Handelshøyskolen BI

MAN 51661 Digital sikkerhet for ledere

Term paper 60% - W

Predefinert informasjon

Startdato:	09-02-2022 09:00	**Termin:**	202210
Sluttdato:	27-05-2022 12:00	**Vurderingsform:**	Norsk 6-trinns skala (A-F)
Eksamensform:	P		
Flowkode:	202210||11587||IN08||W||P		
Intern sensor:	(Anonymisert)		

Deltaker

Erlend Ørjasæter, Rachid Elgarh

Informasjon fra deltaker

Tittel *:	Digitale trusler mot politietaten
Navn på veileder *:	Nils-Otto Ørjasæter

Inneholder besvarelsen konfidensielt materiale?:	Nei	**Kan besvarelsen offentliggjøres?:**	Ja

Gruppe

Gruppenavn:	(Anonymisert)
Gruppenummer:	11
Andre medlemmer i gruppen:	

Innholdsfortegnelse

Sammendrag

I likhet med samfunnsutviklingen har politiets digitale infrastrukturer og systemer er blitt mer komplekse, omfattende og integrerte. Når politiet introduserer ny teknologi for å sikre effektivitet, kommunikasjon og samhandling øker antall menneskelige kontaktflater og med dette nye sårbarheter man ikke engang visste eksisterte. Skillelinjene mellom profesjonell og privat sfære kan bli mer utydelige, og igjennom sosial manipulasjon kan trusselaktør utnytte dette uklare skille for å avdekke eller misbruke passord og brukernavn. Digitale systemer og innebygd sikkerhet er blitt sikrere, og av den grunn har angripere i økende grad skiftet fokus til det menneskelige elementet for å bryte seg inn i virksomheters informasjonssystemer. Dette innebærer at betydningen av den menneskelige faktor ikke kan overdrives. Det å redusere sårbarheter relatert til dette er blitt stadig mer avgjørende for å ivareta god informasjonssikkerhet. Sosial manipulering og phishingangrep har med dette økt i omfang. Forskjeller i målsetninger, behov og interessesfærer vil videre komplisere arbeidet med å implementere et sikkerhetsprogram som motiverer ansatte til å endre sin digitale brukeradferd. Totalt sett kan dette resultere i at politietaten blir mer sårbar for sosial manipulering og phishingangrep. Dette kan i ytterste konsekvens gå utover etatens evne til å utføre sitt samfunnsoppdrag.

Politietatens virksomheter burde starte med å kartlegge hvilke subkulturer og menneskelige barrierer som eksisterer internt, før de iverksetter et sikkerhetsprogram. Dette kan gjøres ved å benytte Kotters 8-trinnsmodell og en LEAN-tilnærming hvor testing, justering og implementering av tiltak skjer i tett dialog med brukermiljøet. Dette kan redusere feilmarginer fordi i store virksomheter som politietaten har ulike enheter og deres ansatte forskjellige behov hvorpå de representerer ulike risikoer og sårbarheter. Sikkerhetsprogrammet og bevisstgjøringsarbeidet burde derfor ikke generaliseres for å sikre ønsket effekt, nemlig økt motstandsdyktighet mot phishingangrep igjennom bedre digital brukeratferd. Det er fordelaktig at framtidige sikkerhetsprogram baseres på ulike scenarioøvelser, spill og konkurranser. Dette vil øke brukerrelevansen, motivere ansatte mer personlig og styrke læringsutbytte og stimulere til å endre digital persepsjon og brukeradferden. Sikkerhetsprogrammer for endringer av brukeradferd må derfor planlegges, organiseres og kontrolleres for å kunne administreres på en god måte. Etter testing av og justering av tiltak konkluderes det med at samtlige tre forslag anbefales implementert på lang sikt. Imidlertid er ikke dette gjennomførbart på kort sikt, og av den grunn faller endelig anbefaling på at PIT fortsetter å videreutvikle konseptet med det digitale kurset kalt sikkerhetsskolen. Sett under ett er dette tiltak som er egnet til å styrke politietatens motstandsdyktighet mot phishingangrep igjennom god brukeratferd.

Innledning

Politiet har en kritisk samfunnsfunksjon, samtidig som at de har mange tjenester som skal være tilgjengelige når mye annet i samfunnet ikke fungerer. Dette gjelder også de digitale løsningene. Dette må derfor sikres godt. Digitaliseringen av politiet i Norge har effektivisert og profesjonalisert etaten betraktelig de seneste årene og etaten har i økende grad har blitt avhengig av informasjonsteknologi (IT) for å ivareta sitt samfunnsoppdrag. I takt med denne utviklingen har digitale sårbarheter og trusler økt parallelt. Ifølge Europols årlige cybersikkerhetsrapport er phishing en av de største truslene mot privatpersoner og organisasjoner (Europol, 2019). Dette fordi angrepene er blitt mer sofistikerte og vanskelige å beskytte seg mot. Igjennom phishingangrep kan ondsinnede aktører skaffe seg tilgang til systemer og informasjon via virksomhetenes ansatte (Abawajy, 2014a). Nylig har det blir rapportert om økning i antall phishingangrep og utviklingen ser ikke ut til å avta (Deloitte, 2022). Denne utviklingen kommer på bakgrunn av at de digitale systemenes innebygde sikkerheten er blitt bedre, og virksomheter er derfor mer beskyttet nå enn tidligere. Dette har medført at angriperne har skiftet fokus over til det menneskelige element for å bane seg adgang til virksomhetenes verdier (Abawajy, 2014a).

Politiets oppgaver og opplysningene etaten har tilgjengelig og behandler, gjør etaten til et særlig attraktivt mål for etterretning, spionasje og angrep i det digitale rom. Skulle en målrettet aktør lykkes med å angripe å få tilgang til politiets IKT-systemer kan det ramme etatens evne til å utføre sitt samfunnsoppdrag. Kommer sensitiv informasjon politiet forvalter på avveie kan det vanskeliggjøre bekjempelse av kriminalitet, skade politioperasjoner, sette tredjepersoners sikkerhet i fare og skade etatens tillit og omdømme (*Riksrevisjonens rapport*, 2018). Flere virksomheter i Norge har de senere årene blitt utsatt for denne typen angrep, noe angrepet på Hydro, Helse Sørøst og NAV Østre Toten illustrer. Sosial manipulering ved phishing utfordrer politietaten på helt nye måter. Oppgavens problemstilling er derfor som følger:

1. **Hvordan kan sosial manipulering, herunder phishing, utgjøre en trussel mot Politiet?**
2. **Hvordan kan politiet endre digital brukeradferd for å øke motstandsdyktigheten mot denne type trussel?**

Leseveiledning og oppgavens oppbygning

Første del av oppgaven omhandler problemidentifisering og hvordan phishing kan utgjøre en trussel mot politiet. Problemidentifiseringen besvares igjennom bruk av både sekundærlitteratur og primærdata fra intervjuer. Dataen som er brukt i først del av oppgaven er fra informanter med ekspertise på digital sikkerhet i politiet og samtlige omtales med fornavn. Viser til metodekapittelet for ytterligere informasjon. I teoridelen vil det redegjøres for relevante teorier brukt til å besvare oppgavens problemstilling. I analysekapittelet presenteres de mest sentrale hovedfunn og tiltakene som er testet. Videre diskuteres viktige suksessfaktorer for at tiltakene skal oppnå ønsket endringseffekt, før vi i oppgavens siste del avslutter med en konklusjon og anbefaling.

Avgrensning

Oppgaven avgrenses til kun omfatte organisatoriske aspekter som kan bidra til endring av digital brukeradferd egnet til å øke motstandsdyktigheten mot phishing. Innebygd sikkerhet som tekniske sikkerhetsinstallasjoner, systemer, programvare, nettverk eller andre tekniske konfigurasjoner vil ikke omfattes.

Problemidentifisering

I sin rapport fra 2018 får politietaten sterk kritikk fra Riksrevisjonen på en rekke punkter. Blant annet påpekes det at er mangelfullt arbeid, planlegging og oppfølging av informasjonssikkerheten. Informasjonssikkerhet kan defineres som *«beskyttelse av informasjonens konfidensialitet, integritet og tilgjengelighet»* (Jøsang, 2021, s. 17) Dette arbeidet vanskeliggjøres ytterligere av kompleks organisering med fragmenterte ansvarsforhold mellom Politidirektoratet (POD), Politiets IKT-tjenester (PIT) og politidistriktene (PD) (*Riksrevisjonens rapport*, 2018). Politietaten består i dag av 18.689 ansatte (både politi og sivilt utdannede) fordelt på 12 politidistrikter og 9 særorganer inkludert politidirektoratet (*Bemanningsstatistikk i Politiet*, 2022). Etaten er geografisk spredt i tillegg til organisatorisk differensierte bestående av ulike kompetansemiljøer og mange spesialiserte underenheter. Disse faktorene gjør det svært utfordrende for etaten å holde oversikt over alle de potensielle sårbarheter, uønskede hendelser og avvik relatert til informasjonssikkerheten. Politietaten mangler med dette oversikt over sikkerhetstilstanden, slik at kunnskapsgrunnlaget for kontinuerlig læring og forbedring blir mangelfullt. Videre hindrer dette etterlevelse av instrukser og

rutiner, i tillegg til det å sikre en tilstrekkelig bevissthet rundt god digital brukeratferd og hvorfor dette er viktig (*Riksrevisjonens rapport*, 2018). Ifølge Simen kan derfor digital sikkerhet bli oppfattet som et hinder i arbeidshverdagen og medføre at ansatte tar snarveier, som eksempelvis å bruke samme brukernavn og passord privat som i jobbsammenheng. Dette illustrerer en brukeratferd som potensielt gjør en mer sårbar mot phishing, fordi at trusselaktører kan utnytte dette uklare skillet. Eksempelvis kan en angriper manipulere til seg brukerinformasjon, og misbruke denne videre til å sende skadelige vedlegg via e-post til godtroende tredjepersoner (Personligkommunikasjon, 2022).

I det meste av hva politiet foretar seg spiller informasjonsteknologi (IT) en sentral rolle. IT er kritisk i alt politiet gjør og med 21.000 brukere, med mer enn 100 nasjonale systemer, applikasjoner og programvare er god digital sikkerhet helt avgjørende (*Politiets IKT-tjenester*, u.å.). I følge NSM representerer ansatte og deres brukertilganger virksomheters største sårbarhet. Dette med tanke på å gi uautorisert tilganger til informasjon (NSM, 2022). Ifølge Trond kan phishing i den sammenheng skape alle tenkelige utfordringer. Klarer angriper å ta over de riktige kontoene vil politietaten få alvorlige problemer. Phishing handler i den forbindelse om å skape en informasjonslekkasje, og kan derfor skade politiet på nær sagt alle områder. Dette ved eksempelvis å få tilgang til politiets til strafferegistre, ressursstyringsprogrammer eller informasjon om politiets infrastruktur, materiell, kapabiliteter og hvilke ressurser som er tilgjengelig. Førstnevnte kan vanskeliggjøre politiet sitt operative arbeid og sistnevnte kan redusere politiets operative evne, omdømme og i verste fall gi ondsinnede aktører tilgang til informasjon som kan benyttes til formål etaten ikke har oversikt over. I tillegg kan angriper benytte phishing til utpressing av enkelte medarbeidere for å skaffe seg *muldvarper* internt i organisasjonen. Allikevel oppgir Trond at politiet har mange lag av sikkerhetssystemer for å beskytte seg best mulig. Han opplever at politiansatte i varierende grad er bevisst denne type trusler, og det er store forskjeller internt i organisasjonen. Politietatens størrelse, geografiske spredning og ansattes ulike roller, gjør det svært vanskelig å ha en god oversikt over samtlige sårbarheter til enhver tid. Inntrykket deres er at det ofte er snakk om enten uvitenhet eller at informasjonssikkerhet ikke er fokuset i en hektisk arbeidshverdag. Dette er noen faktorer som bidrar til dårlige digital brukeratferd

og sikkerhetsbevissthet (Personlig kommunikasjon, 2022). I den forbindelse poengterer Simen at årvåkne ansatte samtidig kan være en viktig ressurs som bidrar til å rapportere om småting som de oppdager, ref. crowdsourcingprinsippet. Det kan eksempelvis være ukjente påloggingger. Dette kan bidra til å avdekke potensielle angrep eller at en trusselaktør har fått tilgang til informasjon og systemer. Med andre ord kan en ansatt være en styrke like mye som en sårbarhet. Det hele handler om god og mindre god atferd (Personlig kommunikasjon, 2022).

I likhet med samfunnsutviklingen har politiets digitale infrastrukturer og systemer er blitt mer komplekse, omfattende og integrerte. Dette skaper avhengigheter og sårbarheter på tvers av politidistrikter, beredskapsetater og ansvarsområder (Regjeringen, 2019). Digitalisering har flyttet politiets verdier, i form av informasjon og opplysninger, over til digital infrastruktur og domener. Dette har medført to sentrale utfordringer. Med økt tilgjengelighet er antall trusselaktører mangedoblet og kan variere fra enkeltindivider til organiserte kriminelle og nasjonalstater (Bakke, 2020). I tillegg øker sårbarhetene som genereres i komplekse verdikjeder i takt med en stadig ekspanderende digitalisering.
Når politiet introduserer ny teknologi for å sikre effektivitet, kommunikasjon og samhandling øker antall kontaktflater og med dette nye sårbarheter man ikke engang visste eksisterte. Skillelinjene mellom profesjonell og privat sfære kan bli mer utydelige, og igjennom sosial manipulasjon og søk i åpne kilder kan passord og brukernavn bli avdekket og misbrukt (*Politiets digitaliseringsstrategi*, 2018). Geografiske og organisatoriske avstander medfører med andre ord svært ulike kulturer mellom politidistriktene samt innad i politidistriktene med sine særegne subkulturer mellom underenheter. Målsetninger, behov og interessesfærer vil derfor være forskjellige som videre kompliserer det å motivere ansatte og vanskeliggjør implementering av kompetansefremmende tiltak. Dette kan resultere i at politietaten blir mer sårbar for sosial manipulering og phishingangrep.

Sosial manipulering og Phishing

Phishing er en form for sosial manipulering hvor angriper forsøker å lure til seg sensitive opplysninger fra en virksomhet eller privatperson. Trusselaktøren forsøker å fremstå legitim gjennom sin kommunikasjon med sitt offer, men som

inneholder en skjult eller en innebygd kode, som ruter offeret sin kommunikasjon til en tredjeparts nettside, i et forsøk på å innhente konfidensiell eller personlig informasjon (Whitman & Mattfort, 2016). Angripere velger ofte minste motstands vei, som oftest er utilsiktede sårbarheter som er skapt av menneskelige faktorer. På bakgrunn av dette er de fleste digitale trusler som utnytter menneskelige sårbarheter økende (Abawajy, 2014b) Sosial manipulering krever ofte undersøkelser og datainnhenting for å gjennomføre et angrep. I den forbindelse vil informasjon vedrørende ansatte, organisasjonsstruktur, leverandørdetaljer og epostadresser være viktig informasjon for angriper. Eksempelvis så utleverte Justisdepartementet en navneliste på 3000 politiansatte til privatpersoner i forbindelse med innsynsforespørsel knyttet til medlemmer i Norsk narkotikapolitiforening, som både illustrerer justissektorens bevissthetsnivå og hvordan utilsiktede sårbarheten kan oppstå (Aarseth, 2022). I dagens teknologiske samfunn kan mye av disse dataen hentes inn ved enkle undersøkelser på internett. Den økende mengden data om menneskers aktiviteter, vaner, livstiler, som er produsert av *Internet of Things* kan bidra til å øke trusselaktørens muligheter for å identifisere politi ansattes unike livstil *blueprint.* Dette vil sannsynligvis gi angriper gode muligheter for innsamling av personopplysninger som kan utnyttes til å fremstå mer troverdig i et phishing forsøk (Europol, 2017).

TEORETISK RAMMEVERK

Utnyttelse av menneskelig adferd og sårbarheter

Menneskers begrensede rasjonalitet og oppmerksomhetsbudsjett kan svekke politiansattes evne til å oppfatte signaler og kan gjøre mennesker mer sårbare for et phishing angrep. Ifølge Kahneman har mennesker kognitive system en rekke sårbarhet for å gjøre feilheuristikker, eksempelvis bekreftelsesfellen. Kahneman forklarer mennesker sine beslutningsprosesser gjennom system 1 og system 2 tenkning. Stress og kapasitetsoverbelastning gjør at mennesker handler innenfor for det intuitive og automatiserte systemet som Kahneman kaller system 1. I system 1 tenkning overforenkler mennesker informasjon som foreligger for å kunne skape mening i et komplekst informasjonsbilde. Dette kan resultere i at mennesker tar avgjørelser på et feilaktig eller mangelfullt grunnlag under stress eller høyt arbeidspress, hvor man er nødt til å handle raskt. Kahneman illustreres

dette gjennom *The invisible gorilla* eksperimentet til Christopher Chabris og Daniel Simons. Deltakerne ble instruert til å telle basketballpasninger mellom to lag. Underveis i eksperimentet dukker det opp en person i gorillakostymet midt mellom lagene. Dette varte i ni sekunder før gorillaen forsvinner ut av bildet igjen. Det overraskende var at over halvparten av deltakerne som så kortfilmen ikke la merke til gorillaen som plutselig dukket midt i skjermen. I den forbindelse er det engelske utrykket *pay attention* treffende. Mennesker har et begrenset oppmerksomhetsbudsjett, overskrides dette kan det gå galt. Dette illustrerer hvordan mennesker utsatt for krevende oppgaver, tidspress og stress kan føre til kognitiv overbelastning og feil, som videre er elementer som kan utnyttes i et phishingangrep. Dette står i kontrast til system 2 tenkning som er langsommere men en mer anstrengt form for tenkning. System 2 muliggjør mer overveide beslutninger som er analytiske og rasjonelle. Med andre ord gir system 2 bedre kapasitet til å oppfatte flere og komplekse signaler (Kahneman, 2012).

Manglende trening, uerfarenhet, og feilaktige antagelser er bare noen av tingene som kan resultere i menneskelige feil. Samtidig resulterer dette i at de ansatte kan bli den største sårbarheten for informasjonssikkerhet i organisasjonen. Menneskelige feilslutninger kan derfor representere en alvorlig trussel mot informasjonens konfidensialitet, tilgjengelighet og integritet. Eksempelvis kan det resultere i at klassifisert data avsløres, utilsiktet sletting og endring av data, inntastning av feilaktig data og feilaktig lagring av data i ubeskyttede områder (Whitman & Mattfort, 2016, s. 23). En naturlig årsak til at de fleste angripere velger å bruke phishingmetoden er at sikkerhetssystemer for IT er objektive, som opererer med sofistikerte målbare parametere og regler som gjør dem mer sikre mot tekniske angrep. Derimot er mennesker subjektive og denne subjektiviteten kan utnyttes for å passere de tekniske barrierene, ved i stedet å utnytte mennesker sine grunnleggende følelser som frykt, fristelser eller tillit. Angriper kan også forsøke å skape eller utnytte et tidspress som kan redusere menneskers vurderingsevne, for å få offeret til å utføre en spesiell handling (Europol, 2017). Dette sammenfaller med erfaringene til spesialrådgiver hos Telenor, Torbjørn Busch (2021) som mener at sosial manipulasjon er nøkkelen til nesten all nettkriminalitet; *«Mange tror at digitale angrep består i å bruke avanserte verktøy for å bryte seg inn på datamaskiner, mobiltelefoner eller ulike kontoer.*

Men det er faktisk veldig vanskelig å hacke en telefon eller en datamaskin. Da er det mye enklere å manipulere deg til å gjøre en sikkerhetsfeil» (Busch, 2021).

Menneskelige sårbarheter kan motvirkes med riktig opplæring, trening, bevisstgjøringsaktiviteter og kontrollmekanismer (Whitman & Mattfort, 2016). Det finnes rikelig med forskning som antyder at sikkerhetsbevissthetstrening er den mest kostnadseffektive formen for kontrollmekanismer (Abawajy, 2014b) Riktig opplæring og bevisstgjøringsaktiviterer vil gjøre det mulig for ansatte å identifisere phishing forsøk og kan bidra til å bedre brukeradferd som kan redusere sårbarhetene for menneskelige feil. Dette blir stadig viktigere ettersom phishing forsøkene i økene grad ser autentiske ut, samt at de økende omfang fremstår som å komme fra tilsynelatende legitime avsendere (Datatilsynet, 2022).Kontroll mekanismene kan være alt fra enkle aktiviteter som eksempelvis systemer for filtrering av spam og ondartede eposter, at kritiske kommandoer må gjennomføres to ganger, eller mer komplekse prosedyrer som sikrer at sårbare menneskelige aktiviteter må godkjennes av en annen person. Systemer for monitorering av menneskelige aktiviteter og krav om bekreftelse av kritiske tilganger, kan derfor være en kontroll mekanisme som kan øke robustheten for menneskelige feil (Whitman & Mattfort, 2016, s. 23).

Informasjon sikkerhet bevisstgjørings program

En sikkerhetsutdannelse, trening og bevisstgjøring (SETA) program kan påvirke politiets digitale sikkerhetskultur fordi det er designet for å redusere antall sikkerhets hendelser som er forårsaket av menneskelige adferd hos de ansatte i organisasjonen. De siste ti årenes forskning på sikkerhetskultur viser at ledelsestøtte, sikkerhets prosedyrer/retningslinjer, og bevissthetstrening er en av de viktigste faktorene for å bygge en sikkerhetskultur (Uchendu et al., 2021) Sikkerhetskultur kan defineres som; *«summen av de ansattes kunnskap, motivasjon, holdninger og adferd som kommer til utrykk gjennom virksomhetens totale sikkerhetsadferd»* (Jøsang, 2021, s. 223). Fordi menneskelige adferd kan være en av de største truslene mot informasjonssikkerheten, gir SETA programmet tre store fordeler for å redusere menneskelige sårbarheter i organisasjonen. For det første kan det bidra til å forbedre ansattes brukeratferd. For det andre kan programmet bidra til å informere ansatte om hvor de skal

rapportere sikkerhetshendelser eller brudd på *policy*. For det tredje kan det muliggjøre ansvarliggjøring av handlinger som er utført av ansatte i organisasjonen. Hvis ansatte forstår at organisasjonen beskytter seg selv ved ansvarliggjøring, vil det sannsynligvis ikke sikkerhetsprogrammene oppleves like belastende. (Whitman & Mattfort, 2016).

Rammeverket for et SETA programmet inneholder tre kjerneelementer som er; utdannelse, trening og bevissthet. Utdannelse søker å lære ansatte i organisasjonen *hvorfor* de har forberedt seg på måten de har gjort, og hvorfor organisasjonen reagerer som de gjør. Utdannelsen gir ansatte dybde og bakgrunnskunnskap som kan gi innsikt i hvordan prosesser er utviklet og muliggjør kontinuerlig forbedringer. Dette kan gi ansatte muligheter til å engasjere seg aktivt i å beskytte organisasjonen mot digitale angrep. Utdannelse fokuserer på grunnleggende teorier, prinsipper og kunnskapsbasert tilnærming. Læremetodene vil være teori undervisning, diskusjoner, seminarer, og lesning. På bakgrunn av dybde forståelsen og kunnskapen som utdannelse gir vil det kunne påvirke ansatte i langtidsperspektiv (Whitman & Mattfort, 2016).

I motsetning til utdannelse som vektlegger hvorfor, er trening mer rettet mot å lære ansatte *hvordan* de skal reagere og respondere på digitale trusler. Treningen har ofte en mer praktisk tilnærming enn utdannelse, som kan gi de nødvendige ferdighetene for å oppdage trusler og for å kunne respondere effektivt. Læremetoden har en problemløsning tilnærming, som eksempelvis kan gjennomføres igjennom formell trening, øvelser eller *workshops*. Treningen vil kunne påvirke ansatte i mellomliggende perspektiv avhengig av treningens varighet og hyppighet. Både trening og utdannelse kan bidra til bedre brukeradferd, men å bruke begge metodene i et samspill kan gi bedre effekter for organisasjonen. I første omgang trenger organisasjonen å utdanne ansatte om ønskelig brukeratferd igjennom *policy*. Deretter vil det være fordelaktig å forsterke hvordan de overholder *policy* igjennom trening på den teknologien de bruker. Jo bedre ansatte forstår intensjonen og mestrer teknologien, vil sannsynligvis minske mulighetene for å gjøre feil, og dermed redusere sannsynligheten for at ansatte setter organisasjonens informasjonssikkerhet i fare (Whitman & Mattfort, 2016).

Bevisstgjøringsaktiviteter søker å lære ansatte i organisasjonen om *hva* sikkerhet er, samt hva ansatte skal gjøre i noen situasjoner. Bevisstgjøringen tilbyr enkel veiledning om trusselen og håndteringen av disse. Formålet med bevisstgjøringsaktiviteter er å gjøre ansatte i stand til å oppfatte trusler og kunne respondere på en enkel måte. Bevisstgjørings aktiviteter kan eksempelvis være nyhetsbrev, plakater, korte videotjenester eller uformell trening. Bevisstgjøringsaktiviteter har ofte en kort tidsramme for påvirkning av ansatte, grunnet enkelheten i sin opplæringsform. Et sikkerhetsprogram for bevisstgjøring kan beholde informasjonssikkerhet i forkant av ansattes minne på daglig basis. Dette gjennomføres ved å kontinuerlig minne ansatte på viktigheten av informasjonssikkerheten, konsekvensene, samt ansattes ansvar for å følge prosedyrer og *policy* i det daglige arbeidet. Ansatte som ikke er bevisst å hvordan deres handlinger vil påvirke sikkerheten for organisasjonen kan gjøre ansatte til den største sårbarheten for organisasjonen. Bevisstgjøringsaktiviteter kan bidra til å gjøre ansatte mer bevisst på deres ansvar for organisasjonens sikkerhet og lære dem riktig brukeratferd som kan hjelpe ansatte å endre dårlig adferd. Ansatte som ikke vet hva som er riktig bruker adferd, kan ikke bli fullstendig ansvarliggjort for deres egen handlinger. Bevisstgjøringsprogrammet bør fokusere på ansatte både som en del av løsningen og som en del av problemet for informasjonssikkerhet.

Endringsledelse og endringsprosesser

Endringsledelse kan ses på som å bevege en nåværende situasjon til en ønsket situasjon. Ifølge Lewin(1947) kan denne endringsprosessen forklares igjennom de tre fasene; *unfreeze, change*, og *refreeze(Sander, 2021).* En planlagt endringsprosess kan derfor beskrives gjennom tre faser:

1. ***Unfreeze****; Endringsprosessen starter med en destabiliseringsfase hvor man søker enighet om at endringer er ønskelig og nødvendig, som danner grunnlag for endringene.*
2. ***Change****; Undersøkelse og bearbeidingsfase for deretter å foreta endringene.*
3. ***Refreeze****; Sørge for at endringene blir varig etter endringen har blitt utført. Fryse situasjonen slik at det skaper den gjeldende standarden.*

John P. Kotter blir regnet som en de største bidragsyterne innenfor endringsledelse. Et av hans viktigste bidrag er utviklingen av en 8 trinns modell for bedre suksess i endringsprosesser (Kotter, 1995a). Dette kan ses som en

videreutvikling av Lewis (1947) sin tre trinns modell. Begge modellene blir derfor sammenfattet under (Sander, 2021):

Unfreeze;

1. *Skape en følelse av nødvendighet eller forståelse, for endring. Dette kan gjøres gjennom å identifisere eller å diskutere kriser, potensielle kriser eller store muligheter.*
2. *Etablere en maktkoalisjon som har nødvendig myndighet til å lede og gjennomføre endringen. Disse endringene er vanskeligere uten aktivt støtte fra øverste ledelse.*
3. *Utvikle en endringsvisjon og strategier for å gjennomføre endringsvisjonen*
4. *Kommunisere visjonen og strategien for endringer ut til hele organisasjonen. Uten en synlig visjon kan endringen bli oppfattet forstyrrende prosjekt som kan utvikle organisasjon i feil retning eller ingensteds.*

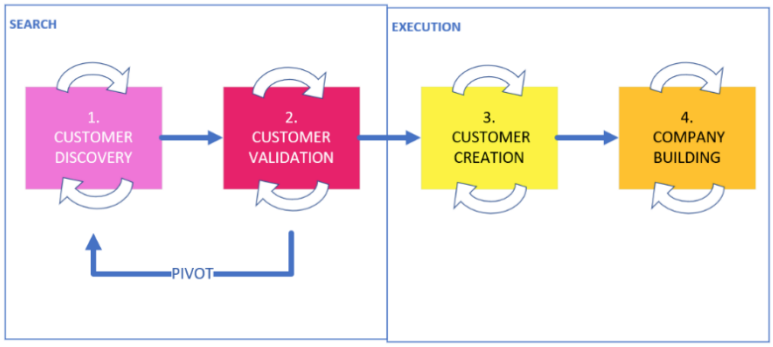
Change*;*

5. *Styrke ansatte for å handle etter visjonen. Fjerne hindringene i systemene og strukturene for å nå oppnå visjonen.*
6. *Planlegge og synliggjøre kortsiktige resultater. Uten kortsiktige resultater kan ansatte gi opp eller aktivt slutte seg til andre ansatte som allerede er motstander av endringene.*
7. *Endre adferdsmønstre og systemer som ikke er i samsvar med visjonen.*

Refreeze*;*

8. *Skape forankring i organisasjon, gjennom å kommunisere forholdet mellom bedre brukeradferd og organisasjonen suksess.*

En studie fra Harvard viser at de fleste oppstartsprosesser feiler. Dette har skapt nye behov for måter å utvikler nye prosesser for å redusere risikoen for å mislykkes i endringsprosesser. Derfor har Lean modellen vokst frem som en attraktiv modell for mange organisasjoner, som kan forklares i modellen under;



Figur 1 – LEAN, lytte til brukeren (Blank, 2013, s. 68)

1. ***I første fase*** *oversettes ideer til hypoteser for sikkerhetsprogrammet, forsøker å teste antagelsene tilpasset ansattes estimerte behov og brukeradferd, og deretter lage et levedyktig produkt for minimumsbruk, for å prøve ut deres foreslåtte løsningsendringer på ansatte.*

2. ***Start-upen*** *for sikkerhetsprogrammet fortsetter å teste alle andre hypotesene samtidig som man validerer ansattes interesser gjennom tidligere bestillinger eller produkt bruk. Hvis ikke det er noen interesse, så kan oppstarten «pivotere» ved å endre en eller flere hypoteser.*
3. ***Produktet*** *er raffinert nok til å bruke på flere ansatte. Bruker den bekreftede hypotesen og start-upen starter økt markedsføring mot flere ansatte samtidig som de skalerer opp virksomheten.*
4. ***Forretningsovergang*** *fra oppstartsmodus med brukerutviklingsteam som søker etter svar, til funksjonelle avdelinger som utfører modellen.*

METODE

Oppgaven er basert på kvalitativ data som ble gjennomført med bruk av spørreskjema, per epost med fem informanter, hvor det ble det undersøkt hvordan phishing kan skape trussel for politiet, og hvordan Politiet kan beskytte seg mot denne typen angrep. Den kvalitative dataen i denne oppgaven er innhentet skriftlig på epost gjennom flere spørsmål som ga dem muligheter til å reflektere over egne personlige forventninger og arbeidserfaringer og i kraft sin rolle eller fagekspertise på fagfeltet. Informantene som er valgt er tre rådgivere innenfor digital sikkerhet i politiet, en rådgiver innenfor IT sikkerhet i det private, samt fagansvarlig på politihøgskolen innenfor faget digitalt politiarbeid. Etter primærdataene ble hentet inn, ble dataen strukturert i temaer, som bidro til problemidentifisering og diskusjonen. Begrensningene ved disse intervjuene er at det er få respondenter og at temaet er sensitivt som medfører at det ikke er mulig å få detaljerte svar vedrørende innebygd sikkerhet eller sårbarheter. Det er allikevel ikke av avgjørende betydning for oppgaven da den i hovedsak omfatter menneskelige, organisatoriske og kulturelle aspekter.

EMPIRISKE FUNN og ANALYSE

Sannsynlighetsreduserende tiltak og økt motstandsdyktighet

Informantene ble stilt spørsmål om hvilke tiltak som kunne virke sannsynlighetsreduserende og bidra til å øke motstandsdyktigheten mot sosial manipulering og Phishing. **Erlend** hevder at det må bygges sikkerhetskultur igjennom brukeropplæring og at viktigheten av dette ikke kan overdrives. I den forbindelse beskriver han ansatte som en ledd i en lang kjetting som utgjør politietaten. Kjettingen er ikke sterkere enn det svakeste ledd. **Torgeir** støtter oppunder dette og svarer at bevisstgjøring ved å tydeliggjøre politietatens

viktigste verdier, aktuelle trusler og dermed hvilke risikoer disse utgjør er svært viktig. Ansatte er enhver virksomhets førstelinjeforsvar fordi de ofte er enklere å utnytte enn datasystemer. Ansatte må derfor være i stand til å gjennomskue forsøk på sosial manipulering ved å forstå hvordan truslene opererer. Dette kan eksempelvis gjøres igjennom *Gameification* av phishingøvelser der de ansatte blir premiert og rangert etter hvor flinke de er til å gjennomskue phishing-eposter. I tillegg burde man ha et systematisk og regelmessig fokus på digital sikkerhet, eksempelvis gjennom foredrag angående trusler, metoder, hendelser og *red team* sikkerhetstester. Elementer som bidro til vellykket kompromittering må gjennomgås i detalj med de ansatte. **Trond** mener at politietaten først og fremst må tilby et grensesnitt som er kjent for brukerne. Det vil si noe som er likt det man har benyttet tidligere eventuelt benytter privat. Mange av angrepene på etaten i dag er de ansatte skjermet for og slipper å forholde seg til fordi vi har en rekke innebygde sikkerhetsmekanismer. Allikevel er sikkerhetsbevissthet blant brukerne viktig fordi man jobber i politietaten. Derfor må alle henvendelser behandles med et kritisk øye. I den forbindelse er det helt kritisk at ansatte ikke benytter etatens systemer til private formål. Dette fordi det kan eksponere den ansatte og politietaten for risiko.

Endring av brukeratferd og digital kompetanse

God digital brukeratferd kan bidra til å redusere sårbarheten ansatte representerer for virksomheter. Skal man oppnå dette må brukeropplæring inn på et tidlig stadium påpeker **Erlend**. Digital sikkerhet burde være en del av studieløpet på PHS, om ikke et eget fag. Fordelen ved dette er at studentene er mer mottakelige for ny informasjon og måter å gjøre ting på. **Torgeir** hevder at bevisstgjøring i en organisasjon best kan oppnås ved *gameification* av phishingøvelser igjennom programmer som *Hoxhunt.* Dette vil vise de ansatte i førstelinja hva som kan være konsekvensen av å åpne et ondsinnet dokument. I tillegg vil det tydeliggjøre indikatorer på ondsinnet framferd. **Trond** gjentar i den forbindelse at det er helt avgjørende at ansatte forstår at de må skille mellom sitt digitale arbeidsliv og privatliv. Oppnår man dette vil alle eposter av privat art man får i jobbsammenheng i praksis ikke være legitime. Selv om politiet har god sikkerhet på epostapplikasjonen sin har ikke nødvendigvis avsender det. Har man eksempelvis benyttet sin politiepostadresse som kontaktinformasjon i borettslag,

idrettslag eller annet så øker mulighetene for at dette kan bli misbrukt. Dette ved at angriper benytter kontaktinformasjonen videre til å framstå som en legitim avsender. Av den grunn burde digital sikkerhet inn i utdannelsen. Grunnprinsipper innen sikkerhet og bevissthet om potensielle konsekvenser av feil bær inn i undervisningen. Dette for at det skal bli så innlært at det blir en del av ryggmargsrefleksen på lik linje med håndtering av våpen. Det burde i tillegg være en lav terskel for alle ansatte å varsle om potensielle hendelser man er usikker på til sentrale ressurser. Slik at man kan få råd til å håndtere den digitale hverdagen både i arbeidssammenheng og privat da skillelinjene ofte er vage. Dette fordi sikkerhetsbrudd kan berøre publikum, den ansatte og i verste fall hele politietaten.

På bakgrunn av de kvalitative intervjuene og relevant litteratur har vi falt ned på følgende tiltak:

1. **Bevissthetskampanjer – igjennom ukentlige nyhetsbrev, opplæringsvideoer og e-læringskurs.**
2. **Opplæring, trening og øving – ved å innføre digital sikkerhet som en del av den årlige innsatspersonelltreningen (IP) i politiet.**
3. **Kunnskapsøking – igjennom å innføre digital sikkerhet som en del av politiutdanningen.**

Testing av tiltak

1. Nyhetsbrev har **Erlend** ingen tro på. Dette synet støttes av **Trond.** Han supplerer med at nyhetsbrev og lignende har liten effekt fordi de fleste ikke føler seg berørt av denne typen problemstillinger. Allikevel er det er rom til å benytte dette til bevisstgjøring så lenge det ikke blir en overflod av informasjon. Både Erlend og Trond tenker at e-læringskurs er bra, men effekten av dem er per nå ikke kjent. I den forbindelse hevder Erlend at det beste er fysiske foredrag.
2. Digital sikkerhet som tema under den årlige IP-treningen for politioperative mannskaper synes **Erlend** er et spennende forslag. Imidlertid vil ulempen ved dette være at man kun omfatter de operative politiansatte som IP-godkjennes. Vi ønsker jo å treffe alle, både sivilt og politiansatte, uavhengig av om de gjennomfører den årlige IP-treningen. Allikevel kan det bidra til å få satt digital sikkerhet på agendaen. **Trond**

tenker at en årlig påminnelse kan være hensiktsmessig, så lenge det ikke går på bekostning av andre emner som føles mer relevante.

3. Det at digital sikkerhet inngår som en del av politiutdanningen mener både **Erlend** og **Trond** er et godt forslag. Det burde definitivt være en del av utdanningen, og er nok det tiltaket som vil ha mest effekt på lang sikt. PIT holder på å utvikle sikkerhetsskolen ved et obligatorisk e-læringskurs innenfor digital sikkerhet. I en perfekt verden burde dette vært et fag på PHS. Dette kan bidra til bedre digital bevissthet og brukeradferd ved at ansatte eksempelvis ikke utleverer informasjon som ikke burde publiseres. Ikke minst at ansatte får et bevisst forhold til det å være politi og skille mellom dette og privatperson. Det å blande disse digitale identitetene innebærer en risiko for vedkommende og etaten ifølge Trond. Jeg håper vi kommer dit en dag sier Erlend. **Torgeir** synes samtlige av disse aktivitetene er veldig viktig. Dette fordi trusselbilde, sårbarhetene og metodene forandrer seg kontinuerlig. Det er derfor ikke en *one-stop-shop,* men noe som må jobbes med systematisk over tid, parallelt som trussel-landskapet utvikler seg. **Robert** fra politihøgskolen (PHS) tror ikke det vil være plass til digital sikkerhet som eget fag på bachelorutdanningen, men inngå som en del av et annet fag. Årsaken til dette er omfanget. Datasikkerhet har vært et tema i faget Digitalt Politiarbeid hvorpå studentene har hatt en forelesning vedrørende trusselbildet og presentert en gruppeoppgave over de vanligste digitale truslene. Suksesskriteriet er nok å få det til å oppleves som relevant for studentene, og at undervisningen er knyttet til kunnskap og refleksjon rundt temaet. Man kunne i den forbindelse sett på en mer praktisk tilnærming.

Viktige suksesskriterier for implementering av tiltak

Informantene ble bedt om å dele sine synspunkter vedrørende hvilke suksesskriterier de mener er viktigst for at tiltakene skal ha ønsket effekt og være gjennomførbare. Samtlige av informantene er nokså enige. De fremhever at brukerrelevans som en viktig faktor for at implementering av tiltak skal bli vellykket. **Erlend** påpeker at god brukeradferd i utgangspunktet burde være av interesse for brukeren. Problemet er ofte at ansatte ikke opplever det som relevant. Videre sier han følgende; *For noen er det bare en IKT-greie og jada, jeg skal*

være forsiktig som alltid, uten at de egentlig fanger opp hva dette handler om. Samtlige i politietaten burde bli flinkere på å si ifra om man opplever at noen driver en digital sikkerhetspraksis som ikke er forsvarlig. Dessverre er det en meget høy terskel for dette i politiet. Særlig om det er leder, de eldste eller mest erfarne som har lagt til seg digitale uvaner. Da er fort gjort at det anses som en grei måte å gjøre ting på. Hadde digital sikkerhet vært en del av grunnutdannelsen fra PHS ville man over tid klare å endre dette. Allikevel vil man nok aldri klare å få alle brukerne til å føle at dette er relevant for dem. Dette fordi politiet er en så stor organisasjon med mange underenheter med stor faglig spennvidde, målsetninger og interesseområder. Imidlertid er dette veldig viktig fordi det holder at en er uvøren. Den beste politietaten kan gjøre er derfor å lage konkrete eksempler som treffer vedkommende på et punkt hvor de bryr seg, som de føler er viktig for dem.

Torgeir er enig i at er svært utfordrende å skape relevans for brukeren og mener at man må starte med ansvarliggjøring av roller i organisasjonen. Hva slags roller som passer, avhenger selvsagt av virksomhetens natur. Rollene *må* i tillegg få ressursene som kreves for å opprettholde god informasjonssikkerhet. Hvis ikke pulveriseres fordelingen av eierskap og risiko. Når en system- eller forretningseier blir nødt til å eie risiko, må vedkommende også sørge for at brukerne nedover i organisasjonen utviser tilstrekkelig grad av sikkerhetsmessig skikkethet i det daglige arbeidet. Det og fasilitere for bevisstgjøringsarbeidet videre ned i de ulike underenhetene blir med dette en naturlig del av disse rollenes ansvarsområder. **Trond** støtter påstanden om at brukerrelevans er viktig. Imidlertid fremhever han at brukeren må informeres om trusselaktører man står ovenfor og tidligere hendelser for å skape relevansen for brukeren. Trusselaktørene er i den forbindelse ikke nødvendigvis kriminelle eller fremmede stater. De kan også være advokater, journalister og lignende, som søker å skaffe informasjon som de ellers ikke har tilgjengelig. Bevisstgjøring og god brukeratferd vil være ekstremt viktig uavhengig av brukerens nivå i hierarkiet. Teknisk sett vil en angriper kunne elevere sine rettigheter uavhengig av hvilke rettigheter en eventuell kompromittert konto måtte ha. Alle brukere bør derfor være bevisst på at deres konto i ytterste konsekvens kan benyttes til å overta ethvert miljø de er en del av.

Informantene ble også spurt om hvordan man kan få satt digital sikkerhet på agendaen i politietaten slik at det i større grad prioriteres. Samtlige retter sitt fokus på ledelsen. **Trond** påpeker at sikkerhet i stor grad er på agendaen hos ledelsen, men for å oppnå virkelig god sikkerhet, så krever det bevissthet på brukernivå. Dette er et lederansvar. Det er i den forbindelse viktig at brukerne får fortløpende informasjon fra ledelsen om pågående hendelser og status på disse. Det er imidlertid kritisk at informasjonen holdes på et passende nivå. En overflod av informasjon vil føre til at de brukerne blir likegyldige til informasjonen. Ledelsen må derfor være bevisste på hvilke trusler etaten står ovenfor. Skal man få virksomheten til å fokusere på digital sikkerhet er det helt essensielt at ledelsen legger til rette for det. **Erlend** opplever at ledelsen i politiet er reaktive fremfor proaktive når det gjelder digital sikkerhet. Imidlertid hevder han at fokuset har begynt å endre seg. På den måten unngår man kanskje at det må gå galt før man innser hvor galt det er. Paradokset er at politiet er god på fysisk sikkerhet men ikke like god når det kommer til det digitale rom. God digital sikkerhet er like viktig. Han tror den beste løsningen er at politiansatte får denne kompetansen så tidlig som mulig i sin politikarriere. Det er helt avgjørende at toppledelsen fremmer digital sikkerhet og hvor ekstremt viktig det er for at politiet skal kunne utføre sitt samfunnsoppdrag. **Torgeir** argumenterer også for at ledelsen må forstå hva risikoen innebærer. Ledelsen er ofte *ikke-teknisk,* derfor har de sikkerhetsansvarlige en særlig viktig rolle vedrørende å oversette teknisk risiko til forretningsmessig risiko. Igjennom en felles forståelse av risikoene kan gode og hensiktsmessige risikoreduserende beslutningstiltak tas. I den forbindelse er det viktig med top-down forankring. Dette er noe ledelsen må jobbe med kontinuerlig og sørge for at policy, prinsipper, roller, ansvarsområder og tekniske mekanismer operasjonaliseres i alle ledd av virksomheten.

DISKUSJON OG IMPLEMENTEREING

Endring av brukeradferd

Samtlige informanter vi har snakket med fremhever at endring av brukeradferd er en viktig faktor for at implementeringen av bevisstgjøringstiltak skal bli vellykket. I den forbindelse påpeker Erlend at brukerrelevans som en viktig faktor. Videre sier han at problemet ofte er at ansatte ikke opplever det som relevant, *for noen er*

det bare en IKT-greie og ja da, jeg skal være forsiktig som alltid, uten at de egentlig fanger opp hva dette handler om (personlig samtale, 2022). Et viktig element i endringsprosessen er å synliggjøre behovet for endringen, samt skape entusiasme og engasjement blant de den berører. Dette kan politietaten oppnå gjennom vise til phishingangrep og hvilke konsekvenser dette hadde for de rammede, slik som NAV i Østre-Toten er et godt eksempel på. De kompetansefremmende tiltakene vil med dette muligens føles nødvendige, relevante, bli positivt mottatt og ikke møte stor motstand. Dette vil kunne bidra til å skape brukerrelevans og er viktig for at sikkerhetsprogrammet skal ha en positiv endringseffekt (Kotter, 1995a). Imidlertid bør det skilles mellom politiets behov for endringer i kunnskap og faktisk brukeradferd. Årsaken til dette er at løsningene for å skape disse endringene vil være forskjellig. Det å formidle digitale sikkerhet og god brukeratferd blant ansatte i politietaten er i seg selv ikke veldig komplisert. Dette kan eksempelvis gjøres gjennom ukentlige nyhetsbrev, opplæringsvideoer, e-læringskurs eller ved undervisning på PHS (Whitman & Mattfort, 2016). Imidlertid vil det være mer tidkrevende og vanskeligere å endre organisasjonskulturen igjennom ansattes virkelighetsoppfatninger, persepsjon og underliggende årsaker til brukeradferden. Dette krever en mer personlig reise og læringserfaring fra ulike aktiviteter som eksempelvis kreative diskusjoner i grupper. Politiet er hierarkisk og byråkratisk organisasjon med strenge krav til linjestyring hvor det kan være vanskelig å innovere og stimulere til endringer. Det kan derfor tenkes at man må introdusere utfordringene og tiltakene gradvis, samtidig som man oppmuntrer til konstruktive samtaler om endringene til de er fullført. Med andre ord er endring av brukeradferd en komplisert prosess som ikke kan løses ved implementering av enkelttiltak. Det vil kreve at hele organisasjonen har god forståelse av ønsket brukeradferd og årsakene til hvorfor dette er viktig i den enkeltes arbeidshverdagen (Lacey, 2009). God kunnskap og forståelse tematikken blant politiledere vil bidra til at de kan gå foran som gode rollemodeller. Videre at de kan benytte disse faktorene til å etablere maktkoalisjoner med myndighet til å gjennomføre endringene. Dette vil overordnet bidra til at politietaten evner overvinne barrierene mot ønsket opptreden, praksis og endring (Kotter, 1995b).

Ansvarliggjøring, eierskap, rolleavklaring og ressurssetting er helt sentralt for å opprettholde god informasjonssikkerhet, sikre etterlevelse av retningslinjer og fasilitere for virksomhetens sikkerhetsprogram ifølge Torgeir (personlig kommunikasjon, 2022). Det er i den forbindelse også viktig at sikkerhetsprogrammet tilpasset virksomhetens underenheter, deres brukernivå, arbeidsoppgaver og kultur. Imidlertid kan dette kreve mer ressurser av virksomheten noe som gjør det vanskeligere å legitimere. Det kan derfor være lettere å for ledelsen falle ned på en standardisert løsning. Risikoen ved dette er at bevisstgjøringsarbeidet ikke oppnår sin hensikt. Det kan i tillegg ha uheldige bieffekter. På den ene siden viser forskning at deltakere utsatt for høyintensitets phishingtrening er flinkere til å detektere phishingeposter sammenlignet med deltakere utsatt for lavere intensitet. På den annen side bidro treningsintensiteten til at de også hadde en høyere feilmargin (feilkategoriserte eposter) og frekvens av falske alarmer. Videre påpekes det at deltakerne kan ha blitt påvirket av en rekke faktorer ved treningsprogrammets innhold. Som hvordan testene ble utført, informasjonen gitt i forkant og feedbacken de mottar underveis og i etterkant. Kognitive prosesser og biaser som menneskers begrensede oppmerksomhetskapasitet, bekreftelsesfeller og overkonfidens på egne evner er faktorer som kan bidra til negativt læringsutbytte og ha uheldige bieffekter om ikke man ikke er det bevisst (Singh et al., 2019). Politietatens ulike virksomheter må derfor starte med å kartlegge hvilke subkulturer og menneskelige barrierer som eksisterer, for å tilpasse sikkerhetsprogrammet deretter. Dette fordi underenhetenes ansatte kan igjennom sine arbeidsoppgaver utgjøre ulike risikoer og sårbarheter. Ledelsen må derfor skreddersy tiltak for hver subkultur. Det vil kunne få en positiv effekt for hele virksomheten ved at det minimerer risikoen som er forbundet med de enkelte subkulturene (da Veiga & Martins, 2017). Dette er spesielt viktig i større virksomheter som politiet, hvor de som utvikler programmet ikke har oversikt over disse faktorene. Informantene fra PIT oppgir at det i disse dager utvikles digitalt sikkerhetskurs som skal bli obligatorisk for alle ansatte i etaten. Det kan tenkes at dette kan oppleves irriterende og forstyrrende hvis kurset blir for generelt slik at det ikke treffer brukermassen, og føles relevant for deres arbeidshverdag (Lain et al., 2021).

Uten undersøkelser rundt ansattes holdninger, kunnskap og adferd vil det være vanskelig å måle og bedømme tiltakene. Derfor vil det være viktig at et endringsprogram inneholder en tydelig strategi og plan som starter med å identifisere krav og problemområder, undersøkelser av bakenforliggende årsaker og deretter utvikle programmet for korrigerende tiltak (Lacey, 2009). Dette kan gjøres ved å utføre spørreundersøkelser, intervjuer for å kartlegge kulturelle og adferdsmessige barrierer for å endre adferd i politietaten. Allikevel er det nærliggende å tro at man vil kunne nå eller bli forstått av samtlige ansatte. Dette kan være på grunn av at verdiene, sårbarhetene og trussellandskapet stadig endrer seg og blir mer sofistikert. Dette kan medføre at problemstillingen blir for kompleks til at den lar seg formilde effektivt og på en måte som vil ha innvirkning. Adferd og holdninger vil variere ut ifra ulike personligstrekk, risikovillighet eller ambisjonene i organisasjonen. Ansatte vil også kunne være opptatt av utføre sine arbeidsoppgaver framfor sikkerhet som flere av informantene opplyser. Man må derfor akseptere at det alltid vil være behov for forbedringer, men at man ikke kan endre alt, hos alle på en gang. Imidlertid kan man håpe på å få effekt innenfor noen områder og sikkerhetsprogrammet bør derfor ta høyde for de mest prioriterte områdene for endring, sette målbare mål for forbedringer, før man beslutter tiltak (Lacey, 2009). Totalt sett vil dette kunne bidra til å stimulere til god digital brukeratferd og gjøre ansatte i politietaten mindre sårbare for sosial manipulering og phishingangrep.

Skape engasjement og læring igjennom trening

Det kan tenkes at spill, øvelser og menneskelig dialog vil oppta oppmerksomhet til ansatte i større grad enn kunnskap via lesing, e-læring eller annen passiv undervisning som er preget av enveiskommunikasjon. Samtidig kan dette føre til at politi ansatte husker og forstår bedre. Det kan derfor antas at programmer som inneholder en større grad av engasjerende aktiviteter vil få større effekt enn å passiv lytting. En av de mest suksessfulle og letteste måtene kan eksempelvis være å engasjere en større gruppe av ansattes oppmerksomhet igjennom konkurranser. For eksempel gjennomførte selskapet Royal Mail Group en konkurranse i et forsøk på å redusere sikkerhetshendelser i hektiske juletider. I denne perioden var ansatte satt under hardt tidspress for å nå rapportfrister før utgangen av året. På grunn av menneskers kognitive begrensede

oppmerksomhetsbudsjett vil disse stressfaktorene kunne bidra til kognitiv overbelastning og at feil eller avvik blir oversett. Intens fokusering på en oppgave kan gjøre at man i praksis blir blinde, illustrert av Christopher Chabris *The Invisible Gorilla* eksperiment. Gorillastudien illustrerer to viktige fakta om hjernen, vi kan være blinde for det åpenbare og for vår egen blindhet (Kahneman, 2012). Med andre ord kan dette øke sårbarheten for digitale angrep. Ansatte fikk derfor beskjed om at de som best kunne svare på noen spørsmål knyttet til digital sikkerhet ville vinne en enkel premie. Innen noen dager hadde sikkerhetsnettsiden i selskapet nærmere 10000 klikk på denne enkle konkurransen. I tillegg viste statistikk at antall sikkerhetshendelser knyttet til menneskelige sårbarheter i samme periode ble redusert. Selskapet gjentok eksperimentet men reduserte premien. Det viste seg at konkurransen fortsatte klarte å engasjere de ansatte med tilsvarende utfall i antall reduserte sikkerhetshendelser. Dette er en god illustrasjon på at spill kan være godt egnet til å engasjere ansatte, men at konkurranser med premier fungerte enda bedre (Lacey, 2009).

Dette viser at for å øke ansattes bevissthet, må de motta riktig informasjon, på en riktig måte, gjennom de riktige kommunikasjonskanalene. Imidlertid er prosessen for å endre adferd langt mer utfordrende, som krever andre metoder. Det krever undersøkelser av de ansatte, samt å engasjere ansatte i en form for eksperimentell læringsprosess. Dette kan eksempelvis innebære å skape engasjement ved å benytte historier eller spill som vil tiltrekke dem mer personlig, og hvor de kan lære fra prosessen. Dette er faktorer som kan bidra til å endre deres fremtidige adferd. Eksempelvis kan man igjennom scenarioøvelser styrke ansattes evne og oppmerksomhetsbudsjett slik at det frigjør kapasitet til å identifisere digitale trusler og nye trender. I tillegg vil man med tiden kunne bidra til å endre persepsjonen til ansatte i organisasjonen. Dette vil stimulere de ansatte til å lære og utvikle seg. Ved å tilrettelegge for eksperimentering med hypotetiske utfordringer i et trygt miljø kan ansatte i politietaten bygge digital kompetanse igjennom erfaringslæring. Ved å delta på ulike øvelser, spill og situasjoner kan man i tillegg forberede seg på tenkte fremtidige trusler. Totalt sett kan dette bidra til at ansatte endrer sine synspunkter og legger vekk sine defensive argumenter til fordel for å løse scenarioet (Lacey, 2009). Sett under ett er derfor å fordelaktig at framtidige sikkerhetskurs inneholder trening på ulike scenarioer, øvelser, spill og

konkurranser. Dette vil i større grad engasjere, øke bevissthetskompetansen og stimulere til å endre brukeradferden enn tradisjonelle e-læringskurs preget av enveiskommunikasjon.

Det er nærliggende å tro at det vil være vanskeligere å endre sikkerhetsadferden til en større kollektiv gruppe som en seksjon, avdeling eller et helt politidistrikt enn eksempelvis et avsnitt. Det kan derfor være hensiktsmessig å starte med det som aktiverer adferd i en organisasjon. Dette kan gjøres igjennom instrukser, retningslinjer, regler, ledelse og ordre. Det er imidlertid ikke nok for å oppnå en varig endring av ønsket brukeradferd. Direkte ordre vil sannsynligvis også fungere dårlig på å skape grunnleggende endringer hos de ansatte i de fleste organisasjoner inkludert politietaten. Det er med andre ord helt essensielt å skape meningsbærende endringer for hvor ansatte er oppriktig interessert i digital sikkerhet for å beskytte politietaten mot phishingtrusler. Det vil si at man i de fleste tilfeller er nødt til å komplimentere med andre aktivatorene enn direkte ordre og detaljfokuserte retningslinjer. I den forbindelse er det sannsynligvis mer hensiktsmessig å fokusere på premiering av ønskede-, eller konsekvenser av uønskede handlinger. Denne formen for ansvarliggjøring vil i større grad motivere adferdsendring, og de meste effektive aktivatorene er ofte som gir umiddelbare utslag med en tydelig årsak – konsekvenssammenheng. Dette illustrert av brent barn skyr ilden metaforen. Denne effekten er det politietaten burde søke å oppnå i sitt arbeid med digital sikkerhetsbevissthet. Hvilke aktivatorer som gir mest effekt over tid er et disputert tema. Imidlertid indikerer flere studier innenfor psykologien at både straff og premiering kan være virkningsfulle, men det avhenger av konteksten og i hvilken sammenheng de brukes (Lacey, 2009). Det er med andre ord viktig å ha et bevisst forhold til hvilke aktivatorer og motivatorer man benytter seg av ved gjennomføring av et sikkerhetsprogram i politiet. Dette for å skape en varig endring i en ønsket brukeratferd egnet til å øke motstandsdyktigheten til ansatte i etaten.

Endringsledelse og implementering av sikkerhetsprogrammet

Samtlige av informantene retter sitt søkelys på ledelsen for få satt digitalsikkerhet på agendaen i politietaten slik at det i større grad prioriteres. Informanten Trond påpeker at sikkerhet i stor grad er på agendaen hos ledelsen, men for å oppnå

virkelig god sikkerhet, så krever det bevissthet på brukernivå, som er et lederansvar. Det er i den forbindelse viktig at brukerne får fortløpende informasjon fra ledelsen om pågående endringsbehov og status på disse. Endringer må planlegges, organiseres og kontrolleres for å kunne administreres på en god måte. Det vil kreve effektivt lederskap for å introdusere endringer på en suksessfull måte slik at det skaper en forskjell. Suksessfull endringer vil derfor kreve at politiledelsen etablerer en tydelig visjon, strategi, et felles sett med organisasjonskultur og verdier, myndiggjøring av ansatte, samt at lederne inspirerer og motiverer ansatte. I stedet feiler ofte endringsprogrammer som et resultat av manglende ledelse, ressurser, kompetanse, monitorering og kontroll i prosessen, og dårlig planlegging for å skape endringer. Øverste ledelse kan også vise manglende forpliktelser som kan resultere i manglende eierskap til endringen, manglende ansvar for at prosessen skal bli suksessfull, samt manglende bevissthet vedrørende egen adferd som påvirker ansatte (Gill, 2002). Eksempelvis så opplever informanten Erlend at ledelsen i politiet er reaktive fremfor proaktive, som kan indikere manglende forpliktelser og eierskap hos politiledelsen

Endringer blir alt for ofte betraktet som *Quick fix* og feiler ofte i å adressere implikasjonene endringene skaper for hele organisasjonen, som kan skape uakseptable og uforutsette forstyrrelser hos ansatte. Initiativet for endringer kan derfor være et resultat av naive ledelses tilnærminger. Mangelfull og dårlig kommunikasjon fra politiledelsen kan resultere i misforståelser vedrørende endringsprosessen og målsetningene sikkerhetsprogrammet, som igjen kan føre til rykter som demotiverer ansatte, samt manglende forpliktelser til endringen. Mangel på forpliktelser til endring kan være et resultat av manglende overbevisning om fordelen med endringen (Gill, 2002). Dette kan eksempelvis illustreres av politiansattes frustrasjon og manglende tillit til ledelsen i gjennomføring av de store endringene i politireformen (Aarseth, 2020). Det kan tenkes at manglende tillit til endringen skyldes manglende kommunikasjon fra ledelsen, og fravær av kommunikasjon vedrørende langsiktige målsetninger ved reformen, og kortsiktige synlige forbedringer vedrørende reformen.

Motstand mot endringer er kjent fenomen. Kubr (1996) fremhever flere årsaker på hva som skaper motstand i endringsprosesser. En kognitiv og adferdsmessig årsak

er manglende kunnskap om *know how*. Manglende overbevisning om at det er behov for endringer, kan gjøre at ansatte stiller spørsmålstegn ved verdien og betydningen av sikkerhetsprogrammet til ansatte, som kan føre til mangel på motivasjon til å endre. En annen stor motstandskraft mot endringer er emosjonelle faktorer. Dette kan føre til at politi ansatte misliker de påtvingende sikkerhetsprogrammet. Dette kan eksempelvis være menneskelige faktorer som å mislike overraskelser, at man frykter det ukjente, at endringen forstyrrer ansattes vaner og praksis i en hektisk arbeidshverdag, eller at det kommer i konflikt med ansattes egeninteresser (Gill, 2002). Sikkerhetsprogrammet bør derfor tilpasses politiansattes behov. I den forbindelse kan *lean* metoden være nyttig, fordi den kan redusere risikoen for at nye ideer og at sikkerhetsprogrammet mislykkes med å endre politiansattes brukeradferd. Årsaken til dette er *lean* modellen vektlegger hypoteser og prosessen ved korte sykluser, som fokuserer på tidlig og hyppige tilbakemeldinger fra brukeren (Blank, 2013). Med andre ord kan de som lager sikkerhetsprogrammet i større grad kartlegge kulturelle og menneskelige barrierene for endring ved å teste tiltakene på politiansatte, før det iverksettes et sikkerhetsbevissthetsprogram. Basert på hyppige tilbakemeldinger fra politiansatte, kan dette programmet skreddersys den enkelte avdeling slik at tiltakene blir mer effektive slik at man oppnår ønsket brukeradferd.

Endringer er en prosess som handler om å ta med en politietat på en reise fra en nåværende tilstand til en ønsket fremtidig tilstand, samtidig som de skal håndtere utfordringer og problemer som oppstår underveis. Derfor er endringsprosesser et ledelsesansvar, hvor politiledere må vise veien og bruke sin maktposisjon for å vinne ansattes sinn til arbeide sammen mot å øke sikkerhetsbevisstheten i organisasjonen. Derfor vil det være viktig for politiledelsen å utvikle en inspirerende fremtidsvisjon, hvor det lages strategier som bringer visjonen til virkelighet, slik at ansatte i organisasjonen mobiliserer for å nå samme mål. Ifølge Kotter(1995), sitert i Gill, så er utgangspunktet for en vellykket endringsprosess at det skapes en følelse av at endringen er viktig og det haster. I den forbindelse kan politiet kommunisere sikkerhetshendelser og trusler politiet står ovenfor, som informantene påpeker. Det kan derfor være fordelaktig å skape misnøye med *status quo* samtidig som de skaper forståelse for behovet for endring blant politiansatte. En vellykket endring vil derfor være å få status quo til å fremstå

farligere, enn å begynne i det ukjente. Dette danner grunnlaget for å utvikle en visjon for endringer. I tillegg vil det være nyttig å skape felles organisasjons verdier, kultur, retningslinjer og praksis for endringer. Kultur endringsprogrammer handler om å endre ansattes virkelighetsoppfattelser som vil kreve lang tid, hvor et eget fag på PHS kan bidra til å skape endringer på sikt. Dette kan resultere at ansatte har mer interesse av jobbe mot et felles problem, som kan skape mer åpenhet, ærlighet, profesjonalitet og tillitt, hvor de har en bedre forståelse for retningen og målsetningene til organisasjonen (Gill, 2002).

Uten strategier for endring vil visjonene som politiet skaper, bare være en drøm. Strategiske planer er måter for å forfølge oppdraget og visjonene. Effektivt lederskap innebærer å skape utvikling, engasjement og implementering av strategier. En annen viktig ledelsesfaktor for suksessfull endring er myndighetsgjøring av ansatte ved å gi dem en større grad av autonomi. I praksis handler det om gi ansatte muligheter, ferdigheter, kunnskap, selvtillit, frihet og ressurser til å klare seg selv, slik at de blir ansvarlige for endringen. Å styrke ansattes riktig praksis innebærer å kvitte seg med hindringene, endre eller fjerne systemer som undergraver visjonen (Gill, 2002). En annen viktig faktor ved endringsledelse er effektive politiledere som inspirerer og motiverer ansatte til å gjøre det som trengs for å oppnå ønsket brukeradferd. Det kan tenkes at mangel på tillit og respekt til de som fremmer endringene, eller ledelsens motvilje for å håndtere vanskelige utfordringer kan skape motstand mot disse endringer. I alle endringsprosesser er det derfor viktig med troverdige ledere og rollemodeller. Troverdighet kommer fra politiansattes oppfatninger av lederens kompetanse og ærlighet, og deres evne til å inspirere. Inspirasjon og motivasjon oppstår som et resultat av et sikkerhetsprogram som tar høyde for ansattes ønsker, behov, interesser, ambisjoner og verdier, samt bruk av tiltalende og positivt språk. Motivere handler også om å skape kortsiktige gevinster som innebærer planlegging og skape synlige forbedringer for ansatte under endringsprosessen, samt belønne ansatte som har gjort gevinstene mulige. (Gill, 2002).

KONKLUSJON OG ANBEFALING

I likhet med samfunnsutviklingen har digitaliseringen i politiet flyttet deres verdier over til det digitale domenet. Denne utviklingen har bidratt til å profesjonalisere og effektivisere politietaten, samtidig som antall trusselaktører er mangedoblet. Digitale infrastrukturer, og systemer er blitt mer komplekse, omfattende og integrerte som gjør det svært utfordrende å ha oversikt over alle sårbarhetene som genereres i verdikjedene. I tillegg har *Internett of Things* og dårlig brukeratferd bidratt til å øke virksomheters sårbarheter ved at skillelinjene mellom profesjonell og privat sfære er blitt utydelige. Eksempelvis ved at man benytter svake og samme passord til pålogging i både privat og jobbsammenheng. Ansattes sårbarheter sammenfattet med at den innebygde IT-sikkerheten er blitt vanskeligere å bryte igjennom har medført at ondsinnede aktører i økende grad har skiftet fokus over til det menneskelige element. Igjennom sosial manipulasjon og phishingangrep forsøker angriper å lure virksomheters ansatte til å utlevere sensitiv data som brukerinformasjon og brukertilganger. Dette for å skaffe seg tilgang til virksomheters informasjonsverdier. Denne typen digitale angrep kan i teorien ramme politietaten på alle tenkelige måter. Til eksempel kan systemer låses, sensitiv informasjon, personopplysninger og opplysninger om politietatens kapasiteter kompromitteres, endres eller slettes. Med andre ord kan sosial manipulering og phishing i ytterste konsekvens gå utover politiets operative evne og hindre etaten i å utføre sitt samfunnsoppdrag.

Politietatens virksomheter burde starte med å kartlegge hvilke subkulturer og menneskelige barrierer som eksisterer internt, før de iverksetter et sikkerhetsprogram. Dette kan gjøres ved å benytte en LEAN-modell hvor testing, justering og implementering av tiltak skjer i tett dialog med brukermiljøet. Dette kan redusere feilmarginer fordi store endringer er vanskelig å gjennomføre i store hierarkiske virksomheter som politiet. På grunn av at etaten er svært differensiert, spesialisert og består av ulike enheter, har deres ansatte forskjellige behov og utgjør ulike sårbarheter. Sikkerhetsprogrammet og bevisstgjøringsarbeidet burde derfor ikke generaliseres for å sikre ønsket effekt. Styrket motstandsdyktighet mot phishingangrep kan oppnås igjennom økt digital kompetanse. Dette innebærer trening, øving og bevisstgjøringskampanjer egnet til å skape varig endring i deres brukeratferd. I den forbindelse anbefaler vi at framtidige sikkerhetsprogrammer og tiltak baseres på ulike scenarioøvelser, spill og konkurranser. Dette vil øke brukerrelevansen, motivere ansatte mer personlig, styrke læringsutbytte og stimulere til å endre ansattes digitale persepsjon og brukeradferd. Sikkerhetsprogrammer for endringer av brukeradferd må derfor planlegges, organiseres og kontrolleres for å

kunne administreres på en god måte. Det vil kreve at tydelig signaler fra politiledelsen at informasjonssikkerhet er viktig og blir prioritert, slik at det kan fasilitere for informasjonssikkerhetsarbeidet og skape en varig endring. Suksessfull implementering avhenger av at politiledelsen etablerer en tydelig visjon, strategi, myndiggjøring av ansatte samt at de inspirerer og tilrettelegger for endringer. Totalt sett er dette viktige momenter som vil bidra til å endre politiansattes digitale brukeratferd å øke motstandsdyktigheten mot sosial manipulering og phishingtrusler.

Etter at vi testet de tre forslagene til tiltak konkluderes det med at samtlige anbefales og er viktige i et langsiktig perspektiv. Imidlertid er det nok de ikke gjennomførbare av årsaker analysen og drøftelsene har redegjort for. Av den grunn faller endelig anbefaling ned på å videreutvikle konseptet PIT har påbegynt med den digitale sikkerhetsskolen, som vil lanseres på politiets intranett. I den forbindelse mener vi det er viktig og kontinuerlig forbedre og utvikle produktet etter brukerfeedback (for å sikre kursets relevans), etatens verdier, sårbarheter og det dynamiske trussellandskapet. Videre vil vi anbefale at politietaten utreder om det burde innføres policyer for hva og hvordan ansatte kommuniserer via epost, både internt og med eksterne aktører. Dette som et mulig risikoreduserende tiltak.

LITTERATURLISTE

Abawajy, J. (2014a). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, *33*(3), 237–248. https://doi.org/10.1080/0144929X.2012.708787

Abawajy, J. (2014b). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, *33*(3), 237–248. https://doi.org/10.1080/0144929X.2012.708787

Bakke, S. (2020, november 2). *Sikkerhet i det digitale samfunnet v2.0*. https://www.politiforum.no/simen-bakke/sikkerhet-i-det-digitale-samfunnet-v20/206644

Bemanningsstatistikk i Politiet. (2022, april 30). Politiet. https://www.politiet.no/aktuelt-tall-og-fakta/tall-og-fakta/bemanning/

Blank, S. (2013). Why the Lean Start-Up Changes Everything. *Harvard Business Review*, *91*(Issue 5), 63–72.

Busch, T. (2021). *Telenor – teknologi, mobil og tester*. https://www.online.no/

da Veiga, A., & Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. *Computers & Security*, *70*, 72–94. https://doi.org/10.1016/j.cose.2017.05.002

Datatilsynet. (2022). *Phishing—Hvordan beskytte virksomheten*. Datatilsynet. https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/phishing---hvordan-beskytte-virksomheten/

Deloitte. (2022). *Phishing—Hvordan skal din virksomhet håndtere et angrep?* Deloitte Norway. https://www2.deloitte.com/no/no/pages/legal/articles/phishing-hvordan-skal-din-virksomhet-haandtere-et-angrep.html

Europol. (2017). *Internet Organised Crime Threat Assessment (IOCTA) 2017*. Europol. https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2017

Europol. (2019). *Internet Organised Crime Threat Assessment (IOCTA) 2019*. Europol. http://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2019

Gill, R. (2002). Change management–or change leadership? *Journal of Change Management*, *3*(4), 307–318. https://doi.org/10.1080/714023845

Jøsang, A. (2021). *Informasjonsikkerhet -teori og praksis*. Universitetsforlaget AS.

Kahneman, D. (2012). *Thinking, fast and slow*. Penguin Books.

Kotter, J. P. (1995a). Leading Change: Why Transformation Efforts Fail. (cover story). *Harvard Business Review*, *73*(2), 59–67.

Kotter, J. P. (1995b). Leading Change: Why Transformation Efforts Fail. (cover story). *Harvard Business Review*, *73*(2), 59–67.

Lacey, D. (2009). *Managing the Human factor in Information Security. -How to win over staff and influence business managers*. John Wiley & Sons, Ltd.

Lain, D., Kostiainen, K., & Capkun, S. (2021). *Phishing in Organizations: Findings from a Large-Scale and Long-Term Study* (arXiv:2112.07498). arXiv. https://doi.org/10.48550/arXiv.2112.07498

NSM. (2022). *Risiko 2022* (NSMs årlige risikorapport 2022 Nr. 137798–1644424185; s. 40). https://nsm.no/getfile.php/137798-1644424185/Filer/Dokumenter/Rapporter/NSM_rapport_final_online_eneltsider.pdf

Politiets IKT-tjenester. (u.å.). Politiet. Hentet 24. mai 2022, fra https://www.politiet.no/om/organisasjonen/sarorganene/pit/om-pit/organisasjonen/

Regjeringen. (2019). *Nasjonal strategi for digital sikkerhet* (s. 32) [Strategidokument]. https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/nasjonal-strategi-for-digital-sikkerhet.pdf

Sander, K. (2021, juli 30). Endringsledelse og endringsprosesser. *eStudie.no*. https://estudie.no/endringsledelse/

Singh, K., Aggarwal, P., Rajivan, P., & Gonzalez, C. (2019). Training to Detect Phishing Emails: Effects of the Frequency of Experienced Phishing Emails. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *63*(1), 453–457. https://doi.org/10.1177/1071181319631355

Strategi for fremtidig IKT-funksjon i politiet. (2018). https://www.politiet.no/globalassets/05-om-oss/03-strategier-og-planer/strategi-for-fremtidig-ikt-funksjon-i-politiet_hoveddokument.pdf

Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security*, *109*, 102387. https://doi.org/10.1016/j.cose.2021.102387

Undersøkelse av angrep mot IKT-systemer i politiet. (2018). https://www.riksrevisjonen.no/rapporter-mappe/no-2019-2020/undersokelse-av-angrep-mot-ikt-systemer-i-politiet/

Whitman, M. E., & Mattfort, H. J. (2016). *Management of information security* (5.). Cengage Learning.

Aarseth, O. (2020, juli 20). *Nær én av tre politiansatte misfornøyd med toppledelsen*. https://www.politiforum.no/medarbeiderundersokelsen-pod/naer-n-av-tre-politiansatte-misfornoyd-med-toppledelsen/202757

Aarseth, O. (2022, februar 14). *Justisdepartementet ga ut navnene på 3000 politifolk – nektet å utlevere navnene på UDI-ansatte*. https://www.politiforum.no/sikkerhet/justisdepartementet-ga-ut-navnene-pa-3000-politifolk-nektet-a-utlevere-navnene-pa-udi-ansatte/222860