennomføre (Bergsjø & Windvik, 2020, s. 140). Dette er tiltak som raske sikkerhetsoppdateringer og utfasing av gamle systemer som anses som sikkerhetsmessig utdaterte, aktiv analyse og testing av eksisterende systemer og en redusert angrepsflate. Som et grunnlag for dette, må det foreligge tydelige strategier og planer som gir klare retningslinjer for hvordan sikkerhetsarbeidet skal gjennomføres.

Disse strategiene og planene anses som grunnlaget for arbeidet med å redusere konsekvensene av at sårbarheter utnyttes, med en erkjennelse om at det vil skje på et eller annet tidspunkt. Her bør det klart og tydelig beskrives hvilken sikkerhetskultur som ønskes og hvordan man aktivt skal jobbe for å nå denne kulturen. Menneskene i en organisasjon – og deres menneskelige sårbarheter – er som nevnt en sårbarhet en virksomhet aldri kommer unna så lenge de har ansatte. Et viktig og forebyggende arbeid vil derfor være å gjennomføre grunnleggende opplæring og bevisstgjøring blant de ansatte for å være i stand til å håndtere hendelser i hverdagen. I tillegg til dette, inngår sikkerhetsprinsipper innenfor risikostyring og – håndtering, som et av de mest grunnleggende prinsippene for digital sikkerhet (Bergsjø & Windvik, 2020, s. 121).

Videre er har vi også mer konkrete tiltak som kan redusere konsekvensen av at sårbarheter utnyttes (Bergsjø & Windvik, 2020, s. 140 & 141). Opplysninger og informasjon skal sikres i tråd med de verdiene som forvaltes og sikkerhetstiltak må være proporsjonale med dataens verdi. Skulle virksomheten være så uheldig å bli utsatt for et angrep, vil konsekvensene kunne reduseres ved å begrense brukernes tilgang til informasjon, så vel som deres rettigheter i et system. Videre kan det å ha mange lag med ulike forsvarsapplikasjoner være veldig hensiktsmessig. Dette gjør at angriper må bryte seg gjennom flere forsvarsmurer for å tak i mer og mer informasjon. Dette bidrar til at angrepet tar lenger tid og dermed også forhåpentligvis kan stanses før det får alvorlige konsekvenser. Jo raskere man får stanset angrepet, desto bedre mulighet har man til å begrense skaden som er gjort. Her vil det eksempelvis være hensiktsmessig med et sentralisert Incident Response Team (IRT), som har ansvar for å håndtere hendelser når de inntreffer. Dette er noe flere virksomheter benytter seg av, blant annet SpareBank 1 SMN som erfart av et av gruppens medlemmer. Selv om det høres ideelt ut med et slikt dedikert team, er ikke jobben gjort når dette teamet er etablert. Dersom de ansatte i bedriften ikke er klar over at dette teamet eksisterer, vil det ta vesentlig lengre tid før informasjon om en eventuell sikkerhetshendelse når frem. Dette er noe det i SpareBank 1 SMN har blitt jobbet aktivt for da man gjennom revisjon avdekket manglende oppmerksomhet i organisasjonen. Jevnlige oppdateringsmoduler for sikkerhet ble derfor iverksatt og oppmerksomheten rundt avvikshåndtering og - forebygging har blitt mye bedre.

Som nevnt helt i starten av oppgaven mener vi at det mest hensiktsmessige er og i praksis utøve en kombinasjon av disse strategiene, dette gjelder for både kjente og ukjente trusler.

Ved kjente trusler har man i større grad mulighet til å sette inn konkrete tiltak som er direkte rettet inn mot den bestemte trusselen. Tiltakene som trekkes frem i teorien er i stor grad generelle, dermed har de i all hovedsak en preventiv og forebyggende funksjon. Dette gjør at tiltakene også egner seg godt mot ukjente trusler, ettersom man her ikke har bruk for smale tiltak mot enkeltsystemer, men heller for overordnede tiltak som reduserer risikoen på tvers av organisasjonen. Det forebyggende arbeidet sammen med reduksjon av konsekvenser, vil også kunne fungere for de sårbarheter man ikke kjenner til, da et overordnet rammeverk preget av en god sikkerhetskultur vil øke den generelle motstandskapabiliteten.

McCumbers kube og safeguards ved kjente og ukjente trusler

McCumbers kube er en grafisk representasjon som består av tre dimensjoner. Disse dimensjonene er sikkerhetsmålene, tilstanden til informasjonen eller data og safeguards for å bevare sikkerheten (Researchgate, 2013). Dimensjonen safeguards innebærer teknologi, organisatoriske regler og retningslinjer i tillegg til menneskelige faktorer og sikkerhetskultur. Målet man ønsker å oppnå gjennom bruk av modellen er å ivareta de tre sikkerhetsprinsippene *konfidensialitet, integritet og tilgjengelighet.* Ved å se disse prinsippene i sammenheng vil man enklere kunne utarbeide en sikkerhetsstrategi som håndterer det aktuelle krysningspunktet på en hensiktsmessig måte.

Teknologiske safeguards kan være teknologiske løsninger i software eller hardware som er designet for å beskytte systemet (en-academic.com, 2010). Eksempler på slike teknologier er brannmurer, anti-virus eller systemer som er laget for å detektere innbrudd. Organisatoriske regler og retningslinjer er safeguards som omhandler administrative kontroller og direktiver, og legger et grunnlag for hvordan informasjonssikkerhet skal håndteres i organisasjonen. Eksempler kan være hvordan organisasjonen reagerer ved ulike hendelser - hvilke mekanismer og systemer man benytter seg av. Et annet eksempel kan være enkle ting som hvilke begrensninger virksomheten setter med tanke på hva som er akseptabel bruk av organisasjonens utstyr og ikke. Safeguards relatert til menneskelige faktorer og sikkerhetskultur handler om brukerne av informasjonssystemet, og også virksomhetens underliggende antakelser og normer rundt sikkerhetsmessige aspekter. Dette handler om å sørge for at brukerne av systemet er klar over sin rolle i forbindelse med både bruk og beskyttelse, så vel som at de er i stand til å følge de standardene og kravene til sikkerhet som forventes. Sikkerhetskulturen ligger som vi tidligere har påpekt forankret i virksomhetens verdier og normer, og er noe ledelsen må bane vei for. I praksis medfører dette å sørge for god opplæring og kunnskap til brukerne av systemet, på denne måten vil brukerne enklere kjenne igjen truende situasjoner og dermed også gjøre bedre valg når situasjonen skal håndteres.

Dimensjonen *safeguards* omfatter ulike teknikker og disipliner IT-personell kan benytte seg av for å ivareta informasjonssikkerheten (Golovatenko, 2018). Tekniske safeguards kan ses på som førstelinjen i informasjonssystemers forsvar, og kan som nevnt bestå av tekniske løsninger som brannmur eller anti-virus. Tekniske angrep mot informasjonssystemer kan komme i mange former, og er kanskje den meste brukte angrepsmetoden hackere benytter seg av i dag. Et eksempel på et slikt angrep kan være et Distributed Denial of Service (DDoS)-angrep. Uavhengig om trusselen er kjent eller ukjent vil tekniske safeguards være

veldig viktige for en virksomhets informasjonssystemer, ettersom det er disse som kan sette en stopper for angrepene mot sikkerhetshull og andre feil i informasjonssystemene hos virksomheten. Det ville for eksempel vært veldig vanskelig å beskytte seg mot et DDoS-angrep uten tekniske safeguards. Her kan man for eksempel benytte seg av et forsvarssystem som hele tiden analyserer innkommende trafikk i form av metadata, og filtrerer ut angrepene før de når tjeneren (Globalconnect, 2021). For kjente trusler kan tekniske safeguards implementeres kontinuerlig etter hvert som truslene oppdages, dette kommer at implementeringen av slike systemer som regel kan innføres med god effekt på relativt kort tid. Ukjente trusler kan være vanskeligere å forholde seg til, her må virksomheter heller prøve å hele tiden sørge for å ha oppdaterte og tilstrekkelig gode safeguards på plass til enhver tid.

Videre skal vi se at organisatoriske safeguards kan være effektive i håndteringen av trusler, men her på et mer overordnet nivå. Gode rutiner og protokoller i en organisasjon er gode forebyggende tiltak som gir organisasjonen et godt grunnlag for å håndtere både kjente og ukjente trusler. Det at en virksomhet har gode systemer og prosedyrer på plass for håndteringen av trusler kan være avgjørende for hvordan virksomheten takler det om truslene utvikler seg til å bli en hendelse. Det kan være enklere for virksomheter å kriseplanlegge for kjente trusler ettersom virkningene av disse også er mer forutsigbare, men det betyr ikke at man ikke bør ha prosedyrer for en ukjent trussel. Ved å planlegge hva man eventuelt kan gjøre hvis en for øyeblikket ukjent trussel skulle realisere seg, unngår man å bli stående på bar bakke når man står midt i situasjonen. I kaotiske og uoversiktlige øyeblikk kan det være gull verdt å ha en god og gjennomtenkt prosedyre å lene seg på, selv om denne ikke nødvendigvis dekker situasjonen hundre prosent.

Til slutt skal vi se at dimensjonen som tar for seg menneskelige faktorer og sikkerhetskultur kan være meget effektive safeguards mot både kjente og ukjente trusler, men kan også være en fallgruve. Menneskene i en virksomhet kan utgjøre en relativ enkel vei inn i virksomheten for en angriper om disse ikke har den rette kunnskapen. Det hjelper ikke om en virksomhet har mange lag med topp-moderne tekniske forsvar rundt sine informasjonssystemer, hvis menneskelige feil eller uforsiktighet råder i organisasjonen. For eksempel er det ikke sikkert at et topp-moderne teknisk sikkerhetssystem vil være til hjelp hvis medarbeidere i organisasjonen trykker på ukjente linker via jobb-epost, eller tilkobler jobb-datamaskinen til tilfeldige minnepinner. På den andre siden er dette trusler som burde være enkle å forhindre. Ved kjente trusler vil bevisstgjøring overfor medarbeidere av de ulike truslene som eksisterer ha en tilstrekkelig effekt. Medarbeidere som er bevisste på at de ikke skal koble ukjente minnepinner til datamaskinen har veldige gode forutsetninger til å lykkes med dette. Naturlig nok er det vanskelig å bevisstgjøre for det ukjente, derfor vil en sterk sikkerhetskultur og kunnskapsrike medarbeidere være virksomhetens beste forsvarsmekanismer i håndteringen av disse. Om virksomheter greier å oppnå dette vil de ha et meget godt grunnlag for å effektivt håndtere både kjente og ukjente trusler.

Referanseliste

Alhaug, G. & Thon, B. E. (2017). Varsel om vedtak - overtredelsesgebyr - Sykehuset Innlandet HF. Datatilsynet.

Bergsjø, H. & Windvik, R. (2020). Digital sikkerhet: En innføring. *Universitetsforlaget*

Effektiv DDoS-beskyttelse. (u.å). *globalconnect.no.* Hentet 10.05.2022:

https://www.globalconnect.no/tjenester/it-sikkerhet/ddos-beskyttelse

Fjeldstad, S. (2014). Soldatselfie kan ha avslørt Russland. *vg.no.* Hentet 15.03.2022:

https://www.vg.no/nyheter/utenriks/i/e36rO/soldatselfie-kan-ha-avsloert-russland

Generelt om sikkerhetstiltak. (2020). *nsm.no*. Hentet 15.03.2022:

https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker-til-sikkerhetsloven/veileder-i-fysisk-sikkerhet/veiledning-til-bestemmelser-om-fysisk-sikkerhet/generelt-om-sikkerhetstiltak-14/

Hesseldahl, A. (2015). Here's What Helped Sony's Hackers Break In: Zero-Day Vulnerability. *vox.com.* Hentet 10.05.2022:
https://www.vox.com/2015/1/20/11557888/heres-what-helped-sonys-hackers-break-in-zero-day-vulnerability

Identifiser trusler. (2020). *nsm.no.* Hentet 15.03.2022:

https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-sikkerhetsstyring/identifisere-og-kartlegge/identifiser-trusler/

McCumbers Cube. (u.å). *en-academic.com.* Hentet 10.05.2022:

https://en-academic.com/dic.nsf/enwiki/2150213#Safeguards

Mullis, M.E. (2019). IT-utstyr fra Equinor stjålet: Vet ikke om flere datamaskiner er på avveie. *Nettavisen.no*. Hentet 10.05.2022:

https://www.nettavisen.no/okonomi/it-utstyr-fra-equinor-stjalet-vet-ikke-om-flere-datamaskiner-er-pa-avveie/s/12-95-3423841233

Pedersen, L.H. (2019). Svensker tatt for å ha stjålet hundre PC-er fra norske rådhus. *nrk.no.* Hentet 10.05.2022:

https://www.nrk.no/osloogviken/svensker-tatt-for-a-ha-stjalet-hundre-pc-er-fra-norske-radhus-1.14499042

Remen, A.C., & Tomter, L. (2017). Helse Sør-Øst: Innrømmer at utenlandske IT-arbeidere fikk tilgang til sensitive pasientdata. *NRK.*
https://www.nrk.no/norge/helse-sor-ost_-innrommer-at-utenlandske-it-arbeidere-har-hatt-tilgang-til-pasientjournaler-1.13478443

Stuxnet. (2021). *wikipedia.org.* Hentet 15.03.2022:

https://no.wikipedia.org/wiki/Stuxnet

Golovatenko, I. (2018, 13. desember). *The Three Dimensions of the Cybersecurity Cube*. Swansoftwaresolutions. https://swansoftwaresolutions.com/the-three-dimensions-of-the-cybersecurity-cube/

What is stuxnet? (u.å). *Trellix.com.* Hentet 15.03.2022: https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-stuxnet.html

Winder, D. (2020). U.S. Government Confirms Critical Browser Zero-Day Security Warning For Windows Users. *Forbes.com.* Hentet 10.05.2022:

https://www.forbes.com/sites/daveywinder/2020/01/18/us-government-confirms-critical-zero-day-security-warning-for-windows-users/?sh=5db6c0cc3212

Øving 5 – Risiko og programvaresikkerhet

Beskriv hva de to ulike måtene for å vurdere risiko er - den 'matematiske' og 'trefaktormodellen'.

De fleste virksomheter er i dag avhengig av gode systemer for å støtte sine forretningsprosesser. Stadig mer komplekse verdikjeder og en økende grad av digitalisering stiller også økende krav til gode risikovurderinger. Risikovurderinger er et viktig hjelpemiddel for virksomhetens ledelse for å bevisstgjøre og ta informerte beslutninger, og for at utviklings- og driftspersonell skal kunne synliggjøre risikoer i egne IKT-systemer (NSM, 2021). Sentralt i en risikovurdering er en forståelse av de relevante trusselaktørene, noe en trussel- og arkitekturanalyse kan bidra med. I denne besvarelsen beskriver vi derfor to ulike tilnærminger for å vurdere risiko - den 'matematiske' og 'trefaktormodellen. Vi vil belyse hvordan usikkerhet vil prege valg av metode og hvordan man møter en slik problemstilling i det virkelige liv. I andre del av besvarelsen redegjør vi for hovedtrekkene i en arkitekturanalyse innen programvaresikkerhet, før vi tar for oss sårbarhetene for tre spesifikke operativsystemer.

Risiko

Risiko er usikkerhet rundt måloppnåelse (NSM, 2021). Måloppnåelse for virksomheter er deres daglige leveranser og oppdrag, og risiko knyttes til faktorer som kan påvirke virksomhetens oppdrag og leveranser innenfor de kravene som er satt. For å minimere risiko vil det derfor være avgjørende for en virksomhet å redusere usikkerheten gjennom en rekke aktiviteter og tiltak. Risikostyring er en samling av de aktiviteter og tiltak en virksomhet utfører for å sikre at virksomheten når sine mål og retter fokus mot de aktiviteter som er mest kritisk for å nå målene. En risikovurdering vil som nevnt være ett av flere nyttige styringsverktøy for en organisasjon, og innebærer de tre stegene *risikoidentifisering, risikoanalyse* og *risikoevaluering* (NSM, 2021). En slik risikovurdering vil derfor danne et beslutningsgrunnlag for virksomhetens ledelse hva gjelder risikostyring og -håndtering. En risikovurdering handler tross alt om å redusere usikkerheten rundt måloppnåelse, og krever derfor effektive tiltak for å realisere dette. Risikohåndtering innebærer derfor å iverksette tiltak for å agere på risikovurderingen.

En god risikovurdering forutsetter inngående kunnskap om systemet som skal beskyttes og verdiene i systemet, og er det som kjennetegner en funksjonsbasert tilnærming (Bergsjø & Windvik, 2020, s. 193). Tilnærmingen fokuserer på sårbarheter som kan påvirke oppgavene og leveransene organisasjonen har ansvar for, hvor virksomhetens kjerneoppgaver vil være naturlig å rette fokus mot (Bergsjø & Windvik, 2020, s. 187). Inngående kjennskap til systemet vil derfor være avgjørende for å forstå *hva* som skal beskyttes, altså hvilke verdier virksomheten ønsker å beskytte. En verdi blir definert som en *"ressurs som hvis den blir utsatt for uønsket påvirkning vil medføre en negativ konsekvens for den som eier, forvalter eller drar fordel av ressursen"* (Bergsjø & Windvik, 2020, s. 193). Risikovurdering innebærer derfor en kartlegging av potensielle trusler for virksomhetens verdier, samt en vurdering av hvor sannsynlig og alvorlig det er dersom virksomheten blir utsatt for uønsket påvirkning. Risikovurderingen skal ta for seg funksjonene til virksomheten, verdiene som behandles, sårbarhetene som eksponerer disse, og truslene for at disse skal utnyttes. Uavhengig av

hvilken metode som benyttes for å gjennomføre risikovurderingen, vil en funksjonsbasert tilnærming gi virksomheten gode forutsetninger for å gjennomføre en mer presis vurdering. Dersom virksomheten er bevisst på hva de ønsker å beskytte, vil det naturligvis bli lettere å identifisere trusler og sårbarheter og kunne iverksette effektive mottiltak.

For den helhetlige forståelsen vil det være nødvendig å utdype hva vi legger i begrepet *sårbarheter*. En sårbarhet omtales også som *sikkerhetshull, sikkerhetsfeil* og *sikkerhetssvikt* (Bergsjø & Windvik, 2020, s. 129). En sårbarhet deles gjerne inn i tre kategorier - menneskelige, teknologiske og organisatoriske. Enhver virksomhet vil avdekke sårbarheter av ulik kategorisering, og vil måtte iverksette forskjellige tiltak for å redusere de aktuelle sårbarhetene. En annen tilnærming til sårbarhet er beskrevet av The Open Group, og sier at en sårbarhet er

> *"sannsynligheten for at en trusselkapabilitet overgår motstandskapabiliteten". (Bergsjø & Windvik, 2020, s. 130).*

Det vil i den forbindelse være viktig å ta hensyn til hvilke trusselaktører en virksomhet **realistisk** vil stå overfor ved vurdering av risiko. Helt grunnleggende finnes de to tilnærminger til hvordan man kan redusere sårbarheten i egne systemer. Tilnærmingene er komplementære, hvor en kombinasjon av begge ofte er nødvendige for å håndtere virkelighetens utfordringer. Den første tilnærmingen søker å unngå at sårbarheter blir utnyttet og er en **proaktiv** og **forebyggende** tilnærming (Bergsjø & Windvik, 2020, s. 139). Den andre tilnærmingen innebærer å redusere konsekvensene av at sårbarheter utnyttes og er derfor en **reaktiv** tilnærming. For denne besvarelsen vil en forebyggende tilnærming være den aktuelle, da risikovurderinger og arkitekturanalyser er eksempler på forebyggende tiltak for å redusere sårbarheter knyttet til egne systemer.

Med dette fokuset vil det være nyttig å se på systemet som en helhet bestående av både digitale og fysiske elementer (Bergsjø & Windvik, 2020, s. 189). Et slikt system vil ofte være svært komplekst og en risikovurdering vil alltid være preget av usikkerhet. Det vil være nødvendig å danne en tverrfaglig gruppe som skal foreta risikovurderingen, da en slik vurdering krever kompetanse fra alle fagområdene i systemet for å minimere usikkerheten. En risikovurdering utgjør ingen verdi i seg selv, og må derfor følges av hele organisasjonen. Det vil derfor, på lik linje som med digital sikkerhetskultur, være viktig å forankre vurderingen hos organisasjonens ledelse. Uten å ha forankret risikovurderingen hos ledelsen, vil det være vanskelig å implementere og drive oppfølging av vurderingen - og spesielt de risikoreduserende tiltakene.

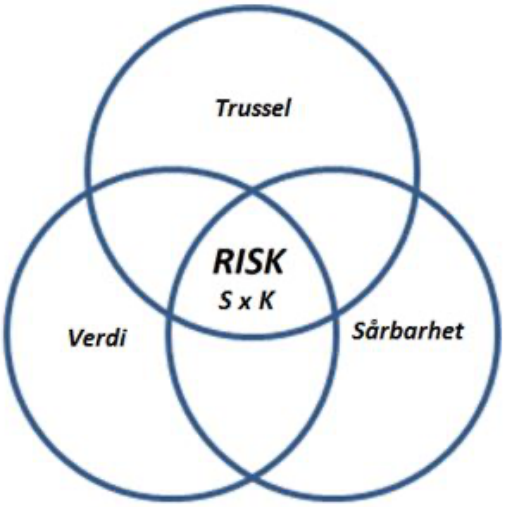
Den matematiske metoden

Når man skal gjennomføre risikovurdering er det to ulike metoder som kan benyttes. Den matematiske metoden vil forsøke å tallfeste risiko som et produkt av sannsynlighet og konsekvens *(risiko = sannsynlighet X konsekvens).* Selv om dette er en ryddig tilnærming til risikovurdering, er problemet innenfor sikkerhetsarbeid at det ofte ikke eksisterer tilstrekkelig datagrunnlag til å gjøre en presis matematisk vurdering av risiko. Risikobildet beskrives ofte som svært komplekst og i stadig endring, og virksomhetene står overfor aktører med mål om å gjennomføre tilsiktede uønskede handlinger, og vil i stor grad være

uforutsigbare (Bergsjø & Windvik, 2020, s. 188). Trusselaktører med ulike intensjoner og kapabiliteter, kombinert med det komplekse systemet som skal beskyttes, gjør det umulig å få fullstendig oversikt over alle potensielle trusler og sårbarheter. Selv om det teoretisk sett kunne ha vært mulig å samle inn all tilgjengelig data fra tidligere utnyttelser av systemet, vil endring i sikkerhetsbildet føre til at statistikken blir utilstrekkelig. Videre vil kompleksiteten i systemet føre til at man umulig kan ha oversikt over alle sårbarhetene i systemet. Når man da skal foreta en matematisk vurdering av risiko vil det derfor være ting man ikke tar med i beregningen som gjør at usikkerheten blir så stor at en matematisk risikovurdering ikke ville kunne ført til noe tilregnelig resultat.

Trefaktormodellen

Ett alternativ til den matematiske metoden skiller seg ut ved at den ikke baserer seg på et kvantitativt datagrunnlag. Trefaktormodellen er en annen metode for risikovurdering som vurderer de tre kvalitative faktorene *trussel, verdi* og *sårbarhet*. Modellen definerer risiko som *"et uttrykk for forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifiserte trusselen"* (NS 5830, 2012, s.5). Modellen er utviklet for å vurdere risiko av tilsiktede uønskede handlinger, og er i våre øyne bedre egnet for å vurdere risiko med dagens risikobilde i mente.



Figur 1: Trefaktormodellen består av de tre faktorene: trussel, verdi og sårbarhet. I skjæringspunktet mellom de tre faktorene er risiko, som også kan regnes ut som summen av sannsynlighet og konsekvens.

Verdien i trefaktormodellen er det virksomheten ønsker å beskytte, og omfatter typisk arbeidsprosesser og informasjon som er viktige for virksomhetens oppgaver og leveranser. Sårbarheter er svakheter i det sammensatte systemet som potensielt kan utnyttes av trusselaktører, og kan kategoriseres i henhold til de tre kategoriene beskrevet i øving 4. Trusler kan være fysiske eller abstrakte, men har til felles at de negativt påvirker et objekt eller et system (Bergsjø & Windvik, 2020, s. 147). Negativ påvirkning vil i denne forstand innebære en svekkelse av de tre sikkerhetsmålene *konfidensialitet, integritet* og

tilgjengelighet. En vurdering av trusselaktørene vil basere seg på en forståelse av aktørens intensjon, mulighet og kapabilitet (Bergsjø & Windvik, 2020, s. 149). Her vil en trusselvurdering være svært nyttig, og søker å skape en bedre forståelse av trusselaktøren med utgangspunkt i de tre faktorene.

Modellen tar høyde for usikkerhet, både når det gjelder det usikre datagrunnlaget og de dynamiske forholdene i omgivelsene (Bergsjø & Windvik, 2020, s. 188). Hver av faktorene i modellen kan tolkes ulikt og de ansvarlige for risikovurderingen mangler ofte en helhetlig oversikt over sårbarheter i systemet samt et detaljert bilde av trusselaktørene. Likevel vil man, med en tverrfaglig gruppe, kunne få tilstrekkelig oversikt over systemet som kan gjøre det mindre sannsynlig at man overser viktige faktorer. Det er tydelig at det vil være vanskelig å kvantifisere disse faktorene, en risikovurdering ved bruk av trefaktormodellen vil derfor være en kvalitativ vurdering. Ved å vurdere verdien som skal beskyttes, sårbarhetene i systemet som kan utnyttes og trusselaktørens intensjon, muligheter og kapabiliteter, er håpet å få en mer presis vurdering av den faktiske risikoen overfor virksomhetens IKT-systemer. På bakgrunn av risikoforståelsen vil man forsøke å minimere risikoen ved å redusere sannsynligheten for en svekkelse i en av de tre faktorene, gjennom risikohåndtering og effektive mottiltak. Dette kan gjøres ved å eksempelvis redusere virksomhetens tekniske sårbarheter ved å innføre ny løsning for antivirus og brannmur.

Valg av modell

Når det skal gjennomføres en risikovurdering, har vi forsøkt å belyse viktigheten av et grundig arbeid gjennom en systematisk og metodisk prosess. En slik tilnærming vil sørge for en objektiv vurdering av risikoen en virksomhet står overfor, og vil være viktig for å unngå systematiske skjevheter (Bias) blant de involverte (Bergsjø & Windvik, 2020, s. 166). Hvilken metode man benytter i virksomhetens risikovurdering vil avhenge av flere faktorer, blant annet hvilket datagrunnlag man har tilgang på og hva som faktisk skal vurderes. Av de to modellene vi har beskrevet er det ikke stor forskjell mellom hvilke faktorer som vurderes. Ved bruk av den matematiske modellen er det en rekke forutsetninger som bør være på plass sammenlignet med bruk av trefaktormodellen. Målbare, fullstendige og formålstjenlige data må være på plass for å gjennomføre en kvantitativ vurdering av risiko, noe vi tidligere har nevnt er en utfordring innenfor sikkerhetsarbeid. Man kan også stille spørsmål til troverdigheten ved det eksisterende datagrunnlaget, og om de egentlig møter kravene den matematiske modellen stiller. Usikkerhet er derfor en nøkkelfaktor ved vurdering av risiko, hvor *risikopersepsjon* ofte er inkludert innenfor samfunnsvitenskapen (Bergsjø & Windvik, 2020, s. 188). Risikopersepsjon er oppfatning av risiko, og muligheten til å vurdere ukjente og usikre risikoer uten å nødvendigvis basere vurderingene på kvantitative statistikkdata. Oversatt betyr dette at man i virkeligheten er nødt til å basere risikovurderingen på flere faktorer enn sannsynlighet og konsekvens. Å ta høyde for usikkerhet, altså det å anerkjenne at det er ting man ikke kan vite, er viktig når man skal gjennomføre risikovurderinger (Bergsjø & Windvik, 2020, s. 189). En sentral del av risikovurderingen som et beslutningsgrunnlag blir derfor å synliggjøre usikkerhetene overfor beslutningstakerne.

En tallfesting av risikoen basert på beregninger av sannsynlighet og konsekvens er oversiktlig og enkelt å forstå, men stiller som nevnt krav til et fullstendig og troverdig datagrunnlag. Med dagens komplekse og dynamisk risikobilde med uforutsigbare trusselaktører, vil det derfor som regel være mer hensiktsmessig å ta utgangspunkt i trefaktormodellen for sammensatte systemer. Denne metoden er bedre egnet til å ta høyde for usikkerheten et slikt risikobilde fører med seg, og inkluderer risikopersepsjon. Modellen skal derfor vurdere risikoen til et gitt system ut fra virksomhetens oppfatning, og ikke utelukkende basert på kvantitative data.

I praksis kan det likevel være et poeng å benytte en kombinasjon av disse to metodene. Ved å vurdere de kvalitative egenskapene ved de tre faktorene i trefaktormodellen kan det være et poeng å tallfeste sannsynligheten for angrep og konsekvensen dersom en trusselaktør påvirker verdien i negativ forstand. En slik tallfesting kan deretter brukes til å regne ut samlet risiko ved bruk av den matematiske metoden. Tall for samlet risiko kan deretter brukes for å rangere risikoene og som beslutningsgrunnlag for hvilke tiltak som skal iverksettes for å redusere risiko. En slik rangering må likevel ta hensyn til usikkerheten knyttet til vurderingen og tidsaspektet det er snakk om. Uavhengig av hvilken metode som benyttes bør det legges vekt på å fremheve usikkerhetene rundt vurderingene. Om vurderingen er gjort på et ufullstendig datagrunnlag eller om troverdigheten ved dataen er lav, er dette viktig å inkludere dette i risikovurderingen. For at risikovurderingen skal fungere som et

beslutningsgrunnlag må beslutningstakerne få innsikt i usikkerhetene før det gjøres beslutninger, og kan være med å belyse de mulige utfallene ved ulike situasjoner.

Som et praktisk eksempel vil vi på et overordnet nivå beskrive hvordan Forsvaret praktiserer risikovurdering og deres tilnærming til å formulere beslutningsgrunnlag. Eksempelet baseres på et av gruppens medlemmers personlige erfaringer, og kan derfor ikke betraktes som sannhet, da det sannsynligvis eksisterer ulike meninger og flere tilnærminger. Tilnærmingen er proaktiv og av prediktiv karakter, og man vil gjennom en systematisk og metodisk prosess søke etter å redusere risikoen til et akseptabelt nivå, slik at den står i forhold til gevinsten.

Hele risikovurderingen på taktisk nivå tar utgangspunkt i spørsmålet *"hva vil hindre meg i å løse mitt eget oppdrag?"*, og vil derfor kunne sammenlignes med en virksomhets verdier. Faktorer som kan påvirke de daglige leveransene og oppdragene utgjør dermed en trussel, og vil også hjelpe til med å definere ens egne verdier. Sårbarheter er dine svakheter, være seg få logistikkressurser eller våpen med kort rekkevidde. I praksis kan vi se en likhet med trefaktormodellen. For interne formål vil en slik tilnærming i mange tilfeller være godt nok. Utfordringen oppstår likevel når denne vurderingen skal formidles til eksterne, som et beslutningsgrunnlag. I slike tilfeller benyttes begrepene sannsynlighet og konsekvens for å tallfeste vurderingene og konkretisere hva dette faktisk vil si for vårt overordnede oppdrag. *"So what - who cares"* er en god huskeregel som benyttes når man skal formidle et budskap, og understreker viktigheten av informasjonen skal kunne benyttes av en beslutningstaker, og at den skal tilføre merverdi. Sannsynligheten for en hendelse er delt inn i en skala på fem sannsynlighetsgrader, fra meget liten til svært stor, og er kvantifisert med tallene 1 til 5. Det samme er graden av konsekvens, fra ubetydelig til kritisk, med tallene 1 til 5. Risikoen beregnes på grunnlag av sannsynligheten og konsekvensen, hvor man til slutt får en tallfestet risiko. Man har på forhånd satt en grense for hvilken verdi man tolererer, altså hvilken risiko man aksepterer. Uavhengig av om tallverdien er for høy eller ikke, vil man prøve å iverksette tiltak for å redusere risikoen og få tallverdien så lav som mulig. Dersom risikoreduserende tiltak ikke er nok for å få en akseptabel tallverdi, anses aktiviteten eller trusselen for stor. Til slutt må vurderingene formidles gjennom skriftlige dokumenter, hvor usikkerhetene kan synliggjøres.

En slik systematisk og metodisk prosess vil lede til en grundig risikovurdering og økt bevissthet blant alle involverte. Like viktig som resultatet er prosessen, og gjør de involverte i stand til å handle når situasjoner oppstår. Sammen med de risikoreduserende tiltakene er derfor den økte bevisstheten med en slik prosess en stor gevinst

Beskriv hovedtrekkene i arkitekturanalyse. Hvilke ulike deler av CIA-triangelet rokker elementene i STRIDE ved?

Arkitekturanalyse er en av de viktigste aktivitetene man kan gjøre i arbeidet med å sørge for programvaresikkerhet, og faller inn under domenet *Trykkpunkter* i rammeverket for programvaresikkerhet, *Building Security In Maturity Model (BSIMM)* (Bergsjø & Windvik, 2020, s. 222). Domenet omfatter praksiser og tiltak assosiert med analyse for å styrke programvaresikkerheten. Programvaresikkerhet handler om å sørge for at all funksjonalitet er sikker, og omfatter programvaren fra den utvikles til implementering og vedlikehold. Den generelle oppfatningen av at absolutt sikkerhet ikke er oppnåelig (Lampson, 2004), gjelder

også for programvaresikkerhet. Det finnes imidlertid flere aktiviteter og tiltak man kan gjennomføre for å bedre sikkerheten.

Arkitekturanalyse på et overordnet nivå har som formål å fungere som kvalitetskontroll, og omfatter en trusselmodellering for å sørge for at strukturelle sikkerhetsfeil oppdages og korrigeres. Dette innebærer å avdekke implementeringsfeil, og kanskje enda viktigere å avdekke designfeil som sannsynligvis vil utgjøre en større risiko i programvaren. En enkel beskrivelse som i mange tilfeller vil være nyttig, er å modellere systemet ved hjelp av et oversiktlig diagram som viser hvordan det helhetlige systemet er bygd opp og henger sammen. Dette vil danne grunnlaget for den videre analysen, som innebærer tre kritiske steg – *motstandsdyktighet mot angrep, tvetydigheter* og *sårbarheter i underliggende systemer* (Bergsjø & Windvik, 2020, s. 223).

Motstandsdyktighet mot angrep handler om å vurdere hvordan systemet evner å håndtere kjente angrep, og kan gjerne ta utgangspunkt i huskelisten STRIDE. STRIDE er en sjekkliste for ulike typer angrep, og vil kunne fungere som et hjelpemiddel for å vurdere hvor motstandsdyktig programvaren er for de ulike typene angrep (Swiderski & Snyder, 2009). I grove trekk handler en analyse av motstandsdyktighet om å finne feil i beskrivelsen av systemet og kartlegge angrepsmønstre for hvordan disse feilene kan utnyttes. Basert på sjekklister som STRIDE, vil man søke å identifisere risikoer i systemets arkitektur. Videre skal hver av angrepstypene vurderes for å finne ut hvor gjennomførbare de er. Til slutt vil man sitte igjen med en forståelse av hvor motstandsdyktig programvaren er med hensyn til de ulike angrepstypene. Sjekklisten kan også kombineres med DREAD, som er en tilsvarende liste som klassifiserer angrepet alvorlighetsgrad. På bakgrunn av analysene fra STRIDE og DREAD vil man ha et grunnlag for å prioritere tiltak for å bedre programvaresikkerheten.

Den neste analysen handler om å kartlegge systemets **tvetydigheter**. Dette er en kreativ tilnærming til å oppdage nye risikoer, og fungerer best dersom erfarne analytikere analyserer systemene hver for seg for deretter å samles (Bergsjø & Windvik, 2020, s. 224). En tvetydighet kan best beskrives som en uenighet om hvordan en funksjon i systemet er ment til å virke, og som potensielt kan utnyttes av en angriper. Det vil være viktig å etablere en forståelse for de tvetydighetene som finnes i systemet, og korrigere disse så fort som mulig som et risikoreduserende tiltak.

Den siste analysen handler om å vurdere **sårbarhetene i det underliggende systemet**. Her ser man i større grad på systemets avhengigheter, som plattformen systemet kjører på og eksterne biblioteker som benyttes. Ved å gjennomføre en slik analyse vil man kunne få oversikt over og tilgang til oppdaterte feil og sårbarheter i det sammensatte systemet. Ved å inkludere de underliggende sårbarhetene i systemet, vil man kunne utforske systembeskrivelsen i sin helhet, og danne seg en best mulig oversikt over sårbarheter som potensielt kan utnyttes.

STRIDE og CIA-triangelet

STRIDE er som tidligere nevnt en sjekkliste for typer angrep. De ulike typene angrep vil påvirke de tre elementene i CIA-triangelet i ulik grad. Konfidensialitet (confidentiality) handler om å forhindre uautorisert formidling av informasjon, integritet (integrity) går ut på

at informasjon er konsistent og ikke endres av uautoriserte, og tilgjengelighet (availability) innebærer at informasjon og ressurser er tilgjengelig for autorisert personell når de trenger det. Angrep som går utover CIA-triangelet er altså hendelser som vil utgjøre en risiko for informasjonssikkerhet.

Spoofing handler om å utgi seg for å være noen andre, som muliggjør tilgang til informasjon man ellers ikke ville hatt tilgang på. Dette rokker ved elementet *konfidensialitet* ved at uvedkommende kan få tilgang på informasjon som vedkommende ikke skal ha tilgang til. Videre kan spoofing føre til at uvedkommende får rettighet til å endre på data, noe som går utover *integritet* og til og med *tilgjengelighet* dersom passord blir endret. Likevel vil slik endring av data passe bedre inn under angrepstypen tampering.

Tampering er når det gjøres urettmessige endringer i data. Dette kan innebære at uvedkommende får tilgang til å endre på data de i utgangspunktet ikke har rettighet til å endre på. Det er klart at slike endringer påvirker *integriteten* til informasjonen, i tillegg til å påvirke dataenes *tilgjengelighet*. Endringer i datagrunnlag kan få katastrofale konsekvenser, for eksempel ved endring eller sletting av pasientjournaler. En helsearbeider har behov for korrekt og oppdatert informasjon om pasientene for å kunne gi riktig behandling. En endring eller sletting av slike data vil potensielt utgjør en fare for pasientens liv dersom feil behandling gis.

Repudiation går ut på at en person forsøker å fornekte at vedkommende har gjennomført en handling. Det motsatte av fornektelse handler om å kunne autentisere og stole på at entiteten er den personen den faktisk utgir seg for å være, i tillegg til å kunne stole på dataen som behandles. Som et eksempel kan man ta for seg digitale signaturer, eksempelvis når du betaler en regning i nettbanken. En slik signatur er vanskelig å fornekte, da man gjennomgår strenge rutiner for autentisering som verifiserer at du er den du utgir deg for å være. Fornektelse kan utfordre programvarens *integritet* ved at man ikke kan bevise hvem som har gjort endringer i data.

Information disclosure handler om hvor utsatt programvaren er for røping av informasjon. Dette kan skje dersom en nettside eller en applikasjon avslører informasjon til uautoriserte brukere, som dermed også får muligheten til å endre informasjon. Andre angrepstyper, eksempelvis spoofing, vil kunne lede til røping av informasjon, og er et eksempel på hvordan de ulike angrepstypene kan kombineres av organiserte aktører. Dersom programvaren er utsatt for slike angrep vil det være en svakhet i *konfidensialiteten* og *integriteten* til programvaren.

Denial of service handler om angrep med den hensikt å blokkere eller nekte programvare å yte tjenester. Slike angrep skjer ofte ved å overbelaste systemer gjennom å sende en rekke tjenesteforespørsler som systemet ikke evner å håndtere. Brukerne får da ikke tilgang til systemet og data vil dermed ikke være mulig å behandle. Tjenestenekt påvirker på denne måten elementet *tilgjengelighet*.

Ransomware er et eksempel på angrep som utfordrer alle sikkerhetsmålene i CIA-triangelet. Ransomware eller løsepengevirus er en klassisk svindelmetode hvor angriperne krypterer enkeltpersoners harddisk eller større organisasjoners systemer, slik at de kan kreve store

pengesummer for å gi opp kontrollen av systemet eller maskinen (Eneroth et. al, 2022, s. 28). Dersom en virksomhet blir utsatt for et slikt angrep vil dataene bli tilgjengelig for uvedkommende, og vil også være gjenstand for endring. Dataens tilgjengelighet blir også påvirket ved at virksomhetene ofte må betale store pengesummer for å få kontroll på dataen igjen.

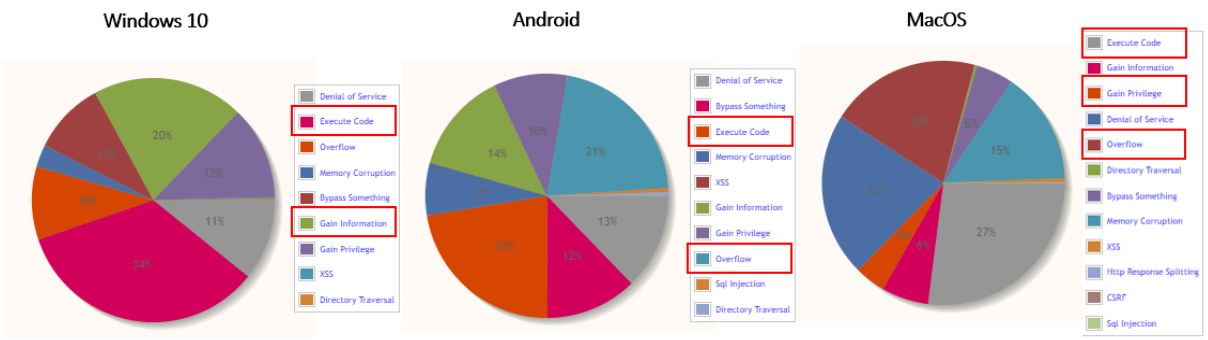
Elevation of privilege er en handling som går ut på å utnytte en implementerings- eller designfeil for å få tilgang på ressurser og informasjon som vanligvis ikke er tilgjengelig for vedkommende. Dette innebærer å utnytte sårbarheter for å få tilganger man egentlig ikke ville hatt, og kan eksempelvis være en vanlig bruker i et system som oppnår en form for administratorrettighet. Dette vil kunne føre til at brukeren får tilgang på informasjon som i utgangspunktet ikke var tiltenkt brukeren, i tillegg til å kunne gjøre endringer på dataen. Denne formen for angrep kan påvirke *konfidensialitet* ved at en bruker får urettmessig tilgang til data og *integritet* ved at vedkommende kan få tilgang på å endre dataen. Videre kan man med et slikt type angrep få rettigheter i systemet til å stenge andre ute, noe som vil gå utover *tilgjengeligheten til systemet.*

Sårbarheter i operativsystem

I denne oppgaven skal vi sammenligne operativsystemer med hensyn til programvaresikkerhet, med utgangspunkt i OWASP Top Ten (Open Web Application Security Project). OWASP presenterer ti av de viktigste sårbarhetene for webapplikasjoner, og oppdateres med jevne mellomrom. En komplett liste over de ti viktigste sårbarhetene vises i figur 5. På bakgrunn av sammenligningen vil vi drøfte hva man bør ta høyde for før man implementerer et operativsystem i en virksomhet.

Figur 5 OWASP Top Ten, 2021.

Dataene er hentet fra nettsiden cvedetails.com, hvor man har samlet sårbarheter fra et bredt spekter av operativsystemer, leverandører og produkter (CVE Details, 2022). De ulike sårbarhetene er beskrevet med hvordan sårbarheten påvirker CIA-triangelet, i tillegg til en beskrivelse av hvor kompleks sårbarheten er, samt en rangering som sier noe om alvorlighetsgraden. Klikker vi oss på inn på et bestemt operativsystem, får vi med en gang en rask oversikt i en tabell som viser antall sårbarheter oppdaget per år, med kategorier for hvilke type sårbarheter det er. Videre kan vi klikke oss inn på hver enkelt sårbarhet og se alvorlighetsgraden av disse. Vi har valgt å sammenligne tre av de mest brukte operativsystemene i verden, MacOS (tidligere MacOS X), Windows 10 og Android. Figur 6 illustrerer de vanligste sårbarhetene knyttet til de forskjellige operativsystemene i perioden 2009 - 2022.



Figur 6 De vanligste sårbarhetene for de tre valgte operativsystemene.

En fellesnevner for sårbarheter på tvers av de forskjellige operativsystemene finner man i typene *execute code* og *overflow*. Førstnevnte er på topp tre blant alle tre systemene, mens overflow er blant topp tre for Android og MacOS. For Windows 10 er også mange av sårbarhetene relatert til *gain information*, og skiller seg noe ut fra de to andre systemene. Disse angrepene utføres ofte i kombinasjon ved at serverne får tilsendt en mengde forespørsler de ikke evner å håndtere, som fører til at angriperne får mulighet til å kjøre ekstern kode på systemene (CVE Details, 2022). Sårbarhetene knyttes til A01, A03, A04 og A10 i OWASP liste over sårbarheter, hvor det ofte oppgis at sårbarhetene utnyttes gjennom eksterne biblioteker, injisering av SQL-kode og på grunn av dårlig aksesskontroll.

Når man skal vurdere hvilke operativsystem som skal tillates i bedriften er det ikke tilstrekkelig å kun basere seg på antall sårbarheter som knyttes til operativsystemet. Eksempelvis har Android 4245 registrerte sårbarheter, MacOS har 2980 og Windows 10 har 2694. For å sette dette i perspektiv, kan vi trekke frem et mindre brukt operativsystem som AIX, med sine 88 sårbarheter. Det er mange faktorer som kan bidra til at operativsystemene MacOS, Android og Windows 10 havner høyt oppe på listen over antall sårbarheter. Dette er tre store operativsystemer med mye funksjonalitet som brukes av millioner av mennesker hver eneste dag. Jo større de er og mer funksjonalitet operativsystemet har, jo mer komplekse kan vi si at de er. Komplekse IT-systemer gjør at det er lettere å begå, og overse, feil som medfører sårbarheter (Bergsjø & Windvik, 2020, s. 130). Målbarhet er derfor en utfordring når det gjelder programvaresikkerhet. I stedet for å sammenligne faktorer som antall sikkerhetsfeil eller hvor mange offentlig kjente angrep som har lyktes mot programmene, er det enklere å måle *andreordens virkninger* (Bergsjø & Windvik, 2020, s. 221-222). Dette ledet videre til det tidligere nevnte rammeverket for programvaresikkerhet - BSIMM. Rammeverket tar for seg distinkte aktiviteter, rangert etter virksomhetens modenhetsnivå. Alle aktivitetene er ikke nødvendigvis relevante for alle virksomheter, men rammeverket er ment som et måleverktøy for sikkerheten til en programvare. Ved å ta utgangspunkt i rammeverket, vil virksomheten ha bedre forutsetninger for å ivareta programvaresikkerheten, kombinert med kunnskap om hvilke sårbarheter de er mest utsatt for, hvor OWASP Top Ten vil være et nyttig hjelpemiddel.

Som vi tidligere har sett, vil økt kompleksitet gjøre det vanskelig å få oversikt alle svakheter som eksisterer i programvaren. Det vil med andre ord være utfordrende å etablere en god systembeskrivelse, med alle avhengigheter og funksjonalitet. En arkitekturanalyse kan i

denne sammenheng være et nyttig verktøy for å danne forståelse for hele systemet med avhengigheter og underliggende systemer.

Videre vil programvarens utbredelse og utstrakte bruk gjøre det mer lukrativt for trusselaktører å forsøke å finne svakheter i programvaren. Dette kan være faktorer som spiller inn med tanke på antall feil som oppdages for de tre populære operativsystemene. Det skal også nevnes at det ikke nødvendigvis er en utelukkende negativ faktor at sårbarhetene er identifisert, da dette gir leverandøren mulighet til å tette sårbarhetene.

Nettsiden har i tillegg tallfestet alvorlighetsgraden av hver sårbarhet. Dette er en viktig faktor når man skal bestemme seg for hvilket operativsystem man kan tillate i bedriften, men det kan være vanskelig å vite hvilke faktorer man skal legge mest vekt på. *Common Vulnerability Scoring System (CVSS)* er en standard for å uttrykke sårbarheters alvorlighetsgrad (Bergsjø & Windvik, 2020, s. 133). Sårbarheter gis en score fra ingen (0) til kritisk (10), og baserer seg på hvor sannsynlig det er for utnyttelse og konsekvensene av en eventuell utnyttelse. Hvis vi ser på alvorlighetsgraden av sårbarheter det siste året, kan vi se at MacOS har flest kritiske sårbarheter på nivå 9-10, men både Windows 10 og Android har flere sårbarheter med middels til høy alvorlighetsgrad. Videre har Android, som er det operativsystemet med flest sårbarheter, også flest sårbarheter med alvorlighetsgrad 7-10. Her er det MacOS som har færrest. Hvis vi går inn på sårbarhetene som rangeres som mest alvorlig, kan vi se at det hovedsakelig er sårbarhetene som tillater trusselaktørene å kjøre ekstern kode i programvaren. Disse sårbarhetene kan potensielt gå utover konfidensialiteten av OSet ved at trusselaktøren får tilgang på data, integritet ved at trusselaktøren gjør endringer i data og tilgjengelighet ved at trusselaktøren overstyrer programmet eller på andre måter tvinger det til å stenge ned tjenester. Av sårbarhetene som rangeres mellom syv og ni er de fleste typer som tillater injisering av SQL spørringer. Slike sårbarheter kan i likhet med ekstern kode, potensielt påvirke alle tre sikkerhetsmålene ved at trusselaktøren får tilgang, endrer eller sletter data.

Det er tydelig at det er vanskelig å bruke slike data til å sammenligne tre såpass like systemer. Det er klart at sårbarheter som tillater trusselaktører å kjøre ekstern kode i operativsystemet kan ha store konsekvenser, men hvor mye større konsekvensene for denne sårbarheten er i forhold til SQL-injisering kan være vanskelig å si. Hvilket operativsystem man velger å benytte i en virksomhet må ta utgangspunkt i behov for funksjonalitet, og krever at man er kjent med operativsystemets sårbarheter, samt alvorlighetsgraden av de. I dette tilfellet vil utfallet være avhengig av hvilken data man ønsker å legge vekt på selv, siden det ikke er et system som objektivt peker seg ut som det beste. På et generelt grunnlag kan vi derfor si at rangeringen av systemet basert på antall sårbarheter ikke har så mye å si. Enhver virksomhet bør derfor ta utgangspunkt i rammeverket for programvaresikkerhet (BSIMM) og gjennomføre de aktivitetene som anses som relevante. Vel så viktig er det å være bevisst på at det finnes sårbarheter som kan utnyttes, og at man uansett hva man velger, har en gjennomtenkt strategi på hvordan man skal forebygge sikkerhetshendelser og håndtere disse når situasjoner oppstår.

Referanser

Bergsjø, H., & Windvik, R. (2020). *Digital sikkerhet - En innføring*. Universitetsforlaget.

CVE Details. (2022). *Top 50 Products*. https://www.cvedetails.com/top-50-products.php

NSM. (2021, Juni). *Risikovurderinger av IKT-systemer*. https://nsm.no/getfile.php/136603-1625054089/Filer/Bildegalleri/Bilder%20til%20grunnprinsipper/Risikovurdering%20av%20IKT-systemer.pdf

Swiderski, F., & Snyder, W. (2009). *Threat Modeling*. Redmond: Microsoft Press.

Standard Norge. (2012, Juni 1). *Samfunnssikkerhet - Beskyttelse mot tilsiktede uønskede handlinger.* https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=718201

Eneroth, C., Nilsen, H. T., Furberg, P. (2021). Digital sikkerhet 2021. *Telenor.* *https://www.telenor.no/binaries/om/digital-sikkerhet/digitalsikkerhet2021.pdf*

Øving 6 - Sikkerhetsstyring

Hva innebærer det at en virksomhet skal ha et styringssystem for sikkerhet?

I NSMs veiledning for sikkerhetsstyring beskrives det hvordan sikkerhetsstyring «(…) handler om systematiske aktiviteter som er nødvendige for å oppnå og opprettholde et forsvarlig sikkerhetsnivå for virksomhetens skjermingsverdige verdier» (NSM, 2020). En viktig del av disse systematiske aktivitetene, er etableringen av et styringssystem for sikkerhetsarbeid. Systemet skal omfatte hvordan forebyggende sikkerhetsarbeid skal gjøres med hensyn til planlegging, etablering, gjennomføring og forbedring. Uavhengig av om virksomheten vurderer sine verdier som skjermingsverdige, kreves det at virksomheten har et styringssystem på plass så lenge de omfattes av sikkerhetsloven. Verdiene som skal beskyttes må ses opp mot den relevante trusselen, og til slutt baseres på en grundig risikovurdering, slik vi redegjorde for i forrige øvingsoppgave. At sikkerhetssystemet skal omfatte alle aktiviteter knyttet til det forebyggende sikkerhetsarbeidet, innebærer at systemet også må understøtte aktiviteter som ikke defineres direkte som sikkerhetstiltak. Dette inkluderer avhengigheter til andre virksomheter og aktiviteter som sikkerhetsledelse og oppfølging. NSM legger vekt på at det forebyggende sikkerhetsarbeidet skal være en kontinuerlig prosess da trusselbildet er i konstant endring. På grunn av dette må prinsippene for sikkerhetsstyring følge de grunnleggende prinsippene for styring og kontinuerlig forbedring. På samme måte som sikkerhetsrutiner og -tiltak må gjennom de samme fasene for å være oppdaterte, må virksomheten ha samme tilnærming for styringssystemet. Systemet må implementeres i virksomhetsstyringen som helhet, og kontinuerlig kontrolleres og forbedres.

Et styringssystem kan ifølge NSM med fordel etableres i henhold til internasjonale standarder, slik som ISO 27001 (NSM, 2020). Standarden beskriver hvordan etableringen og implementeringen av et styringssystem påvirkes av virksomhetens behov og mål, sikkerhetskrav, de organisatoriske prosessene samt størrelsen og strukturen på virksomheten. Formålet med etableringen av et slikt system er å ivareta de tre sikkerhetsfaktorene for informasjonssikkerhet gjennom å benytte en risikostyringsprosess. En prosess for risikostyring har som formål å redusere den totale risikoen for virksomheten, gjennom å være bevisst sine verdier, identifisere trusler og avdekke sårbarheter. På bakgrunn av denne prosessen, må risiko håndteres ved å etablere sikkerhetstiltak, som igjen er tilpasset de skjermingsverdige verdiene virksomheten forvalter, for å redusere sårbarhetene som er blitt avdekket. Denne beskrivelsen av risikostyringen er ment som et illustrativt eksempel på hva som blant annet skal inngå som en del av styringssystemet for sikkerhetsarbeid, og demonstrerer kompleksiteten til systemet.

Hva menes med sikkerhetsledelse?

I henhold til Sikkerhetsloven stilles det krav til at *«virksomhetens leder har ansvaret for det forebyggende sikkerhetsarbeidet»* (Sikkerhetsloven, 2019, §4-1). Med dette menes at lederen har ansvar for å utøve sikkerhetsledelse, som omfatter alt arbeid relatert til sikkerhetsarbeid i virksomheten, herunder prinsipper for forebyggende sikkerhetsarbeid, fordeling av ansvar og myndighet for gjennomføring av arbeidet, tilrettelegging og oppfølging. Det må understrekes at lederen selv ikke skal gjøre alle aktivitetene knyttet til sikkerhetsarbeid, men er til slutt ansvarlig for at arbeidet som gjøres gir forsvarlig sikkerhet

som resultat. Forsvarlig sikkerhet innebærer at virksomhetens verdier beskyttes på tilstrekkelig vis. Det stilles krav til utarbeidelse av et styringsdokument som dokumenterer de nevnte aktivitetene relatert til sikkerhetsledelse. Dokumentet skal gjøres kjent og være tilgjengelig internt i virksomheten og for eksterne samarbeidspartnere. Styringsdokumentet er ikke bare nødvendig for å oppfylle virksomhetens plikter etter sikkerhetsloven, men sørger også for legitimitet og tillit.

En viktig del av sikkerhetsledelse er å tilrettelegge og følge opp arbeidet som gjøres. Som en del av tilretteleggingen, er det kritisk å sørge for at de riktige ressursene og kompetansen er til stede. Dette innebærer å tildele sikkerhetsarbeidet tilstrekkelig med ressurser, både menneskelige og økonomiske, for å kunne utøve aktivitetene relatert til det forebyggende sikkerhetsarbeidet på en tilfredsstillende måte. Sikkerhetsarbeidet må som nevnt utvikles, og i forlengelse av dette må virksomhetens ansatte gis nødvendig kompetanse og opplæring for å kunne løse de gitte oppgavene. Ved å se på aktivitetene knyttet til sikkerhetsledelse, ser vi hvordan ledelsen av sikkerhetsarbeid også er knyttet til den sykliske prosessen og kravet om kontinuerlig forbedring. Lederen har det overordnede ansvaret for å følge opp at virksomheten hele tiden er i utvikling for å være i stand til å håndtere et trusselbilde i konstant endring.

Hva er en **sikkerhetsleder**, og hva er vedkommendes ansvar og arbeidsoppgaver?

En del av sikkerhetsledelse, er som nevnt å fordele ansvar og myndighet for gjennomføring av sikkerhetsarbeidet. Som en del av dette følger også tilrettelegging gjennom relevant informasjon, opplæring og vedlikehold av kompetanse for å kunne løse de gitte oppgavene. Som en del av sikkerhetsorganisasjonen, som omfatter alle som utfører aktiviteter med betydning for sikkerhet, er en sikkerhetsleder en som kan utpekes med et ekstra ansvar for å følge opp det forebyggende sikkerhetsarbeidet. Slik myndigheten er fordelt og sikkerhetsorganisasjonen er bygd opp er det ledelsen som utarbeider prinsipper og overordnede føringer, samt følger opp arbeidet. I virksomheter som benytter digital teknologi i utstrakt grad kan det være behov for å delegere ansvar til linjeledere. Disse linjelederne får ansvar for sikkerhetsarbeidet innen hvert sitt myndighetsområde, og hver medarbeider har ansvar for at eget arbeid er i tråd med virksomhetens føringer og bestemmelser. Som en del av tilpasningen til virksomhetens skjermingsverdige verdier, kan virksomheten utpeke enkelte roller med dedikerte oppgaver i sikkerhetsarbeidet. En sikkerhetsleder har som hovedoppgave å **følge opp** det sikkerhetsarbeidet som gjøres, hvor et viktig prinsipp er at utførelse- og oppfølging av sikkerhetsarbeid må skje uavhengig av hverandre. En ansatt må eksempelvis ikke være den som følger opp og kontrollerer sitt eget sikkerhetsarbeid. Det er viktig at personen som får ansvar for oppfølging, er frittstående fra sikkerhetsarbeidet, og kan gjøre objektive vurderinger. Sikkerhetslederens ansvar ligger da primært innen tilrettelegging og oppfølging av sikkerhetsarbeidet, og kan omfatte oppgaver som kompetansebygging innen sikkerhet, rådgivning for sikkerhetsarbeidet, samt evaluering og forbedring av virksomhetens sikkerhetsarbeid. Sikkerhetslederen er virksomhetens leders forlengede arm, som har fått et ekstra ansvar og myndighet for å sørge for at arbeidet som gjøres gir tilstrekkelig sikkerhet som resultat. Sikkerhetslederen må derfor innlemmes som en del av den sykliske prosessen, hvor vedkommende må kontrollere og forbedre virksomhetens forebyggende sikkerhetsarbeid. For å ha forutsetninger for å løse disse oppgavene, er det

kritisk at sikkerhetslederen har god oversikt over virksomhetens verdier og en god forståelse av risikovurdering og -håndtering.

Hvilke krav gjelder for å ha tilfredsstillende sikkerhetsdokumentasjon?

Styringssystemet for sikkerhet i en virksomhet må være tilstrekkelig dokumentert, og dokumentasjonen skal gjøre rede for hvordan sikkerhetsarbeidet skal utføres og kontrolleres (NSM, 2020). Dokumentasjonen må tilpasses virksomhetens verdier, og må tilpasses et trusselbilde i stadig endring på lik linje med resten av det forebyggende sikkerhetsarbeidet.

Kravene som stilles til dokumentasjon av systemet for sikkerhetsstyring fremkommer gjennom Sikkerhetsloven. Her stilles det krav til dokumentasjon av risikovurdering og -håndtering, samt hvordan styringssystemet for sikkerhet og sikkerhetstiltakene skal gi et forsvarlig sikkerhetsnivå (Sikkerhetsloven, 2019, §4-4, §5 og §11). Formålet med sikkerhetsdokumentasjon er å sikre at aktiviteter utføres på en sikker måte og som besluttet i henhold til sikkerhetsstyringssystemet. Dokumentasjonen vil i tillegg fungere som et grunnlag for håndtering av uønskede hendelser, ved at man kan se tilbake på de beslutninger og resultater av arbeidsutførelse for å gjøre en vurdering av hvor det har gått galt. Sikkerhetsdokumentasjon må også beskyttes, på lik linje som skjermingsverdig informasjon, og må oppbevares i henhold til Sikkerhetsloven og virksomhetsforskriften.

Styringssystemet for sikkerhet kan dokumenteres gjennom ulike dokumenter, hvor NSM fremhever tre sentrale. Styrende dokumenter beskriver både eksterne og interne føringer for det forebyggende sikkerhetsarbeidet, og kan eksempelvis være det tidligere omtalte styringsdokumentet som ledelsen utviklet. Utførende dokumenter beskriver hvordan aktiviteter direkte relatert til sikkerhet utføres. Dette kan gjelde prosedyrebeskrivelser, handlingsplaner og sikkerhetstiltak. Til slutt skal de kontrollerende dokumentene beskrive resultatene fra gjennomføring av aktiviteter relatert til sikkerhet, og kan benyttes i arbeidet med å kontrollere og forbedre virksomhetens sikkerhetsarbeid.

Referanser

Standard Norge. (2017). *Informasjonsteknologi, Sikringsteknikker, Ledelsessystemer for informasjonssikkerhet, Krav, (ISO 27001:2013).* https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=925900

NSM. (2020, 29. mai). *Veileder i sikkerhetsstyring*. https://nsm.no/getfile.php/132933-1591350417/Filer/Dokumenter/Veiledere/veileder-i-sikkerhetsstyring.pdf

Lovdata. (2019, 1. januar). *Lov om nasjonal sikkerhet (sikkerhetsloven).* https://lovdata.no/dokument/NL/lov/2018-06-01-24