Universitetet i Stavanger

DET TEKNISK-NATURVITENSKAPELIGE FAKULTET

MASTEROPPGAVE

Studieprogram/spesialisering: Master i Samfunnssikkerhet	Vårsemesteret, 2021 Åpen
Forfatter: Alyona Trach Oftedahl	Alyona Oftedahl (Signatur forfatter)
Fagansvarlig: Sissel Haugdal Jore **Veileder:** Sissel Haugdal Jore	
Tittel på masteroppgave: Selv-rekognosering som et redskap i organisasjoners forebyggende informasjonssikkerhetsarbeid **Engelsk tittel:** Self-reconnaissance as a preventive tool for organizational information security	
Studiepoeng: 30	
Emneord: Åpen tilgjengelig informasjon, OSINT, trusseletterretning, rekognosering, kartlegging, cybersikkerhet, cyberangrep, informasjonssikkerhet, risikovurdering, trefaktormodellen, situasjonsbevissthet, cyber-risiko, sårbarhetsvurdering, verdivurdering, trusselvurdering, skjermingsverdig informasjonssystemer, skjermingsverdig informasjon	Sidetall: 111 Vedlegg/annet: 53 Total sider: 164 Stavanger, 13 juli 2021

Forside for masteroppgave

Det teknisk-naturvitenskapelige fakultet

Self-reconnaissance as a preventive tool for organizational information security

An exploratory study of how reconnaissance and Open Source Intelligence can be used by adversaries and how companies may benefit from implementing these methods.

Selv-rekognosering som et redskap i organisasjoners forebyggende informasjonssikkerhetsarbeid

En eksplorativ studie av hvordan rekognosering og OSINT brukes av trusselaktører og hvordan organisasjoner kan benytte seg av disse teknikkene til sin fordel

Masteroppgave i samfunnssikkerhet

Universitet i Stavanger

Vår 2021

Alyona Trach Oftedahl

Forord

Denne masteroppgaven markerer avslutning av mine seks år som student ved Universitetet i Stavanger. Arbeidet har vært spennende, lærerikt og utfordrende. Oppgaven har bidratt til erkjennelsen om at vår digitale eksistens gjør oss sårbare ved at vi uunngåelig eksponerer oss selv til trusselaktører. Kunnskapen og de praktiske ferdigheter jeg har tilegnet meg gjennom arbeidet med denne oppgaven er både viktig og dagsaktuelt i et stadig mer digitalisert samfunn.

Jeg vil rette en stor takk til mine informanter som viste enormt engasjement, interesse og bidro til at jeg følte meg velkommen i deres miljø. Takk til Malene Dolven og Karl Stefan Afradi for forslag for oppgavens tema og faglig råd. Takk til min veileder Sissel Haugdal Jore for oppfølging, gode veiledninger og hjelp med utfordringer jeg møtte underveis. Ikke minst er jeg veldig takknemlig for alt støtte jeg har fått av min kone Beate gjennom utfordrende studieår.

Jeg håper leserne finner oppgaven både relevant, lærerik og spennende. Samtidig håper jeg at oppgaven vil bidra til økt cyberbevissthet og mer kunnskap om cyberverdenen.

Alyona Trach Oftedahl,
Stavanger, juli 2021.

Sammendrag

Sikring av informasjonssystemer mot dataangrep er en av de viktigste utfordringene i det tjueførste århundret. Vår avhengighet av digitale systemer har gjort det virtuelle rom til en attraktiv arena for trusselaktører. Stadig flere aktiviteter som truer nasjonale interesser og kritisk infrastruktur foregår i cyberspace. Fremgang innen informasjonsteknologi byr på et mangfold nye utfordringer for risikovurdering og -styring i organisasjoner. Digitalisering medfører at det bevisst og ubevisst offentliggjøres mye informasjon om virksomheter og nøkkelpersoner. Slik informasjon representerer en stor verdi for både nasjonalstater, privat sektor og ikke minst trusselaktører.

Formålet med oppgaven er å undersøke (a) hvordan trusselaktører opererer når de kartlegger organisasjoner og (b) hvordan organisasjoner kan bruke disse kunnskapene i sitt forebyggende informasjonssikkerhetsarbeid. Trefaktormodellen for risikovurderinger, to teoretiske modeller som beskriver cyberangreps forløp og teori om situasjonsbevissthet er benyttet som bakteppe for denne studien. Oppgavens problemstilling er formulert som følger: *Hvordan kartlegger trusselaktører organisasjoner og hvordan kan selv-rekognosering brukes som redskap i organisasjoners forebyggende informasjonssikkerhetsarbeid?*

Jeg har gjennomført en kartlegging av to organisasjoner som driver med forskning og utvikling. Ved hjelp av ulike OSINT-verktøy utførte jeg rekognosering av organisasjonenes nettverk, programvare og nøkkelpersonell og identifiserte dermed potensielle sårbarheter. Resultatene av studien representerer empirisk bevis for effekten og nytten av OSINT-metodikk i arbeid med informasjonssikkerhet i organisasjoner. Forskningsresultatene ble brukt til å lage taktiske og strategiske anbefalinger for organisasjoner, basert på bruk av OSINT for å identifisere verdier og sårbarheter, og dermed redusere risiko. Med denne undersøkelsen ønsker jeg å rette oppmerksomheten mot muligheter som åpnes for organisasjoner ved å implementere OSINT som et element i risikovurderinger.

Abstract

Securing information systems against cyberattacks is one of the most important challenges of the twenty-first century. Our dependence on digital systems has made virtual space an attractive arena for adversaries. Exceedingly more activities that threaten national interests and critical infrastructure are taking place in cyberspace. Advances in information technology offer a variety of new challenges for risk assessment and management in organizations. Digitization means that a lot of information about companies and employees is published. This information represents a great value for nation states, the private sector and adversaries.

The purpose of the thesis is to investigate (a) how threat actors operate when they perform reconnaissance on organization and (b) how organizations can use this knowledge as a preventive strategy. The three-factor model for risk assessments, two theoretical models that describe cyberattacks lifecycle and the theory of situational awareness are used as a backdrop for the study. This study aims to answer: How do adversaries perform reconnaissance on organizations and how can self-reconnaissance be used as a tool in organizations' preventive information security work.

To answer this question, I conducted a survey of two organizations engaged in research and development. Using various OSINT tools, I performed reconnaissance of the organization's network, software, and key personnel, thus identifying organization's potential vulnerabilities. Results of the study represent empirical evidence for the effect and usefulness of OSINT methodology in work with information security in organizations. The research results were used to produce tactical and strategic recommendations for organizations based on the use of OSINT to identify assets and vulnerabilities, thereby reducing risk. With this study, I want to draw attention to opportunities opening up for organizations by implementing OSINT methodology as an element in risk assessments.

Ordliste og forkortelser

Norsk	Engelsk	Definisjon
Angrepsflate	Attack surface	Et system som en angriper vil prøve å komme inn (Ross, Pillitteri, Graubart, Bodeau, & McQuaid, 2019).
Applikasjon	App	Programvare som er laget for å kunne utføre spesifikke tjenester for en bruker (Nätt & Heide, 2021, s. 394).
Autentifikator	Credentials	Brukes for å kontrollere tilgang til informasjon eller andre ressurser (Bergsjø, Windvik, & Øverlier, 2020).
Bot og Botnett	Bot, Botnet	En kapret datamaskin som kan fjernstyres. Et botnett er en samling av slike kaprede maskiner (Nätt & Heide, 2021, s. 395).
BSSID	BSSID	En unik identifikator for hver trådløs enhet.
Brute-force angrep	Brute-force attack	Den enkleste tilnærmingen for å få tilgang til systemer gjennom å prøve alle mulige kombinasjoner av et passord (Kanta, Coisel, & Scanlon, 2020, s. 5).
Drapskjede	Cyber Kill Chain	Modellen som beskriver forløp i et cyberangrep (Hutchins, Cloppert, & Amin, 2011).
Cybersikkerhet	Cyber security	Beskyttelse av «alt» som er sårbart fordi det er koblet til, eller på annen måte er avhengig av informasjon- og kommunikasjons-teknologi» (NOU 2015: 13, s. 34).
Cyberspace	Cyberspace	Kombinasjon av maskinvare, data og mennesker (Edgar & Mantz, 2018).
	Datadumps, pastedumps	Websider som brukes for å dumpe data som tidligere var konfidensiell, eksempelvis e-post adresser med passord.
Datanettverks-operasjoner	Network operations	En prosess der trusselaktører søker å skaffe seg urettmessig tilgang til datanettverk hos en spesifikk virksomhet (PST, 2020b, s. 2).
Datautvinning	Data mining, Data extraction	Prosess av gjennomgåelse av store, eksisterende databaser for å generere ny informasjon med formål om å hente ut informasjon fra datasett og transformere det til en forståelig struktur for videre bruk (Oxford Dictionary, 2021).
Digital verdikjede	Supply Chain	En struktur av leveranser mellom virksomheter, hvor hver leveranse enten er en digital tjeneste, programvare eller maskinvare (NOU 2015: 13).
Digital infrastruktur	Digital infrastructure	Digital infrastruktur består av maskinvare og programvare og utfører en eller flere tjenester (DSB, 2019, s. 10).
Digitalt sertifikat	Digital certificate	Et digitalt sertifikat er en unik datafil som kan utstedes til en person, en organisasjon, et dataprogram osv. som har

		en unik identitet, og brukes som digital legitimasjon (Wilson, 2020).
Digital trusseletterretning	Cyber Threat Intelligence	Vanligvis beskriver aktiviteter knyttet til produsering av kunnskap om cybertrusler iverksatt av sikkerhets-myndigheter. I det siste ble det også brukt som betegnelse på ondsinnede aktiviteter som innebærer innsamling av informasjon om et mål av en trusselaktør. Synonymt til «profilering» og «kartlegging».
Distribuert tjenestenekt	DDoS	Tjenestenekt som forårsaket av et botnett, dvs. flere maskiner sammen angriper et digitalt system (Nätt & Heide, 2021, s. 404).
DNS	DNS - står for Domain Name System	Er et hierarkisk og desentralisert navnesystem for datamaskiner, tjenester eller andre ressurser som er koblet til Internett eller et privat nettverk (Nätt & Heide, 2021, s. 396). Gjør det mulig for datamaskiner å oversette nettadresse til IP-adresse.
DNS-kapring	DNS-hijacking	Betyr å få en maskin til å bruke svindlerens DNS-server istedenfor en ekte (Nätt & Heide, 2021, s. 396).
Domenenavn	Domain name	En unik, hierarkisk oppbygget navnestreng som benyttes til adressering på Internett (Nätt & Heide, 2021, s. 396).
Eksfiltrasjon	Exfiltration	En skjult måte for å stjele data på (Bergsjø et al., 2020, s. 174).
Emneknagg	Hashtag	Firkanttast (#) etterfulgt av et ord som viser temaet eller fungerer som en kommentar til et innlegg/bilde (Stor engelsk ordbok, u.å.).
Etisk hacker	Etical hacker	En cyberekspert som spesialiserer seg på penetrasjons testing.
Fastvare	Firmware	Programvare som ligger fast innebygd i en enhet, for eksempel i en harddisk (Nätt & Heide, 2021, s. 397).
Fisking etter informasjon		Sosial manipulering-teknikk som benyttes for å manipulere et offer til å gi fra seg informasjon. Ikke det samme som nettfisking.
Grunnleggende nasjonale funksjoner		Ulike former for virksomhet som er av en slik betydning at et helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser (Sikkerhetsloven, 2018).
HTTP	Hypertext Transfer Protocol	Navnet på settet av regler for hvordan en nettleser og en webserver skal kommunisere med hverandre (Nätt & Heide, 2021, s. 398).
HTTPS	Hypertext Transfer Protocol Secure	En spesialutgave av HTTP som gjør at samtalen mellom nettleser og webserver kan foregå kryptert (Nätt & Heide, 2021, s. 398).

HUMINT	HUMINT	Innsamling av informasjon ved spørring eller sosial manipulering av mennesker (Akhgar, Sampson, & Bayerl, 2016).
iFrame-injeksjon	iFrame-injection	iFrame er en komponent i et HTML-element som lar en å legge inn dokumenter og interaktive medier på en nettside. iFrame kan bli brukt for såkalt iFrame-injeksjon, som omdirigerer besøkende til et ondsinnet nettsted, som deretter vil installere et virus på PC (Goyal, 2020).
Informasjons-sikkerhet	Information security	Sikring av informasjonens konfidensialitet, integritet og tilgjengelighet, uavhengig av om informasjonen er digital eller analog (Departementene, 2012, s. 28).
Informasjons-system		Informasjonssystem består av programvare, maskinvare og tilknyttede tjenester (NSM, 2020b).
IP-adresse	IP-address	En talladresse som identifiserer en enhet som er knyttet til Internett (Nätt & Heide, 2021, s. 400).
IP-blokk	IP-range	Et sett med IP-er som kan tildeles en organisasjon/person.
Løsepengevirus	Ransomware	En type skadevare som brukes til å kryptere filer hos et mål, og deretter kreve penger for å dekryptere dem (NSM, 2019b).
Maskinvare	Hardware	Et fysisk digitalt produkt, f.eks. en fiberkabel, et kretskort, en chip, en mobiltelefon eller en PC (DSB, 2019, s. 10).
Metadata	Metadata	En informasjon om data (Nätt & Heide, 2021, s. 399). F. eks. vil metadata om et bilde si noe om av hvem, når og hvor tatt den.
Målrettet nettfisking	Spear-phishing	Målrettet nettfisking innebærer at trusselaktør retter angrepet mot en bestemt person/organisasjon. Se også nettfisking.
Nettfisking	Phishing	En måte for kriminelle å få privat informasjon fra et offer ved å sende en e-post som ser ut til å være fra en legitim person/ organisasjon (Marion & Twede, 2020, s. xii).
Nulldagssårbarhet	Zero-day vulnerability	Sårbarhet som noen kjenner til, som ikke er kjent for leverandøren av produktet, eller en kjent sårbarhet som det ennå ikke har blitt utgitt noen sikkerhetsfiks til (Brombach, 2017).
Ordlisteangrep	Dictionary attack	En metode for å knekke passordbeskyttelse som består i å forsøke å logge inn med ordene i en ferdiglaget liste som passord, ett for ett (Nätt & Heide, 2021, s. 400).
OSINT	OSINT	Datainnsamlingsmetode som innebærer innhenting av informasjon fra åpne kilder med formål om å gjennomføre granskning, etterretning, kartlegging osv. (Gibson, 2016).
	Ping/poke	Sondere nettverk for å se hvordan sikkerhetsbarrierer reagerer.

Port	Port	En kanal som gjør at datamaskinen kan skille mellom forskjellige typer internettrafikk basert på forskjellige typer protokoller.
Programvare	Software	En logisk og som oftest tekstlig beskrivelse av hvilke handlinger maskinvare skal utføre. Eksempel er et operativsystem eller en applikasjon (DSB, 2019, s. 10).
Protokoll	Protocol	Et sett med regler som bestemmer hvordan datamaskiner kommuniserer med hverandre.
Rekognosering	Reconnaissance	Innsamling av informasjon om et mål
	Self-doxxing	Uønsket og ikke-planlagt eksponering av dataskjerm som resulterer i at uvedkommende kan lese hva som står på skjerm, hvilke apper som er i bruk osv.
Sensitiv informasjon	Sensitive information	Spesifikk og inngående opplysninger om virksomheten som kan brukes til å skade anlegg/system eller påvirke funksjoner som har betydning for kritisk infrastruktur (NVE, 2019).
Skjermingsverdig informasjon		Informasjon er skjermingsverdig «dersom det kan skade nasjonale sikkerhetsinteresser at informasjonen blir kjent for uvedkommende, går tapt, blir endret eller blir utilgjengelig» (Sikkerhetsloven, 2018).
Skadevare	Malware	En samlebetegnelse på programkode som uten brukerens tillatelse utfører handlinger med brukerens systemer eller informasjon (Nätt & Heide, 2021, s. 403).
SOCMINT	SOCMINT	Innsamling av informasjon fra SoMe (Akhgar et al., 2016)
Sosial manipulering	Social engineering	Manipulasjonsteknikk som utnytter menneskelige egenskaper for å få privat informasjon eller verdier. Angrep kan skje online, personlig og via andre typer interaksjoner (Hatfield, 2018).
SoMe	SoMe	Sosiale media: Facebook, Twitter, LinkedIn osv.
Spoofe	Spoof	Imitere, forfalske
Tilgangsrettigheter	Access rights	Rettigheter til å bruke en enhet eller en ressurs (Nätt & Heide, 2021, s. 404).
Tjenestenekt	DoS	Tjenestenekt (DoS) innebærer at informasjon, ressurser eller tjenester blir helt eller delvis utilgjengelige som følge av et angrep (Nätt & Heide, 2021, s. 404).
TLS, TLS sertifikat	TLS, Transport Layer Security	En protokoll som etablerer en kryptert kobling mellom to datamaskiner knyttet Internett. Det verifiserer serverens identitet og forhindrer hackere i å snappe opp data.
Trusselaktør	Adverssary	En person, gruppe, organisasjon eller regjering som har intensjon om å gjennomføre angrep mot datasystemer for å påføre systemer skade (Edgar & Manz, 2017, s. 40).

Underdomene	Subdomain	Domene som er en del av et domene. For eksempel, hvis et domene tilbød en nettbutikk som en del av nettstedet example.com, kan det bruke underdomenet shop.example.com (Nätt & Heide, 2021, s. 404).
Utnyttelse	Exploitation	Utnyttelse av tekniske sårbarheter i et digitalt system (Bergsjø et al., 2020).
Utnyttelseskode	Exploit	Koden som utnytter sårbarhet i et nettverk (Bergsjø et al., 2020, s. 170).
URL	URL	URL er en standard for angivelse av adresser til dokumenter og andre ressurser på internett (Liseter, 2020).
Vertsnavn	Hostname	Hjelper med å identifisere nettverket som leder brukeren til et bestemt nettsted. Når brukeren besøker en nettside, vises webadressen i nettleseren (Sawakinome, 2021).
VPN	VPN	En dataprogramvare som sender all datatrafikk fra en datamaskin gjennom en kryptert virtuell tunnel. VPN «maskerer» brukernes identitet.
Virus	Virus	En skadelig programvare som lastes opp på datamaskinen av en bruker. Den vil replisere seg selv via f.eks. e-post (Marion & Twede, 2020, s. xiii).
	Web-crawler	En bot som systematisk surfer Internett. Brukt for å indeksere websider til søkemotorer (Abello, Pardalos, & Resende, 2013).
WEBINT	WEBINT	Datainnsamlingsmetode som innebærer innhenting av informasjon fra online kilder (Akhgar et al., 2016, s. 214).
Åpen tilgjengelig informasjon	Open Source Intelligence	Opplysninger som er tilgjengelig for publikum: Internett, møter, anbud, dokumenter, kataloger, arkiv osv.

Visuelle elementer og datapresentasjon

Figurer

Bilder

Tabeller

Innholdsfortegnelse

1. Innledning

1.1. Tema og motivasjon

Hovedtema i denne oppgaven er datanettverksoperasjoner mot norske virksomheter. Med datanettverksoperasjoner menes «en prosess der trusselaktører søker å skaffe seg urettmessig tilgang til datanettverk hos en spesifikk virksomhet» (PST, 2020b, s. 2). I denne oppgaven har jeg fokus på digital trusseletterretning, også kalt «kartlegging», av organisasjoner og hvordan slik sikkerhetstruende virksomhet kan motvirkes.

Det er flere faktorer som ligger bak valget av tema. Blant de viktigste kan nevnes økende trussel av datanettverksoperasjoner, hyppighet og alvorlighetsgrad av målrettede cyberangrep, samt manglende kunnskaper om hvordan vi eksponerer oss selv på Internett og hvordan trusselaktører opererer (CSIS, 2021; NSM, 2017, 2020b, 2020b; PST, 2020b). Ikke minst var min egen interesse for OSINT som datainnsamlingsmetode av betydning.

Fra starten ønsket jeg å forstå og demonstrere hvordan trusselaktører kartlegger organisasjoner. Til tross for flere rapporter som advarer virksomheter om digital kartlegging, mangler det kunnskaper om hvordan kartlegging skjer i praksis, altså på mikro-nivå. Underveis i arbeidet med oppgaven har jeg fått forståelse av at «selv-rekognosering» kan være et nyttig verktøy i organisasjoners forebyggende sikkerhetsarbeid. Jeg ønsker derav å diskutere hvordan selv-rekognosering ved hjelp av OSINT kan brukes for å beskytte skjermingsverdig informasjon og informasjonssystemer mot tilsiktede handlinger.

1.2. Bakgrunn og aktualitet

De siste årenes digitale kartlegging av norske virksomheter og påfølgende utnyttelse av sårbarheter, antas å være en av de mest alvorlige truslene Norge står overfor i dag og i årene fremover (Forsvarets etterretningstjeneste, 2020, s. 12; NSM, 2020c, s. 16, 2020a, s. 14; PST, 2020b, s. 10). Mellom januar og april 2021 har verden allerede opplevd rundt 50 målrettede cyberangrep, som ifølge Senter for Strategiske og Internasjonale Studier, CSIS, (2021) vurderes som alvorlige. Med «alvorlige cyberangrep» mener CSIS (2021) «angrep på offentlige etater, forsvars- og høyteknologiske selskaper eller økonomiske forbrytelser med tap på mer enn en million dollar». Blant de alvorligste hendelsene som rammet Norge kan nevnes

angrepet på Stortinget i august 2020, på ti norske kommuner og Aqua Group i januar 2021 og på cybersikkerhetsrådgivingsselskapet SolarWinds i februar 2021 (Kibar, 2020; Langved & Kibar, 2021; PST, 2020a; Røise, 2021). Vi hører om cyberangrep nesten hver dag. Men hvordan forløper egentlig et cyberangrep, og hvilke teknikker bruker angripere?

Hvert cyberangrep starter med en omfattende trusseletterretning (rekognosering) som innebærer å bli kjent med målet før man går til angrep (Forsvarets etterretningstjeneste, 2021; Hutchins et al., 2011; RSA, 2015; Sanghvi & Dahiya, 2013). Rekognosering er ikke et nytt fenomen, og stammer tilbake like lenge som mennesket har vært kjent med krigføring. Rekognosering kan defineres som «å fremskaffe data eller informasjon om en aktør, aktiviteter eller fysiske karakteristikker i et definert fysisk område eller domene ved et gjennomsøk» (Forsvarets etterretningstjeneste, 2021, s. 105).

Av nyere tid forbindes ofte rekognosering med bruk av OSINT-metodikk, som innebærer innsamling av åpen tilgjengelig informasjon. Dette er en naturlig utvikling da digitalisering har medført en eksplosjon av åpen tilgjengelig informasjon. I dag produserer nettsteder og sosiale medier enormt mye informasjon om mennesker, organisasjoner og infrastruktur. World Wide Web har omkring 200 millioner aktive websider i dag (Internet Live Stats, 2021). Innen 2025 vil verden lagre 200 zettabyte data, 50 prosent av det vil bli lagret i skytjenester (Morgan, 2020). Trusseletterretning har flyttet til cyberspace, som gjør det enklere for trusselaktører å kartlegge virksomheter, skjule sine spor og å forbli usynlig lengre.

1.3. Problemformulering og problemstilling

Det er vanskelig å gi en enkel problemformulering som omfatter alle utfordringene vi står overfor. Blant hoved variablene er (a) digitalisering og globalisering, (b) demokrati og tillitt vs. sikkerhet, (c) dynamisk og endrende risikobilde som utfordrer kunnskapsgrunnlag og dermed vurderinger og beslutninger knyttet til risikohåndtering. I denne matrisen ser digitalisering ut å være den uavhengige variabelen, da vi ikke lenger er i stand til å stanse utviklingen. Det vil si at vi må tilpasse våre aktiviteter for å bevare demokrati, sikkerhet og tillitt, mens vi og må lære oss å leve med risikoer.

Samspillet mellom digitalisering og globalisering medfører at mye forretningsvirksomhet foregår digitalt og på tvers av nasjonale grenser. Avstand er ikke lenger et hinder for etablering av nye forretningsrelasjoner og tjenesteutsetting er blitt vanlig. Verdikjeder er blitt lengre og

mer komplekse. Derav mister virksomheter oversikt over egne verdier, sårbarheter og risiko (DSB, 2019; NorSIS, 2018; NSM, 2020b). På en annen side er digitalisering og globalisering i trusselaktørers favør. Det har aldri vært lettere for dem å forholde seg usynlig, skjule sine spor og kartlegge virksomheter og mennesker. Dette demonstrerer jeg i denne oppgaven.

Digitalisering bidrar til åpenhet og demokrati, men utgjør samtidig en trussel mot demokratiske idealer og prosesser. Organisasjoner i demokratiske samfunn er utsatt for økt eksponering gjennom digitalisering (NorSIS, 2018). I demokratiske land er våre aktiviteter basert på tillitt mellom mennesker og myndigheter, dermed er mye dokumenter, beslutninger, anbud og rapporter åpne for allmennheten. Denne åpent tilgjengelige informasjonen er av stor interesse for trusselaktører, da den kan brukes til å skade organisasjon, systemer eller påvirke funksjoner som har betydning for organisasjonens/samfunnets virke (Hayes & Cappa, 2018; Matvej, Moric, & Papic, 2020; NorSIS, 2018). Digitaliseringen skal skje på en måte som bevarer åpenheten (NorSIS, 2018, s. 8). En anerkjent konklusjon er at vi da må vi lære oss å leve med vedvarende risiko og heller fokusere på samfunnets resiliens (Anholt & Boersma, 2018; Boin & McConnell, 2007; Pellissier, 2010).

Etter den kalde krigen har vi trådd inn i ny verden hvor maktbalansen er uklar, grenser og ideologier endrer seg fort og våpen og motiver er ikke alltid synlig. I kombinasjon med eksponentiell teknologisk utvikling medfører det at vi kontinuerlig er på etterskudd når det gjelder oppdatert kunnskap, lover og situasjonsforståelse. Vi kjenner ikke våre fiender lenger og kjenner oss selv i enda mindre grad enn før.

Problemstilling og forskningsspørsmål

I forbindelse med krigføring brukes ofte utrykket «å kjenne sin fiende». Utrykket stammer fra boken «The Art of War» som ble skrevet for 2400 år siden av den kinesiske generalen Sun Tzu. Sun Tzu (overs. 2009, s. 13) skriver: «If you know the enemy and know yourself, you need not fear the result of a hundred battles». Med dette mente han at når vi har grunnlag for å vurdere trusselaktørets evner og kapasiteter, kan bruke informasjonen til å styrke vår posisjon. I digital tid, når trusselaktører oftest forblir usynlige og det er lett å skjule spor, må vi forstå hvordan «fiender opererer» for å beskytte oss selv.

Med denne oppgaven argumenterer jeg for at vi kan lære mye om både fiender og oss selv ved å forstå handlingsmønster og ved å selv ta i bruk teknikker og verktøy som brukes av

trusselaktører. Organisasjoner kan benytte seg av disse kunnskapene og verktøyene i sitt forebyggende sikkerhetsarbeid. Derav har jeg formulert følgende problemstilling:

Hvordan kartlegger trusselaktører organisasjoner og hvordan kan selv-rekognosering brukes som redskap i organisasjoners forebyggende informasjonssikkerhetsarbeid?

Den underliggende antakelse er at for å beskytte organisasjoners informasjonssystemer, må vi først og fremst forstå hvordan trusselaktører opererer. En god måte å forstå dette på, er ved å undersøke prosessen fra trusselaktørs perspektiv. Jeg har formulert tre forskningsspørsmål som forventes å danne grunnleggende forståelse for hvordan trusselaktører opererer, hvilken risiko åpen tilgjengelig informasjon utgjør for organisasjoners sikkerhet og hvilken betydning rekognosering og OSINT har i angrepenes forløp.

Det første forskningsspørsmålet er

(1) Hvordan fungerer digital rekognosering av organisasjoner i praksis?

Her sikter jeg mot å skape forståelse for selve prosessen, teknikker og verktøy. Dette spørsmålet vil besvares gjennom beskrivelse av hvordan jeg, som en trusselaktør, har kartlagt to norske organisasjoner. Teorier innen cybersikkerhet og intervjuer dannet grunnlag for planlegging og gjennomføring av kartleggingen.

Det andre spørsmålet er

(2) Hvilken informasjon om de utvalgte virksomhetene kan man finne ved hjelp av rekognoseringsteknikker og OSINT?

Her vil jeg demonstrere hvor mye informasjon om de utvalgte organisasjonene man kan samle fra Internett ved hjelp av OSINT-verktøy. Hvor vellykket en datanettverksoperasjon vil være avhengig av hvor mye informasjon en trusselaktør kan samle.

Med det tredje forskningsspørsmålet,

(3) Hvorfor er denne type informasjon av interesse for en trusselaktør?

søker jeg å skissere hvordan denne informasjonen, som ved første øyekast ikke representerer noen fare, har blitt brukt for å skade virksomheter i tidligere cyberangrep. Svaret er basert på granskningsrapporter, rettsaker og intervju.

1.4. Fremgangsmåte og begrunnelsen for valg av forskningsobjekt

For å planlegge rekognoseringen har jeg støttet meg på teoretiske modeller som beskriver cyberangreps livssyklus. Perspektiver på sikkerhetsstyring av informasjonssystemer, samt trefaktormodellen for risikoanalyse er valgt for å danne grunnlag for å besvare andre del av oppgavens problemstilling om forebygging. Teori om situasjonsbevissthet er valgt fordi den er blant de sentrale teorier som brukes i både cybersikkerhet og i samfunnssikkerhet.

Jeg bruker metodetriangulering hvor data er innsamlet ved hjelp av OSINT-metodikk og verktøy, ustrukturerte intervjuer og dokumentstudie. Denne oppgavens metodiske tilnærming tar for seg rekognoseringsprosessen fra et motstander-perspektiv overfor et potensielt mål. OSINT-metodikk brukes for å demonstrere hvordan kartlegging av organisasjoner skjer i praksis og hvor mye informasjon om virksomheter en trusselaktør kan få via åpne tilgjengelige kilder. Dernest brukes resultater av dokumentstudiet for å beskrive hvordan denne typen informasjon har blitt brukt i tidligere cyberangrep. Data innsamlet ved hjelp av ustrukturerte intervjuer er brukt for å utdype forståelsen for hvordan åpen tilgjengelig informasjon kan brukes for å skade organisasjoner.

Forskningsobjekt

For å svare på første del av problemstillingen og forskningsspørsmålene samlet jeg informasjon om to organisasjoner. Organisasjon A er en stor forsknings- og utdanningsinstitusjon. Organisasjon B er en liten privat bedrift som driver med forskning, utvikling og rådgivning for blant annet offentlig sektor og oljebransjen. Felles kjennetegn ved disse virksomhetene er at de produserer, utvikler og forvalter kunnskap og tjenester i form av forskning, teknologiutvikling, risikovurderinger og utredninger. Deres aktiviteter inkluderer blant annet utvikling av metodikk, teoretiske modeller og teknologi for prosjekter relatert til kritiske samfunnsfunksjoner.

Valg av organisasjoner begrunnes med blant annet PSTs (2020, s. 12) trusselvurdering som fremhever at trusseletterretning mot virksomheter som driver med forsknings- og utvikling vil øke i fremtiden. Dette fordi bransjen har en sentral rolle i staters strategiske ambisjoner. Flere andre kilder bekrefter denne trenden (Anderson, 2021; APWG, 2019; Berman, 2018; Coughlan, 2017; Crowdstrike, 2021; Lazzarotti, Dorer, & Khetarpal, 2017; NCSC, 2020, 2021) (Anderson, 2021; APWG, 2019; Berman, 2018; Coughlan, 2017; Crowdstrike, 2021; Lazzarotti et al., 2017; NCSC, 2020).

Jeg vil understrekke at målet med oppgaven ikke er å utpeke mangler ved en bestemt organisasjons sikkerhetsholdninger, men å forklare hvordan OSINT kan brukes i arbeidet med digital sikkerhet ved å identifisere eksponeringer, og til slutt gi anbefalinger for å forbedre sikkerheten og redusere risikoen for nettangrep. I denne studien gir jeg empiriske bevis som viser effekten av denne teknikken for organisasjoner og beslutningstakere som trenger å forbedre organisasjonens og nasjonal sikkerhet.

1.5. Begrepsavklaring

Rekognosering

Rekognosering er en systematisk prosess som innebærer søk, innsamling, identifisering og registrering av informasjon om et mål (Forsvarets etterretningstjeneste, 2021; Kerner, 2015; MITRE, 2021c; POD, 2020; Shimonski, 2015). Rekognoseringen er med andre ord kartlegging av målets styrker og svakheter. Prosessen inkluderer bruk av ulike verktøy og teknikker blant annet OSINT og web-skanning (Chauhan, 2015; MITRE, 2021c; RSA, 2015). På norsk brukes ofte begrepene «kartlegging» og «trusseletterretning» som synonymer for rekognosering (Bergsjø et al., 2020; NSM, 2020a, 2020c; PST, 2020b). Slik er de også brukt i oppgaven.

Selv-rekognosering

Det finnes ikke en vitenskapelig og anerkjent definisjon for selv-rekognosering. Begrepet «etterretning» brukes ofte for å beskrive lignende aktiviteter. Etterretning er imidlertid et veldig et bredt konsept og derfor foreslår jeg å bruke «selv-rekognosering». I denne studien har jeg definert begrepet som «en systematisk kartlegging av egne sosio-tekniske systemer og avhengigheter ved hjelp av digitale verktøy og etterretningsteknikker, med formål om å identifisere organisasjons verdier, sårbarheter og mulige angrepsvektorer og dermed forebygge uønskede hendelser og beskytte skjermingsverdig informasjon mot en trusselaktør».

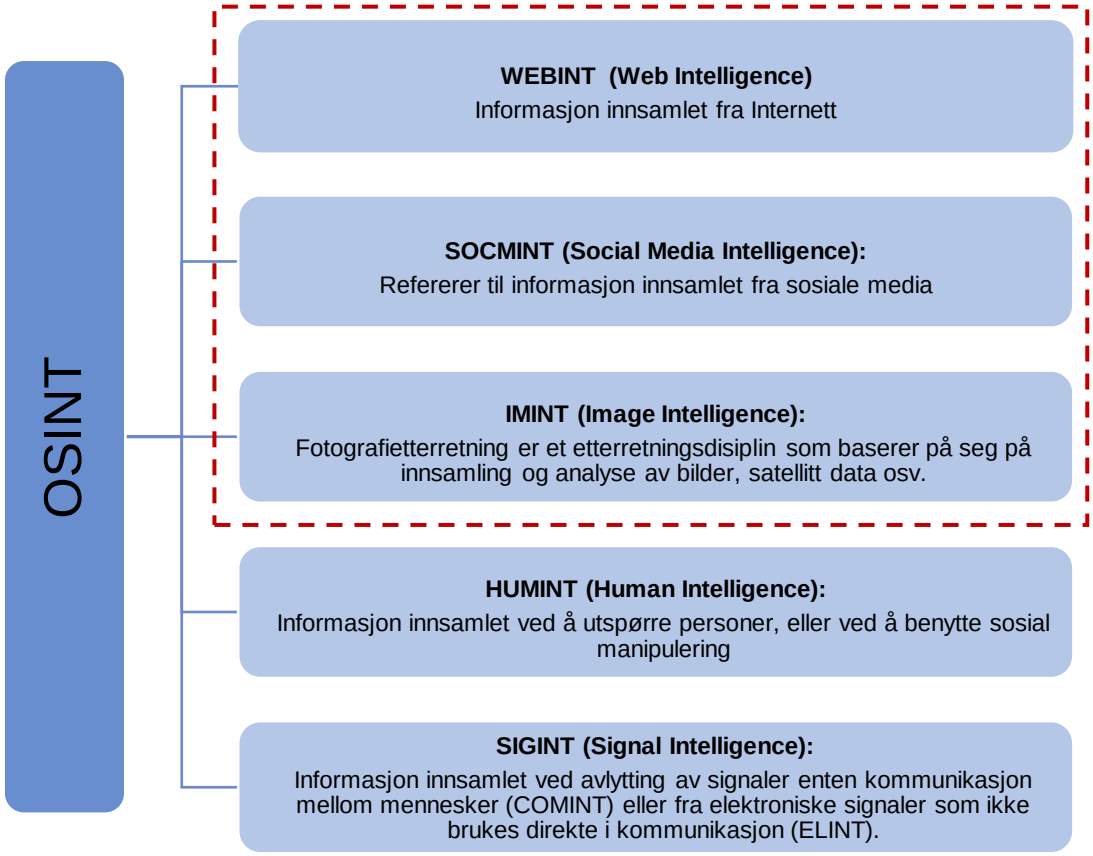
OSINT

OSINT står for Open Source Intelligence og defineres som «[...] an intelligence that is produced from publicly available information and is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement» (refereres til USAs Forsvarsdepartementet i Hassan & Hijazi, 2018, s. 2). Med

andre ord innebærer OSINT innsamling av informasjon fra forskjellige offentlige åpne kilder som kan inkludere både informanter, fysiske dokumenter, video, bildemateriell, uttalelser osv.

I konteksten av denne oppgaven er åpen tilgjengelig informasjon, all informasjon som er offentlig tilgjengelig på Internett. Dette inkluderer både Deep Web og Dark Web, SoMe, databaser, aviser, reklame, stillingsannonser, eller annen form for informasjon som ikke krever noen tilgangsrettigheter eller tillatelser (Pastor-Galindo et al., 2020). Figur 1 illustrerer de ulike elementene OSINT består av. Rød linje markerer oppgavens avgrensning.

Figur 1: Elementer av OSINT (basert på Akhgar et al. 2016, s. 39).



Et viktig skille å bemerke seg er at OSINT-verktøy ikke er det samme som åpent kilde-verktøy. Åpent kilde-verktøy inkluderer alle verktøy som er tilgjengelig online, som kan brukes til eksempelvis å hacke nettverk. Med OSINT-verktøy menes som regel kun verktøy utviklet eller optimalisert for datainnsamling.

Oppsummert kan man si at OSINT er en metode for datainnsamling, som kan brukes blant annet i en rekognoseringsprosess.

Web-skanning

Web-skanning (*eng*. web scraping[1]) innebærer bruk av automatiserte verktøy som skanner internett, herunder websider og nettverk, og innhenter data på en effektiv og systematisk måte (Perez, 2019). Innsamling av store mengder data manuelt vil være en ressurskrevende oppgave, mens det med automatiserte verktøy tar noen sekunder. I denne oppgaven begrunnes bruk av skanningsverktøy med ønske om å demonstrere hvordan trusselaktør gjennomfører rekognosering i virkeligheten.

Trusselaktør

Begrepet «trusselaktør» står sentralt i oppgaven og må derfor avklares. En trusselaktør er en person, gruppe, organisasjon eller regjering som har intensjon om å gjennomføre angrep mot datasystemer for å påføre systemene skade (Edgar & Manz, 2017, s. 40). Trusselaktører kan kategoriseres ut ifra tre faktorer: intensjon, kapabilitet og mulighet (Bergsjø et al., 2020, s. 151). Med *intensjon* menes aktørs motivasjon og formål med operasjon. *Kapabilitet* innebærer aktørs ferdigheter, kunnskaper, ressurser, arbeidskraft osv. *Mulighet* innebærer hvorvidt aktør er målrettet, og/eller opportunistisk (Bergsjø et al., 2020, s. 151-153).

1.6. Avgrensning

Oppgavens avgrensning er knyttet til datainnsamling:

- *Forskningsobjekter:* Det samles informasjon om to organisasjoner tilhørende forsknings- og utviklingssektor.
- *Kilder:* Alle data er innsamlet fra internettbaserte kilder. Dette for å demonstrere hvor mye informasjon kan samles av en trusselaktør som eksempelvis befinner seg i utlandet.
- *Rekognosering:* Verken penetrering av systemets barrierer eller sosial manipulering har vært brukt i denne undersøkelsen. Dette av etiske og juridiske hensyn.
- *Personlige opplysninger:* Navn og personlige opplysninger ble ikke brukt som søkeord. Det vil si at kun organisasjonens navn og domene er brukt. Det ble ikke innhentet data fra ansattes private brukerkontoer, selv om disse som regel er av største interesse for angripere. Det da personsøk er forbundet med flere etiske dilemmaer. Det påpekes at personlige data

[1] Det er også forskjell mellom begrepene «web-crowling» og «web scraping». Forskjellen går ut på hvorvidt en bruker verktøy som laster ned dataene på datamaskin.

kan være en del av funn, selv om forsker bevist prøver å unngå dette. Årsaker til det diskuteres senere i oppgaven.

- *Tidsperiode:* For å gjennomføre søk har jeg brukt innstillinger som definerer tidsperiode. Initiell tidsperiode var avgrenset fra 01.01.2020 til 31.12.2021. Dette til tross, har søkene resultert i flere dokumenter med tidligere datering. Dette kan forklares med at de ble lagt ut på internett i aktuell periode, eller at det ble gjort endringer/oppdateringer på webservere og websider innenfor perioden. Jeg har senere utelukket flere av de eldre dokumentene, da de ikke inneholdt relevant informasjon. Informasjons relevans var avgjørende for hvorvidt dokumenter inkluderes i analyse av funn.

1.7. Oppgavens oppbygging

Oppgaven er bygd opp på følgende måte:

I Kapittel 2, «The State of Art», presenteres oversikt over tidligere forskning som omhandler bruk av OSINT-metodikk i kontekst av cybersikkerhet og risikovurderinger. Kapittelet avsluttes med drøfting av hvordan eksisterende og ikke-eksisterende forskning har motivert denne studien.

Kapittel 3, Teoretisk rammeverk, gjennomgås det teoretiske grunnlaget for studien. Det gjøres rede for to modeller av cyberangrep og sentrale konsepter i cyber- og informasjonssikkerhet. Kapittel avsluttes med redegjørelsen av teorienes relevans for denne oppgaven.

Kapittel 4, Metodisk tilnærming, redegjør for de metodiske valgene som er gjort. Jeg begrunner valg av forskningsdesign og forskningsstrategi, drøfter prosessen av datainnsamling og analyse og studiens begrensninger. Kapittelet avsluttes med etiske refleksjoner som har preget studien.

I kapittel 5, Empiri og analyse, besvarer jeg hvordan trusselaktører kartlegger organisasjoner. Dette ved å presentere empiri innsamlet ved hjelp av OSINT, intervjuer og dokumentstudie.

I kapittel 6, Diskusjon, drøftes hvordan selv-rekognosering kan brukes som redskap i organisasjoners forebyggende informasjons-sikkerhetsarbeid, med utgangspunkt i besvarelse av forskningsspørsmål og teoretisk rammeverk.

Kapittel 7, Konklusjon, oppsummerer studiens funn og drøfter potensialet for fremtidig forskning.

2. «The State of Art»

Dette kapittelet presenterer relevant forskning som omhandler bruk av OSINT i forbindelse med cybersikkerhet.

«Snøballmetoden» er brukt for å finne relevant litteratur. Jeg benyttet meg hovedsakelig av ScienceDirect, ResearchGate, Oria og Scopus, men andre vitenskapelige åpne biblioteker ble også brukt. Følgende søkeord, både på norsk og engelsk, ble brukt: «cybersikkerhet», «informasjonssikkerhet», «datasikkerhet», «cyberangrep», «OSINT», «åpen tilgjengelig informasjon», «rekognosering», «kartlegging», «Internett-etterretning».

Cyber- og informasjonssikkerhet er et fagfelt hvor faglitteratur fort har blitt utdatert, derav har publikasjonsåret vært en viktig faktor i relevansvurdering og de nyeste bidragene ble prioritert. Rekognoseringsteknikkene er i kontinuerlig endring: verktøyene og kilder forsvinner og dukker opp fort, i tråd med utvikling i teknologi og samfunn, samt endrende trusselbilder. Noe som fungerte for 2-5 år siden kan være uaktuelt eller lite anvendelig i dag. Jeg har bevisst begrenset søk til litteratur utgitt etter 2016. Noen eldre artikler/bøker ble vurdert i enkelte tilfeller og er blitt brukt hovedsakelig for gjennomgang av teori og definisjoner.

I dag brukes både OSINT-metodikk og nettverksskanning-verktøy av myndigheter og etterretningstjenester for å gjennomføre granskninger, etterforskning og i politiarbeid med nett- og organisert kriminalitet (Akhgar et al., 2016; Gibson, 2016; Pastor-Galindo, Nespoli, Gomez Marmol, & Martinez Perez, 2020). Metodikken er også populær blant journalister, forskere og private kommersielle virksomheter. Nåværende forskning har fokus på, men ikke avgrenset til, tre sentrale bruksområder, herunder (a) målingsmeninger og samfunnsanalyse, (b) nett- og organisert kriminalitet, herunder terrorisme og (c) cyber- og informasjonssikkerhet (Pastor-Galindo et al., 2020). For denne oppgaven er kun sistnevnte av relevans. Det finnes relativt lite forskning som omhandler bruk av OSINT i risikovurderinger. De få forskningsprosjekter som tar opp dette tema redegjøres for i delkapittelet 2.2.

2.1. Bruk av OSINT i cybersikkerhet

Tabatabaei og Wells (2016) gjennomgår muligheter som bruk av åpen tilgjengelig informasjon representerer for etterforskning av nettkriminalitet og som verktøy for trusselanalyser og forebygging av cybertrussler. Forfatterne diskuterer pågående utvikling av et integrert OSINT

rammeverk for bekjempelse av nettkriminalitet. Det presenteres ulike tilnærminger, metoder og teknikker for bruk av OSINT i kontekst av datakriminalitet, samt redegjøres for rammeverk for etterforskning av nettkriminalitet (Tabatabaei & Wells, 2016, s. 227). Kapittelet vurderes som et relevant teoretisk bidrag, da det inneholder definisjoner og metodiske tilnærminger.

En gruppe forskere fra Universitet i Murcia har utarbeidet en oversikt over OSINT-verktøy og hvordan disse kan anvendes i cybersikkerhet (Pastor-Galindo et al., 2020). Forfatterne betegner åpen tilgjengelig informasjon som en «Internett-gullgruve» (Pastor-Galindo et al., 2020, s. 10283). De argumenterer for at utvinningen av kunnskap fra offentlige kilder representerer en måte å løse eksisterende problemer på, fra et annet og nyskapende perspektiv. Blant annet påpeker Pastor-Galindo et al. (2020, s. 10288) at OSINT kan brukes for å identifisere en trusselaktørets identitet i etterkant av et angrep. Artikkelen beskriver «the state of art» av OSINT i dag. Den konkluderer med at måten organisasjoner og myndigheter bruker metodikken på i dag er lite effektivt, fordi det mangler tilnærminger for å transformere OSINT inn i en robust og selvstyrt løsning (Pastor-Galindo et al., 2020, s. 10302). Likevel, argumenterer forfatterne for at implementering av systematisk bruk av OSINT-verktøy vil bidra positivt til arbeidet med cybersikkerhet.

Også ukrainske forskere ved Institutt for spesiell kommunikasjon og informasjonssikkerhet ved Det Nasjonale Vitenskapelige Akademiet forsker på bruk av OSINT i kontekst av cybersikkerhet (Lande, 2017; Lande, Kalyan, & Matiishin, 2019; Lande, Subach, & Puchkov, 2020; Lande & Shnurko-Tabakova, 2019). Lande som er en internasjonalt anerkjent ekspert i cybersikkerhet, informasjonssikkerhet og informatikk har utarbeidet flere vitenskapelige artikler som omhandler grunnleggende prinsipper for analyse av informasjonsflyter i globale datanettverk ved hjelp av OSINT (Lande, 2017). Han konkluderer med at OSINT i dag er et av de viktigste verktøyene for cybersikkerhet og at metodikken bør implementeres på alle nivå, ikke bare i militære sammenhenger, men også sivil sektor (Lande & Shnurko-Tabakova, 2019).

2.2. Bruk av OSINT i risiko- og sårbarhetsvurderinger

En studie fra Kroatia gjennomførte rekognosering av de ti største kroatiske bankene med formål om å se hva slags og hvor mye sensitiv informasjon om banker og deres kunder som var offentlig tilgjengelig (Matvej et al., 2020). Resultater er presentert i en matrise som ligner på risikomatriser og som brukes for kartlegging av avvik. Matvej et al. (2020, s. 0187) påpeker at selv bruk av lite avanserte verktøy har vært tilstrekkelig for å gjennomføre grunnleggende

rekognosering og innhente mye nyttig informasjon om finanssektor. Det er tydelig at åpen tilgjengelig informasjon i trusselaktørers hender kan brukes som grunnlag i forberedelse med et cyberangrep. Forfatterne påpeker at en ressurssterk trusselaktør vil kunne innhente mer kritisk informasjon ved hjelp av mer sofistikerte verktøy, metoder og ferdigheter. Artikkelen konkluderer med at datainnsamling med hjelp av OSINT-metodikk kan legges til grunn for risikovurderinger og forslag til forebyggende tiltak (Matvej et al., 2020, s. 0187).

NVE (2019) har gjennomført en casestudie av tre kraftselskaper av ulik størrelse med fokus på bruk av OSINT-metoder for kartlegging av kraftsensitiv informasjon på Internett. Funnene viser at alle strømselskapene er eksponert i en viss grad, hvorav den minste er eksponert i større grad og den største er eksponert i mindre grad (NVE, 2019, s. 4). Rapporten argumenterer for å implementere OSINT-metodikk som element i virksomhetenes revisjonsprosesser, samt supplementere NVEs egen tilsynsmetodikk. Studie inkluderer et forslag om hvordan metodikken bør brukes i revisjonsprosesser. NVE (2019, s. 4) konkluderer med at kartlegging av virksomhetens «digitale fotavtrykk» kan brukes som beslutningsgrunnlag i vurderinger om hvorvidt noe av den åpne tilgjengelige informasjon er sensitiv og bør skjermes.

Hayes og Cappa (2018) fra Indiana Universitet har gjennomført en studie hvor de belyser viktigheten av OSINT-verktøy i risikovurderinger for å forhindre dataangrep. Forfatterne utførte en sårbarhetsvurdering for et amerikansk elnett-selskap. Det ble gjennomført kartlegging av selskapets teknisk infrastruktur og profilering av nøkkel-IT-personell ved hjelp av ulike rekognoseringsverktøy. De demonstrerte blant annet hvordan informasjon om en ansatt innsamlet gjennom OSINT kan brukes i risikovurderinger ved hjelp av tildeling av risiko-poeng (Hayes & Cappa, 2018, s. 694). Forfatterne konkluderer med at OSINT bør brukes aktivt for å identifisere sårbarheter og formulere robust politikk for å forhindre dataangrep (Hayes & Cappa, 2018, s. 696).

2.3. Motivasjon for denne oppgaven

Valg av oppgavens problemstillinger, metode og utforming er motivert av at det mangler empirisk forskning som gir leseren detaljert beskrivelse og forklaring på hvordan kartlegging skjer i praksis. Formålet med artiklene til Hayes og Cappa (2018) og Matvej et al. (2020) var å vise hvordan OSINT kan brukes for å kartlegge organisasjoner og hvordan OSINT kan benyttes som basis i risikostyring. De har ikke inkludert grundig beskrivelse av selve prosessen

og verktøy. NVEs (2019) rapport er unntatt offentlighet og kan dermed ikke brukes som grunnlag for læring, dessverre. NSM (2020a, s. 22-23) presenterer et typisk hendelsesforløp og teknikker som trusselaktører bruker for å angripe norske virksomheter, men denne modellen er også ganske generell og går ikke i detaljert beskrivelse av teknikker og verktøy.

Det er derfor har jeg valgt å gå mer detaljert inn på hvordan rekognosering faktisk skjer i praksis. Denne undersøkelsen er bare et eksempel på noen utvalgte teknikker og verktøy. OSINT verden er i kontinuerlig vekst og mitt ønske er å introdusere leserne til det enorme potensialet metodikken byr for forebyggende sikkerhetsarbeidet.

3. Teoretisk rammeverk

Formålet med dette kapittelet er å danne teoretisk grunnlag for å besvare oppgavens problemstilling og forskningsspørsmål ved å diskutere hvordan cyberangrep utvikler seg, og hvordan man styrer digitale risikoer. Teoretisk rammeverk berører hovedkomponentene i cybersikkerhet, informasjonssikkerhet og risikovurdering.

Teorier som beskriver forløp av et cyberangrep, er brukt for å utarbeide metodisk fremgangsmåte og besvare oppgavens forskningsspørsmål:

1. *Hvordan fungerer digital rekognosering av organisasjoner i praksis?*
2. *Hvilken informasjon om de utvalgte virksomhetene kan man finne ved hjelp av rekognoseringsteknikker og OSINT?*
3. *Hvorfor er denne type informasjon av interesse for en trusselaktør?*

Svar på forskningsspørsmålene danner grunnlaget for forståelsen for *hvordan kartlegger trusselaktører organisasjoner*, som er første del av oppgavens problemstilling.

Teoriene som omhandler informasjonssikkerhet, risikostyring av informasjonssystemer og situasjonsbevissthet danner grunnlag for diskusjon av *hvordan kan selv-rekognosering brukes som redskap i organisasjoners forebyggende informasjonssikkerhetsarbeid*. Kapittelet avsluttes med en kort oppsummering av teorienes relevans.

3.1. Cyberangrep: teoretiske modeller

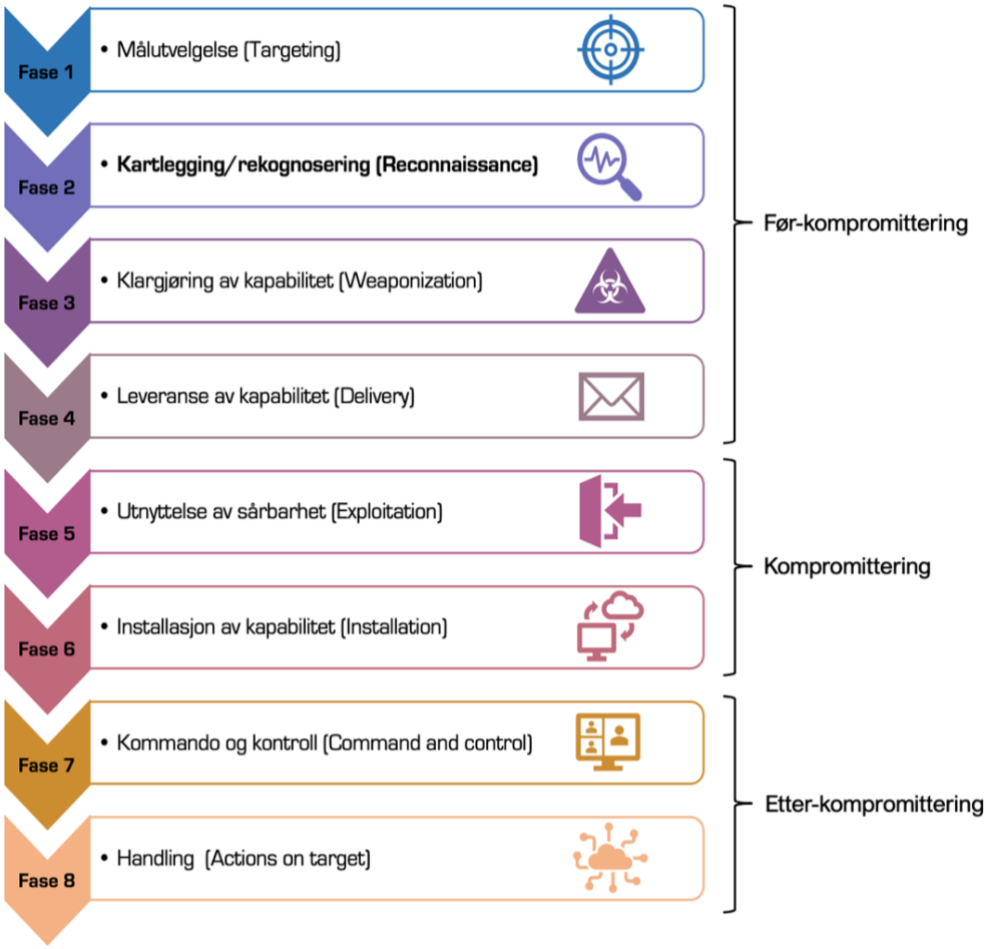
For å forstå hvordan man kan beskytte organisasjoner mot et cyberangrep er det nødvendig med en grunnleggende forståelse for hvordan trusselaktører opererer. Jeg presenterer to teoretiske modeller som viser et typisk forløp av et cyberangrep. Disse er valgt fordi de brukes aktivt i risikostyring av cybersikkerhet.

3.1.1. Cyber Intrusion Kill Chain

Cyber Intrusion Kill Chain (CKC) er en modell som beskriver dataangrepets utvikling: de fasene en trusselaktør går gjennom for å gjennomføre dataangrep. Modellen er utviklet av Hutchins et al. (2011) og er brukt for å analysere trusselaktørers handlingsmønster og angrepsmetoder i kyberrom. CKC modellerer cyberangrep som hendelsessekvenser (Bergsjø et al., 2020, s. 167–174; Katos et al., 2019, s. 8). Ved å illustrere hendelsesforløpet bidrar

modellen til å danne forståelse rundt trusselaktørers handlemåte og mekanismer bak dataangrep. Hutchins et al. (2011) sin modell starter med rekognoseringsfasen som innebærer at målutgivelse inngår implisitt i rekognosering. Bergsjø et al. (2020) skiller mellom de to fasene. I oppgaven tar jeg utgangspunkt i Bergsjø et al. (2020) sin modell, da målutvelgelse diskuteres i kapittel 6.2. Figur 2 er grafisk fremstilling av CKC.

Figur 2: Cyber Intrusion Kill Chain (basert på Hutchins et al., 2011, s. 4-5; Dargahi, Dehghantanha, & Taylor, 2019, s. 4–5)



Den første fasen av angrepet, *målutvelgelse (targeting),* reflekterer trusselaktørens interesser, motivasjoner og hvilke verdier det potensielle målet besitter (Bergsjø et al., 2020). Angrep kan være målrettet eller ikke-målrettet (opportunistisk). Angrepet kan også resultere i at tredje parter eller såkalt «sekundært mål» er blitt rammet. Dette skjer fordi trusselaktør mister kontroll over sitt digitale våpen, eksempelvis når datavirus begynner å «leve sitt eget liv» ved å bli spredt videre uten at trusselaktør har noen påvirkningsmuligheter (Bergsjø et al., 2020).

Den andre fasen er oppgavens hovedtema, *rekognosering (reconnaissance)* av offeret/målet (Bergsjø et al., 2020, s. 168; Hutchins et al., 2011, s. 4–5; Johansen, 2017, s. 274). Ved å

observere den normale driften av en virksomhet samler angriperen data om menneskelige, organisatoriske og tekniske faktorer og komponenter, herunder virksomhetenes digitale og fysiske systemer, programvarer, nettverkskonfigurasjoner, kommunikasjonsmønstre, organisasjonsstruktur osv. (Bergsjø et al., 2020). Rekognoseringen er dermed kartlegging av styrker og sårbarheter som brukes for utarbeidelse av angrepsstrategi.

Formålet med den tredje fasen, *klargjøring av kapabilitet (weaponization)*, er å utvikle det digitale våpen, såkalt utnyttelseskode, som er tilpasset den enkelte organisasjonens egenskaper (Bergsjø et al., 2020, s. 169-170; Hutchins et al., 2011, s. 4). For å utnytte tekniske sårbarheter vil trusselaktør, avhengig av vedkommendes ferdigheter, designe eller kjøpe en utnyttelseskode, som «pakkes» eksempelvis i et tilsynelatende legitimt dokument eller nettsider, for å ikke vekke mistanke (Bergsjø et al., s. 170).

Neste fase, *leveranse av kapabilitet (delivery)*, vil bestå av å finne måter for å levere et infisert dokument til offeret (Bergsjø et al., 2020, s. 170; Hutchins et al., 2011, s. 4). I denne fasen utnyttes både menneskelige, tekniske og organisatoriske sårbarheter. Nettfisking e-post har lenge vært og er fremdeles den vanligste måten å levere en utnyttelseskode (ENISA, 2016; Verizon, 2020). Andre metoder er diskutert i kapittel 5.

Fase fem, *utnyttelse av sårbarhet (exploitation)*, starter med at brukerens datamaskin kompromitteres som resultat av at mottakeren har åpnet vedlegg, installert programdatavare eller trykket på lenken (Bergsjø et al., 2020, s. 172; Hutchins et al., 2011, s. 4). Nå har trusselaktør fått kontroll over ondsinnet kode i organisasjonens digitale system. Et av de viktigste elementene i denne fasen er at trusselaktøren sikrer seg innloggingsdetaljer til offerets datamaskin og operativsystem (ENISA, 2016).

Den sjette fasen, *installasjon av kapabilitet (installation)* innebærer etablering av persistens, som betyr at trusselaktør kan kjøre kode selv etter at operativsystemet er startet på nytt (Bergsjø et al., 2020, s. 173; Hutchins et al., 2011, s. 5). Dersom man lykkes med etablering av persistens trenger man ikke å gjenta fase fem, utnyttelse av sårbarhet, på nytt, skriver Bergsjø et al. (2020).

Den syvende fasen, *kommando og kontroll (command and control)*, dreier seg om at trusselaktør etablerer kontroll over offerets system og utfører handlinger ved å kommunisere med installert skadevare, ofte uten at offeret vet om det (Bergsjø et al., 2020, s. 174).

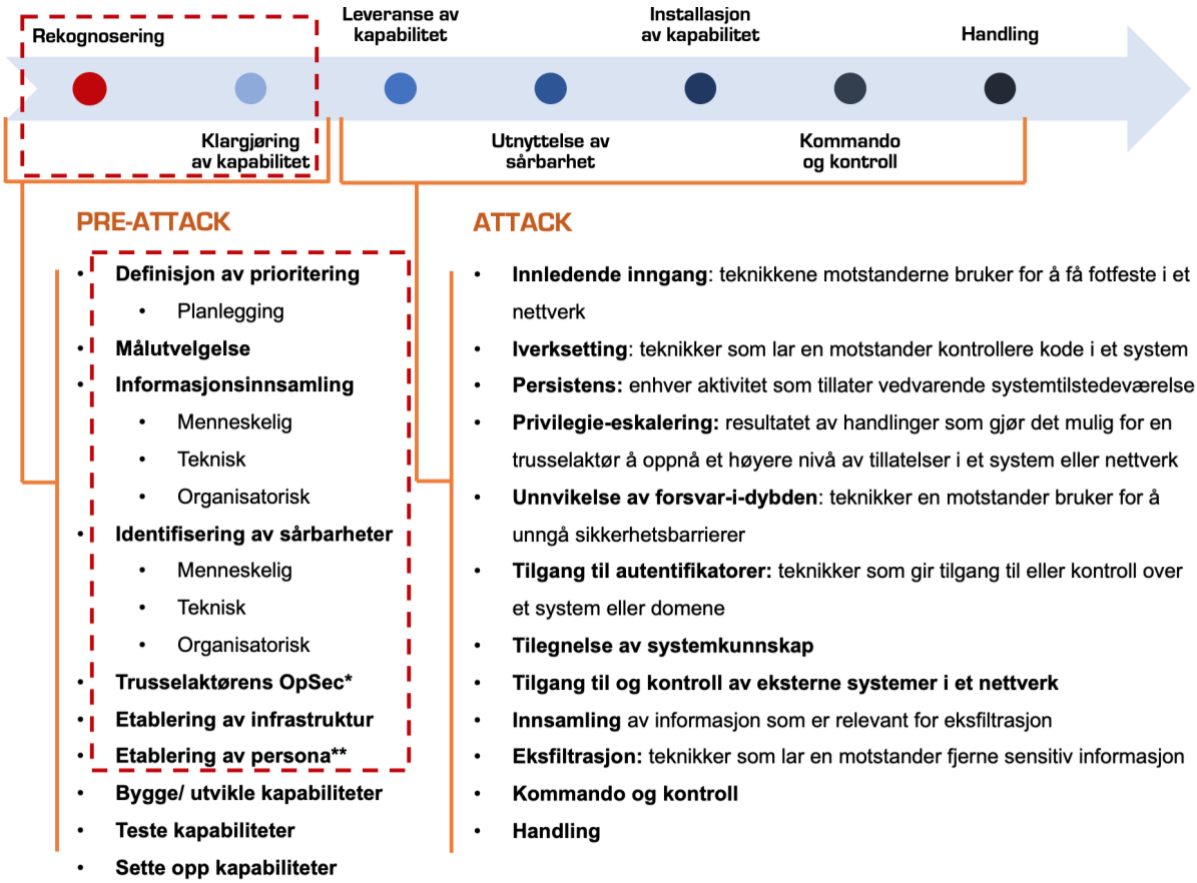
Siste fase, *handling (action on target)*, er angrepets kulminasjon (Bergsjø et al., 2020, s. 174; Hutchins et al., 2011, s. 5). Trusselaktør utfører det opprinnelige målet sitt, for eksempel tjenestenekt, løsepengevirus, spionasje, eksfiltrasjon (skjult overføring av verdier), eksponering, økonomisk kriminalitet osv. (Verizon, 2020). Trusselaktør kan samle inn, kryptere og hente ut informasjon fra offerets nettverk (tap av konfidensialitet); brudd av informasjons integritet eller tilgjengelighet er også potensielle mål (Bergsjø et al., 2020). Alternativt bruker inntrengerne tilgang til offerets systemer som et mellompunkt, for å få tilgang til og kompromittere flere systemer og bevege seg lateralt inne i nettverket (Hutchins et al., 2011).

3.1.2. MITRE ATT&CK

MITRE «ATT&CK»-rammeverk beskriver trusselaktørers handlingsmåter og mulige angrepsvektorer og er implementert i risikovurderinger for cybersikkerhet i både statlige og private virksomheter i flere land (MITRE, 2021a). Modellen brukes til å bedre kunnskapen til nettverksforsvarere og til å prioritere barrierer ved å spesifisere taktikker, teknikker og prosedyrer som angripere bruker for å få tilgang til- og utføre ondsinnede handlinger i et nettverk (MITRE, 2021).

Som Figur 3 illustrerer, utfyller ATT&CK-modellen Hutchins CKC-modell, men viser mer detaljert relasjon mellom ulike fasene i dataangrep. Mens CKC kjennetegnes ved en klart lineær sekvens bestående av et visst antall faser, presenteres ATT&CK-rammeverket i form av en matrise hvor innbruddsteknikker ikke nødvendigvis følger en bestemt rekkefølge.

Figur 3: MITRE ATT&CK-rammeverk - relasjon mellom taktikk og rekognoseringsfase



Kommentar til Figur 3:

Den røde linjen markerer oppgavens avgrensning.

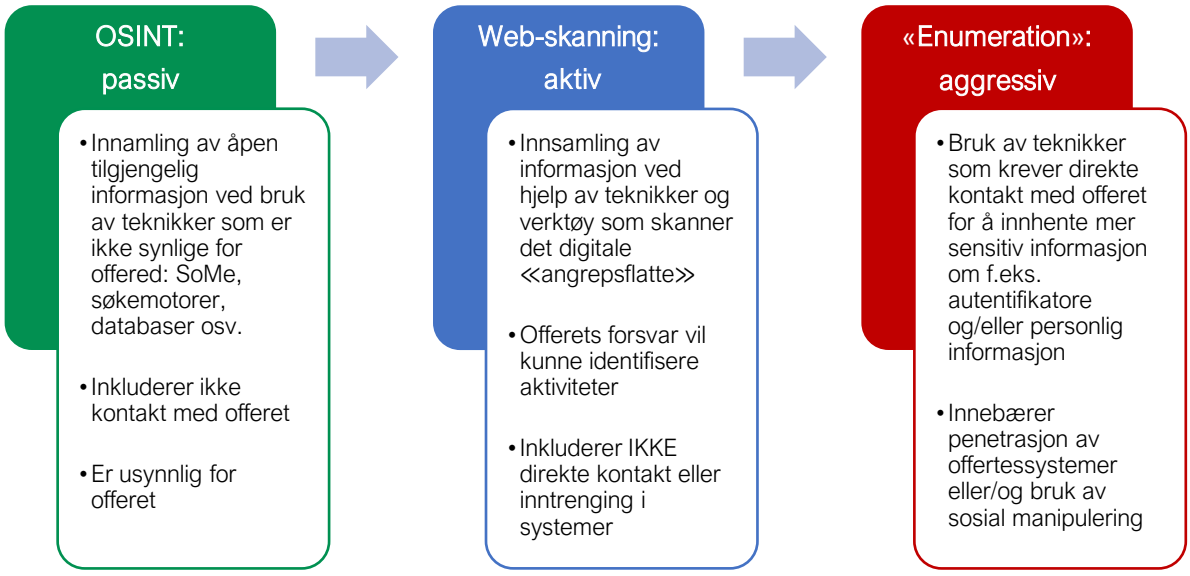
** OpSec (Operation Security) er en prosess som innebærer ulike tiltak for å sikre sin anonymitet og sikkerhet på Internett.*

*** Trusselaktør oppretter kontoer (sokkedukker) som kan brukes til å bygge en tilsynelatende legitimt persona med tilknytning til offeret.*

3.1.3. Sentrale elementer i en rekognoseringsprosess

Begge de teoretiske modellene starter med rekognoseringsfasen. Rekognosering er en systematisk prosess som innebærer søk, innsamling, identifisering og registrering av informasjon om et mål med hensikt om å kartlegge målets styrker og svakheter (Chauhan, 2015; Kerner, 2015; MITRE, 2021c; Sanghvi & Dahiya, 2013). Da jeg ikke har funnet en eksisterende visuell fremstilling av selve rekognosering, har jeg utarbeidet en teoretisk modell som er basert på ulike rammeverk og forskningsartikler (se Figur 4). Jeg kommer tilbake til denne teoretiske modellen i kapittel 5 hvor jeg beskriver hvordan prosessen fungerer i praksis.

Figur 4: Rekognoseringsprosess (basert på Chauhan, 2015; MITRE, 2021c; RSA, 2015; Sanghvi & Dahiya, 2013)



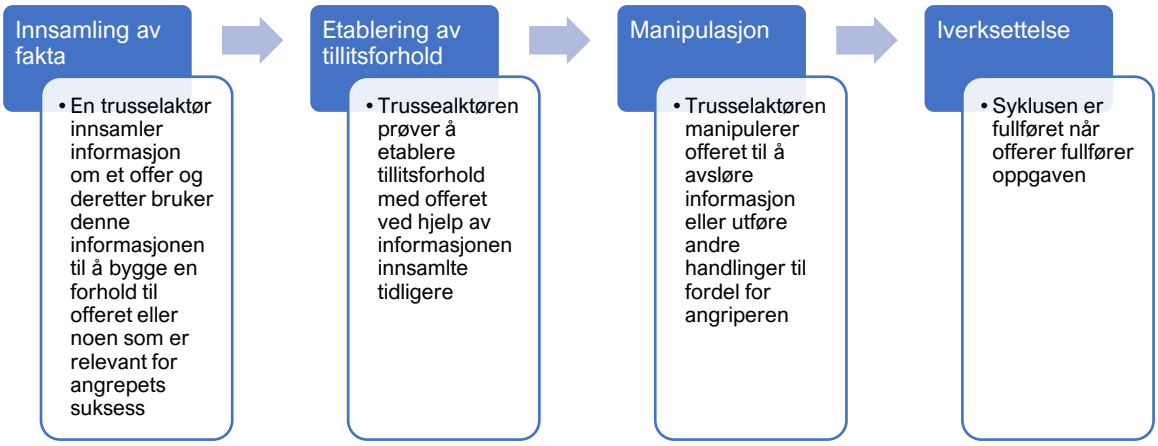
OSINT og web-skanning konsepter er definert i kapittel 1 og diskutert mer inngående senere i oppgaven. Modellens siste fase, «sosial manipulering», også står sentralt i denne oppgaven og derfor må forklares mer inngående.

Sosial manipulering

I cybersikkerhet betegner sosial manipulering (*eng.* social engineering) bruk av ulike teknikker med formål om å manipulere folk til å gi fra seg sensitiv informasjon. Sosial manipulering defineres som «[t]he use of deception in order to induce a person to divulge private information or esp. unwittingly provide unauthorized access to a computer system or network» (Oxford English Dictionary, referert i Hatfield, 2018, s. 102).

Strategien utnytter mellommenneskelig tillitsforhold: man stoler naturlig på en som ber om hjelp og er villig til å hjelpe. Hackere derimot søker å dra nytte av slik godhet (Salahdine & Kaabouch, 2019). Ved å bruke allerede eksisterende kunnskap om offeret kan man få tilgang til mer sensitive opplysninger som er ikke åpen tilgjengelige, eksempelvis kontoopplysninger, sikkerhetsinnstillinger mm. Dette vil innebære utnyttelsen av sårbarheter som man oppdaget under passiv og aktiv rekognosering. Figur 5 illustrerer utvikling av et sosial-manipulerings-angrep.

Figur 5: Sosial manipuleringsangrep - utvikling (Wilcox & Bhattacharya, 2020, 2. 2; Wilcox, Bhattacharya, & Islam, 2014)



Ifølge forskere er sosial manipulering det vanligste kilde til aller flest datainnbrudd (Junger, Montoya, & Overink, 2017; Krombholz, Hobel, Huber, & Weippl, 2015; Salahdine & Kaabouch, 2019; Wilcox & Bhattacharya, 2020; Wilcox et al., 2014). Forskningslitteratur viser at samfunnets stadig økende avhengighet av pålitelige digitale systemer gjør sosial manipulering til en av de største utfordringene for samfunnssikkerhet og særlig informasjonssikkerhet i årene fremover.

3.2. Informasjonssikkerhet

3.2.1. Begrepsavklaring

Oppgavens problemstilling inkluderer begrepet «*forebyggende informasjonssikkerhets-arbeid*». For å forstå forebyggende informasjonssikkerhetsarbeid er det nødvendig med avklaring av noen grunnleggende begrep; «informasjonssikkerhet», «cybersikkerhet», «informasjonssystemer», «digital infrastruktur», «skjermingsverdig» og «forebygging».

Begrepet «*informasjonssikkerhet*» defineres som «beskyttelse av informasjonens konfidensialitet, integritet og tilgjengelighet», uavhengig av om den er digital eller analog. Dette er hovedprinsippet for sikkerhet i *informasjonssystemer* (Departementene, 2012, s. 28; Bergsjø et al., 2020, s. 21).

Informasjonssystemer er systemer som anvendes for å utføre oppgaver og/eller funksjoner som eksempelvis innsamling av informasjon fra omgivelsene, lagring av informasjon over tid,

overføring av informasjon fra et sted til et annet, presentasjon av informasjon osv. (Stair & Reynolds, 2018, s. 6). Informasjonssystemer består av både menneskelige, teknologiske og organisatoriske elementer, til forskjell fra et datasystem som er rent teknisk (NSM, 2020b, s. 3; Stair & Reynolds, 2018, s. 8). Dette forankrer arbeidet med informasjonssystemer i MTO-perspektivet. I relasjon til virksomheter som driver med forsknings- og utvikling omfatter begrepet alt fra kommunikasjons-, saksbehandlings-, kontorstøtte-, kontroll- og styringssystemer.

Ifølge Sikkerhetsloven (2018) skal virksomheter sørge for et forsvarlig sikkerhetsnivå for *skjermingsverdige informasjonssystemer* (§2-2). Informasjon er skjermingsverdig «dersom det kan skade nasjonale sikkerhetsinteresser at informasjonen blir kjent for uvedkommende, går tapt, blir endret eller blir utilgjengelig» (Sikkerhetsloven, 2018, § 5-1). Skjermingsverdig informasjon kan være sikkerhetsgradert eller ugradert. Den siste type informasjon er av stor relevans i oppgaven, da den vanligvis er åpent tilgjengelig og er av interesse for trusselaktører.

Flere informasjonssystemer utgjør en *digital infrastruktur* som er eiet, vedlikeholdt og forvaltet av forskjellige organisasjoner (DSB, 2019, s. 10). Hver av disse utfører viktige funksjoner eller leverer digitale tjenester til andre deler i infrastrukturen. Derav vil resultat avhenge av hvorvidt de forskjellige delsystemene hver for seg utfører sine funksjoner eller leverer digitale tjenester til hverandre (DSB, 2019, s. 10). Å etablere en robust og felles infrastruktur som er tilpasset samhandling og kobling av data, anses derav som nødvendig (NSM, 2017, s. 40).

Informasjonssikkerhet brukes ofte synonymt eller i kombinasjon med *cybersikkerhet. Cybersikkerhet* er et paraplybegrep for sikkerhet i cyberspace, med tilhørende sosio-tekniske digitale systemer, kommunikasjonsinfrastruktur, samt informasjon som lagres og overføres (NOU 2015: 13, s. 34). Forenklet handler cybersikkerhet om «[...] å beskytte «alt» som er sårbart fordi det er koblet til, eller på annen måte er avhengig av informasjon- og kommunikasjonsteknologi» (NOU 2015: 13, s. 34).

I oppgaven brukes begrepene *cybersikkerhet, digital sikkerhet og IKT-sikkerhet* som synonymer, mens *informasjonssikkerhet* brukes som eget begrep. Oppsummert kan man si at informasjonssikkerhet er et bredere konsept som inkluderer generell beskyttelse av informasjon, mens cybersikkerhet omhandler å beskytte digitale systemer mot cyberangrep.

Ifølge Njå et al. (2020, s. 266) omfatter *forebyggende sikkerhetsarbeid* alle tekniske, operasjonelle og organisatoriske tiltak som hindrer at en uønsket hendelse oppstår. Eller som

hindrer, motvirker eller reduserer konsekvenser om en uønsket hendelse oppstår. I forbindelse med informasjonssikkerhet innebærer begrepet planlegging, tilrettelegging, gjennomføring og kontroll av forebyggende tiltak mot aktiviteter som kan true informasjonssystemer og konfidensialitet, integritet og tilgjengelighet av informasjon (Departementene, 2012; NSM, 2020b; Sikkerhetsloven, 2018).

Relatert til organisasjoner som jobber med forskning og utvikling vil forebyggende informasjonssikkerhet bety identifisering av skjermingsverdige informasjonssystemer og informasjon, samt alle tiltak som er rettet mot å motvirke og forhindre at uvedkommende får tilgang til informasjon og kunnskap som produseres i organisasjoner. Det kan være forskningsrapporter, risikovurderinger, utredninger og analyser knyttet til kritisk infrastruktur, intern og ekstern korrespondanse, personlige opplysninger om nøkkelpersonell og samarbeidspartnere mm.

3.2.2. Informasjons- og cybersikkerhet: «safety» eller «security»?

Informasjons- og cybersikkerhet er en relativt ny fagdisiplin og mangler derav et tilstrekkelig begrepsapparat i det norske språket. Det norske faglige miljøet er imidlertid preget av semantiske uenigheter ved tolkning av «sikkerhet og «security», da begge begrepene oversettes som «sikkerhet». I det siste er begrepet «sikring» tatt i bruk (NOU 2006: 6, s. 38). Sikkerhet omhandler ikke-tilsiktede hendelser, eksempelvis ulykker, kontinuerlig eksponering, menneskelige feil og naturhendelser. På den annen side er sikring mottiltak til tilsiktede handlinger fra rasjonelle aktører (SRA, 2020).

Jore (2019) argumenterer for at konseptene ikke nødvendigvis er så adskilt. Hennes hovedargument er at intensjonalitet som hovedfaktor, ikke nødvendigvis er helt fraværende i sikkerhetskontekst. Faglig litteratur har i flere tiår erkjent at ulykker verken er vilkårlige eller tilfeldige, men snarere et resultat av manglende fokus på sikkerhetsplanlegging (Dekker, 2014, 2016; Perrow, 1999; Reason, 1997, 2016; Turner, 1976; Turner & Pidgeon, 1997).

I oppgaven brukes «sikkerhet» for både sikkerhet og security. Fordi jeg tar utgangspunkt i at det (a) eksisterer en hypotetisk trusselaktør som har kapasitet og intensjon om å skade et system eller organisasjon og (b) manglende situasjonsbevissthet har betydning for i hvilken grad organisasjoner er eksponert for trusselaktører. Innen cybersikkerhet er skillet mellom «intensjon» og «feil» enda mer uklart, da trusselaktører utnytter menneskelige egenskaper og

tillit. Det vil si at både intensjon og iboende sårbarhet er til stede. En kan derfor argumentere for at inkluderingen av begge perspektivene vil være viktig for å beskytte informasjonssystemer i organisasjoner.

Sikkerhet versus sikring debatten har betydning for utforming av lov- og reguleringsrammeverk, som i sin tur har implikasjoner for hvordan organisasjoner jobber med forebyggende informasjonssikkerhet. Det er derfor nødvendig å se på rettslig regulering av informasjonssikkerhet og på risiko-begrepet i relasjon til sikring av informasjonssystemer.

3.2.3. Rettslig regulering av informasjonssikkerhet

Formålet med dette kapittelet er å redegjøre for ansvarsfordeling og krav som rettslig regulering stiller til forvaltere av informasjonssystemer.

Den nye sikkerhetsloven (2018), den nye personopplysningsloven (2019) og virksomhets-sikkerhetsforskriften (2019) som regulerer informasjonssikkerhet er sektorovergripende og har noen felles krav. I dag har regelverkene mer fokus på sikring av tre sentrale pilarer i informasjonssikkerhet: konfidensialitet, integritet og tilgjengelighet (Bergsjø et al., 2020).

Sikkerhetsloven som trådte i kraft 1. januar 2019 skal tilrettelegge for *forebygging, avdekking og motvirkning av sikkerhetstruende virksomhet* (§1-1) og skal beskytte de nasjonale sikkerhetsinteressene, herunder «landets suverenitet, territorielle integritet og demokratiske styreform og overordnede sikkerhetspolitiske interesser [...]» (Sikkerhetsloven, 2018, §1-5). Loven gjelder for både statlige, fylkeskommunale og kommunale organer (§1-2). Ansvar for sikkerheten pålegges hver enkelt virksomhet. Private organisasjoner kan underlegges sikkerhetsloven når de (a) behandler sikkerhetsgradert informasjon, (b) råder over informasjon, informasjonssystemer, objekter eller infrastruktur som har avgjørende betydning for grunnleggende nasjonale funksjoner eller (c) driver aktivitet som har avgjørende betydning for grunnleggende nasjonale funksjoner (Sikkerhetsloven §1-3). Eksempelvis er Organisasjon A underlagt sikkerhetsloven, mens Organisasjon B ikke nødvendigvis er det.

Ifølge sikkerhetsloven (2018) skal virksomheter etablere sikkerhetsstyring for forebyggende sikkerhet i samsvar med krav i loven. Virksomhetene skal blant annet;

- være pådrivere av forebyggende sikkerhetsarbeidet (§ 4-1),

- regelmessig gjennomføre vurdering av risiko som skal danne grunnlag for iverksetting av forebyggende sikkerhetstiltak (§ 4-2),
- gjennomføre de forebyggende sikkerhetstiltakene som må til for å gi et forsvarlig sikkerhetsnivå og redusere risikoen knyttet til sikkerhetstruende virksomhet (§ 4-3),
- kontinuerlig overvåke sine skjermingsverdige informasjonssystemer for å forebygge, avdekke og motvirke hendelser som kan skade nasjonale sikkerhetsinteresser (§ 6-4),
- iverksette nødvendige tiltak for å opprettholde et forsvarlig sikkerhetsnivå (§ 7-3).

I loven påpekes det at kostnadene ved et sikkerhetstiltak skal stå i et rimelig forhold til det som kan oppnås ved tiltaket (§ 4-3).

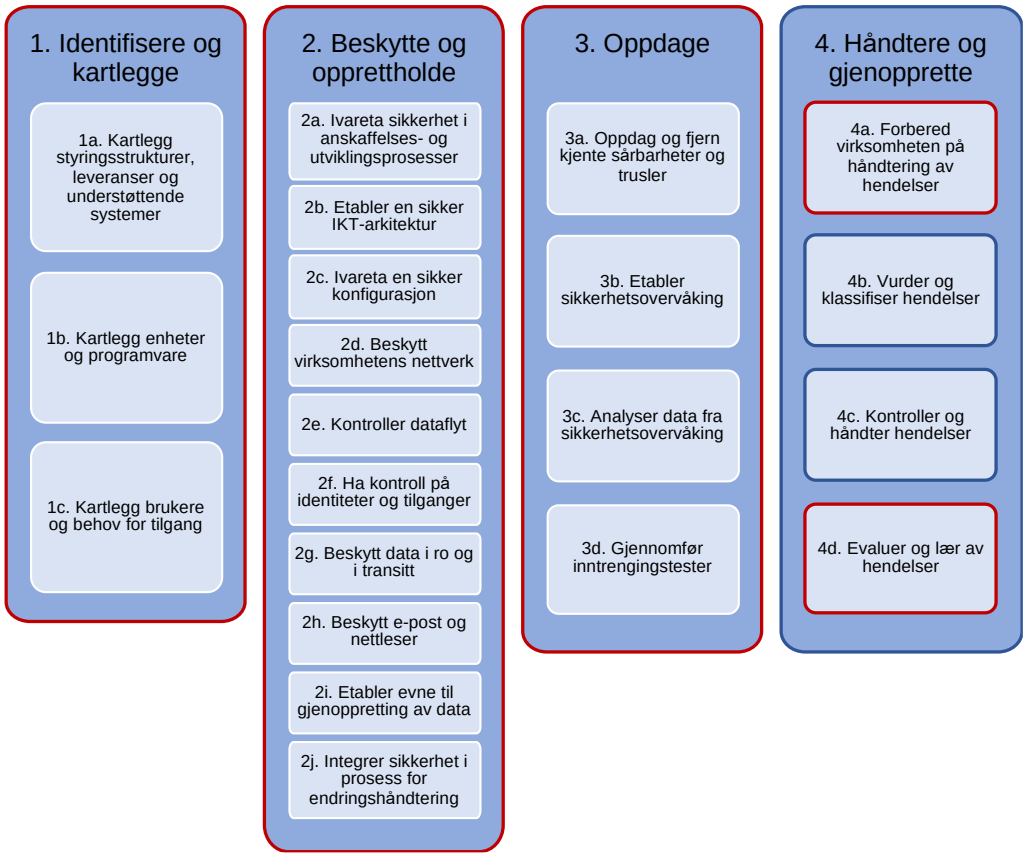
Virksomhetssikkerhetsforskriften (2019) og *Personopplysningsloven* (2019) komplementerer Sikkerhetsloven. Den første stiller krav til at virksomheter etablerer dokumentert sikkerhetsstyring (§3). Den andre er mer avgrenset og regulerer behandling av personopplysninger. Da personopplysninger behandles i informasjonssystemer er disse en viktig del av informasjonssikkerhetsarbeid.

3.2.4. Grunnprinsipper for informasjonssikkerhet

For å operasjonalisere lovverkene har NSM utarbeidet fire grunnprinsipper for informasjonssikkerhet, som skal beskytte organisasjoners informasjonssystemer mot uautorisert tilgang eller/og skade (NSM, 2020d). De fleste tiltakene er av forebyggende karakter. Den siste fasen, håndtering og gjenoppretting, innebærer tre tiltak som skjer etter at hendelser oppstår. Evaluering og læring spiller og en forebyggende rolle, selv om de kommer i etterkant av uønsket hendelse. Figur 6 viser hvilke aktiviteter som inngår i de fire prinsippene. Grunnprinsippene beskriver hva en virksomhet bør gjøre for å sikre et informasjonssystem og hvorfor det skal gjøres. Det de ikke beskriver er hvordan organisasjoner skal gjøre det.

NSM (2020d) påpeker at virksomhetene selv kan bestemme hvilke tiltak som er relevante og ikke. Det kan tenkes at for store virksomheter som Organisasjon A, vil de fleste tiltakene være relevante. Mens mindre virksomheter som Organisasjon B, må prioritere tiltakene avhengig av sine funksjoner, oppgaver og infrastruktur. Dette diskuteres mer inngående i kapittel 6.

Figur 6: NSMs prinsipper for IKT-sikkerhet (NSM, 2020d)



Kommentar til Figur 6: Elementer som tilhører forebyggende fase er markert med rød. Blå farge markerer elementer som tilhører håndtering av hendelser

Gjennomgang av regelverket og grunnleggende prinsipper for informasjonssikkerhet viser at risikostyring, som er et av hovedelementer i forebyggende arbeid, står sentralt. Både sikkerhetsloven og virksomhetssikkerhetsforskriften stiller krav til risikostyring/vurdering. Risikostyring innebærer at organisasjonen skal gjennomføre verdivurdering, sårbarhets- og trusselanalyser. Regelverk er funksjonsbasert, det vil si det ikke stilles konkrete detaljkrav til hvilke rammeverk for risikostyring skal virksomheter bruke. I det neste delkapittelet ser jeg nærmere på cyberrisiko og risikostyring av informasjonssystemer.

3.3. Risiko i informasjonssystemer

3.3.1. Risiko og risikostyring: begrepsavklaring

Forskere og eksperter innen cybersikkerhetsfelt beskriver *cyberrisiko* som dynamisk, grenseoverskridende, kompleks, preget av usikkerhet, økende, kan forårsake dominoeffekt,

ikke observerbar eller håndfast, skjult, anonym og ubegrenset, vanskelig å vurdere omfanget av, flerdimensjonell mm. (Alhayani, Abbas, Khutar, & Mohammed, 2021, s. 1; Florin & Nursimulu, 2018, s. 12; Hubbard & Seiersen, 2016, s. 10, 12, 29; Kshetri, 2016, s. 2; Lervik, 2018, s. 13, 16; Mirzaei, de Fuentes, & Lorena González Manzano, 2018, s. 234; Skopik, 2017, s. 45; Skotnes, 2020, s. 177; Ulsch, 2014, s. 8; Aakre, 2020, s. 37).

Beskrivelsen illustrerer hvor kompleks cyberrisiko er. Derfor er det delte meninger om tradisjonelle kvantitative tilnærminger til risiko er anvendelig i cybersikkerhet. Flere forskere argumenterer for at et statisk og ensidig kvantitativt syn på risiko er lite anvendelig i samfunnsvitenskap, særlig innen informasjons- og cybersikkerhet (se f.eks. Bergsjø et al., 2020, s. 188; Edgar & Manz, 2017, s. 51; Mirzaei et al., 2018, s. 234). Dette begrunner de med at kvantitative risikoanalyser er forhåndsplanlagt og uegnet for å vurdere dynamiske risikoer. Enkelte argumenterer imidlertid for at semi-kvantitative tilnærminger kan brukes i vurderinger av cyberrisiko (Derbyshire, Green, & Hutchison, 2021; Hubbard & Seiersen, 2016; Mirzaei et al., 2018).

I denne oppgaven forstås risiko som «potensialet for at en gitt trussel vil utnytte sårbarhetene til et sett av verdier og derigjennom forårsake skade» (ISO/IEC 27005:2018, s. 33). Definisjonen forankrer risiko i menneskelig verdi. Dette er aktuelt i cybersikkerhet, hvor mennesker og teknologi eksisterer i synergi og dermed utgjør et helhetlig sosio-teknisk system. Dermed tar jeg utgangspunkt i en systemorientert perspektiv på risiko som innebærer at alle systemkomponenter, aktører og aktiviteter inngår i et større nettverk av samhandlende systemer som består av mange delsystemer (Bertalanffy, 2003; Lussier, 2012, s. 42; Smith & Brooks, 2013, s. 25–26). *Systemisk risiko* er et konsept som i stor grad overlapper begrepet «risiko i digitale verdikjeder» (DSB, 2019; NOU 2015: 13,). Begrepet betegner risiko knyttet til tap av konfidensialitet, integritet, og/eller tilgjengelighet av informasjon eller informasjonssystemer, som medfører *konsekvenser for* egen organisasjon, *andre organisasjoner, enkeltpersoner og/eller samfunnet* (DSB, 2019; NOU 2015: 13).

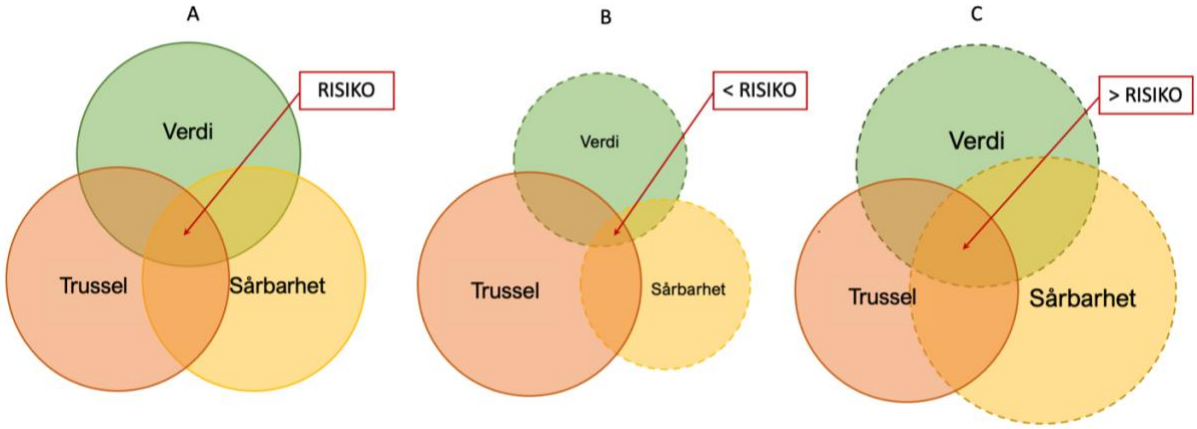
Videre knyttes risikobegrepet til trefaktormodellen (NS 5832:2014, s. 5).

3.3.2. Trefaktormodellen for risikoanalyse

Ifølge modellen kan risiko ses som en kombinasjon av trussel, sårbarhet og verdi, hvor trusselbildet er dynamisk og skiftende, hvor nye sårbarheter med kjente og ukjente

konsekvenser kontinuerlig dukker opp. Definisjonen skiller seg fra den tradisjonelle forståelsen av risiko ved at sannsynlighets-konseptet og dermed usikkerhet ikke eksplisitt er inkludert (Busmundrud, Endregard, Kiran, & Maal, 2015; Jore, 2019b; NS 5832:2014). Figur 7a illustrerer hvordan risiko forstås i henhold til trefaktormodellen. Figurer 7b og 7c viser at redusering av sårbarhet og/eller verdi vil redusere risiko og motsatt.

Figur 7: Risiko som kombinasjon av trussel, sårbarhet og verdi (basert på NS 5832:14; FFI, 2015)



Som nevnt tidligere skal virksomheter regelmessig gjennomføre vurdering av risiko som skal danne grunnlag for iverksetting av forebyggende sikkerhetstiltak (Sikkerhetsloven, 2018). Trefaktormodellen er kjernen i både norske og internasjonale standarder for risikostyring av informasjonssikkerhet (ISO 2700X-serie og NS 583X-serie).

Risikovurdering er en overordnet, systematisk og gjentakende prosess som i henhold til trefaktormodellen inkluderer vurdering av trusler, verdier og sårbarheter. Resultater av verdi- og trusselvurdering skal legges til grunn for sårbarhetsvurdering. Risikovurderingen skal danne grunnlag for iverksetting av forebyggende sikkerhetstiltak. Begrepene «verdi», «trussel» og «sårbarhet» står sentralt i denne studien, da hovedmålet er å demonstrere hvordan selv-rekognosering og OSINT kan være redskap i å identifisere verdier og sårbarheter som må beskyttes mot en trusselaktør.

Verdi

Ved en risikovurdering er det nødvendig med en grundig beskrivelse av systemet som skal beskyttes. Kartlegging og vurdering av verdier er en viktig del av denne prosessen, som bidrar til å identifisere konsekvensene av uønskede tilsiktede hendelser.

Verdi defineres 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» (NS 5830:2012, s. 4). Organisasjonene A og Bs verdier kan eksempelvis være «informasjon», «økonomi» og «omdømme» (NS 5832:2014, s. 6). Det finnes ikke noe regelsett som spesifiserer nøyaktig hvordan disse verdiene skal identifiseres og defineres. Vurderingen handler om hvor kritisk tapet av en slik verdi vil være (Jore, 2017). I denne studien er informasjon den dedikerte verdien som organisasjonene vil beskytte, og som trusselaktør vil få tilgang til.

Verdivurdering i cybersikkerhets kontekst er ikke en enkel oppgave. Problemet er at vi ofte ikke ser verdien i informasjonen vi besitter, produserer eller formidler. Dette er knyttet til at vi mangler forståelse for kompleksiteten i risikobildet, eksisterende sammenkoplinger og hvorfor en tilsynelatende ubetydelig informasjon kan representere en verdi for en trusselaktør.

Trussel

I denne oppgaven brukes begrepet i kontekst av digital sikkerhet. ENISA (2021) og NIST (2011, s. B-15) definerer trussel som enhver omstendighet eller hendelse med potensial til å påvirke en eiendel negativt gjennom uautorisert tilgang, ødeleggelse, avsløring, modifisering av data og/eller nektelse av tjeneste. Konfidensialitet, integritet og tilgjengelighet, er sentrale variabler i definisjonen. Trusselvurdering er dermed en evaluering av aktørers intensjoner, evner og handlingsmåter.

Trusselvurdering og verdivurdering danner grunnlag for å utarbeide scenarioer som beskriver hvordan trusselaktører kan gå fram for å skade verdiene (NS 5832:2014, s. 6). Dette, ifølge standarden, for å avdekke organisasjonens sårbarheter opp mot valgte scenarioer.

Sårbarhet

En sårbarhet i IKT-systemer er en svakhet ved design, konfigurasjon eller prosess som kan utnyttes og forårsake brudd i IKT-systemet (Edgar & Manz, 2017, s. 39). Intensjon og kapasitet hos en trusselaktør er forutsetninger for utnyttelse av digitale sårbarheter. Et system ansees å være sårbart når det gir mulighet for en trussel å bryte seg gjennom en sikkerhetsbarriere (Edgar & Manz, 2017, s. 39).

System-begrepet inkluderes ofte i definisjoner av sårbarhet (Edgar & Manz, 2017). I oppgaven brukes begrepet i dets brede forstand, ved at menneskelige, organisatoriske og tekniske barrierer alle kan representere systemiske sårbarheter som kan utnyttes av trusselaktører. Det betyr at det ikke er nok å fjerne sårbarheter i tekniske delsystemer som programvare, nettverk eller maskinkomponent. Den menneskelige og organisatoriske faktoren må og tas med i ligningen.

Sårbarheter er ikke alltid forårsaket av feil og vår begrensede evne til å utforme sikre systemer. Som jeg har nevnt innledningsvis, eksponerer organisasjoner mye informasjon som er av interesse for en trusselaktør fordi demokratiske prosesser stiller krav til åpenhet, når det gjelder dokumentering av blant annet styringsprosesser. Dessuten er ikke alltid enkelt å skille mellom sårbarheter og verdier i informasjonssystemer. Dette fordi noe som en trusselaktør anser som verdi kan representere sårbarhet for en organisasjon. I tillegg kan eksempelvis bruk av tredje part utgjøre både sikkerhetsbarriere og sårbarhet for en virksomhet som tjenesteutsetter.

Alle disse faktorene vanskeliggjør risikovurderinger i informasjonssystemer. Forskere fremhever at etablering av *situasjonsbevissthet* er av stor betydning for risikostyring av IKT-systemer (Akhgar et al., 2016; Brooks, Grow, Craig, & Short, 2018; Grassegger & Nedbal, 2021; Hai-Jew, 2018; Ross et al., 2019; Settanni et al., 2017; Tounsi & Rais, 2018; Varga, Brynielsson, & Franke, 2021).

3.4. Situasjonsbevissthet

3.4.1. Begrepsavklaring

I forbindelse med cybersikkerhet brukes ofte begrepet «cyber situational awareness» (videre: situasjonsbevissthet) (se f.eks. Akhgar et al., 2016; Brooks, Grow, Craig, & Short, 2018; Grassegger & Nedbal, 2021; Hai-Jew, 2018; Ross et al., 2019; Settanni et al., 2017; Tounsi & Rais, 2018; Varga, Brynielsson, & Franke, 2021). Situasjonsbevissthet er et begrep som i likhet med «rekognosering» stammer fra krigsføringsstudier og betyr forståelse av alle forhold og deres betydning i og omkring operasjonsområdet (miljøet) og projeksjon av deres status i nær fremtid som er nødvendig for å fatte informerte beslutninger (Forsvarets Etterretningstjeneste, 2021, s. 106; Endsley, 2016, s. 13).

Begrepet har tradisjonelt vært brukt i forbindelse med krisehåndtering, krisekommunikasjon og beslutningstaking (Boin, 't Hart, Stern, & Sundelis, 2005; Endsley, 2016; Kruke & Olsen, 2012). I de siste årene er situasjonsbevissthet oftere brukt i kontekst av teorier som omhandler High Reliability Organisations (HRO) og Resilience Engineering (RE) (Nyssen, 2011; Pariès, 2011; Ross et al., 2019; Tjørhom & Aase, 2011; Weick & Sutcliffe, 2003). Disse teoriene fremhever proaktivt sikkerhetsarbeid som strategi for å håndtere iboende kompleksitet og det raskt skiftende risikobildet.

Ifølge Hollnagel et al. (2011) er det fire egenskaper som er nødvendige for å skape og opprettholde situasjonsbevissthet og dermed gjøre et system resilient:

- *evnen til å forutse* mulig situasjonsutvikling,
- *evnen til å lære* for å forstå hva som går bra og hva som går dårlig,
- *evnen til å overvåke* som innebærer å aktivt søke etter fremtidige trusler og endringer,
- *evnen til å reagere og respondere* som forutsetter at organisasjonen har kapasitet til å håndtere endringer og forstyrrelser i systemet på en proaktiv og fleksibel måte (Hollnagel et al., 2011).

HRO- og RE-teoriene er mye forsket på i dag og representerer to svært omfattende perspektiver. I denne oppgaven avgrenses teoretisk fokus til *situasjonsbevissthet* og hvordan selv-rekognosering og OSINT kan bidra til bevissthet og dermed styrke informasjonssikkerhet. I denne oppgaven forstås begrepet som «bevissthet om systemelementer, trusler og avhengigheter mellom elementene» (Ross et al., 2019, s. 114). Bevissthet om at systemelementer er avhengig av systemforståelse, ytelsesovervåkning og statusvurderinger. Bevissthet om trusler innebærer innhenting og bruk av etterretning, samt erkjennelsen av at angriperes metoder, motivasjon og teknikker utvikler seg (Ross et al., 2019). Denne definisjonen kan derav sees sammen med systemisk risiko-konseptet som vil si at situasjonsbevissthet er nødvendig for å kunne håndtere systemiske risikoer.

Her er det viktig å nevne at det rettes en del kritikk mot begrepet «situasjonsbevissthet». Eksempelvis påstår Weick et al. (2003, s. 45 referert til Roth, 1997, s. 178) at begrepet er altfor statisk og verken er dypt eller dynamisk nok til å fange alle elementer som er nødvendige for kontinuerlig sikkerhetsarbeid. Det foreslås alternative begreper, eksempelvis «situational assessment» og «operational awareness» (Roth, 1997; Weick & Sutcliffe, 2003). I denne oppgaven bruker jeg «situasjonsbevissthet», uten å inngå i diskusjon rundt begrepsbruk. Dette begrunnes med at (a) begrepet fremstår som et paraplykonsept som kan romme både

«situational assessment» og «operational awareness» og (b) begrepet brukes aktivt i dag innen cyber- og informasjonssikkerhet.

3.4.2. Tre nivåer av situasjonsbevissthet

Ifølge Endsley (2016, s. 14) er situasjonsbevissthet tredimensjonelt. Det består av tre nivåer: *oppfatningsnivå* som betegner persepsjon av elementer i miljøet eller systemet, *forståelsesnivå* som innebærer tolkning av nåværende situasjon og *projeksjonsnivå* ved evne til å forestille fremtidig utvikling og status.

Oppfatningsnivået handler om å avdekke og/eller gjennkjenne relevant informasjon. Dette har to viktige implikasjoner (Endsley, 2016, s. 14). For det første må man *ha tilgang til relevant informasjon*. Når det er på plass, må man kunne gjenkjenne informasjonen som er eller kan være relevent. Her fremhever Endsley (2016, s. 14) to viktige virkemidler: kommunikasjon og visualisering av informasjon.

Forståelsesnivå refererer til evnen å tolke relevant informasjon riktig (Endsley, 2016, s. 16). Det krever relevant kunnskap å kunne filtrere, tolke og håndtere den ervervede informasjonen. Ifølge Endsley (2016, s. 18) spiller mentale modeller en viktig rolle for å etablere forståelse.

Projeksjonsnivå refererer til forutanelsesevne (Endsley, 2016, s. 18). Med det mener hun å forestille den fremtidige tilstanden basert på innsamlet, oppfattet og forstått informasjon. Hun fremhever at bruk av nåværende situasjonsforståelse for projeksjoner krever god forståelse av fagområdet, da utvikling av mentale modeller kan være en krevende oppgave. Endsley (2016, s. 18) eksemplifiserer med de utfordringene man må håndtere når man opererer i komplekse systemer preget av et høyt nivå av gjensidig avhengighet. I slike miljø er det vanskelig å forutsi hvordan endringer i en variabel kan påvirke den generelle systemtilstanden. Feil- eller uoppdatert mental modell er en kilde til systemets sammenbrudd (Endsley, 2016, s. 18).

«Nivåer av situasjonsbevissthet» kan fremstå som et abstrakt konsept. Jeg vil derfor operasjonalisere det ved å redegjøre for syv betingelser som er nødvendige for etablering av situasjonsbevissthet, utarbeidet av Barford et al. (2010). Barford et al. (2010, s. 3) foreslår at for å oppnå «full situasjonsbevissthet for cyberforsvar» skal organisasjoner forholde seg til syv krav i sitt forebyggende sikkerhetsarbeid. De syv kravene inkluderer:

1. bevissthet om dagens situasjon,

2. bevissthet om mulig konsekvens av et angrep,
3. bevissthet om hvordan situasjonen utvikler seg,
4. bevissthet om trusselaktørs adferd,
5. bevissthet om hvordan og hvorfor den nåværende situasjonen har utviklet seg,
6. bevissthet om kvaliteten og påliteligheten til informasjon om situasjonsbevissthet og
7. vurdering av sannsynlig utvikling av dagens situasjon (Barford et al., 2010, s. 3–4).

Man legger merke til at kravene for å oppnå situasjonsbevissthet har mye til felles med NSMs prinsipper for IKT-sikkerhet (se Figur 6). Begge modellene vektlegger viktigheten av oversikt over kritiske eiendeler/elementer for å utarbeide mulige scenarioer for hvordan angrep kan utvikle seg. Med systemelementer menes alle elementer i MTO-perspektivet: mennesker, teknologi og organisasjon. Flere forskere påpeker at det er viktig for organisasjoner å forstå at tekniske tiltak alene ikke er nok til å sikre informasjonssikkerhet (Barford et al., 2010; Grassegger & Nedbal, 2021; Hai-Jew, 2018; Ross et al., 2019).

Man kan oppsummere med at beslutningstakers bevissthet om en situasjon, en forutsetning for kunnskapsgenerering og forståelse av situasjonen frem til det punktet en beslutning tas.

3.5. Oppsummering

Cyber- og informasjonssikkerhet forener sikkerhets- og security tankeganger. Dette fordi digitalisering har endret risikobildet ved å øke trussel-potensialet og kompleksiteten i sosio-tekniske systemer. For å tilpasse forebyggende arbeid til den dynamiske teknologiske utviklingen må organisasjoner tenke nytt og å ta i bruk nye verktøy. Dette krever et høyt nivå av situasjonsbevissthet, herunder evne til å søke, avdekke og gjenkjenne relevant informasjon, tolke informasjonen og utvikle mentale modeller. Forståelse av systemet man skal beskytte står sentralt i sikkerhetsarbeidet og risikovurderinger.

Som jeg viser videre i oppgaven er det ikke lenger hensiktsmessig å skille mellom ulike delsystemer. Man bør heller se på helhetlig samhandling mellom mennesker, teknologi og organisasjon da det er akkurat det en trusselaktør vil gjøre. Videre argumenterer jeg for at kjennskap til cyberangrepets forløp og teknikker som brukes av trusselaktører er essensielt for å beskytte skjermingsverdige informasjonssystemer. Dette fordi strategiske beslutninger baseres på etterretning om endringer i trusselaktørers motivasjoner og handlingsmåter, egenskaper ved systemelementer, samt teknologisk utvikling og samfunnsutvikling.

4. Metodisk tilnærming

I dette kapittelet gjøres rede for forskningsmetode som er lagt til grunn i dette studiet. Først beskriver jeg forskningsdesign og -logikken. Videre redegjør jeg for og begrunner valg av metoder for datainnsamling og -analyse. Til slutt drøftes vektlagte kvalitetskriterier og metodiske begrensninger, samt diskuteres etiske vurderinger som har preget arbeidet.

4.1. Forskningsdesign

Formålet med oppgaven er å *utforske* et sosialt fenomen, *forstå* motivasjoner og handlinger til sosiale aktører og *beskrive* fenomenet og dets konsekvenser for andre sosiale aktører. Derav var kvalitativ forskningsmetode et naturlig valg.

Studien kan beskrives som eksplorativ og empirisk-basert, ved at oppgavens problemstilling og forskningsspørsmål er av utforskende karakter. Dette innebærer at å gi ett entydig svar ikke er hovedmålet med studien. Hovedmålet er å danne dypere forståelse for et fenomen. Eksplorativ design brukes ofte i studier om fenomener som er lite forsket på og som søker å utvikle en innledende beskrivelse eller forståelse av et sosialt fenomen (Blaikie & Priest, 2019). Slike studier er basert på «muddling through»-tilnærming, som er en mindre systematisk måte å gjennomføre et forskningsprosjekt på. Mens eksplorativ forskning vanligvis utføres i begynnelsen av et forskningsprosjekt, kan det også være nødvendig på andre stadier for å overvinne et uventet problem eller for å forstå et uventet funn bedre. *Empiriske* studie sikter på å gi svar på forskningsspørsmål ved å samle inn og analysere data relatert til noen aspekter av det sosiale livet.

Ny kunnskap erverves gjennom en, eller kombinasjon av flere forskningsstrategier; induksjon, deduksjon, retroduksjon og/eller abduksjon (Blaikie og Priest, 2019, s. 21). Strategiene representerer ulike logikker som brukes for å besvare en problemstilling. For denne studien ble en abduktiv forskningsstrategi med utgangspunkt i Blaikie ag Priest sin tolkning et naturlig valg. Forfatterne mener at abduktiv forskningslogikk passer best for en eksplorativ, empirisk-basert studie (Blaikie & Priest, 2019). Induktiv eller deduktiv forskningslogikk kunne blitt brukt for å besvare forskningsspørsmålene, men resultatet hadde vært annerledes. Forskjellen mellom deduksjon og abduksjon er at deduksjon viser at noe må være på en bestemt måte, mens abduksjon viser *hvordan noe kan være* (Habermas & Shapiro, 1971, s. 113). Induksjon

baseres på og konkluderer med generaliserte antakelser som ikke er et formålet med denne studien (Habermas & Shapiro, 1971, s. 113).

Abduksjon er godt egnet til å forstå sosiale fenomener og aktørers adferd, herunder deres konstruksjon av realitet, måte å konseptualisere verden på og «taus» kunnskap. Blaikie & Priest (2019, s. 99) argumenterer for at abduksjon gir en mulighet for å oppleve en sosial verden fra innsiden. Fokuset er på forståelse snarere enn forklaring, og grunner snarere enn årsaker. Målet er å presentere fenomener med utgangspunkt i de sosiale aktørenes synspunkt, heller enn forskers synspunkt. De skriver blant annet at «[...] social scientists must draw on the same 'mutual knowledge' that social actors use to make sense of their activity» (Blaikie & Priest, 2019, s. 99). Med denne undersøkelsen vil jeg forstå hvorfor noe gir mening for et individ, hvorfor trusselaktører handler som de gjør. Jeg valgte å finne svaret på spørsmålet om hvordan trusselaktører kartlegger organisasjoner ved å gå inn i trusselaktørs verden og prøve å forstå motiver, meninger og handlingsmåter. En måte å gjøre det på er «learning by doing». Dermed er studien preget av en «bottom-up»-tilnærming, som er vanlig for abduktiv forskningsstrategi.

Forskningsprosessen var ledet av metode og datainnsamling fremfor teori. Slik eksplorativ forskningsdesign er også i tråd med abduktiv forskningsmetode. Forskningen ble preget av kontinuerlig og nokså usystematisk vandring mellom empiri, metode og teori. Denne måten å finne svar på problemstillingen og forskningsspørsmålene var nokså uvanlig for meg og forårsaket en del frustrasjon. Jeg ble belønnet ved øyeblikkene jeg kom over interessante funn og nye kunnskaper, som gjorde at ting etter hvert begynte å falle på plass og gi nye meninger.

I løpet av arbeidet med oppgaven har jeg lært ting som krevde revurdering av mitt eget syn på designet og fokuset. Jeg måtte lære meg å erkjenne at den ufullkomne og mangelfulle naturen av jakten på vitenskap, er avgjørende når en driver med forskning. Edgar og Manz (2017, s. 66) advarer mot jakten på den «perfekte» vitenskapelige metode eller «feilfri» tilnærming til forskning. De mener en slik holdning lett kan blinde forskeren, ved at hen vil ende opp med «delvise løsninger», eller å forhindre seg selv fra å oppdage og anerkjenne feil i metodiske elementer eller analyse av resultater.

4.2. Metodetriangulering

I denne studien bruker jeg tre ulike metoder for datainnsamling, noe som refereres til som triangulering (Christensen, Johnson, & Turner, 2015, s. 69; Denzin, 1978, s. 292; Patton, 2015,

s. 478). Denzin (1978, s. 304) mener kombinasjon av flere datainnsamlingsmetoder i samme studie, til en viss grad kan kompensere for begrensninger ved de enkelte metodene. Man kan spille de ulike bevis mot hverandre for å øke troverdighet, ved at funn bekreftes på tvers av datasett. Dermed reduseres virkningen av potensielle skjevheter knyttet til en enkelt metodisk tilnærming (Denzin, 1978, s. 304; Patton, 2015).

I tillegg brukes ulike metoder i denne oppgaven fordi forskningsspørsmålene ikke kan besvares ved hjelp av én metode for datainnsamling. For å svare på det første spørsmålet, *hvordan fungerer digital rekognosering av organisasjoner i praksis*, ble data innsamlet ved hjelp av uformelle intervjuer og OSINT-metode. For å svare på det andre spørsmålet, *hvilken informasjon om de utvalgte virksomhetene kan man finne ved hjelp av rekognoseringsteknikker og OSINT*, er data innsamlet ved hjelp av OSINT-metode og -verktøy. Det tredje forskningsspørsmålet, *hvorfor er denne type informasjon av interesse for en trusselaktør*, besvares gjennom dokumentanalyse og intervjuer. Datainnsamling ved hjelp av OSINT ble utført de to første ukene i april. Det første intervjuet ble avholdt 22.01, det siste i mai. Dokumentanalyse ble gjennomført mellom 15 april og 15 mai.

4.2.1. OSINT

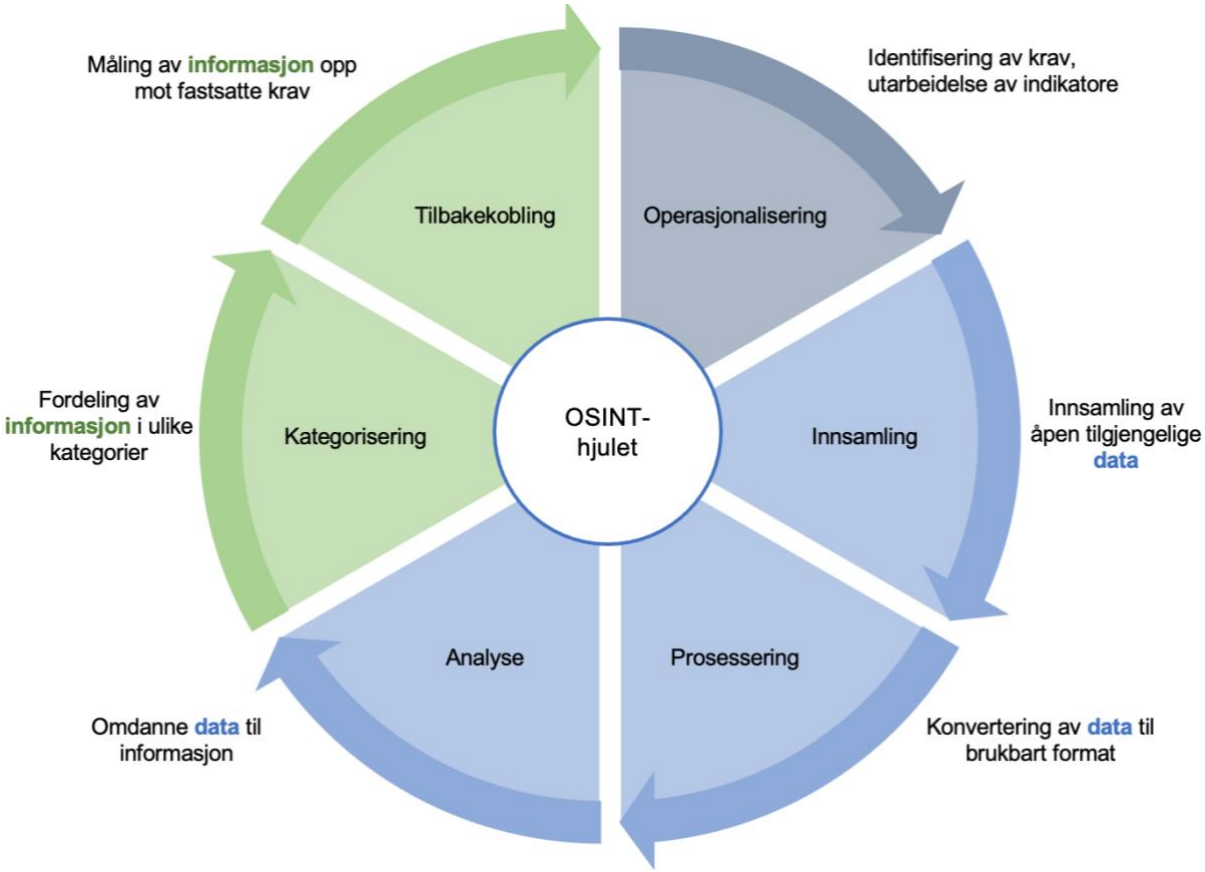
I delkapittel 1.5 presenteres en mer generell definisjon av OSINT-konseptet. I dette delkapittelet beskrives hvordan OSINT ble brukt for innsamling av data for dette prosjektet.

Samfunnets digitalisering resulterer i at store mengder data er nå tilgjengelige for allmenheten. Dette er et av årsakene til at OSINT har blitt mer og mer aktuelt de siste årene. De enorme mengdene åpen tilgjengelige data representerer både muligheter og utfordringer. Innsamling skjer relativt fort, mens forberedelser, prosessering og analyse er de mest utfordrende delene i OSINT-granskninger. Data er egentlig bare tekst eller tall. For å bli til meningsfull informasjon må data behandles, tolkes og struktureres (Gibson, 2016, s. 72; Halvorsen, 2008, s. 128).

OSINT-forskere bruker mest tid på å samle sammen informasjonsbiter, vurdere relevans, konvertere dataene til passende for analyse format, «smelte» dataene sammen, og deretter starte utvinnings- og aggregeringsprosessene (Akhgar et al., 2016; Bazzell, 2021; Gibson, 2016). Uten å ha en god strategi for datainnsamling vil man ende opp med enorme mengder av ustrukturerte data, som ved første øyekast gir lite mening. Nøye planlegging og operasjonalisering er nødvendig for å identifisere dataene som er relevante for å besvare

forskningsspørsmål (Gibson, 2016). Figur 8 fremstiller OSINT-hjulet, som illustrerer hvordan data er blitt til informasjon. Denne modellen er blitt brukt som veiledende for planlegging og gjennomføring av min datainnsamling.

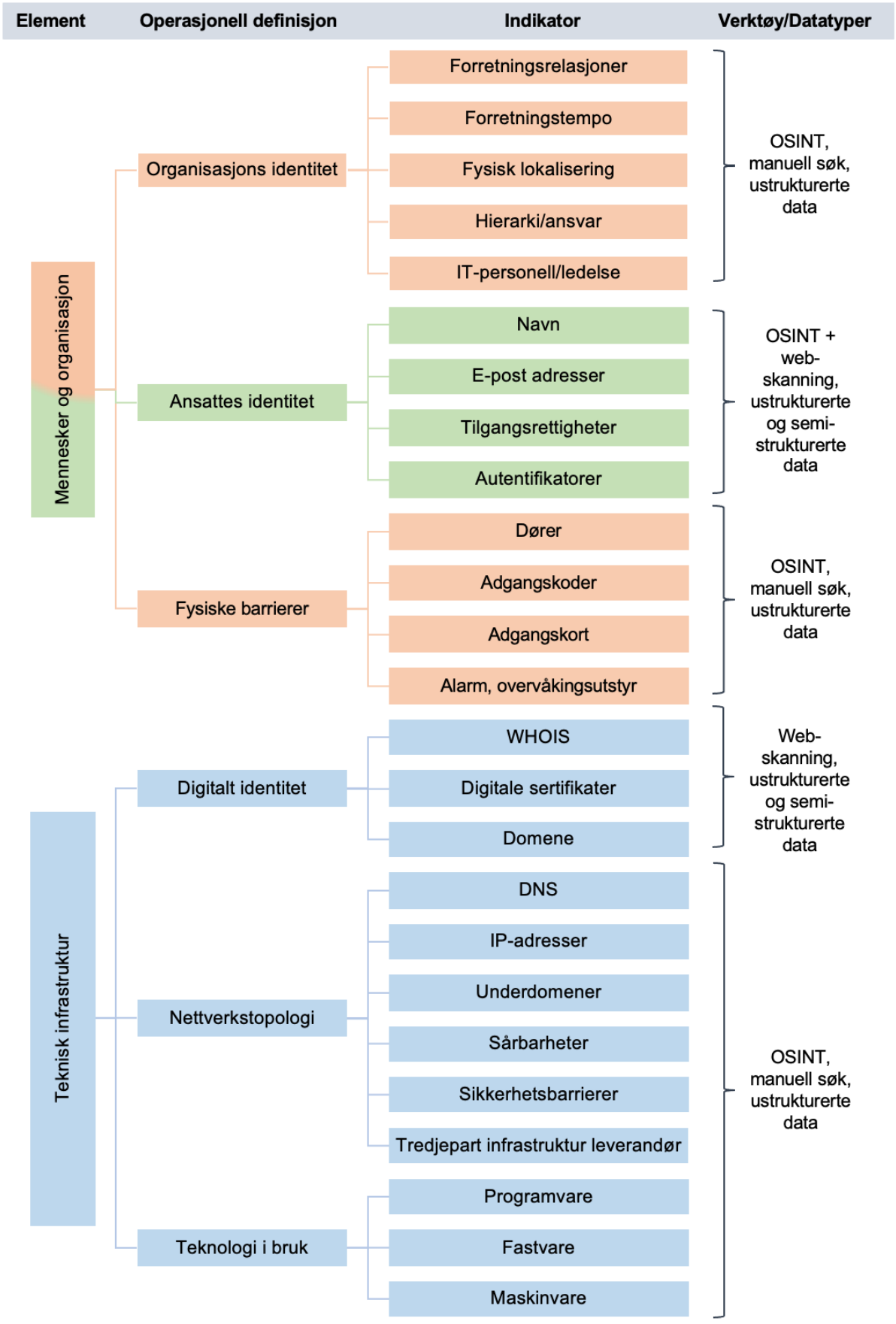
Figur 8: OSINT-hjulet (basert på Gibson, 2016, s. 72)



Operasjonalisering

Figur 8 viser at initialfasen i datainnsamling innebærer fastsettelse av operasjonelle definisjoner, det vil si formulering av indikatorer eller kriterier som data skal oppfylle. Operasjonelle definisjoner klargjør hvordan en skal gå fram for å samle inn nødvendige og relevante data (Eisner, 2017, s. 61; Halvorsen, 2008, s. 64; Patton, 2015, s. 541). Figur 9 illustrerer denne studiens operasjonaliseringsprosessen. Modellen er inspirert av MTO-tankegangen, intervjuer og MITRE rammeverk (se Figur 3). Den viser hvordan operasjonelle definisjoner og indikatorer ble utviklet, samt hvilke teknikker som ble brukt underveis. I sin helhet illustrerer modellen hvordan en trusselaktør, i dette tilfelle – meg, kan planlegge rekognosering på et mål.

Figur 9: Datainnsamling ved hjelp av OSINT - operasjonalisering



Menneske og organisasjon

Kartlegging av organisasjonens identitet innebærer innsamling av data som kan inneholde organisasjons adresse, organisasjonshierarki, økonomi, avdelinger, spesifikasjoner for forretningsdrift, forretningsrelasjoner, ansattes navn og kontaktinformasjon, samt roller og ansvar for nøkkelmedarbeidere. Dataene er ustrukturerte og innhentes manuelt fra offerets websider, søkemotorer, jobbannonser, avisinnlegg og SoMe.

Kartlegging av ansattes identitet er en målrettet kartlegging av personlige data om ansatte. Herunder navn, private e-postadresser og kontoer, samt autentifikator-data som passord til brukerkontoer. Disse dataene er ustrukturert og samles via web-skanning og manuelt søk i datalekkasjer mm. Noen indikatorer er tilsynelatende overlappende med indikatorer nevnt i forrige avsnittet. Forskjellen går ut på at i første fase innsamles kontaktinformasjon tilknyttet organisasjon. I andre fase samles personlige data. Søk på organisasjonsdomene og individets navn gir ulike resultater.

Kartlegging av fysiske barrierer. Trusselaktør leter etter visuelle dokumenter som kan avsløre informasjon om fysiske barrierer. Man gjennomgår organisasjons SoMe og gransker innlegg, bilder og videoer som kan vise eksempelvis en ansatt som slår inn adgangskode eller viser et adgangskort, plassering av overvåkningskameraer eller alarm osv. Alternativt kan data fra overvåkningskameraer brukes, hvis kameraene ikke er passordbeskyttet.

Teknisk infrastruktur

Digital identitet. Her innsamles data som sier noe om organisasjonens digitale identitet. Med digital identitet menes registrerte IP-adresser, domenenavn og digitale sertifikater. Et digitalt sertifikat er en unik datafil som utgis av sertifikatmyndighet (CA). Filen innebærer informasjon om kryptert nettrafikk og brukes som digital legitimasjon (Wilson, 2020). Dataene samles via enkle manuelle søk i åpne tekniske databaser og kan være ustrukturerte eller semi-strukturerte.

Kartlegging av nettverkstopologi innebærer automatisert web-skanning med formål å kartlegge IP-blokk, domener og underdomener, åpne porter, servere og programvarer i bruk. Skanning resulterer i store mengder semi-strukturerte data. Flere verktøy som brukes i denne fasen gir mye data som ikke nødvendigvis er relevant. Kjennskap til filtreringsinstruksjoner er dermed avgjørende for effektiviteten i dette stadiet.

Kartlegging av teknologi som er i bruk består av de samme teknikkene som ved kartlegging av barrierer. Vanligvis vil det innebære manuelt søk for bilder, videoer, blogginnlegg, innlegg i sosiale media som viser/omtaler elektronisk utstyr som brukes i organisasjonen. Informasjon om rutere, PC, web-kamera og overvåkningskamera og fysiske sikkerhetsbarrierer er av særlig interesse.

Etablering av teknisk infrastruktur for å skape kontrollert miljø for datainnsamling

I delkapittel 2.2 henviser jeg til tre studier hvor OSINT er brukt som datainnsamlingsmetode. Jeg har lagt merke til en metodisk svakhet ved disse studier. Svakheten består i at forskere ikke har etablert et kontrollert miljø for datainnsamling. Det vil si at det ikke ble brukt VPN[2] som sikrer at ens geografisk plassering, personlige innstillinger og tidligere websøk ikke kan påvirke resultater av datainnsamling. Etter å ha tatt kontakt med NVE og Hayes & Cappa, fikk jeg bekreftet at ingen av de brukte VPN eller isolert og nullstilt datamaskin. Matvej har ikke svart på min henvendelse.

En av de viktigste metodiske forutsetningene i dette prosjektet er å samle informasjon fra trusselaktørs perspektiv. Det vil si at dataene vil ikke må kunne påvirkes av min identitet, herunder min eksisterende kunnskap om forskningsobjekt og min internetthistorikk. Brukernes tidligere internettaktiviteter og personlige innstillinger påvirker resultater av internettsøk. For å sikre «teknisk» objektivitet og etterprøvbarhet, har jeg tatt i bruk en datamaskin som var nullstilt til standardinnstillinger og som utelukkende ble brukt til datainnsamling. Jeg har brukt VPN og unngått å logge på mine private kontoer fra den designerte PC. Ved å bruke VPN og isolert utstyr ønsket jeg å sikre at jeg samler inn informasjon som er tilgjengelig for en anonym trusselaktør som ikke nødvendigvis befinner seg i Norge eller har noen som helst tidligere kjennskap til organisasjonene.

Videre har jeg bygget mitt eget digitalt laboratoriet ved å installere operativ system Kali Linux og laste ned ulike programvarer som ble brukt for datainnsamling. Jeg hadde ikke noen tidligere kjennskap til det operative systemet eller verktøyene, men lærte dette underveis med hjelp av videoer, blogger og e-bøker.

[2] VPN er en dataprogramvare som sender all datatrafikk fra en datamaskin gjennom en kryptert virtuell tunnel. Dette gjør at brukeren kan forbli anonym på nettet ved at IP-adresse og beliggenhet vil ikke være synlig for andre. Den krypterte tunellen vil også forhindre at brukerens datamaskin vil kunne være utsatt for dataangrep.

For å demonstrere hvor mye informasjon og verktøy som er tilgjengelig for trusselaktør med begrensede ressurser og kunnskaper, har jeg brukt datainnsamlingsverktøy som er relativt enkle å bruke. For å få tilgang til tjenester som krever pålogging har jeg opprettet en såkalt «sokkedukke» (*eng*. «sockpuppet»), som er en brukerkonto tilhørende en ikke-eksisterende person (Bazzell, 2021). Som det er vist i Figur 3 og bekreftes av empiri er dette en del av forberedelser til et cyberangrep. Hensikten med en slik konto ved Internett-granskninger er at ens identitet ikke vil påvirke granskningsresultater og at trusselaktører ikke vil kunne spore aktiviteter tilbake til granskeren.

En av de største utfordringene var å minimere forskers bias. I starten av prosjektet etablerte jeg kontakt med virksomheter for å få deres samtykke. Jeg måtte påse på at mine tidligere kunnskaper om organisasjonen har ikke påvirket datainnsamling, særlig i prosjektets startfase. Jeg måtte innhente den samme informasjonen via internett. Å skille mellom eksisterende kunnskap og funn tilhørende min «trusselaktør»-identitet var ikke en enkel oppgave. Til slutt lyktes jeg ved å kontinuerlig evaluere datainnsamlingsgrunnlaget.

4.2.2. Uformelle intervjuer med nøkkelinformanter

Et intervju betyr vanligvis en slags formell og nøye planlagt kommunikasjon. Noe som ikke er tilfelle i dette prosjektet. Jeg har gjennomført uformelle og ustrukturerte samtaler med nøkkelinformanter. Gilchriest og Williams (1999, s. 73) definerer nøkkelinformanter som individer som er nøkkelen til forskerens forståelse av deres kultur, fenomener og sosial virkelighet. Nøkkelinformanter har spesiell/unik kunnskap, status eller kommunikasjonsevner, vilje til å dele sin kunnskap og ferdigheter med forskeren, og tilgang til perspektiver eller observasjoner utilgjengelige for forskeren (Goetz & LeCompte, 1984 referert i Gilchriest & Williams, 1999, s. 73). Deres posisjon i en kultur, informasjon om fenomener de sitter på og forholdet til forskeren gjør de til en uvurderlig informasjonskilde. I tillegg spilte nøkkelinformanter en viktig rolle når det gjelder kvalitetssjekken av oppgavens tekniske deler.

Informantintervjuer som datainnsamlingsmetode står sjelden alene, om noen gang (Gilchriest & Williams, 1999). Som regel er de komplementære til andre metoder og datasett. Eksempelvis i denne studien supplerer samtalene dokumentstudiet og OSINT. Uformelle samtaler av denne type er en metodisk tilnærming som stammer fra etnografi og brukes sjelden i samfunnssikkerhetsrelaterte studier. Ifølge Spradley (1979, s. 3) brukes uformelle samtaler for å lære *av mennesker* istedenfor å lære *om mennesker*, og det er denne rollen samtalene spiller

i denne studien. Det ble gjennomført fem samtaler med individer som har relevant faglig ekspertise, herunder cybereksperter og etiske hackere. Tabell 1 viser oversikt over informanter, deres faglige bakgrunn, og hvilke temaer som ble diskutert med hver enkelt.

Tabell 1: Informanter

Kode forklaring: CE - cybereksperт, EH - etisk hacker

Informant	Faglig ekspertise	Diskuterte temaer	Erfaring	Land
CE1	Cybersikkerhet-ingeniør og etisk hacker i Facebook. Aktiv deltaker i ulike OSINT-nettsamfunn hvor han er engasjert i å hjelpe med tekniske spørsmål og formidling av kunnskap om cybersikkerhet	Hvordan fungerer digital rekognosering av organisasjoner i praksis? Herunder: • anonymitet på Internett, • hvordan å sikre objektivitet av datainnsamling, • hvordan å bygge digitalt kontrollert miljø • hvordan å analysere nettverksskanning-data Hvorfor er denne type informasjon av interesse for en trusselaktør?	15 år	USA
CE2	Cybersikkerhet-ingeniør i et stort amerikansk IT-selskap. På fri tid driver med OSINT-granskninger for å bekjempe informasjons-operasjoner, «fake news» og «deepfakes».		17 år	USA
CE3	Ekspert i cybersikkerhet i et av de store konsulentbyråene		4 år	NO
EH1	Security analytiker, etisk hacker i et stort IT-konsulentbyrå	Hvorfor er denne type informasjon er av interesse for en trusselaktør?	5 år	NO
EH2	Dataingeniør i et ukrainsk IT-selskap, tidligere etisk hacker og før det såkalt «grå hacker»	Hvorfor er denne type informasjon er av interesse for en trusselaktør? Hvordan har trusselaktører innsamlet og brukt informasjon for å gjennomføre cyberangrepene i Ukraina i 2015-2017	6 år	UKR

Hvordan jeg kom i kontakt med informantene

Å gjennomføre intervjuer var ikke jeg planlagt på forhånd og de første samtalene skjedde spontant. Tre av informantene kontaktet meg på eget initiativ, fordi de var interessert i prosjektet. Dette skjedde som resultat av min deltakelse i et nettsamfunn hvor eksperter i OSINT-granskninger samles og diskuterer aktuelle temaer, utfordringer, nye verktøy mm.. Formålet med min deltakelse i nettsamfunnet var å observere og lære. Etter hvert la jeg ut et

innlegg hvor jeg kort beskrev mitt prosjekt og ba om tips og råd. Deretter ble jeg kontaktet av CE1, som er cybersikkerhetsekspert i et av de verdens største SoMe-selskapene. Vedkommende var villig å hjelpe meg i oppstartfasen og delte sine tanker om hvordan man starter rekognosering på et mål. Vi avtalte en digital samtale via Skype, hvor vi diskuterte rekognosering samt tekniske utfordringer. Vi har vært i kontakt flere ganger etter det første møtet, men da hovedsakelig gjennom skriftlig kommunikasjon i privat gruppe på nettsamfunnet Discord.

En annen samtale skjedde og spontant som en del av diskusjon i den private gruppen TraceLab i nettsamfunnet Slack. Jeg deltok som observatør i gruppen, som driver med søk etter forsvunne personer. Min deltakelse var som ledd i å lære OSINT-teknikker. CE2 tok kontakt med meg etter at jeg la ut et spørsmål om etablering av kontrollert miljø for datainnsamling. Vedkommende jobber som dataingeniør i USA og er på fritiden involvert i granskninger av påvirkningsoperasjoner.

Tre påfølgende samtaler har skjedd på mitt initiativ. Samtale med CE3 og EH1 tok sted rett etter datainnsamling. EH2 kontaktet meg etter å ha fått informasjon om prosjektet fra våre felles venner. I samtalene fokuserte vi på hvordan den type informasjon jeg har innsamlet, kan brukes for å forårsake skade. Etiske hackere har førstehåndskunnskap til trusselaktørers teknikker og metoder. EH2 hadde i tillegg førstehåndskunnskap om cyberangrepene i Ukraina som diskuteres i empiri-delene. Samtalene bidro til å gi meg en mer helhetlig forståelse av cyberangreps prosesser og mekanismer.

CE3, EH1 og EH2 har og hjulpet meg med å tolke data jeg samlet ved bruk av OSINT. Herunder ved at jeg viste dem en tilsvarende anonymisert oversikt over funn som er gjengitt i denne oppgaven, som filtyper, portnummer og lignende, hvorpå de forklarte for meg hvordan en trusselaktør kan bruke slik informasjon.

I løpet av arbeidet med oppgaven har jeg opplevd at mennesker som jobber med cybersikkerhet viste stor interesse i å hjelpe med et samfunnsvitenskapelig prosjekt. De tok kontakt flere ganger og etterspurte hvordan prosjektet går og om jeg trengte hjelp. Tre av informantene fortalte at de setter stor pris på hvert forsøk på å formidle kunnskap om cybersikkerhet på slik måte at flere mennesker, særlig de uten teknisk kompetanse, kan forstå «hvordan ting i cyberspace fungerer». De sier det vil kunne øke cyber-situasjonsbevissthet.

Kildekritikk

Fordelene med uformelle og ustrukturerte intervju er fleksibilitet og åpenhet. Dette bidrar til at informanter føler seg avslappet og ikke tvinges til å tenke på en bestemt måte. Det var et bevist valg å ikke ta opp samtalene. Det var ikke alltid mulig å notere aktivt underveis fordi informantene var engasjert og snakket mye og fort. Jeg notert fra intervjuene like etter samtalene. Aktiv notering kunne distrahert informanten og forstyrret prosessen. Dette i kombinasjon med at informantene brukte mye sjargong og tekniske begreper, som i starten var ukjente for meg, er en svakhet ved denne studien da noe informasjon muligens gikk tapt. Etter hvert lærte jeg noe sjargong og fikk mer teknisk kunnskap, som hadde positiv effekt på samtalene med de etiske hackerne. Min bruk tekniske begrep og sjargong ble møtt med overraskelse og lettelse, da informantene slapp å «overforklare» hvert begrep, men fikk snakke fritt og uforstyrret. For å sikre at minst mulig informasjon gikk tapt og for korrigering av eventuelle feil, ble empiri-delen av oppgaven sendt til de norsktalende informantene. De har fått mulighet til å korrigere og komme med innvendinger.

4.2.3. Dokumentstudie

Dokumentstudie er en metode for datainnsamling som består av en systematisk innholdsanalyse av dokumenter (Bowen, 2009, s. 27; Neuman, 2014, s. 49). Hensikten med denne studien er å samle data av relevans for å besvare forskningsspørsmålet om hvordan åpen tilgjengelig informasjon har vært brukt i tidligere cyberangrep. Denzin (1978, s. 291) nevner dokumentanalyse blant de datainnsamlingsmetodene som ofte kombineres med andre kvalitative forskningsmetoder for undersøkelser basert på triangulering.

I denne studien gir dokumenter bakgrunnsinformasjon. Slik informasjon og innsikt kan hjelpe forskere til å identifisere forhold som påvirker fenomenene som studeres. Jeg bruker data hentet fra dokumenter for å kontekstualisere data innsamlet under intervjuer og for å bekrefte bevis fra andre kilder (Angrosino & Coffey, 2000). Bowen (2009, s. 30) argumenterer også for at når det er samsvar i informasjon fra forskjellige kilder, vil lesere av forskningsrapporten vanligvis ha større tillit til funnenes troverdigheten.

Fordeler med dokumentstudier er, ifølge Bowen (2009, s. 30) at de beskriver allerede fortolket fenomen og gir grunnlag for ytterligere spørsmål som skal stilles. Videre skriver han at dokumenter er et middel for å verifisere funn fra andre datakilder og ikke minst den mest

effektive måten å samle data når hendelser ikke lenger kan observeres. Forskeren kan se på temaet fra et annet perspektiv, kunnskapen er oppsummert og systematisert og man får hele puslespillet servert (Bowen, 2009; Halvorsen, 2008; Jesson, Matheson, & Lacey, 2011). Begrensninger består av at man må bruke dokumenter som er produsert for annen vinkling eller formål enn forskeren selv ville hatt (Bowen, 2009; Neuman, 2014).

For denne undersøkelsen har jeg gjennomført systematisk dokumentstudie. Det kjennetegnes ved smalt, svært godt definert tema med forskningsspørsmål og forhåndsdefinerte inklusjon- og eksklusjonskriterier (Jesson et al., 2011, s. 103). Tabell 2 oppsummerer kriterier og søkeord som er brukt i innsamling av dokumenter.

Tabell 2: Dokumentstudie - kriterier og søkeord

Inklusjons- og eksklusjonskriterier	Søkeord

• Tidsperiode: 2016-2021(se kommentar)
• Dokumenttype: granskningsrapporter, rettsaker
• Skal omhandle:
  ○ tidligere hendelser hvor trusselaktører har brukt OSINT for å forberede et cyberangrep mot organisasjoner, store grupper av individer og stater
  ○ målrettet angrep
• Skal ikke omhandle:
  ○ avanserte hacking angrep uten bruk av sosial manipulering og rekognosering tekniker
  ○ handlinger mot enkelte individer (cyberstalking, kjærlighetssvindel og lignende)
	• «cyber attack»
	• «reconnaissance»
	• «phishing»
	• «social engineering»
	• «vulnerability exploitation»
	• «APT»
	• «spoofing»
	• «* injection»
	• «hacking»
	• «credentials»
	• «brute-force»

Kommentar til Tabell 2: Mens selve dokumenter var produsert/utgitt i peridoen 2016-2021, kan de omhandle hendelser som har skjedd før 2016.

Jeg har lett etter granskningsrapporter og rettsaker, da jeg forventet at disse vil inneholde detaljert redegjørelse for hvert trinn i tidligere cyberangrep. Søk i Lovdata[3] viste at i Norge eksisterer ikke rettspraksis som samsvarer med oppgavens problemstilling. Jeg har derfor gjennomført søk i en database tilhørende USAs Justisdepartementet (The United States Department of Justice, 2015). Søket viste at slike rettsaker er mer vanlige i USA, jeg fant elleve saker som ble behandlet mellom 2016 og 2021. Jeg ekskluderte saker som omhandlet

[3] Straffeloven (LOV-2005-05-20-28) kap. 21 om Vern av informasjon og informasjonsutveksling. Sikkerhetslovens (LOV-2018-06-01-24) kap. 5 og 6 om informasjonssikkerhet og informasjonssystemsikkerhet

kriminelle handlinger mot enkelte personer, som nettstalking, kjærlighetssvindel og lignende, samt saker hvor rekognoseringsprosessen ikke var beskrevet særlig grundig.

Det endelige utvalget besto av fire tiltalebeslutninger, en anmeldelse, to granskningsrapporter og noe supplerende materiale. Alle dokumentene omhandler målrettede cyberangrep mot organisasjoner, nasjonalstater og/eller store grupper av mennesker. Tabell 3 presenterer oversikt over studerte dokumenter. Tabell 9 i Vedlegg D viser hvordan dokumentene ble analysert. Hovedfokus ved dokumentanalyse var på de delene av dokumenter som omhandler «fremgangsmåte og midler».

Tabell 3: Oversikt over studerte dokumenter

Kodeforklaring: RS - rettsak, V- vitnemål, AN- anmeldelse, R - rapport, AR - artikkel

	Kode	Årstall	Tittel
1	RS	2016	United States of America v. Fathi et al. (Bharara, 2016).
2	RS	2017	United States of America v. Dokuchaev et al. (Stretch, 2017).
3	RS	2018	United States of America v. Rafatnejad et al. (Berman, 2018).
4	V*	2018	Testimony of Crane Hassold Director [...] (Hassold, 2018b).
5	AR*	2018	Silent Librarian: More to the Story of the Iranian Mabna Institute Indictment (Hassold, 2018a).
6	AN	2018	United States of America v. Park et al. (Oliver & Shields, 2018).
7	RS	2020	United States of America v. Andrienko et al. (Coville, 2020).
8	R	2020	Pawn Storm in 2019. A Year of Scanning and Credential Phishing on High-Profile Targets (Hacquebord, 2020) **.
9	R	2021	«Lebanese Cedar» APT. Global Lebanese Espionage Campaign Leveraging Web Servers (ClearSky Cyber Security ltd, 2021).

Kommentar til Tabell 4:

** Supplerer num. 4;*

*** Rapporten suppleres med YouTube video som er produsert av Dr. Feike Hacquebord og Forward-Looking Threat Research. Videoen omhandler den samme rapporten, men inkluderer noen refleksjoner og audiovisuelle data som er ikke en del av rapporten.*

Kildekritikk

Fordelen med å studere granskningsrapporter og rettsdokumenter, er at de kan regnes som pålitelige kilder for informasjon om en kriminell handling. Det vil si at de gir relativt korrekt og nøytral gjengivelse av hendelser og formålet med dokumentet er klart og avgrenset. Tolkning av slike dokumenter forenkles av at det ikke brukes følelsesmessige ord og retorikk. Språket er klart, forståelig og nøytralt. Rapportene som er brukt kjennetegnes ved relativt nøytral fremstilling av informasjon. Slike nøytrale og faktabaserte beskrivelser av hendelser gjør analysen enklere ved at man ble ikke påvirket av retorikken og at fakta er presentert på en klart og strukturert måte.

4.3. Dataanalyse

Teori innen cybersikkerhet, tidligere forskning og kunnskaper ervervet via personlig kommunikasjon ligger til grunn for dataanalysen. Hovedkriteriet for å avgjøre dataenes relevans var vurderinger av hvorvidt informasjonen kan brukes av trusselaktør for å skade en organisasjon. Innhenting og analyse foregikk samtidig. Dette på grunn av behovet for kontinuerlig evaluering av innsamlet informasjon for å avgjøre (a) hvorvidt data/dokumenter inneholder informasjon som kan lede til andre kilder, (b) hvorvidt informasjonen må dobbeltsjekkes eller bekreftes ved bruk av andre kilder/verktøy. I tillegg medførte kontinuerlig læring behov for gjennomgang av allerede innsamlede og analyserte data for analyse i lys av nyervervet kunnskap. Tabell 4 oppsummerer kategorisering og koding av data.

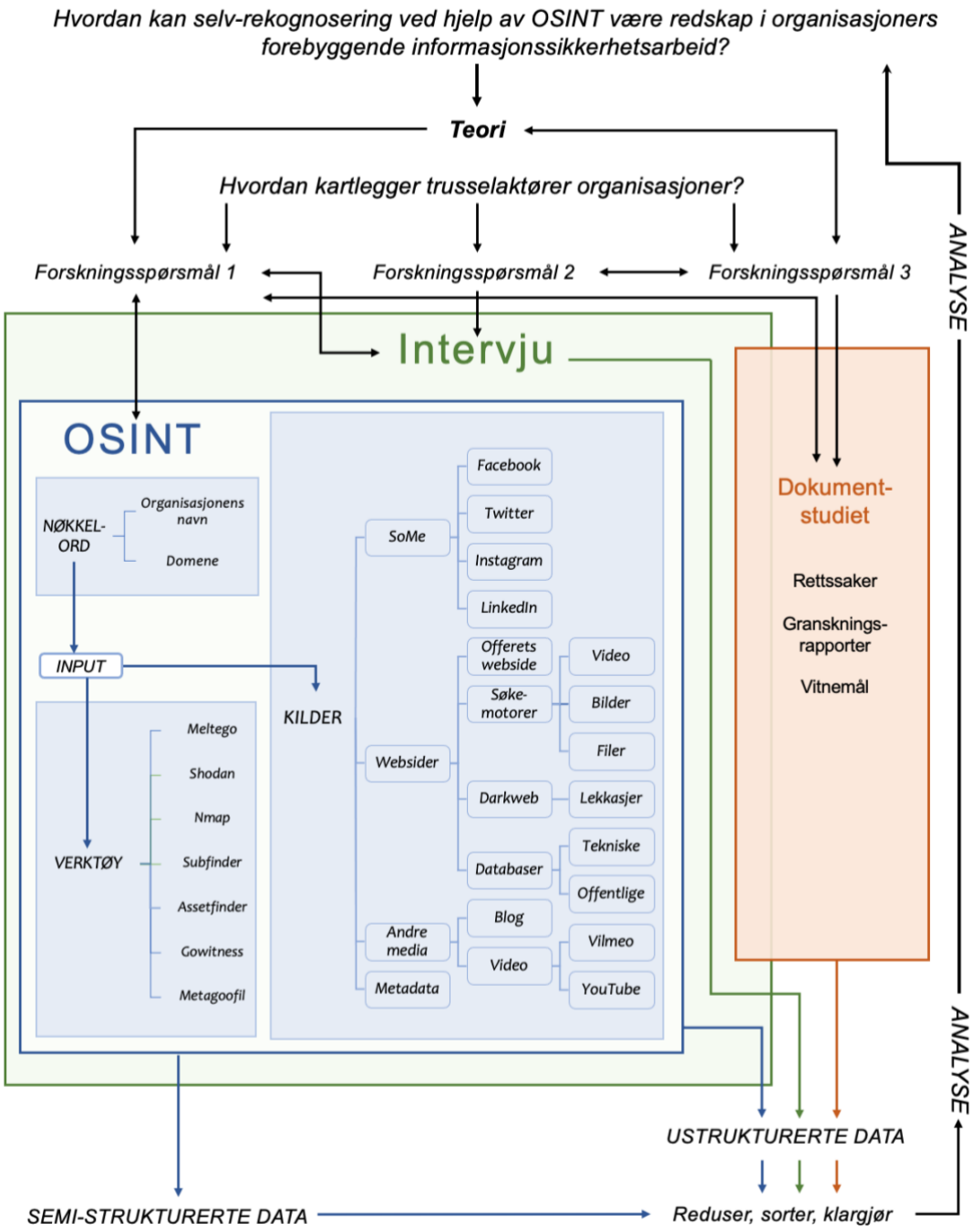
Tabell 4: Kategorisering og koding av data

	Informasjon om	**Utnyttelsesform**
Organisasjon/ Menneske	*Generelle opplysninger*: adresser, telefonnummer, antall ansatte og ansvar, organisasjonens økonomi, tidligere og pågående prosjekter og forretningsrelasjoner. *Fysiske sikkerhetsbarrierer*: inngangskoder og inngangskort, alarm plassering. *Autentifikatorer:* passord, e-post, signatur, bilder, rolle osv. *Personlige opplysninger:* hobby, relasjoner og andre opplysninger. *(disse er ikke en del av datainnsamling, men er en del av diskusjon)*	Sosial manipulasjon
Nettverk	*Nettverkstopologi*: IP, domener og underdomener, porter og status, OS osv. *Programdatavare og maskinvare*: oppdateringer, versjoner og sårbarheter	Penetrering av forsvar, hacking

Kommentar til Tabell 4: Dataene innsamlet gjennom OSINT-metode ble fordelt i to kategorier etter de teknikkene som brukes for å forårsake skade; sosial manipulasjon og penetrering av forsvar.

Dataanalyse og datareduksjon var en svært tidskrevende prosess, hovedsakelig på grunn av omfattende datagrunnlag og min manglende erfaring med analyse av OSINT-data. For erfarne granskere hadde det vært en mye lettere og mindre tidskrevende prosess. Figur 10 illustrerer prosessen for datainnsamling og analyse, samt datakilder og verktøy.

Figur 10: Datainnsamling - Prosess, kilder og verktøy



4.4. Kvalitetskriterier

4.4.1. Hvordan måles kvalitet i kvalitativ forskning?

All forskning vurderes mot ulike kvalitetskriterier. Kriteriene som vanligvis brukes innen det rasjonalistiske (naturvitenskapelige) paradigmet er intern og ekstern validitet, pålitelighet, generalisering og/eller objektivitet. I noen forskningsmiljøer eksisterer en overbevisning om at kvalitative studier generelt og digitale metoder spesielt er mangelfulle med hensyn til ovennevnte metodiske kvalitetskriterier (Blaikie & Priest, 2019; Fielding, Lee, & Blank, 2017; Snee, Hine, Morey, Roberts, & Watson, 2016; Guba & Lincoln, 1982).

Etter å ha gjennomgått en del litteratur som omhandler kvalitetskriterier i kvalitativ forskning, har jeg bestemt meg for at validitet, generalisering og pålitelighet ikke er passende konsepter i denne undersøkelsen. Corbin og Strauss (2015, s. 337) påstår at høykvalitets forskning er den som er interessant, klar, logisk, og får leseren til å tenke og ønske å lese mer. Det er forskning som har substans, gir innsikt og ikke bare er en gjentagelse av noe som er sagt/skrevet mange ganger før. Slik forskning konseptualiserer ved å gi tilstrekkelig beskrivende detalj, skriver forfatterne, for å la leseren komme til sine egne konklusjoner om dataene og bedømme troverdigheten til forskerens data og analyse.

Min personlig ambisjon med denne forskningen er å produsere noe som er kreativt i sin konseptualisering, som er nyttig og kan oppfordre til diskusjon, samtidig som den kan ha praktisk verdi og er forankret i data. Med andre ord, ønsker jeg å produsere forskning som er både vitenskapelig og kreativ. Jeg velger derav å etterstrebe kvalitetskriterier foreslått av Guba og Lincoln (1982, s. 246) og for oppnå disse bruker jeg prosedyrer foreslått av Creswell og Creswell (2018, s. 274–275).

4.4.2. Kvalitetskriterier i denne studien

Guba og Lincoln (1982, s. 246) foreslår fire alternative begreper som passer bedre i naturalistisk kvalitativ forskning. Disse kriteriene er sannhetsverdi (*true value*), anvendelighet (*applicability*), holdbarhet (*consistency*) og nøytralitet (*neutrality*). Sannhetsverdi innebærer hvordan man etablerer tillit til sannhet i funn som er innsamlet for en spesifikk studie. Anvendbarhet sier noe om i hvilken grad funnene kan anvendes i andre sammenhenger eller/og med andre respondenter. Holdbarhet avgjør om funnene fra en undersøkelse vil bli konsekvente

hvis forskningen blir replisert under de samme eller tilsvarende forhold. Med nøytralitet menes i hvilken grad funnene preges av forskers bias, personlige motivasjoner, interesser osv. (Guba & Lincoln, 1982, s. 246).

Troverdighet, som sidestilles av Guba og Lincoln (1982, s. 246) med «intern validitet», demonstreres best gjennom isomorfisme mellom data og fenomenene dataene representerer. Det vil si om dataene bærer sannsynlighetspreg sett i forhold til forklaringer av fenomenene. I denne studien kan dette kontrolleres ved å eksempelvis spørre deltakerne om deres realiteter har blitt representert på en riktig måte.

Creswell og Creswell (2018, s. 274–275) foreslår åtte forskjellige prosedyrer for å oppnå Guba og Lincolns kriterier. Disse inkluderer (1) «langvarig engasjement og vedvarende observasjon i felt», (2) «triangulering», (3) «bruk av fagfellevurdering eller debriefing», (4) «søk etter uoverensstemmende og/eller motstridende informasjon», (5) «klargjøring av forskers bias», (6) «deltaker-kontroll», (7) «fyldig og detaljert beskrivelse», og (8) «eksterne revisjoner». Fordelene ved triangulering er allerede diskutert i delkapittel 4.3. Jeg hadde ikke anledning til å bruke helt uavhengig «debriefer» i denne oppgaven. Med «debriefer» menes en «revisor» som ikke er kjent med forsker eller prosjekt og som har relevant kompetanse for å rette kritisk blikk mot teoretisk og metodisk fremgangsmåte. Videre avklares de prosedyrene som er brukt i oppgaven.

«Langvarig engasjement og vedvarende observasjon i felt»

Arbeidet med oppgaven startet allerede i september da jeg utarbeidet en skisse for prosjektet. De påfølgende månedene samlet jeg litteratur og ble medlem i ulike nettsamfunn dedikert til OSINT. Jeg tilbrakte derav nesten 10 måneder «i felt». Creswell og Creswell (2018, s. 275) skriver at ved å tilbringe lang tid «i felt» utvikler forskeren en inngående dyp forståelse av fenomenet som studeres og kan formidle detaljer om tema og deltakere som bidrar til studiens troverdighet. Jo mer erfaring en forsker får i løpet av et prosjekt, jo mer nøyaktige eller gyldige vil funnene være.

«Søk etter uoverensstemmende og/eller motstridende informasjon» og «Deltaker-kontroll»

Formålet med å søke etter informasjon som strider med hypoteser eller andre bevis er å øke studiens troverdighet (Creswell & Creswell, 2018, s. 275). En forsker kan oppnå dette ved å sette spørsmålstegn ved eksisterende paradigmer eller perspektiver.

Deltaker-kontroll og triangulering ble brukt med formål å søke etter slik uoverensstemmende og/eller motstridende informasjon. Triangulering var med på å kontroll-sjekke hvorvidt bevisene fra ulike kilder er konsistente. Formålet med deltaker-kontroll var å bekrefte nøyaktigheten av de kvalitative funnene og hvordan de er formidlet. Dette ble gjort ved å gi den endelige rapporten til (a) informantene for å bekrefte at deres erfaringer og informasjon er formidlet nøyaktig og riktig og (b) deltakerne for å forsikre at anonymiseringstiltak er tilstrekkelige. Deltakere og norsktalende informantene har fått mulighet til å kommentere og «godkjenne» oppgaven.

Jeg har i tillegg vurdert mine funn mot studier som har samme formål og hvor samme metode og liknende settinger ble brukt (se delkapittel 2.2.). Funnene i alle studier fremstår som konsistente, uten avvik som kan stamme fra metodiske valg. De forskjellene man finner har å gjøre med valg av studieobjekt, heller enn metodisk tilnærming.

«Klargjøring av forskers bias»

Det var svært viktig for meg å være objektiv og påvirke studiens resultater minst mulig. For å oppnå dette skal forsker reflektere over eget bias som kan være forårsaket av personlige verdier, bakgrunn osv. og hvordan disse aspektene påvirker ens fortolkninger, foreslår Creswell & Creswell (2018, s. 334). Refleksiviteten, ifølge forskere, skal bidra til en åpen og ærlig fortelling som vil resonere godt med leserne (Blaikie & Priest, 2020; Creswell & Creswell, 2018). I denne studien var min manglende kunnskap om tema til fordel for å sikre at mine formeninger eller bakgrunn ikke påvirker resultater og fortolkninger. Jeg har basert datainnsamling utelukkende på teori og data fordi jeg rett og slett ikke hadde erfaringer, tilstrekkelig kompetanse eller egne meninger om fenomener under studiet. At temaet var nytt og ukjent bidro, etter min mening, til relativ nøytralitet fra min side.

«Fyldig og detaljert beskrivelse»

Creswell og Creswell (1998, s. 274) argumenterer også for at forskningen skal inkludere en «fyldig» beskrivelse når det gjelder representasjon av funn. Med dette menes at beskrivelser av funn bør være så detaljert som mulig, for å skape interesse og bidra til at resultatene blir mer realistiske som i sin tur vil øke forskningens «kvalitativ validitet». Fra starten var formålet med oppgaven å gi en mer detaljert forklaring av et fenomen som de aller fleste kjenner til på et overfladisk nivå. Min ambisjon er å formidle noen tekniske konsepter og beskrivelser til lesere som har en annen faglig bakgrunn enn teknisk. Informanter fremhevet hvor viktig er det å

formidle denne informasjonen til «folk som er redd for tech». Senere i prosessen har jeg fått beskjed fra en av informantene at jeg har brukt «gode formuleringer» og at det var «forfriskende å lese om temaet på norsk».

Avslutningsvis kan man si at forskningens troverdighet indikerer at funnene er pålitelige og troverdige ved at de gjenspeiler deltakeres og forskers erfaringer med fenomener. Samtidig må man huske at studier som denne, eksplorative og baserte på abduksjon, bare gir en av mange mulige tolkninger av funn og fenomener.

Internett-forskning og holdbarhet

Holdbarhet avgjør om funnene fra en undersøkelse forblir konsekvente hvis forskningen repliseres under samme eller tilsvarende forhold (Guba & Lincoln, 1982, s. 246). En faktor som er særegen for bruk av Internett som datakilde, er at oppdatering av nettsteder og digitale applikasjoner gjør data ustabile. Dette utfordrer datakvaliteten når det gjelder nøyaktighet og konsistens. Det finnes imidlertid et virkemiddel som kan løse dette problemet. Wayback Machine er et digitalt arkiv for World Wide Web som gir bruker mulighet til å gå «tilbake i tid» og se hvordan websider så ut tidligere (Internet Archive, 2021).

Et annet grep for å styrke studiens holdbarhet er bruk av såkalte «test-retest» og «inter-method» som vanligvis refererer til reliabilitet-konseptet (Dawson, 2020, s. 258). Jeg har brukt flere verktøy med samme funksjoner for å kompensere for eventuelle svakheter ved enkelte verktøy. For nettverksskanning har jeg brukt syv ulike verktøy som samler den samme type informasjon, for å sikre at man får så mange unike funn som mulig. Noen av verktøyene har bredere bruksområde, men de grunnleggende funksjoner er like. Verktøyene skanner offers nettverk og returnerer informasjon om IP-adresser, DNS, MAC-adresser, port og deres status osv. Noen datainnhentinger har jeg utført to ganger for å sammenligne resultatene. For å styrke holdbarheten ytterligere har jeg beskrevet prosess og metodisk tilnærming så detaljert som mulig, hensyntatt oppgavens begrensninger. Verktøyene beskrives i delkapittel 5.1.

Overførbarhet

Jeg har tidligere nevnt at funnene fra denne studien ble sammenlignet med funn i studier som har samme formål og hvor samme metode og liknende settinger ble brukt. Jeg konkluderte med at forskjeller i hva slags informasjon forskere har innsamlet kan sannsynligvis stamme fra valg av bransje som ble studert. Her drøfter jeg dette mer inngående.

Mitt forskningsprosjekt er avgrenset til én sektor og undersøker to organisasjoner av ulik størrelse. I slike studier vil man vanligvis ikke påberope seg høy grad av overførbarhet og påstå at funnene fra en så liten studie kan generaliseres til andre sektorer og organisasjoner. Min konklusjon er ikke så entydig. På bakgrunn av empiri og tidligere forskning vil jeg argumentere for at (a) funnene kan generaliseres i en viss grad på tvers av sektorer og (b) funnene ikke kan generaliseres til alle organisasjoner da det eksisterer forskjeller mellom organisasjoner av ulik størrelse i ulike bransjer.

Dette kan fremstå som motstridende konklusjon og derfor krever avklaring. Empirien viser at på tvers av bransjer kan funnene generaliseres i en viss grad. Vi kan påstå at alle organisasjoner er eksponert i mindre eller store grad. Videre kan vi påstå at trusselaktører bruker de samme teknikkene uavhengig av hvilken organisasjon de kartlegger. Dette kan sannsynligvis forklares med at digitaliseringen visket ut de store forskjellene mellom ulike sektorer. Eksempelvis både i industri og i forskning er flest operasjoner digitalisert og automatisert, som innebærer en stor grad av eksponering. Det som ikke kan generaliseres er i hvilken grad er organisasjoner av ulik størrelse eksponert. I min studie har jeg funnet betydelig mer informasjon om Organisasjon A, enn om Organisasjon B. NVEs studie som undersøkte strømleverandører viser derimot at jo mindre er en organisasjon, desto mer er den eksponert. Altså, typer informasjon jeg har funnet om utvalgte organisasjoner er konsistent med funnene i tidligere studiene (Hayes & Cappa, 2018; Matvej et al., 2020; NVE, 2019). Samtidig eksisterer det store forskjeller for i hvilken grad er de små og de store organisasjoner i ulike bransjer eksponert.

4.5. Etiske vurderinger

Fra oppstarten var studien preget av flere etiske dilemmaer og vurderinger knyttet til bruk av OSINT-metode med forsknings formål.

Bruk av OSINT som datainnsamlingsmetode er lite dokumentert i Norge. Enhver som innhenter og bruker åpen tilgjengelig informasjon, bærer selv ansvaret for å vurdere praksisens etiske problemstillinger. I utgangspunktet kan slik informasjon samles uten tillatelse. Når det gjelder bruk av data for forskningsformål og påfølgende publisering av funnene, er det imidlertid ikke så enkelt. Rønn og Søye (2019, s. 2) stiller spørsmålstegn ved følgende: under hvilke omstendigheter er det moralsk tillatt for forskeren å bruke åpen tilgjengelig informasjon, selv om formålet er å bidra til samfunnssikkerhet? Jeg opplevde at det er vanskelig å finne noe

konkret informasjon om retningslinjer som omhandler innsamling av åpen tilgjengelig informasjon. Derfor tok jeg utgangspunkt i generelle prinsipper for etisk forsvarlig forskning, samt eksisterende lover som omhandler informasjonssikkerhet.

Samfunnsforskere må balansere mellom de forventede fordelene med forskningen og potensialet for psykologisk, sosial, politisk, økonomisk eller juridisk skade den kan forårsake (Blaikie & Priest, 2019). Blaikie og Priest (2019, s. 55) presenterer sentrale etiske prinsipper som gjelder studieobjekter og deltakere, herunder frivillig deltakelse, informert samtykke, frihet til å trekke seg, rett til personvern, beskyttelse mot skade og risiko, unngåelse av datamanipulasjon og unngåelse av skjult forskning.

Organisasjoners deltakelse i denne studien var frivillig og ansvarlige har signert samtykkeerklæring (se Vedlegg A). De var muntlig informert om at de har rett til å trekke seg. Jeg har tatt grep for å anonymisere virksomhetene og nøkkelpersoner mest mulig. Videre har vi avtalt at ledere som signerte samtykkeskjema vil kunne lese empiri- og analyse-del før oppgaven er levert. Dette for å sikre at informasjonen presentert i oppgaven ikke vil skade virksomhetene og at anonymiseringstiltak er tilstrekkelige.

Jeg har imidlertid møtt en del andre utfordringer. For det første var det ikke så enkelt å registrere oppgaven i NSD i starten av prosjektet. Dette fordi jeg ikke visste på forhånd hva slags data jeg vil finne. Jeg bestemte meg tidlig for å ikke samle personlige data, og da er det ikke nødvendig med registrering av prosjektet. Senere i prosessen oppdaget jeg at selv om jeg ikke søkte på personers navn, fant jeg noen dokumenter som inneholdt personlige data. Dette fordi ansatte har brukt virksomhets e-postadresser i private sammenhenger. Disse, sammen med omfattende passord database jeg fant på Dark Web, medførte at det var nødvendig å registrere oppgaven hos NSD. Rådgiver fra NSD hadde ikke kjennskap til OSINT, som førte til en periode med aktiv korrespondanse for å avklare alle forhold rundt datainnsamling. Til slutt fikk jeg tillatelse til å bruke dataene slik jeg gjør i denne oppgaven.

Den andre etisk vurdering av stor betydning, omhandlet hvorvidt jeg bør informere virksomhetene om passord lekkasjer. Passord som ligger i åpen tilgang på World Wide Web og Dark Web er tilgjengelig for allmennheten. Ifølge lov tilhører e-postadressene og passord hver enkelt person og ikke virksomheten (Datatilsynet, u.å.). Derav ble det besluttet at å overgi databaser til ledelsen ikke er forsvarlig. Isteden vil jeg informere organisasjonene på generelt grunnlag, det vil si opplyse ledelsen om at bruk av jobb e-post i private sammenhenger samt

tendens til svake passord representerer sårbarhet for organisasjonen. På denne måten vil organisasjonene få mulighet til å iverksette opplæringstiltak, samtidig som personvern bevares. Videre måtte jeg vurdere om hver enkelt person skal informeres om at deres passord er offentlig tilgjengelig. Det ble besluttet å ikke informere hver enkelt ansatt, men heller insistere på at ledelsen gir informasjon om at ansatte selv bør sjekke om deres personlige data er offentlig tilgjengelig. Kjennskap om at en ukjent masterstudent har tilgang til ens personlige data kunne medføre psykologisk ubehag for de enkelte og jeg ville naturligvis unngå det. Alle dataene som faller under «personlige opplysninger» ble slettet umiddelbart etter dataanalyse. NSD har bekreftet dette å være beste løsning i forskningsøyemed.

Hovedmålet med oppgaven er å rette oppmerksomhet mot hvordan vi eksponerer oss på Internett og hvordan det utgjør sårbarhet på alle nivåer. Den vanskeligste oppgaven her var tiltak for å beholde balanse mellom forskningshensyn og persondatavern. Derfor presenterer jeg ikke bilder av alle funn, eller andre bevis som kan spores tilbake til konkrete personer og organisasjoner.

4.6. Metodiske begrensninger

Oppgaven ikke gjengir data som viser hvor mye informasjon som kan samles inn om et individ, er en begrensning ved denne studien. Svaret på det andre forskningsspørsmålet, *hvilken informasjon om de utvalgte virksomhetene kan man finne ved hjelp av rekognoseringsteknikker og OSINT*, blir derav ikke fullkomment. Sosial manipulering er et svært effektivt virkemiddel for å anskaffe sensitiv informasjon og dermed hovedmålet for trusselaktører. Beslutningen om å ikke hente inn persondata beror på etiske vurderinger.

En del funn diskuteres med utgangspunkt i teori og ikke empiri. Etiske retningslinjer og lover er hovedårsak til det. Jeg har funnet flere passord til e-post kontoer, men ikke forsøkt å få tilgang til kontoene, som kunne demonstrert at det er mulig. Jeg har heller ikke forsøkt å endre data eller bruke verktøy for passordgjetting for å få tilgang til andre tjenester som er åpne for pålogging. Det hadde vært ikke bare umoralsk, men også ulovlig. Jeg vil allikevel påpeke at det hadde ikke vært et problem for en trusselaktør.

Kompetanse og ferdigheter er avgjørende for hvor mye informasjon man finner. Det er vanskelig å si noe om det foreligger mer informasjon om organisatoriske forhold enn den som er presentert i oppgaven. Det er stor sannsynlighet for at en mer ressurssterk aktør vil kunne

innhente mer sensitiv informasjon på kortere tid, særlig om de tekniske og menneskelige elementene. Men for meg var det viktig å demonstrere at selv en med begrensede kunnskaper og teknisk kompetanse kan innhente en del informasjon som vil være av betydning i forberedelsen av cyberangrep.

5. Empiri og analyse: Hvordan kartlegges organisasjoner?

I dette kapittelet presenteres funn som er kommet frem ved bruk av OSINT-metodikk, dokumentstudiet og intervju med informantene. Funnene danner grunnlag for å besvare første del av oppgavens problemstilling:

Hvordan kartlegger trusselaktører organisasjoner?

Kapittelet er delt i fire deler. Først demonstreres *hvordan digital rekognosering av organisasjoner fungerer i praksis*. Dernest redegjøres for *hvilken informasjon om de utvalgte virksomhetene kan man finne ved hjelp av rekognoseringsteknikker og OSINT*. Videre forklares *hvorfor denne type informasjon er av interesse for en trusselaktør*. Delkapittelet 5.4 oppsummerer funnene.

5.1. Hvordan fungerer digital rekognosering av organisasjoner i praksis?

I delkapittel 3.1.3 introduserer jeg en teoretisk modell som beskriver rekognoseringsprosessen. Modellen er utarbeidet på bakgrunn av MITRE-rammeverk (se Figur 4). I denne delen av oppgaven redegjør jeg for hvordan prosessen kan foregå i praksis, herunder hvilke verktøy og teknikker som kan brukes og hvilken informasjon som er av interesse for en trusselaktør. Både intervjuene, dokumentanalyse og OSINT danner empirisk grunnlag for dette delkapittelet. Bilder er brukt for å skape bedre forståelsen for selve prosessen.

Informasjon innsamlet gjennom intervjuer var til hjelp i planlegging av rekognoserings-prosessen og etablering av infrastruktur, herunder valg av operativt system (videre OS) og OSINT-verktøy. OSINT-metodikken er brukt for å illustrere hvordan prosessen kan skje i praksis. Jeg beskriver de enkelte verktøyene og teknikker som er brukt i denne studien. Tabell 8 i Vedlegg B presenterer mer detaljert oversikt over brukte verktøy og deres egenskaper. Resultater av dokumentanalyse (Tabell 9 i Vedlegg D) er brukt for å sammenligne rekognoseringsprosessene i de ulike angrepene, samt belyse ulike tilnærminger og verktøy.

5.1.1. Etablering av den tekniske infrastrukturen

Både intervjuene og dokumentanalyse viser at en hypotetisk trusselaktør vanligvis starter rekognosering av et mål med å enten etablere infrastruktur for datainnsamling og/eller gjennomføre manuell rekognosering (Berman, 2018; CE1; CE2; CE3; Coville, 2020; Oliver & Shields, 2018; Stretch, 2017). Da det ikke fremgår klart fra alle dokumenter, kan man anta at en erfarne trusselaktører allerede har en del infrastrukturen klar til bruk fra tidligere.

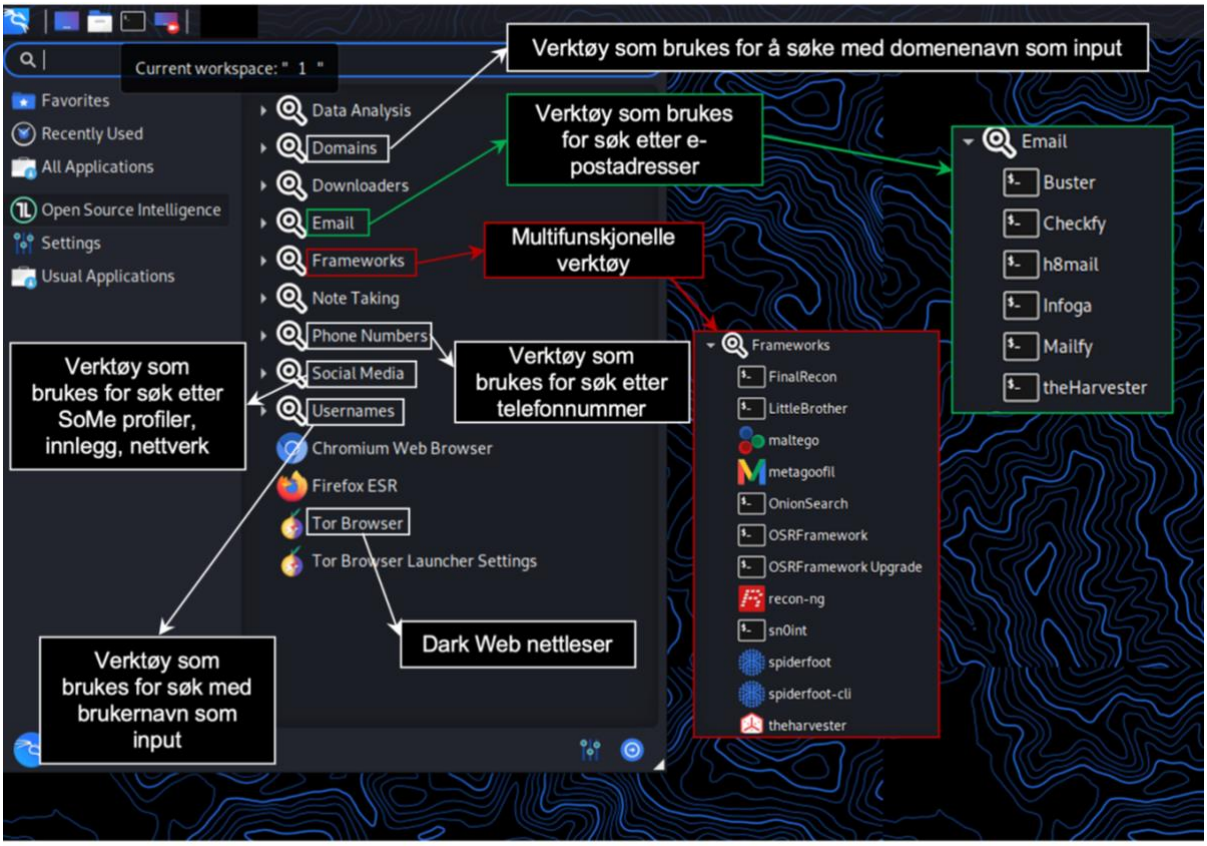
Intervjuene og dokumentanalysen viser at denne fasen innebærer opprettelse av fiktive identiteter og den tekniske infrastrukturen, herunder servere, domener, kryptovaluta, e-postkontoer, sosiale mediekontoer og andre nettbaserte tjenester (CE1; CE2; ClearSky Cyber Security ltd, 2021, s. 9; Coville, 2020, s. 7, pkt. 12; Oliver & Shields, 2018, s. 21, 126, 134; Stretch, 2017, s. 9). Formålet med den tekniske infrastrukturen er blant annet å sikre anonymitet på Internett og skjule spor for å ikke oppdages av politi eller offer (Berman, 2018; Coville, 2020; Oliver & Shields, 2018).

I denne studien besto den tekniske infrastrukturen i opprettelse og bruk av (a) en isolert datamaskin som var nullstilt til standard innstillinger, (b) fiktive brukerkontoer for bruk av tjenester som krever pålogging og (c) VPN-tjenesten. Hensikten er å sikre anonymitet og unngå påvirkning av resultat ved datainnsamling. Mer om dette fremgår i delkapittel 4.2.1.

Ifølge informanter bruker trusselaktører gjerne operativsystemet Linux med Kali distribusjon[4]. Det er godt egnet til installering av ulike verktøy som brukes for rekognosering av et mål, samt hacking av et nettverk (CE1; CE2; CE3). Det er tre typer verktøy som er brukt i denne studien: (a) programvare som lastes ned og installeres på datamaskin, (b) skript, eller kode, som lastes ned og brukes fra kommandolinje og (c) verktøy som installeres på nettleseren. Verktøyene som brukes fra kommandolinjen kan lastes ned fra utviklingsplattformen GitHub. Slike utviklingsplattformer muliggjør nedlasting av verktøy for rekognosering, skanning eller/og hacking, uten verken kostnader, programmeringserfaring eller avanserte tekniske ferdigheter. GitHub er størst og mest avansert, hvor millioner av utviklere bygger og vedlikeholder programvarene sine (GitHub, 2021). Det er fra GitHub jeg har lastet ned verktøyene brukt i denne studien. Bilde 1 viser arbeidsflate på datamaskin som er brukt i undersøkelsen og innholdet i noen av fanene.

[4] En linuxdistribusjon er et operativsystem sammensatt av flere programvarer. Distribusjonene er tilgjengelig for flere system, og kan som regel lastes ned fra internett.

Bilde 1: Linux Kali med ulike verktøy for rekognosering på et mål



Dokumentanalyse viser videre at falske identiteter og brukerkontoer hovedsakelig brukes til passiv rekognosering, personellprofilering og påfølgende målrettede nettfisking-kampanjer. For eksempel «GRU hackers» og «Silent Librarian»-gruppen opprettet flere e-postadresser som imiterte adressene fra tjenestetilbydere eller kollegaer til potensielle ofre (Coville, 2020, s. 15, 45; Hassold, 2018b, s. 4). «GRU-hackers» brukte blant annet en avsender-konto som imiterte navnet til President Macrons pressesekretær for å sende e-poster med infiserte Google Docs lenker til ca. 30 partimedlemmer (Coville, 2020, s. 15). «Silent Librarian»-gruppen brukte ulike kontoer som var tilpasset mottakere i ulike land. Park et al. brukte en mer kompleks alias-infrastruktur for sine angrep. De opererte med ca. 30 ulike e-postadresser og kontoer som ble brukt i ulike angrep (Oliver & Shields, 2018, s. 134).

Etablering av teknisk infrastrukturen kan bestå av både relativt enkle og mer avanserte tiltak. Hvilken infrastruktur som etableres vil avhenge av formålet. For eksempel registrerte «GRU hackers» domenenavn og opprettet nettadresser som var utformet for å «spoofe», det vil si etterligne, de legitime nettstedene som ofrene var kjent med. Herunder e-post-påloggingssider, fildelings- og lagringstjenester, nettsider for tilbakestilling av passord mm.. I forbindelse med

sine aktiviteter rettet mot OL 2018 etablerte de et underdomene[5] som etterlignet et nettsted tilhørende Microsoft, og et underdomenet[6] som etterlignet et nettsted tilhørende det koreanske Landbruksdepartementet, MAFRA (Coville, 2020, s. 26). De brukte domenenavnene i nettfisking-kampanjer mot organisasjoner og enkeltpersoner tilknyttet vinter-OL 2018 (Coville, 2020).

Dokumentstudiet viser at i noen tilfeller er passiv rekognosering et nødvendig første steg før trusselaktørene etablerer infrastruktur. For eksempel etablerte ikke «Silent Librarian»-gruppen infrastrukturen i den initiale fasen. De startet med passiv manuell digital rekognosering av universitetsprofessorer, herunder profilering av vedkommendes biografi, forskningsinteresser og publiserte artikler (Berman, 2018, s. 3, pkt. 4a). Deretter etablerte de teknisk infrastruktur tilpasset de enkelte universitetene og organisasjoner (Berman, 2018, s. 3; Hassold, 2018a; 2018b, s. 4).

5.1.2. Organisasjonskartlegging

Både intervjuene og dokumentanalyse viser at etter å ha etablert den tekniske infrastrukturen, vil en trusselaktør starte innsamling av åpen tilgjengelig informasjon om en mål-organisasjon ved hjelp av OSINT (Berman, 2018, s. 3; CE1; CE2; CE3; Coville, 2020, s. 6–40; Hassold, 2018b, s. 4; Oliver & Shields, 2018, s. 19, 140, 171; Stretch, 2017). Formålet er å samle mengder av relevante data, som ved analyse vil gi mulighet til å skissere organisasjonens profil. Herunder virksomhetenes fysiske lokalisering, forretningsrelasjoner, pågående, planlagte og avsluttede prosjekter osv. (CE1; CE2; CE3). For å effektivisere prosessen og få mest mulig informasjon kan man benytte flere verktøy i tillegg til manuelle søk i søkemotorer og databaser.

Generelt initierende søk

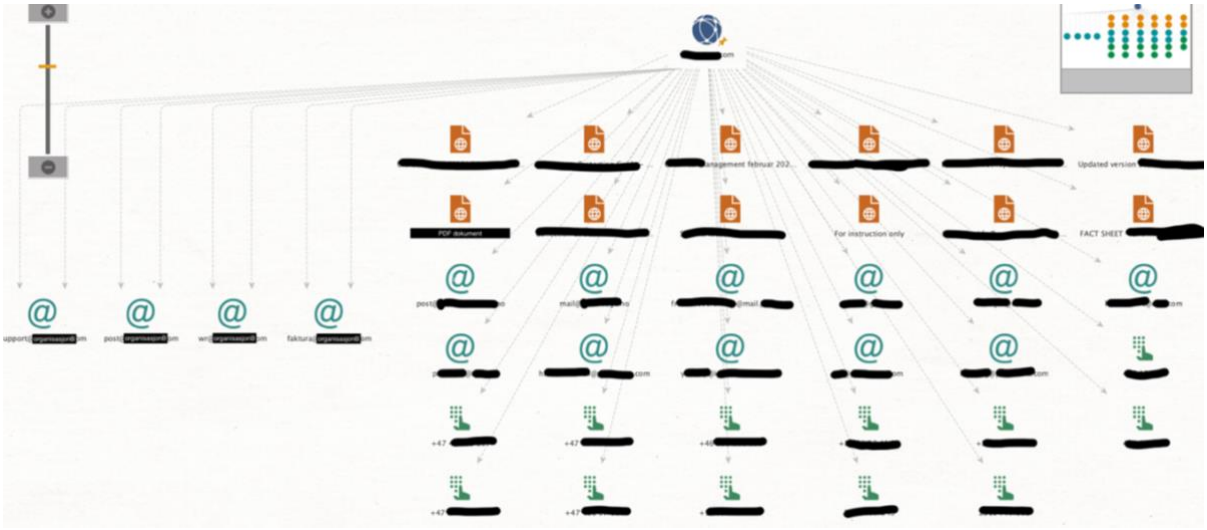
Vanligvis starter man med manuelt søk i ulike søkemotorer. Man bør bruke ulike søkemotorer fordi hver enkelt gir delvis forskjellige resultater, sier CE1. Eksempelvis er Yandex rettet mot russisktalende brukere, mens Bing er optimalisert for kinesisk publikum. Dette er også bekreftet i min studie. Etter vanlig søk i ulike søkemotorer (Bing, DuckDuckGo, Yahoo, Yandex) og granskning av organisasjonenes nettsider, iverksatte jeg mer målrettet søk med bruk av Google Dorks operatører. Operatører er kombinasjoner av søkeord og tegn som hjelper

[5] www.msrole.com/office_conf
[6] mafra.go.kr.jeojang.ga

brukere å gjennomføre avgrenset søk etter spesifikk type data, eksempelvis visse typer filer, åpne FTP-tjenere eller webkameraer. Google Dorks-listen 2020 kan avdekke informasjon om e-postadresser, pålogging-autentifikatorer, filer med sensitive opplysninger, tekniske sårbarheter, finansiell informasjon osv.

Etter anbefaling fra CE1 og CE3 benyttet jeg Maltego, som er et godt egnet verktøy til både personprofilering og organisasjons- og nettverkskartlegging. Maltego-applikasjonen er et analytisk rammeverk optimalisert for visualisering av søkeresultater (Maltego Technologies, 2021). Verktøyet tilbyr sanntids datautvinning og informasjonsinnhenting, samt representasjon av denne informasjonen i form av grafer, som viser relasjoner og forbindelser mellom en organisasjon og omgivelser.

Bilde 2: Resultater av et søk på Organisasjon B med Maltego



Kommentar til Bilde 2: Som input er Organisasjons B domene brukt (www.organisasjonB.com). Gjennomføringstid ca. 5 sekund.

Bilde 2 viser resultater av søk med Maltego hvor domene tilhørende Organisasjon B er brukt som søkeord. Denne grafen viser utvalgte e-postadresser, dokumenter, samarbeidspartnere, telefonnummer og e-postadresser tilhørende tredjeparter. Resultater av søk vil avhenge av input og innstillinger angitt av brukeren. Færre filtre gir mer omfattende graf og motsatt. Alternativer på input er presentert i Vedlegg C.

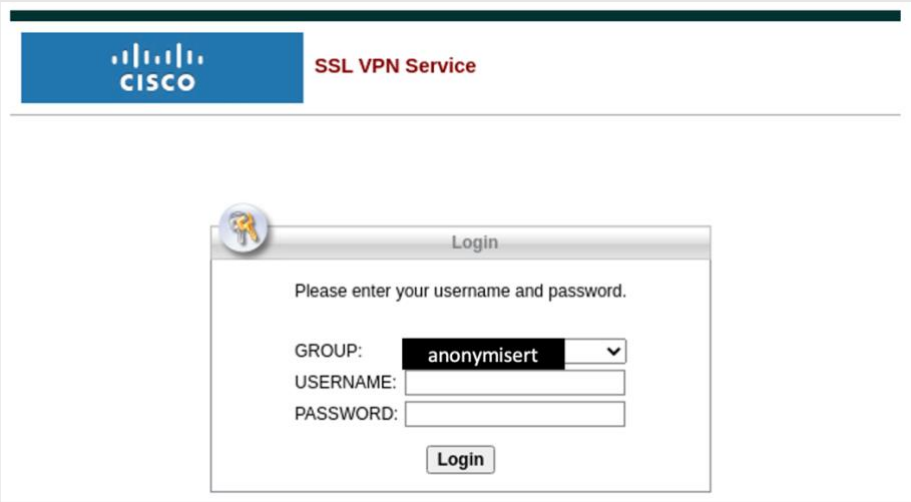
På anbefaling fra informantene brukte jeg verktøyet theHarvester til innsamling av informasjon om e-poster, tidligere og nåværende ansatte og deres roller, LinkedIn kontoer mm. (Martorella, 2011/2021). Bruk av theHarvester avdekket blant annet en mulighet for innsamling av data fra LinkedIn uten å gå på personlige profiler og derav uten å etterlate spor. Det er grunn til å tro at

GRU-hackers brukte theHarvester eller lignende i forberedelser av angrep på vinter OL-2018 (Coville, 2020, s. 34-35).

Audiovisuelle data og metadata

Dernest iverksatt jeg søk og innsamling av audiovisuell data. Ifølge CE1 er dette en viktig del av rekognoseringsprosessen, da bildene kan avdekke mye informasjon om utstyr og sikkerhetsbarrierer. Bilder ble innsamlet både manuelt og ved hjelp av verktøyet Gowitness (SensePost, 2017/2021). Gowitness skanner nettsider, henter inn skjermbilder fra underdomener og lagrer de på brukerens datamaskin (se Bilde 3). Dette effektiviserer søk etter påloggingssider som er åpne for Internett. Ved hjelp av manuelt søk i SoMe fant jeg en rekke bilder og videoer som etter analyse har gitt noen interessante funn som diskuteres videre.

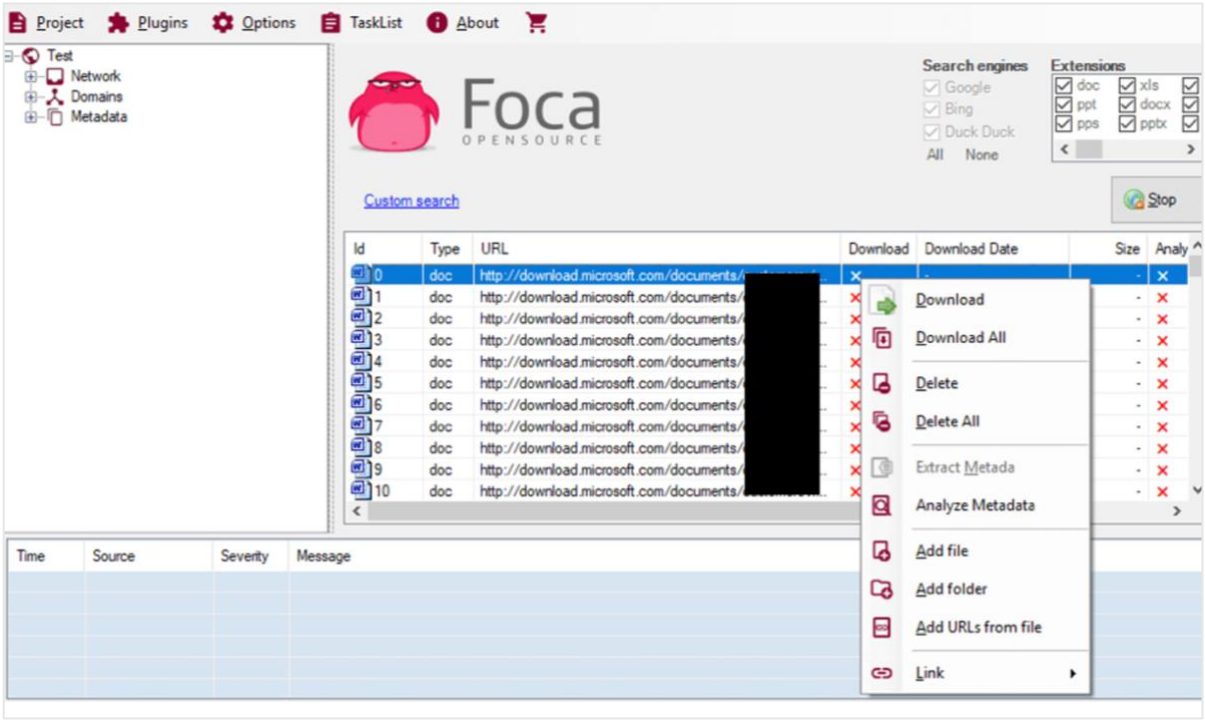
Bilde 3: Eksempel på output fra Gowitness



Kommentar til Bilde 3: Skjermbilde som er innhentet og lagret gjennom Gowitness. Bildet viser en påloggingsside som er åpen for Internett. Dette kan brukes av en trusselaktør for å forsøke å logge seg på ved hjelp av annen innsamlet informasjon.

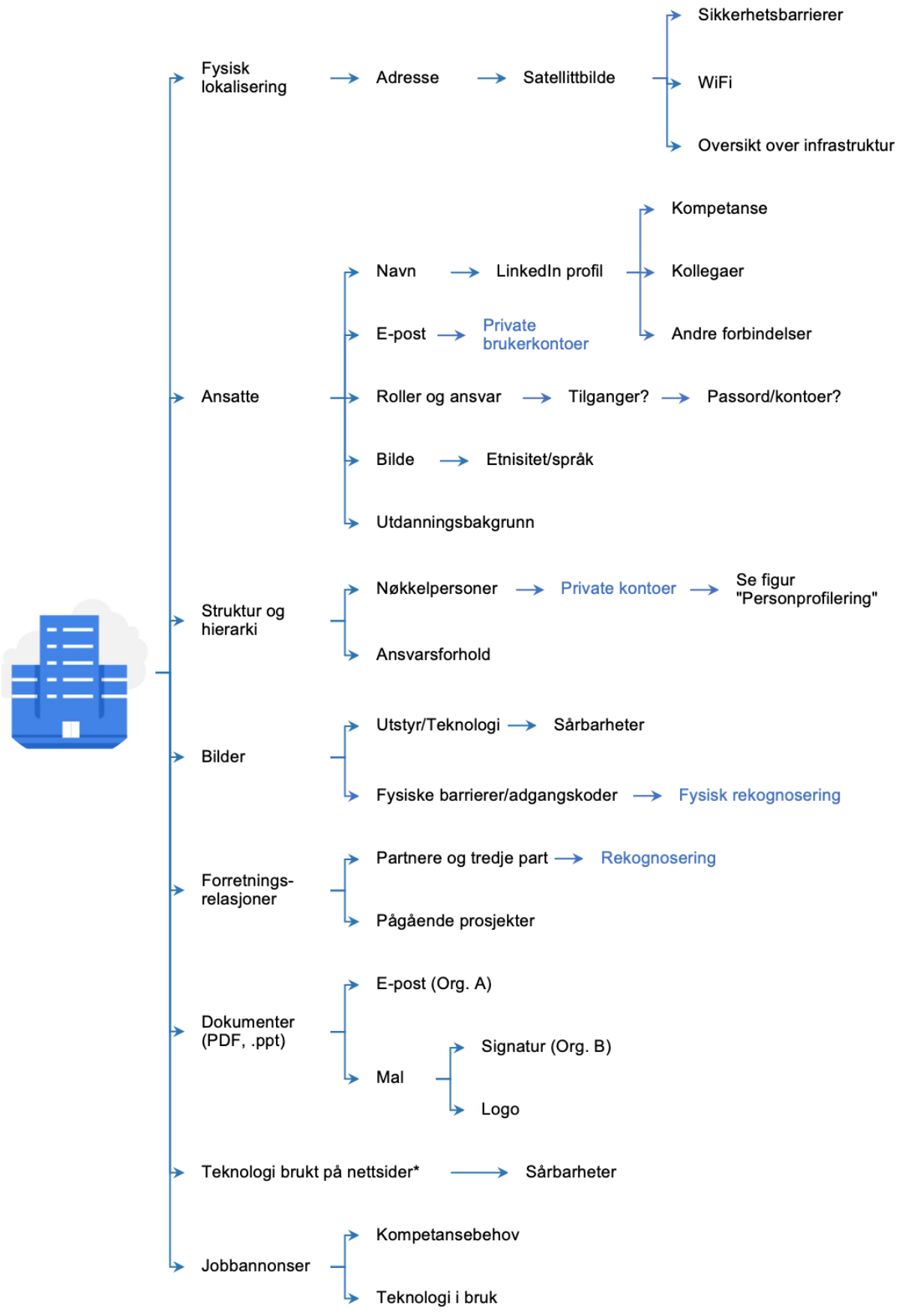
Videre brukte jeg FOCA (Fingerprinting Organisations with Collected Archives) - et verktøy som finner dokumenter og tilhørende metadata og skjult informasjon i dokumenter, herunder Microsoft Office- eller PDF-filer (ElevenPaths, 2021). Dokumentene søkes automatisk ved hjelp av tre mulige søkemotorer: Google, Bing og DuckDuckGo. Et søk vil vanligvis resultere i mange filer som videre analyseres og sammenlignes av programvaren. Etter analysen trekker FOCA slutninger om for eksempel hvilke dokumenter som er opprettet av samme team, hvilke servere og klienter som er brukt osv. (ElevenPaths, 2021). FOCA er enkelt å bruke, det kreves ikke førkunnskaper (se Bilde 4).

Bilde 4: Skjermbilde av FOCAs brukersnitt



Figur 11 oppsummerer datainnsamlingsprosessen hvor organisasjon A og Bs nettsider var utgangspunkt for bruk av ulike verktøy og teknikker. Blå farge er brukt for å markere elementer som er ikke en del av studien.

Figur 11: Organisasjonskartlegging - prosess



5.1.3. Personellprofilering

Informasjon samlet i første fase brukes videre for å kartlegge organisasjonens nøkkelpersonell. Ifølge informanter og dokumentanalyse er personprofilering det viktigste elementet i enhver rekognoseringsprosess (Berman, 2018; CE1; CE2; CE3; Coville, 2020; EH1; EH2; Oliver & Shields, 2018; Stretch, 2017). Med nøkkelpersonell menes personer med tilgangsrettigheter, som er av stor interesse for en trusselaktør. Herunder ledelse, teknologi-eksperter, forskere, IT-personell, økonomi-personell, ansvarlig for anskaffelser og sikkerhet mm. (Berman, 2018; CE1; CE2; Coville, 2020).

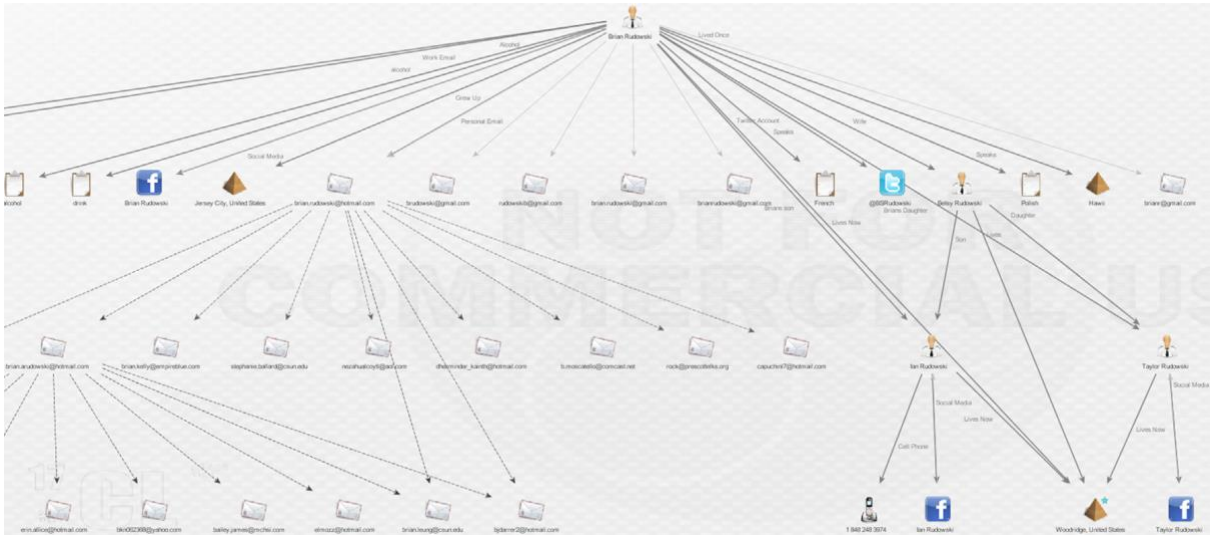
Dokumentanalyse viser at personprofilering var et sentralt element i operasjoner for både «GRU-hackers», «Silent Librarian»-gruppen, Park et al. og Dokuchaev et al. -saken. Sistnevnte er særlig interessant, da gjerningsmennene fokuserte på private e-postadresser og ikke bare profilerte nøkkelinformanter, men også deres familiemedlemmer, blant annet ektefeller (Stretch, 2017, s. 10, 16). «GRU hackere» profilerte ulike grupper personer avhengig av mål. I angrepet på ukrainske myndigheter og selskaper fokuserte de på IT-personell, kollegaer og kontaktpersoner hos leverandører, mens i angrepet på Macrons valgkampanje profilerte de kjente journalister, presse-sekretæren til President Macron og enkelte partimedlemmer (Coville, 2020, s. 11–23). Hele operasjonen gjennomført av «Silent Librarian»-gruppen var rettet mot universitetsprofessorer og personer med tilgang til forskning som var av interesse for trusselaktørene (Berman, 2018).

Andre kategorier ansatte som er av interesse for trusselaktører er nyansatte, vikarer, praktikanter og/eller generelt alle som tilhører såkalt Generasjon Z og «babyboomers» (CE1). Årsaker til det diskuteres i delkapittel 5.2. Man kan finne nyansatte og praktikanter ved å søke etter `#førstedag, #internship, #nyjobb, #firstday` og lignende i kombinasjon med organisasjonens navn.

En trusselaktør vil interessere seg for all personlig informasjon om disse kategorier av ansatte, herunder navn, alder, brukerkontoer, venner, familiemedlemmer, hobby, favoritt steder, fakta om vedkommendes fortid og lignende (CE1). Personsøk gjennomføres ved hjelp av manuelle søk i søkemotorer, SoMe, Dark Web, pastebin-nettsider og ulike databaser. Maltego er også et svært effektivt verktøy for personsøk. Resultater av søk vil se ulike ut avhengig av innstillinger eller filtre for søk. Verktøyet muliggjør kartlegging av en persons tilstedeværelse på Internett, som kan inkludere brukerkontoer på sosiale medier, personlig tilknytning til andre mennesker

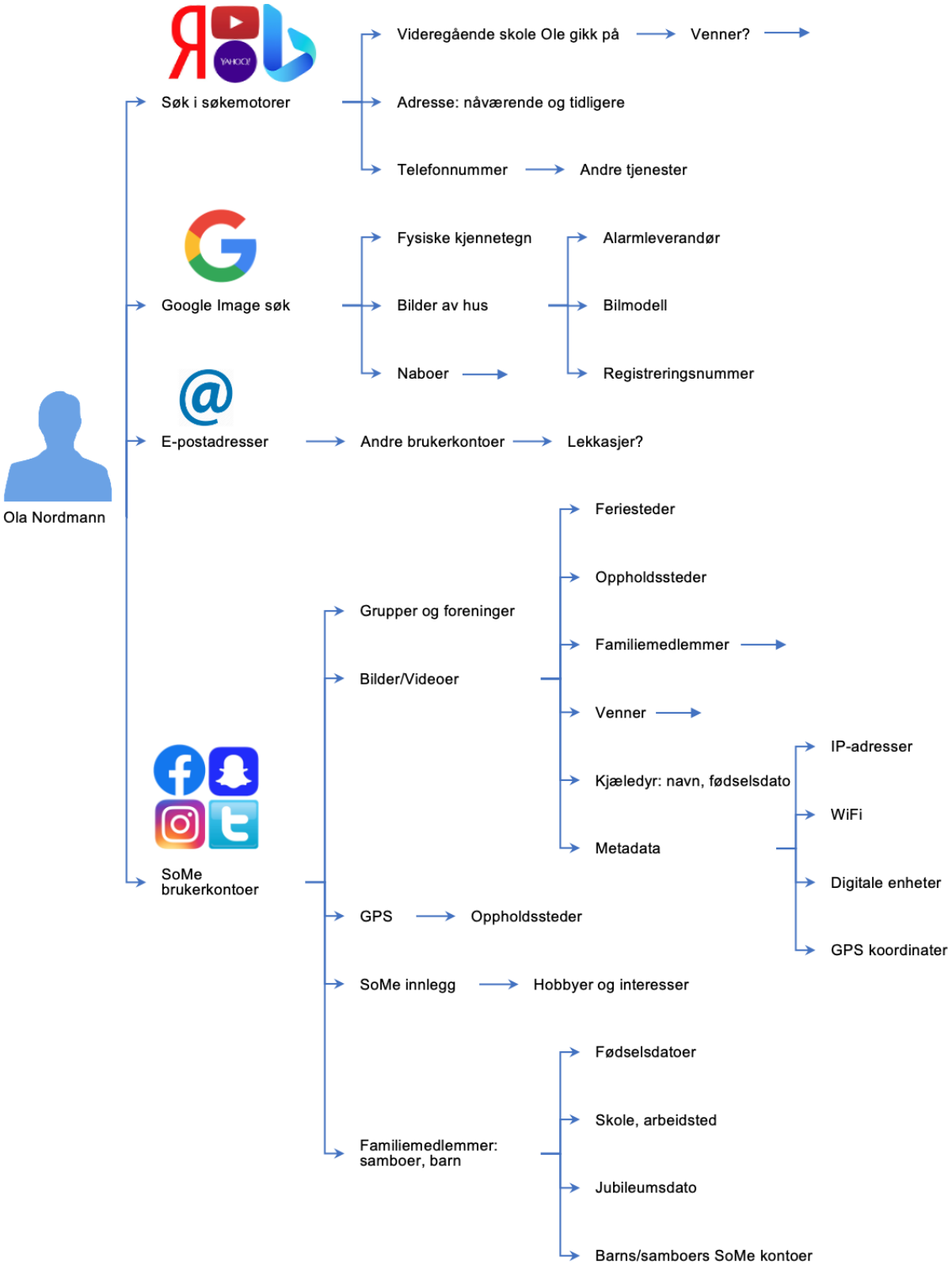
av interesse osv. (Maltego Technologies, 2021). Bilde 5 illustrerer et eksempel på hvordan resultater av personprofilering med Maltego kan se ut. For å eksemplifisere har jeg lånt et bilde fra Hayes og Cappa (2018, s. 692) sin artikkel. Dette fordi jeg selv har ikke gjennomført denne delen av rekognoseringsprosessen.

Bilde 5: Resultater av personprofilering med Maltego (Hayes & Cappa, 2018, s. 692)



Et hypotetisk forløp av personprofilering er illustrert i Figur 12.

Figur 12: Personprofilering - prosess

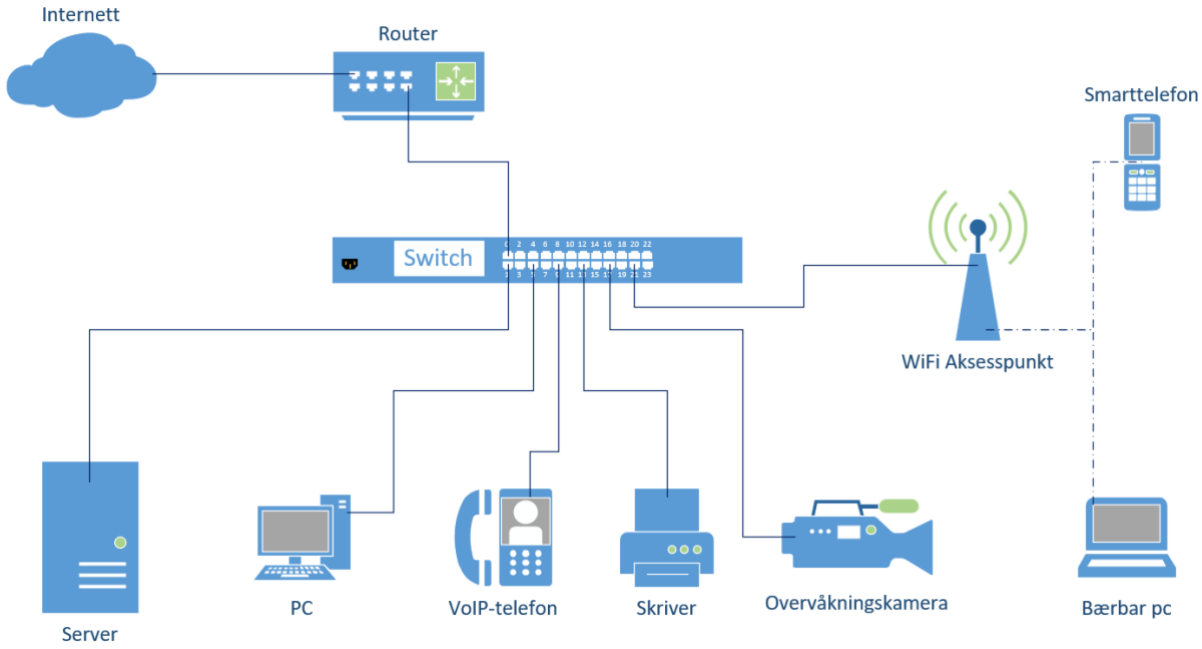


5.1.4. Kartlegging av teknisk infrastruktur og utstyr

Både dokumentstudiet og intervjuene viser at etter kartlegging av personer og organisatoriske forhold starter en trusselaktør vanligvis med nettverkskartlegging (Berman, 2018; CE1; CE2; CE3; Coville, 2020; EH1; EH2; Oliver & Shields, 2018). I noen tilfeller starter trusselaktører direkte med denne fasen, som eksempelvis Fathi et al., «Pawn Storm» og «Lebanese Cedar» APT-gruppene (Bharara, 2016; ClearSky Cyber Security ltd, 2021; Hacquebord, 2020).

Nettverkskartlegging er en aktiv del av rekognoseringsprosessen som innebærer teknikker som offerets sikkerhetsbarrierer potensielt kan registrere og/eller avdekke. Figur 13 viser en forenklet fremstilling av et datanettverk i en organisasjon. De fleste enheter er koplet sammen og har en unik IP-adresse (Bergsjø et al., 2020; Nätt & Heide, 2021). Et reelt nettverk i en stor organisasjon vil bestå av hundrevis IP-adresser. For eksempel har Organisasjon A 903 IP-adresser som er synlige for skannere, men alle disse er ikke nødvendigvis i bruk.

Figur 13: Forenklet fremstilling av et datanettverk i en organisasjon



Grovt kan nettverksskanning deles i «IP-adresse- og portskanning» og «OS fingerprinting» (CE1; EH1).

Portskanning er en systematisk skanning av datamaskinporter. Formålet med portskanning er å identifisere åpne porter i et nettverk. En port er en nummerert identifikator som forteller hvilken prosess eller tjeneste i et datasystem som er avsender eller mottaker for en datapakke. Gjennom portskanning kan angriper utlede hvilke tjenester som er synlige og hvor angrep er

mulig. Nettlesere kommuniserer for eksempel ofte over port 80 eller 8080, sikker nettlesing skjer ofte over port 443, og visse e-postprotokoller bruker port 25, 110 eller 143. Portskanning diskuteres mer inngående i delkapitlene 5.2 og 5.3.

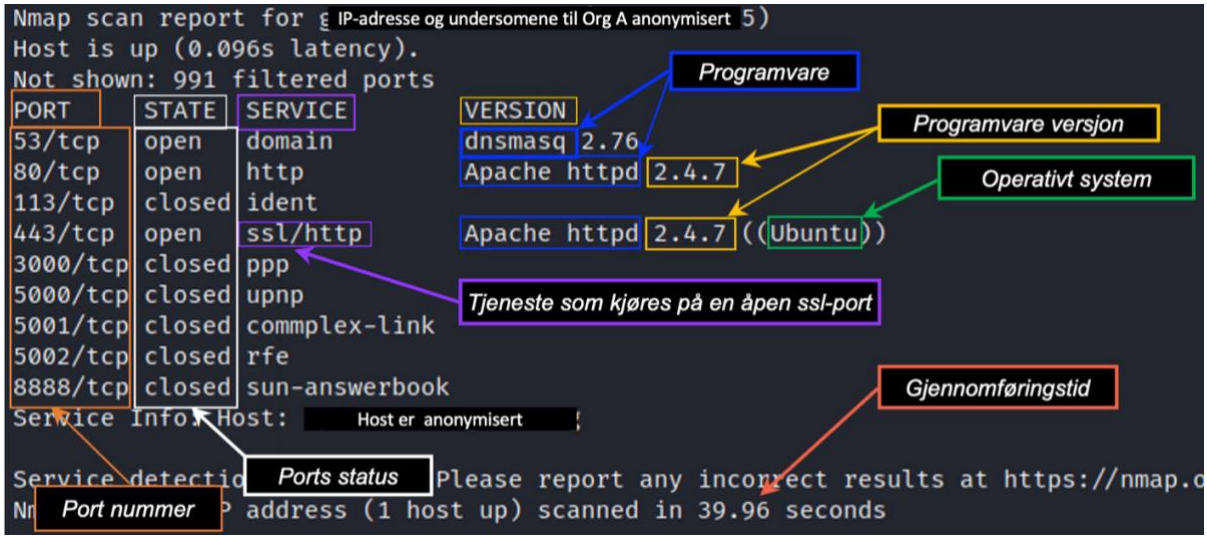
OS fingerprinting er en metode som brukes for å undersøke hvilket operativsystem og tjenester den eksterne datamaskinen eller serveren kjører (CE1; CE2; CE3; EH1, EH2). OS fingerprinting brukes mye i cyber-rekognosering, fordi enkelte utnyttbare sårbarheter er operativsystem-, og/eller applikasjonsspesifikke. Programvarers versjoner er og av betydning. For eksempel er WordPress en av de mest hackede applikasjonene som finnes, og den brukes på et utall operative systemer (CE3). Her er det verdt å bemerke at både Organisasjon A og Organisasjon B bruker WordPress plattformen (se Bilde 8).

Skanning av nettverk kan gjennomføres ved hjelp av ulike verktøy, som vil gi ulike resultater avhengig av verktøyets optimalisering, funksjoner, formål og input. Eksempelvis fremgår det i granskningsrapporten om «Lebanese Cedar» sine aktiviteter at APT-gruppen brukte Censys, Shodan og ZoomEye for å skanne nettverk (ClearSky Cyber Security ltd, 2021, s. 8).

I denne undersøkelsen brukte jeg først og fremst Nmap, Shodan, Maltego og DNSdumpster. Etter anbefaling fra CE1 benyttet jeg og Assetfinder, theHarvester og Httprobe for å sjekke hvorvidt alle verktøyene vil gi samme resultater (HackerTarget, 2021; Hudson, 2019/2021, 2017/2021; Lyon, 2021; Maltego Technologies, 2021; Martorella, 2011/2021; Shodan, 2021). Retest-skanning med de forskjellige verktøyene avdekket enkelte mangler, og jeg fikk noe ulike resultater med hver av dem. Ingen av verktøyene var altså perfekt.

Nmap brukes ofte til portskanning, OS-fingerprinting, gjenkjenning av programvare og versjon og mange andre teknikker (CE1; CE2; CE3; Lyon, 2021). Det er et svært effektivt verktøy, da det skanner et stort antall enheter samtidig og støttes av de fleste operativsystemer. Et Nmap søk på en organisasjons domene vil vise så godt som alle aktive IP-adresser, port, tjeneste de leverer og deres status. Bilde 6 viser hvordan noen resultater av skanning ser ut.

Bilde 6: Utklipp som viser resultater av skanning med Nmap

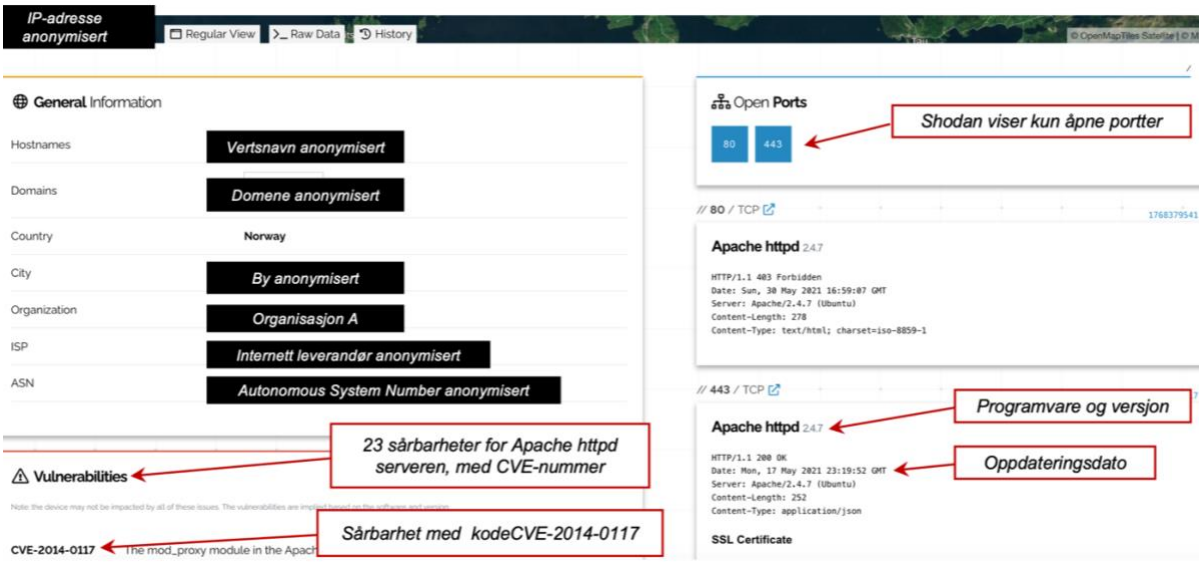


Kommentar til Bilde 6: En IP-adresse tilhørende Organisasjon A er brukt som input. Dette er en skanning av én IP-adresse. Resultater (output): 9 ulike porter, hvorav tre av de er åpne. En av de åpne portene er ssl-port (443). Videre viser resultatene programvare som kjører på portene, eksempelvis på den åpne 443 ssl-port kjøres Apache, versjon 2.4.7. på Linux Ubuntu distribusjon. Denne skanningen ble gjennomført på 39.96 sekund. Gjennomføringstid avhenger av flere faktorer, som nettverksforbindelse og ulike forhold hos motpart. Effektiv Nmap-skanning kan gjennomføres fra ganske beskjeden maskinvare, noe jeg har bekreftet i denne undersøkelsen.

Bilde 7 viser resultat av en enkel skanning på den samme IP-adressen med Shodan (Shodan, 2021). Et søk gir informasjon om organisasjonens plassering, siste oppdatering av programvarer, hvilke programvarer og versjon som er i bruk, samt kjente sårbarheter assosierte med programvaren og versjonen. Det kreves ikke spesielle ferdigheter for å utføre denne type skanning, da man kan finne veiledninger på Internett. Tolkning av resultater krever derimot grunnleggende kunnskaper om nettverksarkitektur.

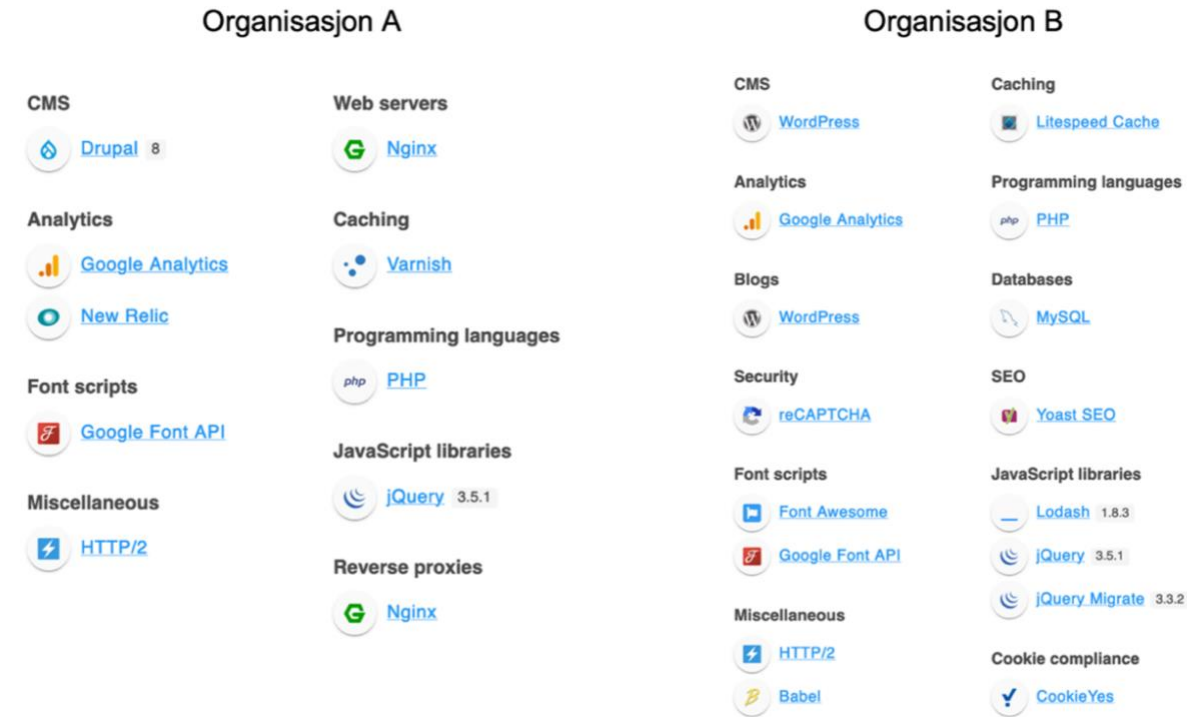
Bilde 8 demonstrerer hvilken teknologi som er brukt på organisasjonenes nettsider. Informasjonen fås via add-on app Wappalyzer som kan installeres på nettleser, i dette tilfelle Firefox (Wappalyzer, 2021). Ved å søke opp teknologien i sårbarhetsdatabaser kan man kartlegge sårbarheter assosiert med disse. Her ser vi blant annet WordPress som er nevnt før. WordPress er en CMS-programvare som hjelper brukere med å opprette, administrere og modifisere innhold på et nettsted, uten behov for spesialisert teknisk kunnskap. Organisasjoner flest bruker slike plattformer i dag for å opprette og vedlikeholde side nettsider.

Bilde 7: Et eksempel på resultater av nettverksskanning med Shodan



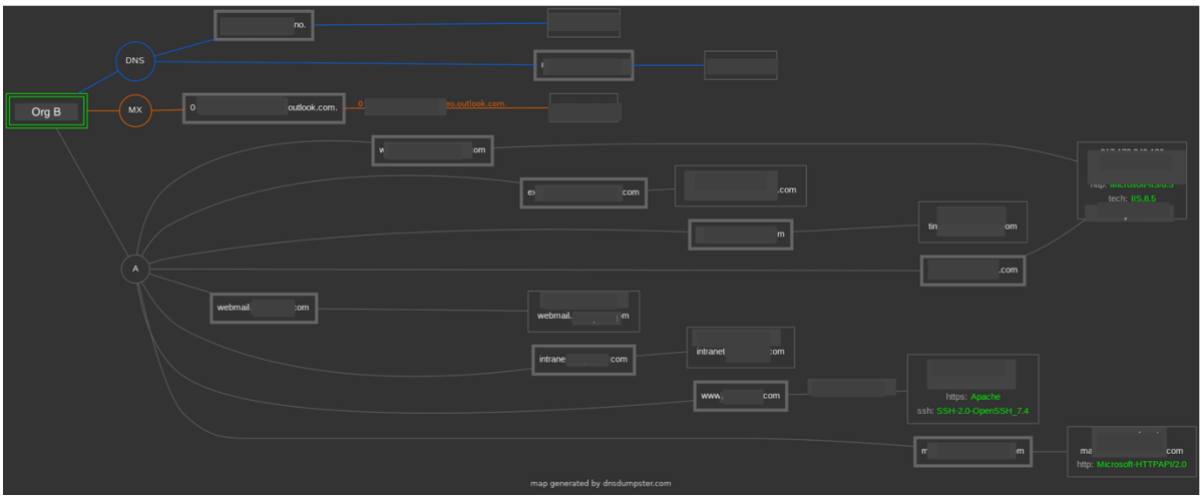
Kommentar til Bilde 7: Gjennomføringstid på skanning er ca. 5 sekunder. Organisasjon A's IP-adresse er brukt som input. IP-adresse (den samme som ble brukt i Nmap skanning illustrert i Bilde 6) ble innhentet tidligere ved å søke på organisasjonens domene. Dette søket gir geografiske koordinater, organisasjons navn, by, land, åpne porter, programvare som kjøres på IP-adressen, versjon, oppdateringsdato og sårbarheter. Sårbarheter er innhentet fra sårbarhets-database CVE-details. Shodan viser at det er 23 sårbarheter av ulik alvorlighetsgrad som er forbundet med denne programvaren. Det betyr ikke nødvendigvis at programvaren vil påvirkes av alle disse sårbarhetene, det vil avhenge av hver enkelt programvare og versjon.

Bilde 8: Resultater av søk med Wappalyzer - teknologi brukt på organisasjonenes nettsider



Til slutt brukte jeg DNSdumpster som er optimalisert for visuell fremstilling av nettverk på en litt annen måte enn Maltego gjør det. Bilde 9 viser resultatene av nettverkskanning av Organisasjon B.

Bilde 9: Organisasjons B nettverk - resultater av nettverksskanning med DNSdumpster



I neste delkapittel redegjør jeg for resultater av rekognosering av de to utvalgte organisasjoner, hvor ovennevnte verktøy og teknikker er brukt. Det drøftes og hvorfor denne type informasjon er av interesse for en trusselaktør. Intervjue og dokumentanalyse danner empirisk grunnlag for denne delen. Dataene ble innsamlet med utgangspunkt i modellen vist i Figur 9 (se kap. 4.2.1).

5.2. Hvilken informasjon om de utvalgte virksomhetene kan man finne ved bruk av rekognoseringsteknikker og OSINT?

I Tabell 5-7 presenteres informasjon om Organisasjon A og B innsamlet ved hjelp av metoder og verktøy beskrevet i delkapittel 5.1. Deretter diskuteres noen av funnene mer detaljert.

Tabell 5: Organisasjonskartlegging - resultater

Funn	Org A	Org B
Generelle opplysninger		
Nettsider	+	+
Sosiale media (Facebook, Instagram, Twitter)	+++	+++
Fysisk lokalisering, kart over område	+	+
Organisasjonsnummer	+	+

Forretningsforhold og relasjoner		noen	noen
Forretningstempo		+	+
Organisasjonens hierarki og struktur		delvis	+
Roller/ansvar:	ledelse	+	+
	lønnsmedarbeidere	+	+
	IT-personell	+	- *
	IT-sjef	+	- *
	ansvarlig for anskaffelser	+	+
	avdelingsledere	+	+
	ansvarlig for adgangskoder og kort	+	- **
	sikkerhetsansvarlig	+	-
Jobbannonser (se kommentar) ***		1	-
Dokumenter (.pdf, .txt, .doc, .xls, .ppt)			
Pdf dokumenter		> 10	> 10
E-post med innhold		1	-
Power Point dokumenter		> 10	> 10
Word dokumenter		> 5	-
Excel dokumenter		>5	2
Fysiske sikkerhetsbarrierer			
Plassering av alarmknapp		+	-
ID-kort/adgangskort standard		3	-
Adgangskode til en ansatt		1	-
Mønster på utforming av adgangskoder		+	-

Kommentar til Tabell 5:

**Det er ukjent om Organisasjon B har egen IT-personell da de utsetter tjenester til tredje part.*

*** Det er ukjent om Organisasjon B har sikkerhetsansvarlig eller lignende rolle. De eier ikke egne lokaler og da er det mest sannsynlig at utleieren er ansvarlig for adgangskort og lignende.*

**** Jeg har søkt kun jobbannonser som er av interesse for en trusselaktør, herunder IT-personell, teknologieksperter og økonomi-ansvarlige.*

Tabell 6: Profilering av personell - resultater

Funn		Org A	Org B
Navn		i viss grad	i stor grad
Alder		i viss grad	i viss grad
E-post		i viss grad	i stor grad
Telefonnummer		i viss grad	i stor grad
Bilde		i viss grad	i stor grad
Nyansatte		9	4
Kompetanse, ansvar og roller		i viss grad	i stor grad
Fødselsdato til enkelte		1	-
Autentifikatorer	passord til e-post	263	67
	visittkort	-	1
	bilde	i viss grad	i stor grad
	signatur	-	5
SoMe (kun LinkedIn her)		i stor grad	i stor grad
Ansattes forretningskontakter		i viss grad	i viss grad
Andre opplysninger		- *	+ **

Kommentarer til Tabell 6:

** se «Analyse av audiovisuelle data»;*

****** se «Analyse av filer»;*

«-» viser mangel på funn.

«I viss grad» betyr at det er ikke alle ansatte i en organisasjon som identifisert, men det er ikke «alle» som var målet. I tilfelle med Organisasjon A som har over 2000 ansatte er det omkring 30% ansatte identifisert. De som er identifisert er nøkkelpersonell: IT-personell, ledelse, forskere, økonomi-medarbeidere, sikkerhetsansvarlige.

«I stor grad» betyr at rundt 85-90% av ansatte identifisert. I tilfelle med Organisasjon B som har rundt 100 ansatte er rundt 90% identifisert. Disse er nøkkelpersonell.

E-post til IT-ansvarlige i Organisasjon A og B var eksponert i data-lekkasjer i 2018 og 2019, men jeg har ikke funnet passord. IT-ansvarlig i Organisasjon A har LinkedIn profil, mens IT-ansvarlig i Organisasjon B har ikke det.

Tabell 7: Resultater av rekognosering - Tekniske elementer/nettverk

Funn	Org A	Org B
Cloud	+	+
Registrert domene og utløpsdato	+	+
Underdomener	+	+
Eierskap	+	+
Host	+	+
DNS/Passiv DNS	+	+
Digitale sertifikater	+	+
IP-blokk og -adresser	+	+
Maskinvare	• 3 typer bærbar datamaskin • 2 typer LCD display • Prosjektor • Aksesspunkt	• 1 type bærbar datamaskin • Stasjonær PC
Nettverkstopologi	+	+ (se bilde 9)
Nettverks tiltrodde avhengigheter	noen	+
Port	Identifisert over 100 ulike porter. Bl. a. portene som leverer følgende tjenester: • Datatrafikk • VPN, OpenVPN • E-post tjenester • FTP (File Transfer Protocol) • RDP (port 3389) Remote Protocol Desktop (datamaskin med Windows OS med RDP den er rutet til). • mm..	• E-post tjenester • To ulike databaser • Web hosting server
Programvarer	noen	noen
Sårbarheter	• En åpen FTP 220 Server som inneholder dokumenter, video, programvare osv. (se Bilde 14). Man kan laste ned innholdet. • Utdaterte versjoner av programvarer • Flere åpne ssh-porter*	• Utdaterte versjon av programvarer
WiFi, WiFi BBSID	noen	+
Whois data	+	+

Kommentar til Tabell 7: En åpen SSH-port er ikke nødvendigvis en sårbarhet. De fleste servere kan fjernstyres via SSH, og det er helt vanlig å ha åpne porter for SSH. Det som er viktig er hvordan SSH-serveren er konfigurert og at denne er oppdatert.

5.2.1. Særlig interessante funn

Audiovisuelle data

Organisasjon B har lukket Facebook gruppe, mens Organisasjon A har offentlig Facebook gruppe. I en offentlig gruppe kan alle se hvem som er medlemmer og hva som legges ut. Jeg søkte om å bli medlem i en gruppe tilhørende Organisasjon A. Den ble godkjent umiddelbart, uten noen form for kontroll eller identitets-sjekk. Dette kan sannsynligvis forklares med at i store virksomheter som Organisasjon A, er det vanskelig å kontrollere en persons tilhørighet til organisasjonen. Jeg forsøkte ikke å bli medlem på Facebook side tilhørende Organisasjon B, da den kun består av 40 personer og hadde lite aktivitet ifølge Facebook analytiske data. Jeg besluttet å ikke forsøke da jeg ikke ønsket oppmerksomhet fra ansatte.

På Organisasjon A sin Facebook side fant jeg fem bilder som identifiserte maskinvare som er i bruk, herunder tre ulike modeller på bærbare datamaskiner og en modell WiFi aksesspunkt. Denne type informasjon brukes videre for å finne maskinvarers sårbarheter. Jeg fant ikke alvorlige sårbarheter knyttet til de identifiserte bærbare datamaskinene. Modellen på aksesspunkt er derimot forbundet med tre sårbarheter som vurderes å være relativt alvorlige (CVE Details, 2021).

Et av bildene viser en bærbar PC så klart at man kan identifisere modell og lese hva som står på skjerm. Herunder hvilke programvarer som er i bruk og korrespondanse mellom datamaskinens eier og en tredje person (identifiserbar). Hackere og cybereksperter kaller en slik uønsket skjerm-eksponering for «self-doxxing» (CE1).

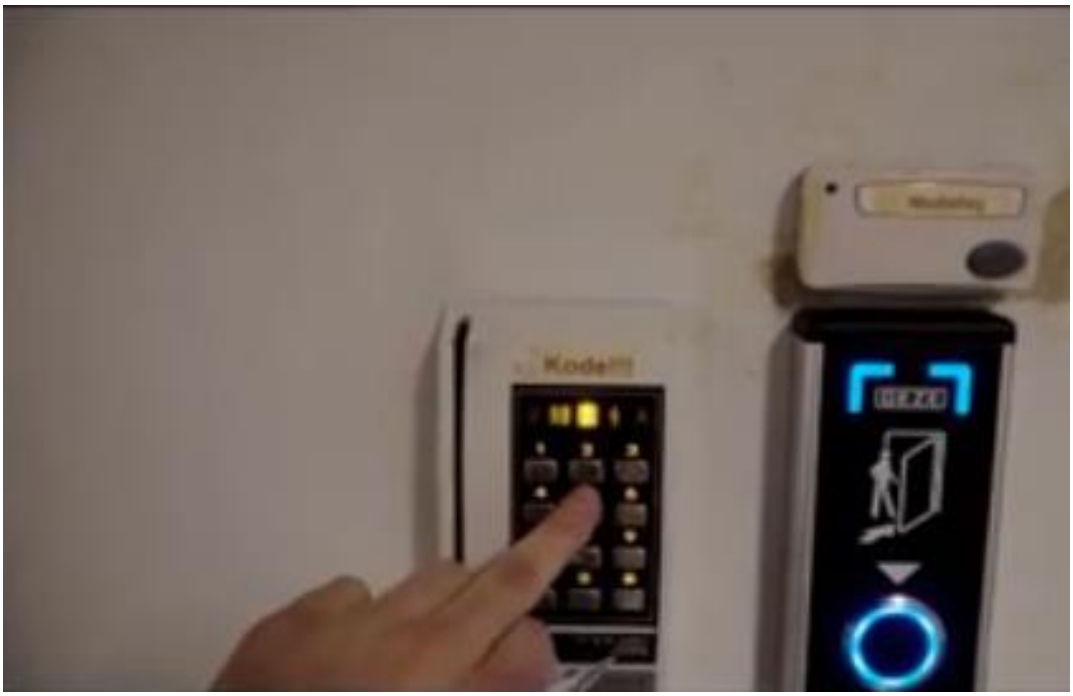
Et bilde funnet på Facebook avslører format på ID-kort brukt av ansatte i Organisasjon A. Et annet bilde viser et kontor pyntet til bursdagsfeiring av en konkret alder. Innlegget inneholdt informasjon som identifiserer en ansatt. Bildets metadata avslører dato og GPS-koordinater for når og hvor bildet ble tatt.

En video innhentet fra Organisasjon A's webside avslører trådløst utstyr tilhørende en identifiserbar ansatt. Videoen viser den ansattes hjem og elektroniske utstyr så klart at utstyret

kan identifiseres. Ut fra etiske hensyn velger jeg å ikke vise ovennevnte bilder og utklipp fra video, da det er vanskelig å anonymisere innhold uten å fjerne for mye informasjon.

Jeg fant og to videoer på Organisasjon A's offisielle Instagram-konto. De avslører en firesifret adgangskode til et lokale tilhørende Organisasjon A og adgangskortet til en person som er identifisert med navn i en video (se Bilde 10).

Bilde 10: Utklipp fra en video som er lagt ut på Instagram-konto tilhørende Organisasjon A



Dernest fant jeg et innlegg hvor en ansatt stiller spørsmål om adgangskode (se Bilde 11). Bildet viser svar på spørsmålet fra et annet gruppemedlem. Svaret avdekker mønsteret på hvordan adgangskoder i Organisasjon A er generert. Disse funnene sett sammen ga informasjon om ikke bare adgangskode til et lokal i Organisasjon A, men også et personnummer til den identifiserte personen fra Instagram-video[7]. I tillegg fikk jeg informasjon om hvem som er ansvarlig for å «fikse» adgangskort og hvor en kan endre kode.

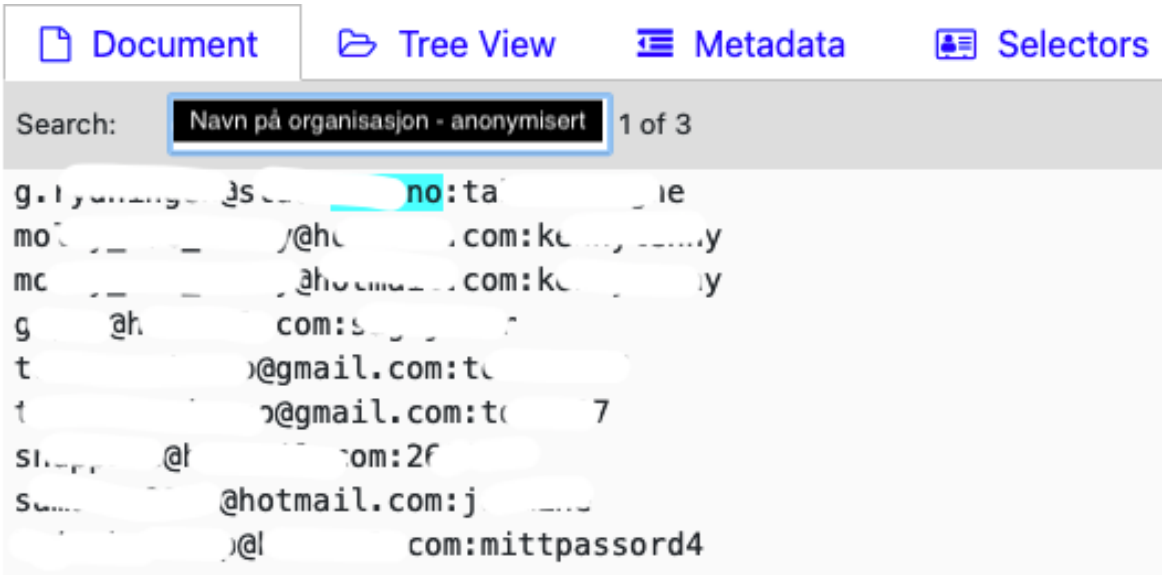
[7] Det er mulig å finne ut fødselsdato på vedkommende, trusselaktør vil da mangle kun et siffer fra 0 til 9 som er enkelt å finne ut.

Bilde 11: Utklipp fra Organisasjon A sin Facebook-side

Datalekkasjer

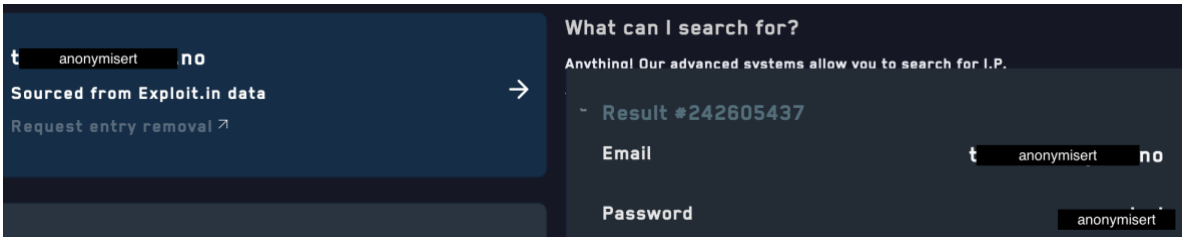
Bilde 12 er et utklipp fra et skjermbilde som viser resultater av et manuelt søk i en lekkasje-database (Intelligence X, 2021). Som søkeord brukte jeg `@organisasjonA.no` og `@organisasjonB.com`. Søket resulterte i en fil inneholdende e-post adresser med tilhørende passord. Denne databasen inneholder flere titusen eksponerte e-poster til begge organisasjonene, samt flere andre norske og internasjonale organisasjoner.

Bilde 12: Utklipp fra resultater av søk i en samling av datalekkasjer (Intelligence X, 2021)



Bilde 13 viser resultat av et søk i en annen database (DeHashed, 2021). Denne databasen i kombinasjon med andre lekkasjer resulterte i 263 eksponerte e-post adresser og passord tilhørende Organisasjon A og 67 e-post adresser og passord tilhørende Organisasjon B.

Bilde 13: Utklipp fra resultater av søk i DeHashed



Dokumenter

I forbindelse med søk etter dokumenter av ulike format samlet jeg inn seks eksempler på signaturer tilhørende ledelsen i Organisasjon B. Som regel brukes signaturer i forbindelse med validering av ulike dokumenter, herunder avtaler og kontrakter som er offentlig tilgjengelige. Det er per i dag ikke noe som antas å være skjermingsverdig, selv om signaturer kan kopieres/forfalskes og brukes med ondsinnede formål (CE1; EH2). Det kan allikevel argumenteres for at de i kombinasjon med bilder og andre personlige opplysninger kan utgjøre potensiell sårbarhet.

Et annet funn jeg vil rette søkelys mot er et Excel-dokument som inneholdt sensitive data om et familiemedlem til en ansatt i Organisasjon B. Dokumentet inneholdt navn og fødselsdato til et barn, den ansattes private adresse og telefonnummer. Som avklart tidligere brukte jeg kun organisasjons e-post format, uten ansattes navn for å søke dokumenter. Det var derfor ikke forventet å få et dokument med sensitive personlige data som ikke var knyttet til organisasjonens aktiviteter. Årsaken til funnet er at en ansatt registrerte sin jobb e-post adresse på et skjema i forbindelse med barnets fritidsaktivitet.

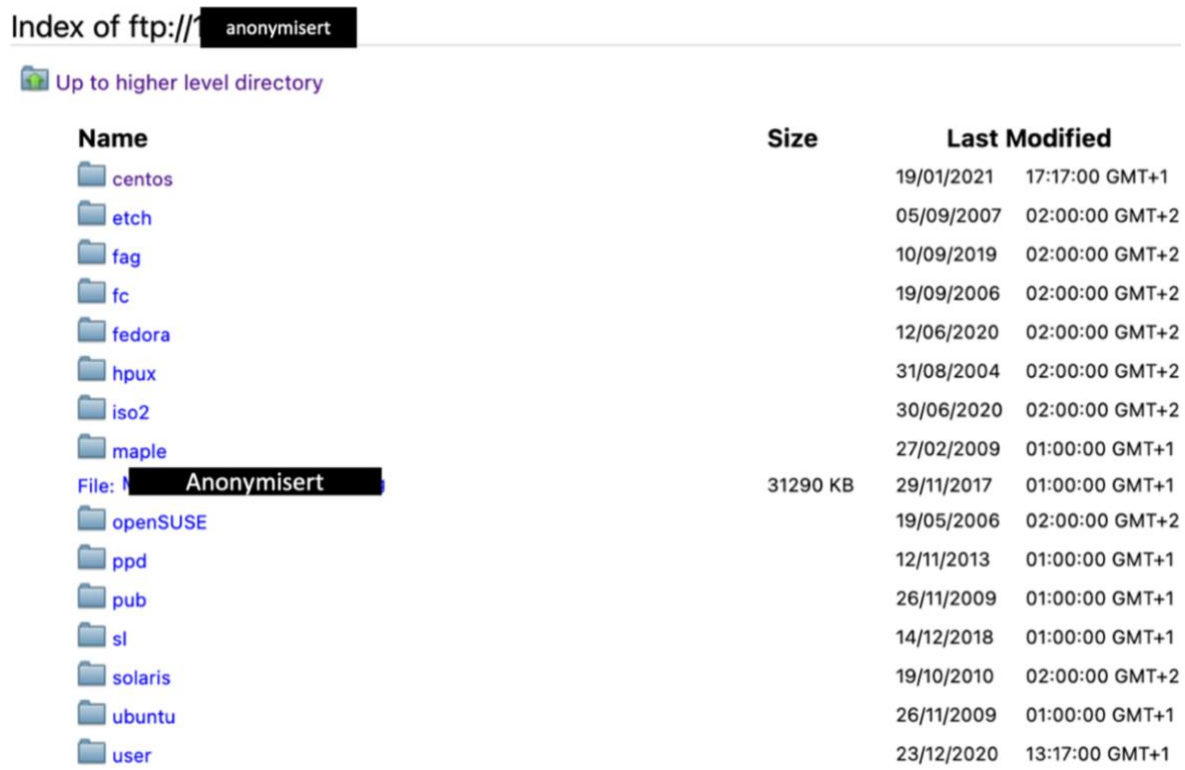
Dette i kombinasjon med e-postadresser som brukes i private sammenhenger, og hvordan personer ofte generer sine passord, viser at en trusselaktør kan få personlige opplysninger uten å søke på personer. Noe som i utgangspunktet er en mye mer krevende prosess enn å søke på en organisasjon. Vedkommende blir da en «lavt hengende frukt», og foretrekkes gjerne som inngangspunkt for videre angrepsprosess (CE1). Det kan derfor argumenteres for at bruk av jobb e-post adresser i private sammenhenger utgjør en betydelig risiko-faktor.

En åpen FTP-server

Skanning av Organisasjon As nettverk avslørte en åpen FTP-server, hvor man uten pålogging får tilgang til og kan laste ned en mengde datafiler, hovedsakelig programdatavarer og tilhørende dokumentasjon (se Bilde 14).

Jeg fant ikke dokumenter som inneholdt personlige sensitive opplysninger, men funnet *kan* representere sårbarhet. Jeg kunne ikke teste hvorvidt jeg kan endre/slette filene, da det er ulovlig. *En feil konfigurert server* kan medføre at en trusselaktør får tilgang til dokumenter og kan fjerne, endre, erstatte eller infisere innhold i disse. Det representerer dermed en trussel for informasjons konfidensialitet, integritet og/eller tilgjengelighet (CE1; CE3). Om det ikke er absolutt nødvendig å holde en port/tjeneste åpen, er hovedregelen at den bør skjermes/lukkes slik at den ikke er synlige ved skann av nettverk, eller at de krever pålogging. Videre kan informasjon om porter og tjenester brukes til å søke sårbarheter og eksisterende «exploits», eller man kan forsøke å teste ut passord som en tror kan funke.

Bilde 14: Innhold i en åpen FTP-server tilhørende Organisasjon A



5.2.2. Oppsummering

Kartlegging av organisasjonenes profiler resulterte i store mengder informasjon om infrastruktur, sikkerhetsbarrierer[8], ansvarsfordeling, hierarki, både pågående, tidligere og planlagte prosjekter, tredje parter og partnere, økonomi[9], dokumentmaler osv. *Personellprofilering* resulterte i informasjon om roller, telefonnummer, e-post adresser og tidligere brukte passord[10], eksempler på ledelsens signatur/underskrift[11], fødselsdatoer osv.

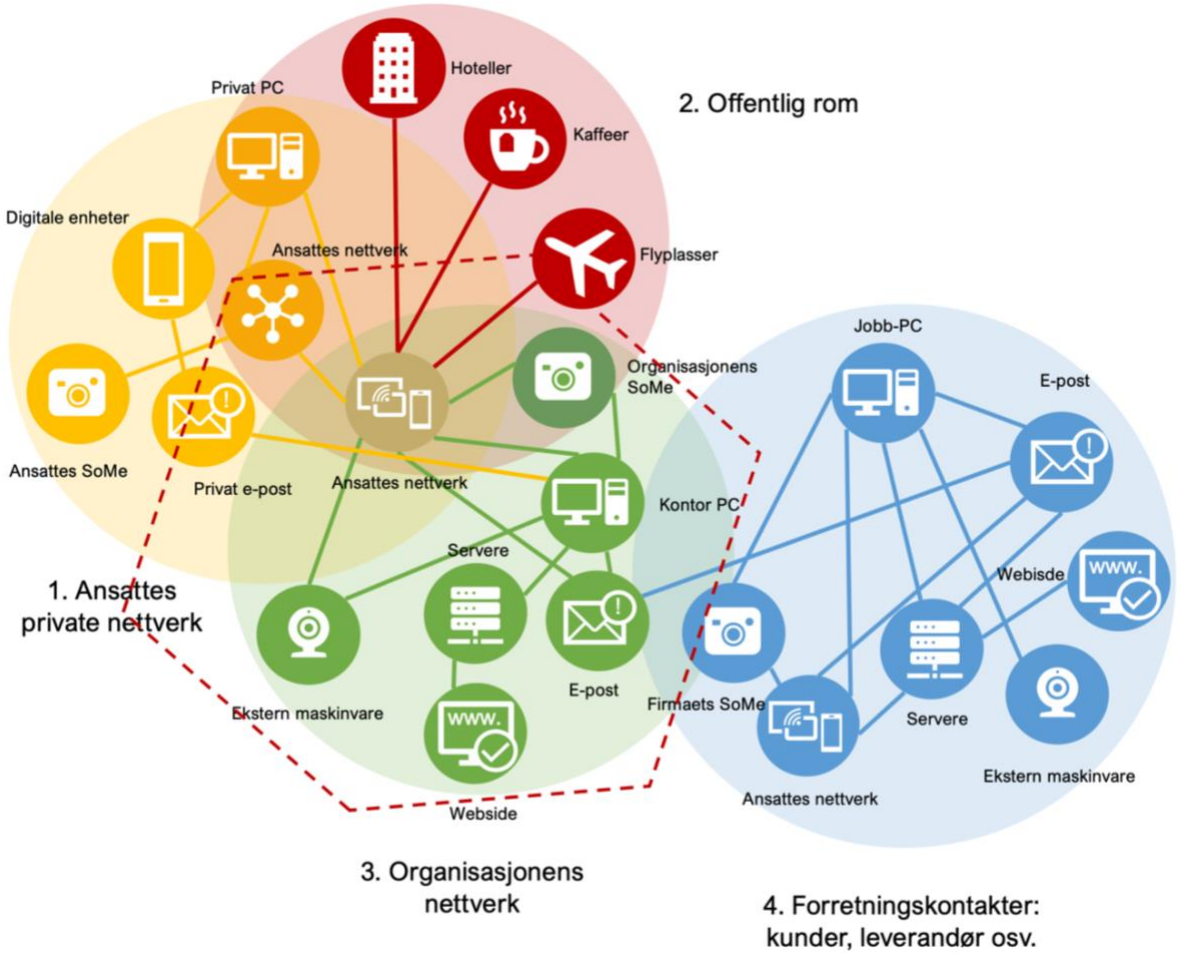
Kartlegging av teknisk infrastruktur resulterte i identifisering av teknologi som er i bruk, nettverkstopologi, sårbarheter, programvarer i bruk og versjoner osv. (se Tabell 7). Jeg har også i en viss grad kartlagt rutiner for oppdateringer av programvarer. Gjennom skanning av nettverket tilhørende Organisasjon A ble det identifisert hundrevis IP-adresser, 144 ulike porter, forskjellige operativsystemer, programvarer og deres versjoner. Dette muliggjorde identifisering av tjenester og sårbarheter forbundet med disse. Noen programvarer er ikke oppdaterte med nyeste versjoner, men overordnet kan man si at Organisasjon A har gode rutiner for oppdateringer. Organisasjon B bruker tredjepart for å hoste og vedlikeholde systemene. At organisasjonen tjenesteutsetter sine IKT-tjenester gjør det utfordrende for meg å konkludere med noe konkret.

På bakgrunn av informasjon innsamlet for denne undersøkelsen kan en trusselaktør (jeg) nå kartlegge organisasjonenes «angrepsflate» som er det endelige resultatet av rekognoseringsprosessen (se Figur 14, rød linje markerer oppgavens fokusområde).

Generelt kan man ikke vurdere hvorvidt organisasjonenes systemer er sårbare eller ikke uten å gjennomføre mer aggressive tiltak, eksempelvis «password-spraying» eller lignende teknikker (CSIS, 2021; CE1; EH1). Dessuten er ikke tekniske sårbarheter den eneste faktoren som avgjør hvorvidt organisasjons digitale systemer er sikre, sier EH1. Organisasjonens situasjons-bevissthet må inkluderes i vurderingen. Ifølge informantene er situasjonsbevissthet hos ansatte og ledelsen det mest avgjørende elementet for en organisasjons sikkerhet (CE1; EH1).

[8] Organisasjon A
[9] Organisasjon B
[10] Det er mulig at noen passord er fremdeles i bruk, men å kontrollere hvorvidt det er sant er en ulovlig aktivitet.
[11] Organisasjon B

Figur 14: Rekognosering på et mål - sluttresultat



5.3. Hvorfor er denne type informasjon av interesse for trusselaktør?

5.3.1. Hvorfor er åpen tilgjengelig informasjon om organisasjoner av interesse for en trusselaktør?

Nettsider som informasjonskilde

Figur 11 og Tabell 5 demonstrerer at nettsidene til de to valgte organisasjonene inneholder mye informasjon om organisasjonenes struktur og hierarki, navn på avdelinger, fysiske steder, data om nøkkelmedarbeidere som navn, roller og kontaktinformasjon, forretningsdrift og relasjoner. Denne type informasjon er av stor interesse for en trusselaktør av flere grunner.

OSINT og intervjuene viser at informasjon om målorganisasjons fysiske lokalisering kan inneholde en rekke detaljer om infrastruktur, hvilke myndigheter offeret er underlagt osv. (CE1; EH1). Ved bruk av Google Maps kan man se både satellitt bilder og «street-view» som kan avsløre sikkerhetsbarrierer, innkjøringsmuligheter, sperringer og lignende, sier CE1. I denne studien har jeg eksempelvis brukt organisasjonenes GPS-koordinater som input i verktøyet WiGLE for å finne deres trådløse nettverk (WiGLE, 2021).

Både intervju og dokumentanalyse viser at andre typer opplysninger, eksempelvis organisasjonsnummer, forretningstempo, bransjeaktivitet og forretningsrelasjoner kan brukes for å utføre avansert sosial manipulering eller andre typer angrep (Berman, 2018; CE1; CE2; Coville, 2020; Oliver & Shields, 2018). Informasjon om organisasjoners forretningsforhold kan inneholde flere detaljer om tredjepartsorganisasjoner, som leverer eller vedlikeholder IKT-systemer. Denne type informasjon ble brukt aktivt av blant annet «GRU-hackers», «Silent Librarian»-gruppen og Park et al. Dokumentanalyse viser at trusselaktører bruker denne type informasjon i sosial manipulerings-forsøk, eksempelvis i utforming av troverdige e-poster eller vedlegg (Berman, 2018; Coville, 2020; Oliver & Shields, 2018). Organisasjonens forretningstempo eller skiftordninger kan avsløre tider og datoer for kjøp og forsendelse av offers maskin- og programvarer, sier EH2. CE1 forteller at ved kjennskap til forretningstempo, ferieavvikling og prosjekter, kan en trusselaktør velge og planlegge utsendelse av målrettede nettfisking-e-poster, slik at angrepet vil ha større sjanser til å lykkes. Det kan eksempelvis være fredag kl. 15:30 eller dagen før feriestart, tidspunkter hvor de fleste vil ha «dårlig tid» og derav kanskje være mer ukritiske.

Nettsider som cybervåpen

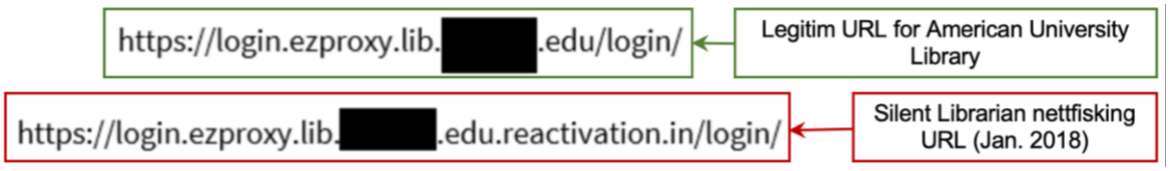
I tillegg til informasjonskilde, kan organisasjoners nettsider brukes til nettfiskingskampanje, forfalsking, infisering eller kapring. Dette bekreftes av både intervjuene og dokumentanalysen (Berman, 2018; CE1; CE2; Coville, 2020; EH1; Hacquebord, 2020; Hassold, 2018a, 2018b; Oliver & Shields, 2018). Eksempelvis brukte ofte Park et al. infisering av organisasjoners websider som nettfisking-teknikk. Blant annet infisert og kompromitterte han Polens finanstilsyn `www.knf.gov.pl` med skadelig programvare, i det som kalles et «vannhull»-angrep (Oliver & Shields, 2018, s. 88). Vannhullangrep er når hackere kompromitterer et nettsted som besøkes av tiltenkte ofre. Når ofrene besøker nettstedet, vanligvis som del av sin vanlige forretningspraksis, blir de (og noen ganger utilsiktede ofre) infisert av skadelig

programvare som gir hacker tilgang til deres nettverk. Polens finanstilsyn var en ideell kandidat å bruke som «vannhull» for å infisere banker i Polen (Oliver & Shields, 2018, s. 88-89).

Med hensyn til funnene i denne studien kan man anta at samme teknikk kunne blitt anvendt for å gjennomføre vannhullangrep på Organisasjon A og B. Dette kunne effektivt gitt tilgang til kunder av Organisasjon Bs nettverk. Hvorav flere organisasjoner som forvalter kritisk infrastruktur, som bruker digitale tjenester levert av Organisasjon B.

«Silent Librarian»-casen er et godt eksempel på hvordan organisasjoners nettsider kan forfalskes. Gruppen brukte denne metoden som hoved teknikk for å anskaffe tilgang til offers autentifikatorer (Berman, 2018; Hassold, 2018a, 2018b). Granskere har identifisert 127 forskjellige domener som hostet falsifiserte nettsteder brukt av APT-gruppen siden 2013. Gruppen forfalsket blant annet nettsider bibliotektjenester brukt av flere universiteter og andre forskningsinstitusjoner. URL-ene tilknyttet nettsidene, gjenspeiler de legitime URL-ene til innloggingssiden for bibliotekene (se Bilde 15).

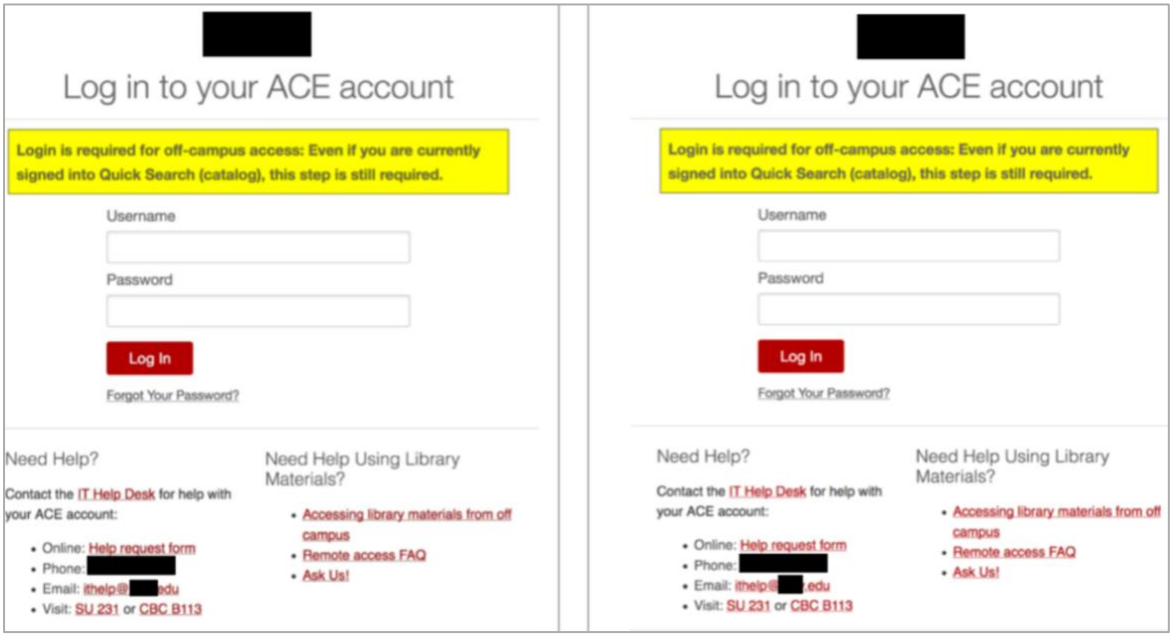
Bilde 15: «Silent Librarian»-saken - påloggings URL (Hassold, 2018a)



Bilde 16 demonstrerer at innholdet på «Silent Librarian» forfalskede nettsider nesten er identisk med de legitime nettsidene (Hassold, 2018a). Det har gjerningsmennene sannsynligvis oppnådd ved å kopiere den opprinnelige HTML-kildekoden og ved å bruke samme design-elementer, eksempelvis bilder, JavaScript osv. (Hassold, 2018b, s. 16).

Med hensyn til funnene i denne studien kan man anta at denne teknikken kunne vært effektiv for å gjennomføre cyberangrep på Organisasjon A og B. Organisasjon A bruker en bibliotektjeneste som jeg klarte å identifisere, med påloggingsside som er åpen på Internett. Da noen ansatte i Organisasjon A har forretningsengasjement i Organisasjon B, kan man videre anta en mulighet for at trusselaktør videre kunne fått tilgang til Organisasjon Bs e-postkontoer.

Bilde 16: Til venstre - ekte påloggingsside, til høyre - falsk nettside (Hassold, 2018a)



SoMe: bruke eller ikke?

I likhet med nettsider kan en organisasjons SoMe brukes som både informasjonskilde og angrepsteknikk. CE1 påpeker at til og med *ikke-bruk* av SoMe kan representere risiko.

Hvis en organisasjon bruker SoMe medfører det økt eksponering i form av publiserte bilder, videoer og innlegg som kan avsløre sensitiv eller skjermingsverdig informasjon. Analyse av «likes» under innlegg på organisasjons SoMe-sider kan gi verdifull informasjon om ansatte og deres roller og lede videre til ansattes private kontoer (CE1; CE2). Dette bekreftes i min studie, da jeg identifiserte noen nøkkelpersoner i Organisasjon A ved å se på «likes» under organisasjonens innlegg på SoMe-sider. Audiovisuelle data og kommentarer under innlegg inneholder og informasjon av interesse for en trusselaktør, som demonstrert tidligere.

Hvis en organisasjon ikke bruker en eller flere sosiale medier, kan og det brukes til angripers fordel i følge CE1. Eksempelvis hvis en trusselaktør har kartlagt at en organisasjon bruker Facebook, men ikke Twitter, kan det utnyttes ved sosial manipulering. Trusselaktør kan opprette en konto på Twitter, gjerne med organisasjonens logo og andre egenskaper som gir et legitimt utseende. En slik konto kan videre brukes for målrettede nettfisking meldinger, i forsøk på å få sensitiv informasjon. Teknikken kan og brukes for å skade organisasjoners omdømme. Ifølge CE1 er forfalsking av sosial media kontoer en ganske populær teknikk blant hackere, blant annet fordi «it's way too easy and way too effective».

Dokumentanalysen bekrefter dette, og viser at den samme teknikken tidligere ble brukt av Park et al. (Oliver & Shields, 2018). Deres kampanje mot SPE opprettet blant annet to Facebook-kontoer. De tilhørte tilsynelatende to kjente skuespillere involvert i produksjonen av «The Interview»[12], som var målet for en rekke angrep regissert av Park et al. På de falske Facebook-sidene la trusselaktørene ut en rekke kompromitterende bilder og lenker, brukt til nettfisking-kampanjer (Oliver & Shields, 2018, s. 34).

Jobbannonser

Ifølge CE1, CE2 og EH1 representerer jobbannonser stor verdi for en trusselaktør, det er en av de første ting en trusselaktør vil lete etter. Hayes & Cappa (2018) og Matvej et al., (2020) har konkludert med det samme. Hovedsakelig ser man etter annonser som beskriver IT- og andre typer teknologi brukt i organisasjonen. I denne studien fant jeg en jobbannonse som avslører teknologi brukt i en av organisasjonene (se Bilde 17). Det bemerkes at denne annonsen ikke inneholdt navn på IT-ansvarlig, som i dette tilfelle er positivt.

Bilde 17: En jobbannonse for utvikler-stilling utlyst av en av organisasjonene på Finn.no

Datalekkasjer

Både dokumentstudiet og intervjuene viser at datalekkasjer er blant de første ting en trusselaktør vil lete etter (Berman, 2018; CE1; CE2; CE3; EH1; EH2; Stretch, 2017). OSINT viser at datalekkasjer kan inneholde store mengder sensitiv informasjon. Eksempelvis e-postadresser, IP-adresser, navn, adresse, telefonnummer, passord og lignende. All denne

[12] «The Interview» er en komedie «which depicted a fictional Kim Jong-Un, the Chairman of the Workers' Party of Korea and the "supreme leader" of North Korea» (Oliver & Shileds, 2018, s. 3).

informasjonen kan brukes til å hacke kontoer. Informantene var enige om at mennesker tenderer til å gjenbruke de samme passordene, herunder på tvers av personlige kontoer og forretningskontoer. Dette gir databaser med tidligere brukte passord stor verdi (CE1; CE2; CE3; EH1; EH2). I det siste store angrepet mot Colonial Pipes i USA brukte trusselaktører et tidligere kompromittert passord for å få tilgang til nettverket (Turton & Mhrotra, 2021). Data innhentet fra lekkasjer i denne undersøkelsen viser at tendensen i stor grad kan stemme.

I tillegg til data fra lekkasjer vil en angriper prøve å få tilgang til detaljert informasjon om organisasjonens passord-policy (CE1; CE3; EH1). Passord-policy for nettverk metoder for å håndheve komplekse passord som er vanskelig å gjette eller knekke gjennom brute-force angrep. Hvis minimum passordlengde eksempelvis er åtte tegn, skal man ikke prøve passord som «pass123». Man skal heller ikke sjekke mer enn tre eller fire ulike passord per konto, for ikke å låse kontoen (CE1; EH1). Ved å sammenligne passord fra lekkasjer kan man trekke en rekke slutninger om passord-policy (CE3).

Som nevnt tidligere fant jeg 263 eksponerte e-post adresser og passord tilhørende Organisasjon A og 67 e-post adresser og passord til Organisasjon B. Analyse av eksponerte passord avdekket noen elementer ved passord-policyen til de to organisasjonene, og viser at flere er «lite kreative» ved passordgenerering. Noen e-post-adresser er eksponert i flere lekkasjer, som gjør det mulig å analysere hvordan enkelte utformer passord over tid. Et flertall passord tilhørende kontoer som er eksponert flere ganger, er varianter av tidligere passord. Eksempelvis en tallrekke kombinert med det fiktive passordet «banan», «banan1», «banan2», «banan3» og «banan4» osv. - er et gjentakende mønster. Funnene viser at til tross kampanjer som oppfordrer til å unngå enkle passord, som «passord123», brukes slike fremdeles av mange.

Et annet kjennetegn er bruk av navn kombinert med to tall, som sannsynligvis markerer et fødselsår. Passord av type «Camilla78» eller «Martin 92» og lignende brukes mye. Selv om eier av eksponerte e-post-adresser bytter passord, kan trusselaktør enkelt å gjette seg til et nytt passord. Eventuelt via kartlegging av vedkommendes familie, eller ved såkalt «ordlisteangrep». Metoden ble eksempelvis brukt under cyberangrepet på Stortinget i august 2020 (PST, 2020a).

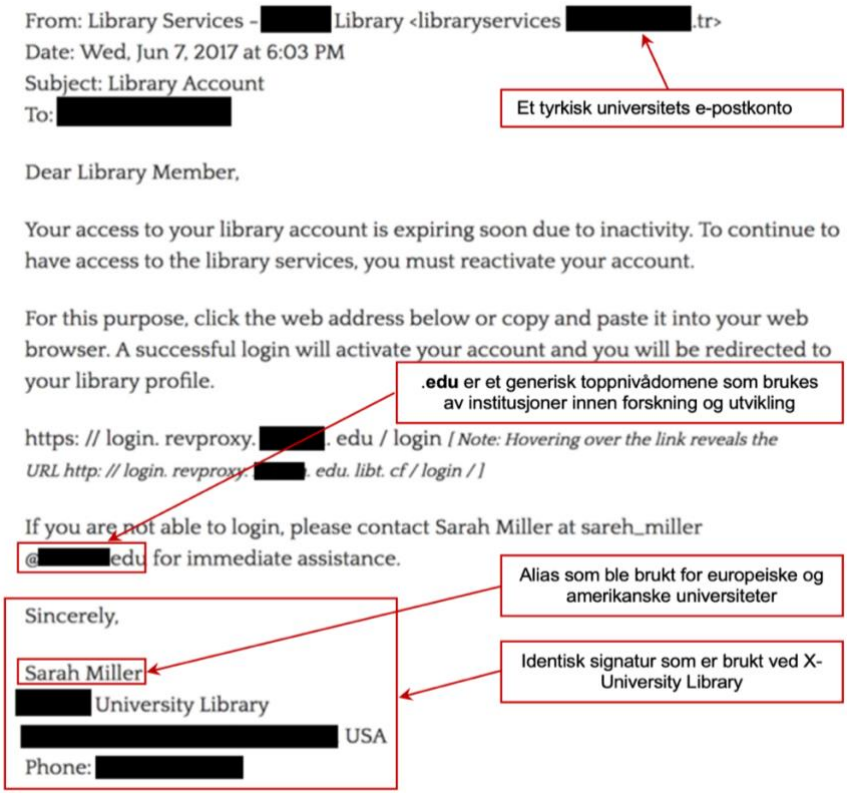
Denne undersøkelsen viser at hovedsakelig én felles faktor kjennetegner e-poster som har vært del av lekkasjer flere ganger. De fleste er brukt av ansatte i private sammenhenger, for eksempel registrering på diverse apper som MyFitnessPal og lignende.

Hvorfor er dokumenter av interesse for en trusselaktør?

Som nevnt i delkapittel 5.2 ble det innhentet flere typer filer som viser organisasjonenes maler for ulike dokumenter, både PDF, e-post og Power Point. Slik informasjon kan brukes til å utforme mer troverdige e-poster eller vedlegg til e-post (CE1; CE2; EH2). Vedlegg kan inneholde skadevare, virus osv.

Her kan «Silent Librarian» trekkes inn som et eksempel. Ifølge granskere hadde alle e-poster og nettsider konstruert av «Silent Librarian» bemerkelsesverdig autentisk utseende (Berman, 2018; Hassold, 2018a, 2018b). Stavekontroll og grammatikk, to av de vanligste indikatorene for en ondsinnet e-post, er nesten perfekt. Meldingene er kontekstmessig legitime, altså noe mottaker med rimelighet kan forvente å motta. De fleste e-postene inneholdt falske avsender-adresser, tilsynelatende fra legitime kilder (se Bilde 18). E-postene rundet av med en realistisk utseende signatur med kontaktinformasjon. Denne informasjonen ble anskaffet gjennom OSINT-granskning utført av hackerne (Hassold, 2018a). I noen tilfeller finner man all kontaktinformasjon samlet på en nettside. Hackerne samlet mye informasjon fra ulike steder, som indikerer manuell rekognosering av enkelte personer (Hassold, 2018a).

Bilde 18: Eksempel på nettfisking e-post sendt av Silent Librarian (Hassold, 2018a)



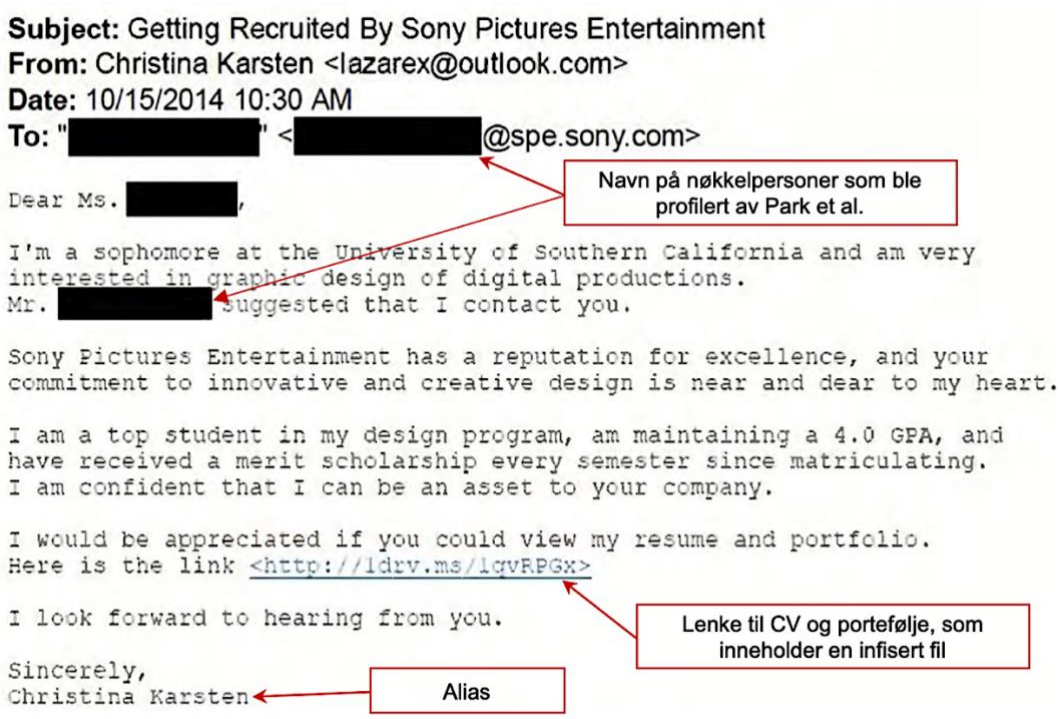
Flere av hackerne brukte i følge Hassold (2018a) fiktive identiteter for å utforme tilsynelatende autentiske e-poster. De endret og navn for å matche plasseringen til måluniversitetet. For eksempel brukte en kampanje mot et australsk universitet sokkedukke «Jonathan Dixon», mens «Shinsuke Hamada» ble brukt i en e-post rettet mot en japansk skole. E-postenes innhold og emnelinje holdt seg konsistent over tid (Hassold, 2018a).

5.3.2. Hvorfor er åpen tilgjengelig informasjon om ansatte av interesse for trusselaktør?

Både intervjuene og dokumentanalyse viser at nøkkelpersonell er av stor interesse for trusselaktører (ClearSky Cyber Security ltd, 2021; CE1; CE3; Coville, 2020; EH1; EH2; Oliver & Shields, 2018; Stretch, 2017). Med nøkkelpersonell menes her personer med beslutningsmyndighet som har tilgang til organisasjons ressurser, særlig de som har tilgang til informasjon. Det kan være ledelse, teknologieksperter, forskere, IT-personell, økonomi-, sikkerhet- og anskaffelsesansvarlige, personell med myndighet til å be om pengeoverføringer mm. (ClearSky Cyber Security ltd, 2021; CE1; CE3; Coville, 2020; EH1; EH2; Oliver & Shields, 2018; Stretch, 2017).

For eksempel gjennomførte Park et al. rekognosering på nøkkelpersoner i SPE. Informasjonen ble brukt til å sende infiserte søknadsbrev og CVer for å få tilgang til ofres nettverk (Oliver & Shields, 2018, s. 48, 58, 60–62). Det kan tenkes at det ikke er vanlig for alle typer organisasjoner å motta CV og søknadsbrev i form av lenke eller .zip-fil. Men for organisasjoner i eksempelvis filmbransje eller spillutvikling, som SPE, er det svært vanlig og representerer dermed sårbarhet. Bilde 19 viser et eksempel på hvordan informasjonen som ble innsamlet utgjorde grunnlag for påfølgende sosial manipulering av ofre. Dette sammenfaller med elementer i CKC illustrert tidligere i Figur 2.

Bilde 19: Målrettet nettfisking e-post sendt av Park et al. (Oliver & Shields, 2018, s. 48)



Informasjon om ledelse, IT-personell og økonomiansvarlige er av interesse for trusselaktør, fordi disse har tilgangsrettigheter til «privilegerte kontoer» (ClearSky Cyber Security ltd, 2021; Coville, 2020). Blant annet ikke-personlige kontoer som gir administrativ tilgang til hele nettverket. Lokale administratorkontoer brukes rutinemessig av IT-personell til å utføre vedlikehold på nettverksenheter. CE1, ET1 og EH2 påpeker at disse kontoene er særlig problematiske, fordi samme passord ofte benyttes på tvers av hele nettverket. Andre privilegerte brukerkontoer med tilgangsrettigheter av høyere nivåer gir administrative rettigheter på ett eller flere systemer. Til tross for at disse ofte har unike og komplekse passord, er det kontinuerlig overvåking av kontoer og bruken av dem nødvendig, advarer CE1 og EH1.

Ifølge informantene og dokumentanalyse er IT-personell ofte utsatt for manipuleringsteknikker med formål å finne ut mer om organisasjons programvarer og sikkerhetsrutiner (CE1; CE2; EH2). Dette kan gjøres via å lokke med et interessant jobbtilbud, eller eksempelvis et falskt jobbintervju. Et annet alternativ er å invitere eksperter til en prøveperiode for en ny programvare, gjennom e-post fra en tilsynelatende legitim avsender (CE1).

Andre kategorier ansatte av interesse for trusselaktører er nyansatte, vikarer, praktikanter og «generally zoomers and boomers», sier CE1. Med «zoomers» menes representanter av Generasjon Z, også kalt Zillennials, som er de født mellom 1997 og 2012. De er nå 9-24 år gamle. Med «boomers» mener CE1 de født mellom 1946 og 1964, som nå er 57-75 år.

«Zoomers» er av stor interesse fordi «they are SoMe-junkies, but digital wizzards they are not», sier CE1[13]. Med det menes at de fleste er svært aktive brukere av SoMe, men mangler tilstrekkelig digital kompetanse. Informanten henviser til Strauss (2019) som bekrefter hypotesen. «Boomers» er ifølge CE1 en gruppe som begynte å bruke SoMe aktivt de siste årene, til tross for svært lav digital kompetanse.

CE1 skiller mellom gruppenes digitale adferd: «Zoomers» deler mindre direkte personlig informasjon om eksempelvis familie, men er «uncritical in their tendency to document and share publicly every single moment of their lives» (i form av bilder og videoer). «Boomers» på den andre side deler innlegg, bilder, videoer som eksponerer mye personlig informasjon om familiemedlemmer, venner, omgivelser osv. Disse kan eksponere familiemedlemmer uten at vedkommende vet om det, ved å legge ut eksempelvis bilder av barn/barnebarn, hus, elektronisk utstyr osv. De tenderer og til å legge ved kommentarer som kan avsløre navn, bursdagsdato, arbeidssted og lignende.

Som vist tidligere kan audiovisuell dokumentasjon avsløre sensitiv informasjon om ansatte og organisasjon. Videre kan metadata i bilder og videoer avsløre IP-adresser, GPS koordinater og andre typer sensitiv informasjon, som kan brukes for både sosial manipulering og hacking (CE1; EH1). CE1 konkluderer med at når en trusselaktør kartlegger nøkkelpersoner «zoomers and boomers are the first thing you wanna do recon on».

Intervjuene og dokumentanalyse viser at informasjon om familiemedlemmer generelt kan brukes for andre typer sosial manipulering, for eksempel personifisering med formål om å fiske mer sensitiv informasjon (CE1; CE2; EH1; EH2; Stretch, 2017, s. 6, 12, 16). Publiserte bilder av familiemedlemmer eller kjæledyr med emneknagg, avslører navn til personer på bilder samt inneholder hyperlinker til personlige profiler. Dette omtales som «gift that keeps on giving» av CE1. Mange bruker navn til nærstående som passord eller del av passord (CE1; CE2; EH1; EH2). Noen funn presentert senere i dette delkapittelet viser at det stemmer i en viss grad. Hva ansattes personlige kontoer kan avsløre er illustrert i Figur 12, delkapittel 5.1. Informasjon på SoMe kan og brukes for å få tilgang til kontoer ved å svare på «kontroll spørsmål» som ved riktig svar kan tillate brukeren å endre passord og dermed få tilgang til kontoer, sier CE1.

[13] Ifølge Pew Research Center bruker et flertall 18- til 29-åringer Instagram (71%) eller Snapchat (65%), mens omtrent halvparten sier det samme for TikTok. Bruk av YouTube øker, konstaterer forskere. Hele 81% av amerikanerne sier at de noen gang bruker videodelingssiden, opp fra 73% i 2019 (Brooke & Anderson, 2021).

Nyansatte, praktikanter og vikarer er av interesse fordi de (a) ikke kjenner organisasjon og kolleger i tilstrekkelig grad og (b) ønsker å være ekstra hjelpsomme (CE1; EH1; EH2). Når man ikke er god bekjent med organisasjonens rutiner, struktur og hierarki, er det enkelt å bli manipulert til å gi fra seg sensitive opplysninger ved å tro en hjelper kollega/ledelse. Praktikanter og vikarer har ikke stabil en posisjon i organisasjonen, de er særlig sårbare da de ofte vil være ekstra hjelpsomme (CE1; EH2). De kan manipuleres ved personifisering av ledelse eller andre autoritetspersoner. «Du kan utnytte varierende grad av kunnskap om selskapets interne prosesser, ved å overbevise folk at du har rett til å være steder du ikke burde ha vært eller se ting du ikke burde ha sett», sier EH2. CE1 fremhever personifisering av ledere som en effektiv teknikk, «not that many can say "no" to boss, that's why it's almost always working». En annen vinkling for informasjonsinnhenting er å personifisere praktikanter eller nyansatte, som alltid trenger hjelp med for eksempel dokumenter eller IT-spørsmål, sier CE1.

Videre kan informasjonen om språk, kultur, hendelser og arrangementer brukes til å utforme avanserte sosiale manipuleringsforsøk, eller planlegge fysiske handlinger (Berman, 2018; CE1; CE2; Coville, 2020; EH1; Oliver & Shields, 2018, s. 44). Eksempelvis i «Park et al.»-anmeldelsen fremgår at trusselaktørene gjennomførte rekognosering av ofrenes websider med fokus på kartlegging av ansatte, tredjepart, arrangementer osv. (Oliver & Shields, 2018, s. 19, 53, 72 og 90). Senere brukte de informasjonen til å utforme målrettede nettfisking-eposter som fremsto som ekte, da de inneholdt en rekke detalj om en kommende arrangement og organisasjons ansatte (Oliver & Shields, 2018, s. 44).

«GRU-hackers» brukte informasjon om språk og arrangementer i forberedelse av alle sine angrep (Coville, 2020, s. 15–16, 27). I tillegg planla de aktiviteter slik at angrepene kom på større «røde» dager, som eksempelvis Ukrainas Grunnlovsdagen (Coville, 2020, s. 16). «Silent Librarian»-gruppen brukte informasjon om etnisitet og språk for å tilpasse sine e-poster (Hassold, 2018b, s. 4). «Pawn Storm» designet og sine nettfisking-kampanjer slik at e-poster fremstod aktuelle. De brukte aktuelle hendelser og arrangementer i emne-felt, for eksempel en reel konferanse i London, et politisk arrangement osv. (Hacquebord & Hilt, 2016).

5.3.3. Hvorfor er åpen tilgjengelig informasjon om infrastruktur av interesse for en trusselaktør?

Skanning av organisasjonenes nettverk gjennomført i denne studien lot meg kartlegge teknologi som er i bruk, nettverkstopologi, sårbarheter, programvarer i bruk, versjoner osv. (se

Tabell 7). Jeg kartla og i en viss grad rutiner for oppdateringer av programvarer, IP-adresser, porter, forskjellige OS, applikasjoner og deres versjoner.

Funnene viser at informasjon om IP-adresser som er i bruk sier noe om organisasjonsstørrelse, fysisk beliggenhet, Internett-tjenesteleverandør mm. Informasjon om nettverks sikkerhetsprodukter vil si noe om eksisterende brannmurer og andre cyberbarrierer. Dette bekreftes av informantene (CE1; CE2; CE3).

Informasjon om domener og deres egenskaper kan inneholde en rekke administrative data som navn, registrator, e-postadresser, telefonnumre, forretningsadresser og navneservere. CE1 forteller om måter dette kan utnyttes på. Trusselaktør kan søke informasjon om tidspunkt for utløp av en organisasjons eierskap til et domene, for så å selv kjøpe domenet dersom organisasjonens administrator eller IT-ansvarlig glemmer å fornye avtalen. Videre sier informanten at om navn på IT-ansvarlig eller annen ansvarlig er angitt i offentlige registrer, kan en trusselaktør iverksette sosial manipulering ved å (a) kontakte ansvarlig via e-post eller lignende eller (b) personifisere IT-ansvarlig overfor myndigheter som utgir digitale sertifikater eller registrerer domener for å gjøre endringer (CE1).

DNS-informasjon kan inneholde registrerte navneservere, underdomener, e-post servere mm. DNS kan i tillegg forfalskes eller kapres (CE1; CE2; EH1; EH2). Informasjon om nettverkets betrodde avhengigheter kan brukes for å kartlegge tredjepartsorganisasjoner/domener, herunder tjenesteleverandører, entreprenører osv. (CE1; EH2; Hayes & Cappa, 2018; Matvej et al., 2020). For eksempel brukte «Lebanese Cedar» sårbarhetsskannerne Censys og Shodan for å kartlegge tredjeparts infrastrukturtjenester og avhengigheter (ClearSky Cyber Security ltd, 2021, s. 9). Oversikt over nettverkstopologi gir informasjon om fysisk/logisk utforming av eksterne og interne nettverksmiljø, spesifikasjoner på nettverksenheter og annen infrastruktur. Dette muliggjør å «kartlegge korteste vei» inn i systemet (CE1; EH1; EH2) (se Bilde 9).

Informasjon om WiFi og BSSID gir mulighet til å hacke en organisasjons trådløse nettverk, ifølge CE1. CE3 fremhever imidlertid at slike angrep har fått langt mindre verdi de siste årene. Dette henger sammen med at «[...] trafikken nå ofte er kryptert på høyere lag [...], som gjør at f.eks. WIFI-kryptering ikke har samme verdi eller nødvendighet som før». Tidligere var det enkelt å avlytte trafikk på trådløse nettverk. Nå er det vanskeligere da trafikken er kryptert mellom avsender og mottaker, selv over åpne trådløse nettverk.

Ifølge informantene er portskanning en av de viktigste deler i nettverkskanning (CE1; CE3; EH1; EH2). En trusselaktør fokuserer først på søk etter åpne porter, som kan brukes til å angripe offers datamaskin. Åpne porter kan påvirke konfidensialitet, integritet og tilgjengelighet av informasjon ved at de «lytter» og «svarer» på skanning og kan dermed avsløre informasjon om systemet og nettverksarkitekturen (CE1; EH1). «Ports leak information: software versions, content, what type of OS it is... you name it. Just ask them, they [porter] will answer», sier CE1.

Åpne porter er nødvendige kommunikasjonskanaler, som kan representere sårbarhet «dersom en usikker tjeneste lytter på porten», sier CE3. De kan utnyttes ved at trusselaktør får uautorisert tilgang til systemer og sensitive data (CE1; CE3; EH1). Organisasjoner bør derfor ha oversikt over hvilke porter i nettverket som er åpne, hvorfor de er åpne, og hvilke som ikke skal være åpne, sier CE1. Eksempelvis brukte Lebanese Cedar portskanning for å finne Oracle og Atlassian WEB-servere. Innbrudd i disse systemene ble gjort ved å utnytte kjente sårbarheter i systemer som ikke ble patchet, og oppdage smutthull ved hjelp av åpen kilde-hackingsverktøy.

For å finne en sårbarhet må angriperen «fingeravtrykke» alle tjenester som kjører i et nettverk, inkludert hvilke protokoller, programvarer og deres versjoner er i bruk. Som demonstrert i delkapittel 5.1 kan skanning ved hjelp av Nmap (se Bilde 6) gi informasjon om programvarer, og noen ganger deres versjon og applikasjoner som «kjøres» på en server. Utdaterte versjoner kan ha offentlig kjente sårbarheter som kan utnyttes. Ved å søke opp teknologien i sårbarhetsdatabaser kan man kartlegge sårbarheter assosiert med disse (CE1; CE3; EH1; EH2). Dokumentanalyse viser at eksempelvis «Pawn Storm» og «Lebanese Cedar» brukte port-skanning aktivt i forberedelse av et cyberangrep (ClearSky Cyber Security ltd, 2021, s. 21; Hacquebord, 2020, s. 13). «Pawn Storm» gjennomførte store skanninger på TCP-porter 445 og 1433, tilsynelatende et forsøk på å finne sårbare servere som kjører Microsoft SQL (Hacquebord, 2020, s. 7).

5.4. Oppsummering: Hvordan kartlegger trusselaktører organisasjoner?

Empirien viser at rekognoseringsprosessen kan utvikle seg på ulike måter, avhengig av mål/offer, formål, omgivelser og andre faktorer. Funnene indikerer at de aller fleste nettangrep starter med anskaffelse av infrastruktur og fiktive identiteter, herunder brukerkontoer, e-

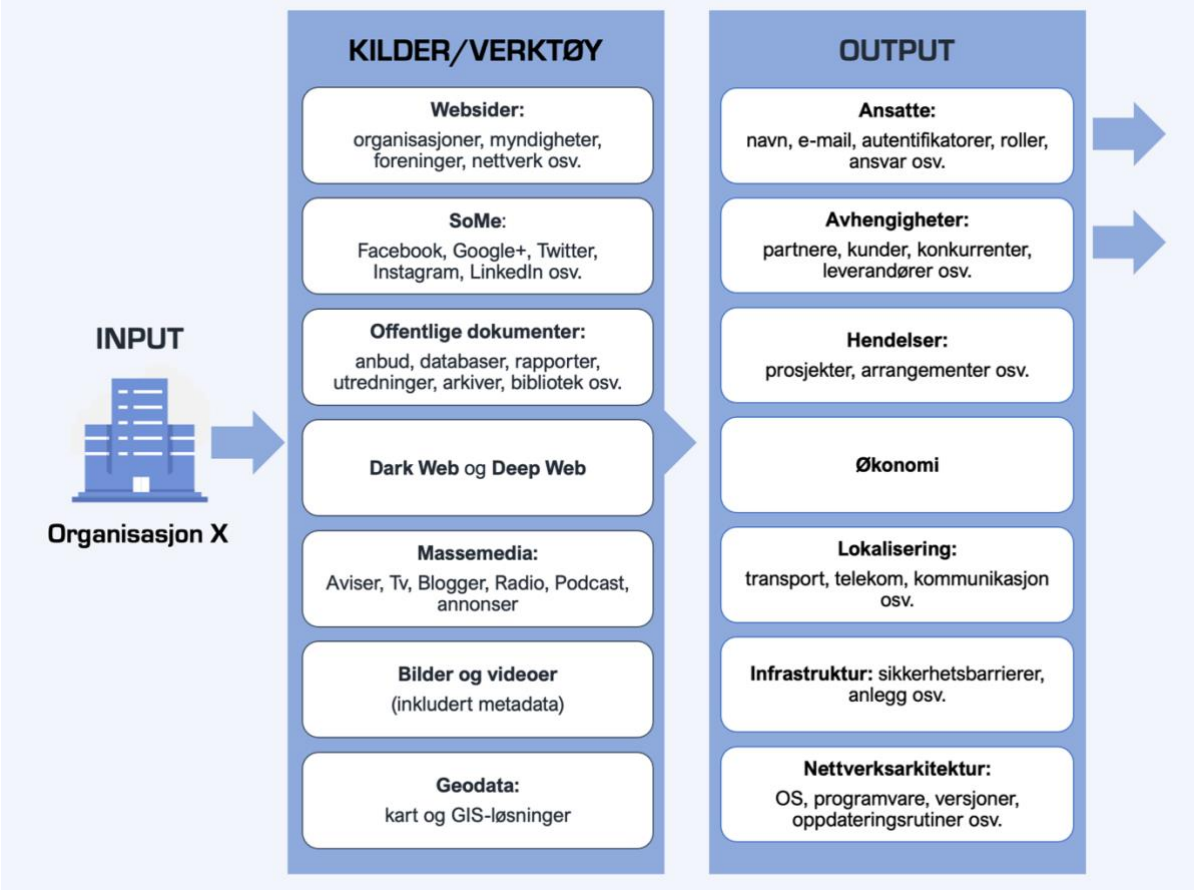
postadresser, domener, servere osv. Dette for å unngå deteksjon og dekke over tilhørighet til en stat/organisasjon. Noe av den samme infrastrukturen kan bli gjenbrukt i angrep mot flere ofre og individer.

Dokumentanalyse viser at rekognoseringsprosessen inkluderer alle de tre fasene illustrert i, men rekkefølgen er ikke statisk. Fasene er heller overlappende og kan skje samtidig eller/og i flere omganger. Prosessen er dermed iterativ og sirkulær, og ikke lineær som vist i den teoretiske modellen. Dette kan henge sammen med skiftende formål og kontinuerlig tilflyt av ny informasjon.

Funnene indikerer at passiv rekognosering er til stede og et viktig element i alle tilfeller, selv i de mer «upersonlige» eller «tekniske» angrepene som «Pawn Storm»- og «Lebanese Cedar»-operasjonene. For eksempel konkluderte «Lebanese Cedar»-rapporten med at målene til APT-gruppen var nøye valgt og at angriperne gjennomførte omfattende rekognosering for å skreddersy hvert angrep til sitt spesifikke mål (ClearSky Cyber Security ltd, 2021). Blant informasjon som ble brukt for å forberede cyberangrep var brukernavn og passord til web-administratorer, generell informasjon om maskinvarer (inkludert PC) og versjon som er i bruk, IIS versjon, IP-adresser, resultater av port-skanning, FTP-servere mm. (ClearSky Cyber Security Ltd, 2021, s. 9–10).

Videre kan man konkludere med at selv ressurssterke trusselaktører med avanserte, tekniske ferdigheter og kapabiliteter foretrekker enkleste vei, altså passiv rekognosering, fremfor mer aggressive teknikker. Blant hovedårsakene er sannsynligvis et ønske om å forbli anonym lengst mulig. Passiv rekognosering etterlater lite spor, og er billig men effektivt som demonstrert i delkapittel 5.1 og 5.2. Figur 15 illustrerer hvordan passiv rekognosering og OSINT brukes mot organisasjoner.

Figur 15: OSINT i organisatorisk kontekst



Sett i lys av de teoretiske modellene presentert i delkapittel 3.1, kan man konkludere med at modellene fremdeles er aktuelle, men den store betydningen som rekognosering og sosial manipulering har for cyberangrep bør synliggjøres i større grad. Hvorvidt en trusselaktør lykkes med *klargjøring* og *leveranse av kapabilitet* (se Figur 2), avhenger av hvor grundig rekognoseringsfasen er gjennomført. Jo flere pålitelige opplysninger om organisasjonens arbeidsmåter, kunder, leverandører, standarder for dokumentutforming, ansatte, osv. som er innhentet, desto mer troverdig vil en e-post, et vedlegg eller lenke se ut. Følgelig desto enklere vil det være for angriper å få tilgang til organisasjonens digitale systemer. Det kan og argumenteres for at rekognosering har blitt en mye enklere oppgave de siste årene. Det finnes mer åpen tilgjengelig informasjon og flere og mer effektive verktøy. Dermed sparer en trusselaktør tid og økonomiske midler, samtidig som omfanget av informasjon øker.

Personprofilering antas å være av største betydning for trusselaktører. Ifølge informanter og dokumentstudiet forklares det med at enhver organisasjon først og fremst består av mennesker. I motsetning til teknologi kan ikke folk «patches» for å fjerne sårbarheter (CE1; EH1; Hassold, 2018b, s. 2). Dokumentanalyse viser at en trusselaktør vil søke internett og sosiale medier etter

bestemte enheter/individer og etter personer tilknyttet disse. Resultatene av rekognoseringen blir videre brukt til å utforme og gjennomføre sosial manipulering-angrep, oftest ved målrettede nettfisking e-poster med inkluderer lenke til et infisert domene eller dokument. Formålet er å manipulere ofrene til å åpne vedlegg/nettside mens de bruker arbeidsgivers systemer. Hvor vellykket et manipuleringsforsøk er, avhenger av hvor grundig målet er rekognosert. Denne studien har demonstrert at rekognoseringsprosessen spiller en viktig rolle, i den forstand at «våpenets» effektivitet betinges av rekognoseringsfasen.

Man kan konkludere med at all informasjon er av betydning for trusselaktør, fordi den kan brukes til «hacking of people and hacking of systems» (CE1). Det vil si å identifisere og planlegge angrepsvektorer med utgangspunkt i (1) sosial manipulering på nøkkelansatte og (2) eksisterende tekniske sårbarheter.

6. Diskusjon: Selv-rekognosering som forebyggende redskap

I dette delkapittelet drøftes andre del av oppgavens problemstilling:

Hvordan kan selv-rekognosering ved hjelp av OSINT brukes som redskap i organisasjoners forebyggende informasjonssikkerhetsarbeid?

Analyse av funnene redegjort for i kapittel 5 bidrar til forståelse for hvordan trusselaktører kartlegger organisasjoner og hvilken rolle rekognosering og OSINT har i et cyberangrep. I denne studien argumenterer jeg for at organisasjoner bør inkludere selv-rekognosering i sitt forebyggende sikkerhetsarbeid. Teoriene presentert i delkapitler 3.2-3.4 utgjør teoretisk bakgrunn for drøftingen. Tidligere forskning som støtter både empiri og teori, inkluderes der det fremstår relevant i drøftingen.

6.1. Hvordan kan selv-rekognosering brukes som redskap i organisasjoners forebyggende informasjonssikkerhetsarbeid?

Innledningsvis har jeg nevnt at en av de største utfordringene organisasjoner må håndtere i dag er at risikobildet er så komplekst og dynamisk at det øker usikkerheten. Dette må påvirke beslutninger knyttet til risikohåndtering. I denne delen argumenterer jeg for at selv-rekognosering kan tjene som redskap i organisasjoners forebyggende sikkerhetsarbeid ved å blant annet (a) *etablere situasjonsbevissthet* og (b) *danne grunnlag for risikovurdering*. Listen over potensielle bruksområder er lang, men jeg avgrenser oppgaven til disse to.

6.1.1. Selv-rekognosering som redskap for etablering av situasjonsbevissthet

Teori-delen redegjør for at etablering av situasjonsbevissthet er nødvendig for å tilpasse forebyggende arbeid til den dynamiske teknologiske utviklingen. Organisasjoner må tenke nytt og å ta i bruk nye verktøy for å henge med. Situasjonsbevissthet forutsetter at en organisasjon har evne til å søke, avdekke og gjenkjenne relevant informasjon, tolke informasjonen og utvikle mentale modeller. Forståelse av systemet man skal beskytte står derav sentralt i sikkerhetsarbeidet og risikovurderinger.

Selv-rekognosering og OSINT som redskap for etablering av systemforståelse

Systemforståelse innebærer at man har oversikt over alle systemelementer, herunder både tekniske, organisatoriske og menneskelige (Barford et al., 2010; Grassegger & Nedbal, 2021; Hai-Jew, 2018; Ross et al., 2019). Dette vil også danne grunnlag for identifisering av verdier, sårbarheter og avhengigheter, som er en del av risikovurdering.

OSINT-metode og -verktøy kan som vist i empiri-del være et effektivt redskap for kartlegging av sosio-tekniske systemer. Med effektivt mener jeg her at bruk av verktøyene er tidsbesparende og ikke krever store økonomiske investeringer. De fleste verktøy er åpent tilgjengelige og relativt enkle å bruke (med noen unntak). Dette er også konklusjonen i undersøkelsene til Hayes og Cappa (2018) og Matvej et al. (2020). Ved å bruke nettverkskartleggingsverktøy som Nmap og/eller Shodan kunne jeg kartlegge IKT-arkitektur, enheter og programvare, sikkerhetskonfigurasjoner mm. til både organisasjon A og B på svært kort tid. For å kartlegge menneskelige, organisatoriske elementer og avhengigheter kan man bruke multifunksjonelle rammeverk, eksempelvis Maltego. Selv-rekognosering ved OSINT vil kunne oppfylle NSMs (2020d) IKT-prinsipp 1: Identifisere og kartlegge (se Figur 6).

Bruk av slike verktøy kan gjøre organisasjoner mer proaktive og tilpasningsdyktige, ved at de selv avdekker systemiske sårbarheter før en eventuell trusselaktør gjør det. Et slikt element vil gjøre dem mindre attraktive for opportunistiske trusselaktører. Eksempelvis kan nettverkskartlegging gjennomføres systematisk med korte mellomrom. Organisasjoner kan selv vurdere hvor ofte de vil skanne nettverk, da semi-strukturerte data er enkle å tolke. NSM (2020a, s. 17) også fremhever at bruk av slike verktøy «kan gi mer helhetlig situasjonsbilde og er et viktig bidrag i videreutvikling av sikkerhetsarbeidet».

Det kan tenkes at kartlegging av organisatoriske og menneskelige elementer og avhengigheter ikke nødvendigvis kan gjennomføres like lett og ofte, da analyse av dataene er mer krevende. Små og store organisasjoner vil kreve ulik hyppighet av slike kartlegginger, avhengig av deres aktivitet, funksjoner og situasjon de befinner seg i. Risikostyring må således være funksjonsbasert.

Å kartlegge et system er ikke nok for å kunne beskytte det, man må også forstå systemet, fremhever Endsley (2016, s. 14). Dette kan oppnås ved hjelp av mentale modeller og visualiseringsverktøy (Endsley 2016, s. 18). Jeg har demonstrert hvordan OSINT-verktøy kan være nyttige her (se eksempelvis Bilde 2 og Bilde 9). Nettverket til store og mellomstore

organisasjoner, som for eksempel Organisasjon A, kan bestå av hundrevis enheter og brukere, som gjør systemer uoversiklige. Visualisering via OSINT-verktøy vil da kunne bidra til å skape og presentere en helhetlig systemoversikt.

Systemforståelse er kun et av de nødvendige elementene for etablering av situasjonsbevisthet. For å kartlegge mulige konsekvenser av uønskede handlinger må man også etablere situasjonsforståelse (Endsley, 2016; Barfort et al., 2010).

Selv-rekognosering som redskap for etablering av situasjonsforståelse og forutanelsesevne

Med situasjonsforståelse menes bevissthet om dagens situasjon (Barford et al., 2010). Det kan omhandle bevissthet om status og utvikling i trusselaktørers adferd, politiske forhold, juridiske forhold mm., samt hva som er åpenbare og bakenforliggende årsaker til utviklingen (Barford et al., 2010, s. 3-4). Jeg tolker situasjonsforståelse som kontinuerlig erververlse og oppdatering av kunnskaper om det som måtte være relevant for en organisasjon.

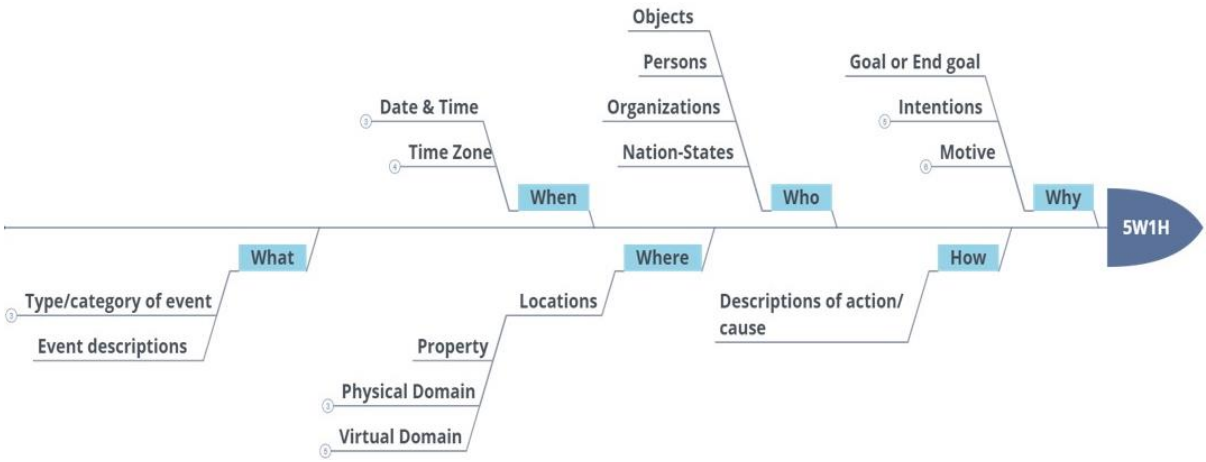
Dynamikk i trusselbilde kan følges ved eksempelvis overvåking av såkalte «real time cyber attack maps». Sanntids kart viser i tillegg hvilke bransjer som er av interesse for trusselaktører i de siste dagene eller ukene. Overvåking av utviklers plattformer, eksempelvis GitHub, kan bidra til å fange opp endringer i trusselaktørers kapabiliteter og adferd. På slike plattformer legges det ut nye verktøy som blant annet trusselaktører benytter seg av. Dette er anbefalt å gjøre av informanter i forbindelse med denne studien. Informantene fremhever slike plattformer som helt essensielt for at sikkerhetseksperter kan dele erfaringer og observere trender (CE1; CE2; CE3). Dette kan ifølge informantene bidra til å forebygge og avverge angrep ved tidlig deteksjon, bedre beredskap og erfaringsutveksling.

Overvåking av systemer og omgivelser kan bidra til etablering/utvikling av forutannelsesevne, som ifølge forskere er en nødvendig egenskap for etablering av situasjonsbevissthet (Barford et al., 2010, s. 3; Endsley, 2016, s. 18; Hollnagel et al., 2011). Forutannelsesevne innebærer å kunne forestille den fremtidige tilstanden eller angrepsvektor basert på innsamlet, oppfattet og forstått informasjon. Men, for å kunne forutsi fremtidig utvikling, må man forstå dagens situasjon. I komplekse systemer med stor gjensidig avhengighet er det vanskelig å forutsi hvordan endringer i en variabel kan påvirke resten av systemet (Endsley, 2016).

Kunnskap om delelementer i systemet og hvordan de henger sammen, kan kombinert med oppdaterte kunnskaper om situasjonsutvikling bidra til forutannelsesevne. Figur 16 illustrerer

5W1H-modellen, også kalt for «Five Ws»[14] som er et eksempel på hvordan resultater av selv-rekognosering kan bidra til situasjonsforståelse. Modellen brukes blant annet i granskninger, etterforskning og som hjelpemiddel i beslutningstaking (Breivikås, 2021b, 2021a).

Figur 16: Situasjonsforståelse (Breivikås, 2021)



5W1H er bare et av flere eksempler på hvordan resultater av rekognosering kan brukes for å etablere situasjonsforståelse ved å lage mentalle modeller. Et annet eksempel vist i empiri-del er lenke-diagrammer (se eksempelvis Bilde 2 og Bilde 5). Slike diagrammer kan lages svært effektiv med eksempelvis Maltego.

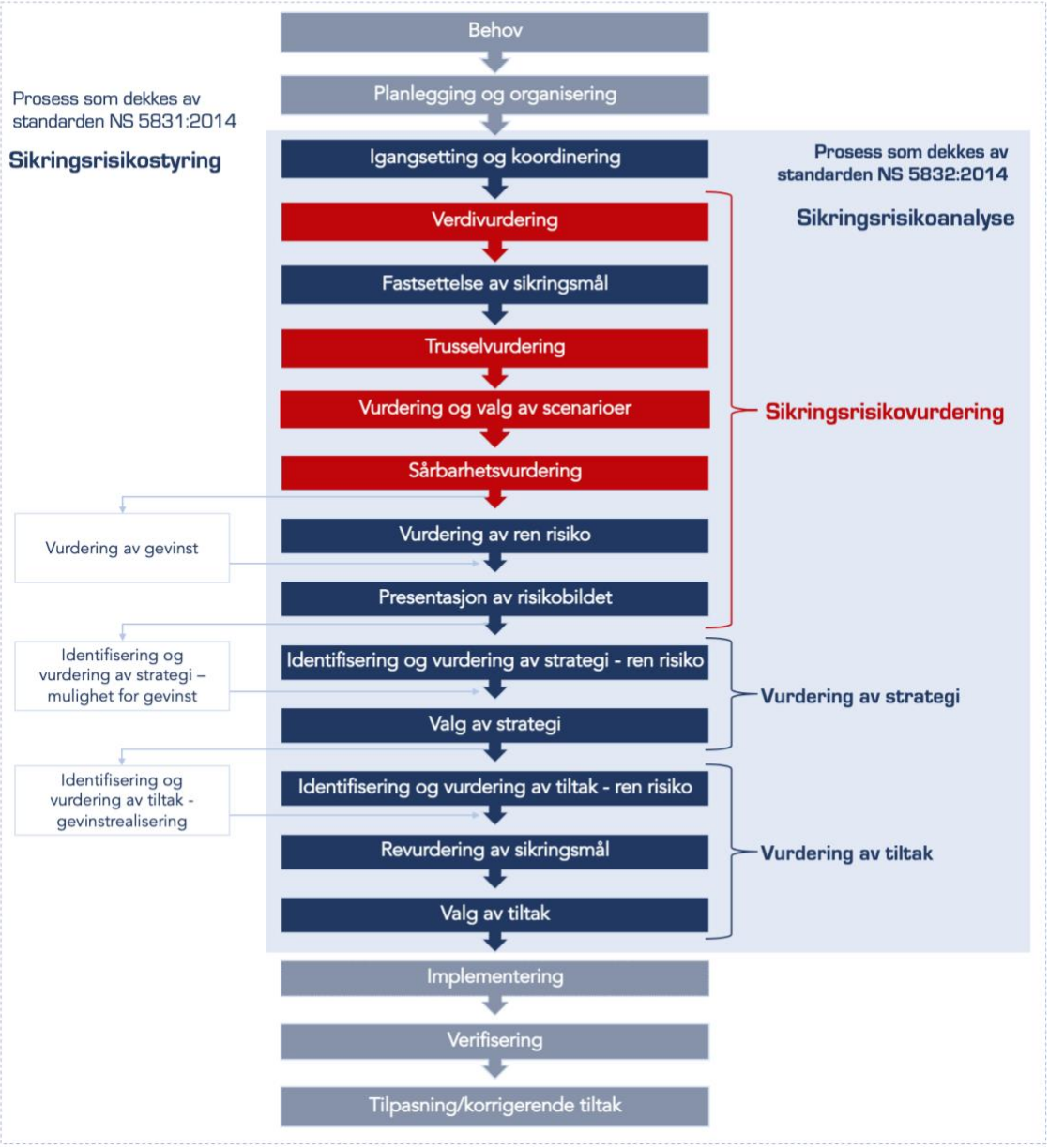
6.1.2. Selv-rekognosering og OSINT som basis for risikovurdering

Som nevnt tidligere stiller sikkerhetsloven (2018) krav til at virksomheter underlagt loven skal etablere sikkerhetsstyring for forebyggende sikkerhet i samsvar med krav i loven. Dette innebærer blant annet gjennomføring og iverksettelse av sikkerhetstiltak basert på risikovurdering (Sikkerhetsloven, 2018). I informasjonssikkerhet brukes ofte Norsk Standard 583X:2014 som krav til helhetlig prosess av risikostyring for uønskede tilsiktede hendelser.

Figur 17 viser at risikovurdering i henhold til trefaktormodellen innebærer en helhetsvurdering basert på blant annet verdi-, trussel-, scenario- og sårbarhetsvurdering, samt presentasjon av risikobilde. I denne oppgaven ser jeg på bruk av selv-rekognosering i risikovurderingsfase (markert med rødt i modellen).

[14] Det er uklart hva er det opprinnelige kilde til «Five Ws» modellen.

Figur 17: Sammenhengen mellom sikringsrisikostyring, -analyse og -vurdering (NS 583X:2014)



Kommentar til Figur 17: Lyseblått område i modellen markerer delprosesser som dekkes av risikoanalyse, herunder vurdering av sikringsrisiko, strategi og tiltak. Risikovurdering består av (a) verdivurdering, (b) fastsettelse av sikringsmål, (c) trusselvurdering, (d) vurdering og valg av scenarioer, (e) sårbarhetsvurdering, (f) vurdering av ren risiko og (h)presentasjon av risikobilde. Oppgavens diskusjon er avgrenset til delprosesser a, c, d og e (markert med rød).

Sårbarhets- og verdivurdering

Standarden presenterer risikovurdering i form av en lineær prosess, hvor verdivurdering kommer først, deretter gjennomføres trusselvurdering. Resultater av disse to aktivitetene legges til grunn for utarbeidelse av scenarioer, som samsvarer med hvordan trusselaktører kan

skade verdiene (NS 5832:2014, s. 6). Dette er, ifølge standarden, for å avdekke organisasjonens sårbarheter opp mot valgte scenarioer. Det vil si at sårbarhetsvurdering kommer til slutt.

Her er det nødvendig å nevne tre utfordringer. For det første gir ikke NS 5832:2014 detaljerte forklaring på hvordan man skal fastsette eller definere verdiene. Verdiene kan være svært forskjellige fra virksomhet til virksomhet, og det finnes ingen god operasjonalisering som kan hjelpe virksomheter med denne delprosessen. For det andre er mange virksomheter og individer av den oppfatning at de ikke besitter verdier som er av interesse for målrettede digitale operasjoner (NSM, 2020a). For det tredje, når vi risikovurderer IT-systemer forholder vi oss til tilsiktede så vel som utilsiktede handlinger.

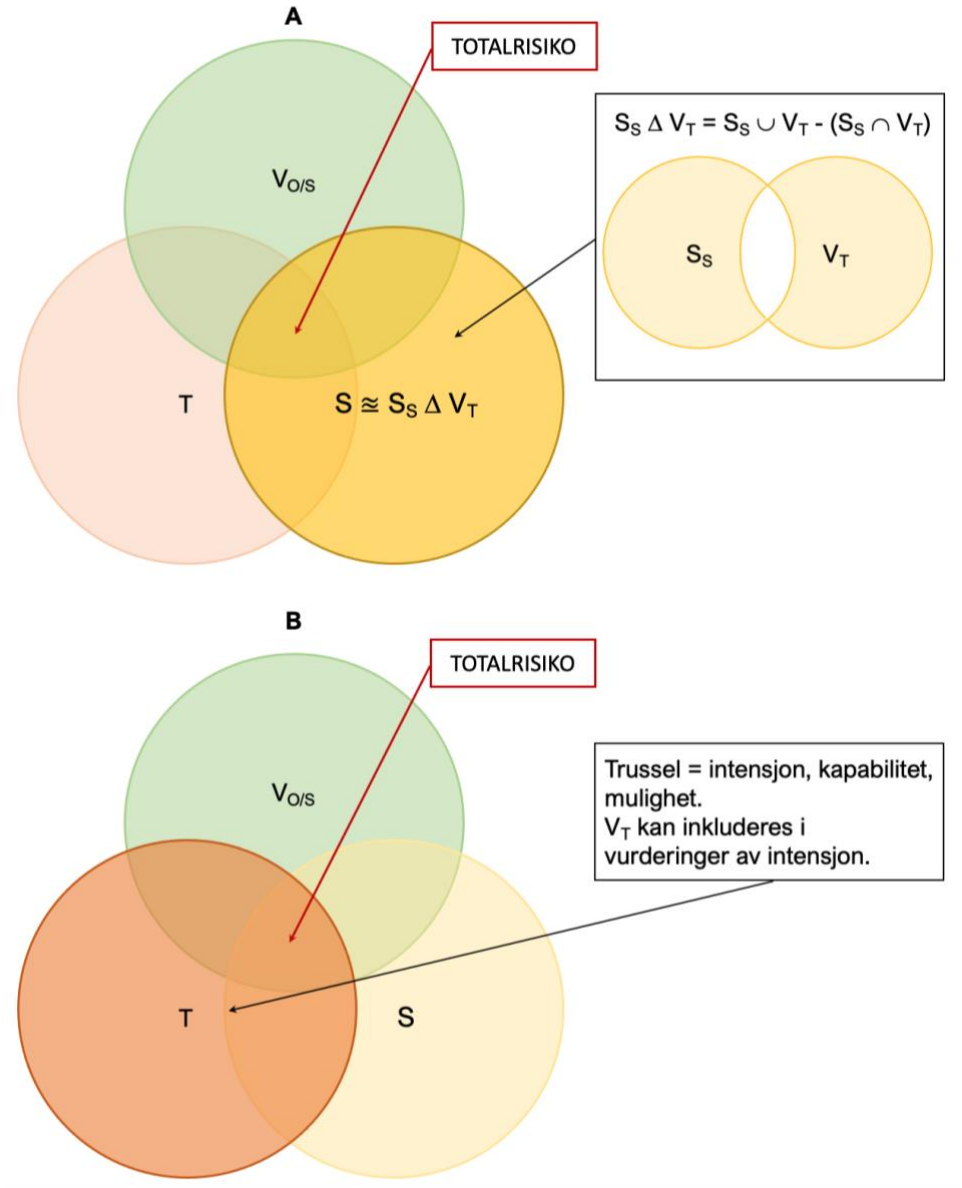
For å møte disse utfordringene bør man se på sin egen virksomhet med trusselaktørs øyene. Dette kan gjøres ved å inkludere noe som kan være av verdi for en trusselaktør i sårbarhetsvurdering. Forenklet kan det vises som $S \cong S_S \Delta V_T$[15], hvor V_T er noe av interesse for en trusselaktør, S_S er en potensiell sårbarhet i en organisasjons sosio-tekniske systemer forårsaket av fravær av sikkerhetstiltak mot trusler og S er totalsårbarhet. Inkludering av trusselaktørs perspektiv forutsetter at verdier og sårbarheter vurderes samtidig. Ved å identifisere hva som kan representere verdi for en angriper, kan man vurdere hvorvidt denne «verdien» representerer sårbarhet for en organisasjon og kan skjermes, fjernes eller sikres på andre måter. Fjerner man sårbarhet og skjermer verdier, minimerer man risiko. Dette illustreres i Figur 18A.

Det kan rettes kritikk mot modellen illustrert i Figur 18A. Det kan argumenteres for at man i kontekst av trefaktormodellen må skille klart mellom som hva er verdi for trusselaktør og hva som er verdi for virksomhet. Man søker da å identifisere hvilken risiko, verdi, trussel og sårbarhet representerer for virksomheten. Avsløring eller offentliggjøring av sårbarhet utgjør ikke nødvendigvis tap for virksomheten i seg selv. Det er når sårbarheter utnyttes for å nå de andre verdiene at risiko og konsekvens materialiserer seg. Det betyr ikke nødvendigvis at trefaktormodellen bør erstattes, men man bør ha et bevisst forhold til verdier som ikke alltid er like synlige gjennom «risikoeiers briller». Alternativt kan man inkludere vurdering av V_T som

[15] $S \cong S_S \Delta V_T$ er lik $S_S \cup V_T - (S_S \cap V_T)$. Jeg bruker «*tilnærmet lik*» istedenfor «*er lik*» fordi det ikke alltid er tilfelle. Selv om jeg bruker et matematisk symbol, bør ikke formelen leses som et matematisk uttrykk, men en illustrasjon av tankegangen.

del av trusselvurdering, som det er illustrert i Figur 18B. Denne modellen vil også være i tråd med sikkerhet vs. security-tankegangen.

Figur 18: Trefaktormodellen hvor trusselaktørs perspektiv er inkludert



Kommentar til Figur 18:

$V_{O/S}$ – noe som er av verdi for organisasjon og/eller samfunn, eks. informasjon, kritisk infrastruktur, kompetanse osv.,

T – trussel som består av intensjon, mulighet og kapabilitet,

S -totalsårbarhet,

S_S - sårbarhet i en sosio-tekniske systemer forårsaket av fravær av sikkerhetstiltak mot trusler,

V_T – noe som er av verdi for en trusselaktør og ikke ansees nødvendigvis som verdi av et offer.

Vi kan eksempelvis ta for oss en forenklet verdivurdering for de to organisasjonene som jeg har undersøkt i studien. Organisasjonene driver med forskning og utvikling. Empiri i studien viser at verdiene vanligvis vil være i form av dokumentert kunnskap. Det vil si elektroniske og/eller fysiske dokumenter som inneholder resultater av forskning som er av relevans for andre organiserte aktører eller stater. Økonomiske midler kan selvfølgelig også være verdier av interesse for trusselaktører.

Verdier for en trussealktør vil i tillegg være flere typer informasjon. Det kan være for eksempel SoMe innlegg, bilder som avslører sikkerhetsbarrierer eller teknisk infrasruktur, personlige opplysninger om ansatte og deres omgangskrets. Denne informasjon inkluderes sjelden i risikobildet, selv om den kan utgjøre sårbarhet hvis den er åpen tilgjengelig. Som empirien i tillegg viser, kan en aktør selge sårbarheter videre og de derigjennom blir en verdi (se «Silent Librarian»-case). Hvorvidt Organisasjon A og B faktisk inkluderer disse verdiene i sin risikovurdering, er imidlertid uvisst for meg på nåværende tidspunkt.

Målutvelgelse og trusselvurdering

I IKT-sikkerhet vil trusselvurdering innebære vurdering av trusselaktørs intensjon, kapabilitet og mulighet (Bergsjø et al., 2020, s. 151-153; NSM, 2020c). Med *intensjon* menes motivasjon og formål med angrep. *Kapabilitet* innebærer aktørs ferdigheter, kunnskaper, ressurser, arbeidskraft osv. *Mulighet* innebærer hvorvidt aktør er målrettet, og/eller opportunistisk (Bergsjø et al., 2020, s. 151-153; NSM, 2020c).

CKC-modellen illustrert i Figur 2 starter med målutvelgelse. *Målutvelgelse* ved vurderingen av om det er antydninger til at noe kan skje snart, kan også være aktuelt å inkludere her (Busmundrud et al., 2015, s. 32). Vurderinger av målutvelgelse innbefatter sannsynlighets-elementet, som ifølge FFI ikke er med i trefaktormodellen som et eksplisitt parameter, men som implisitt er med i trusselvurderingen.

Ifølge Bergsjø et al. (2020) reflekterer målutvelgelse trusselaktørens interesser, motivasjoner og hvilke verdier det potensielle målet besitter (Bergsjø et al., 2020). Dette argumentet henger sammen med tidligere nevnt utfordring at komponenter til en viss grad flyter inn i hverandre. Eksempelvis kan ansatte både være en verdi, en trussel og en sårbarhet (Hayes & Cappa, 2018, s. 694; Sikkerhetsloven, 2018). Dette bør inkluderes i risikoanalyser. Hayes og Cappa (2018, 693-694) presenterer et eksempel på hvordan dette kan gjøres. De henviser til en praksis som

innebærer generering av risikopoeng for hver ansatt som er basert på personlige forutsetninger. Dette utgjør grunnlag for vurdering av risiko og identifisering av personell som er mest utsatt for angrep. Forfattere argumenterer for at denne metoden tillater en organisasjon å prioritere ressurser, utforme policyer og gi målrettet og tilpasset sikkerhetstrening til ansatte. Hayes og Cappa (2018, s. 693) fremhever at risikorangering skal ikke brukes til å forhindre individets tilgang til skjermingsverdig eller sikkerhetsgradert informasjon. Disse tallene bør benyttes kun som indikatorer for å gjøre både ledelsen og personell bevisst på potensielle trusler. Dette kan brukes av alle organisasjoner uansett størrelse, skriver forfatterne.

Hvordan kan det hjelpe organisasjoner?

Ifølge NS 5832:2014 skal trusselvurderingene og verdivurderingene legges til grunn for scenarioer som beskriver trusselaktørers fremgangsmåter for å skade verdiene, og derav er relevante for videre analyse.

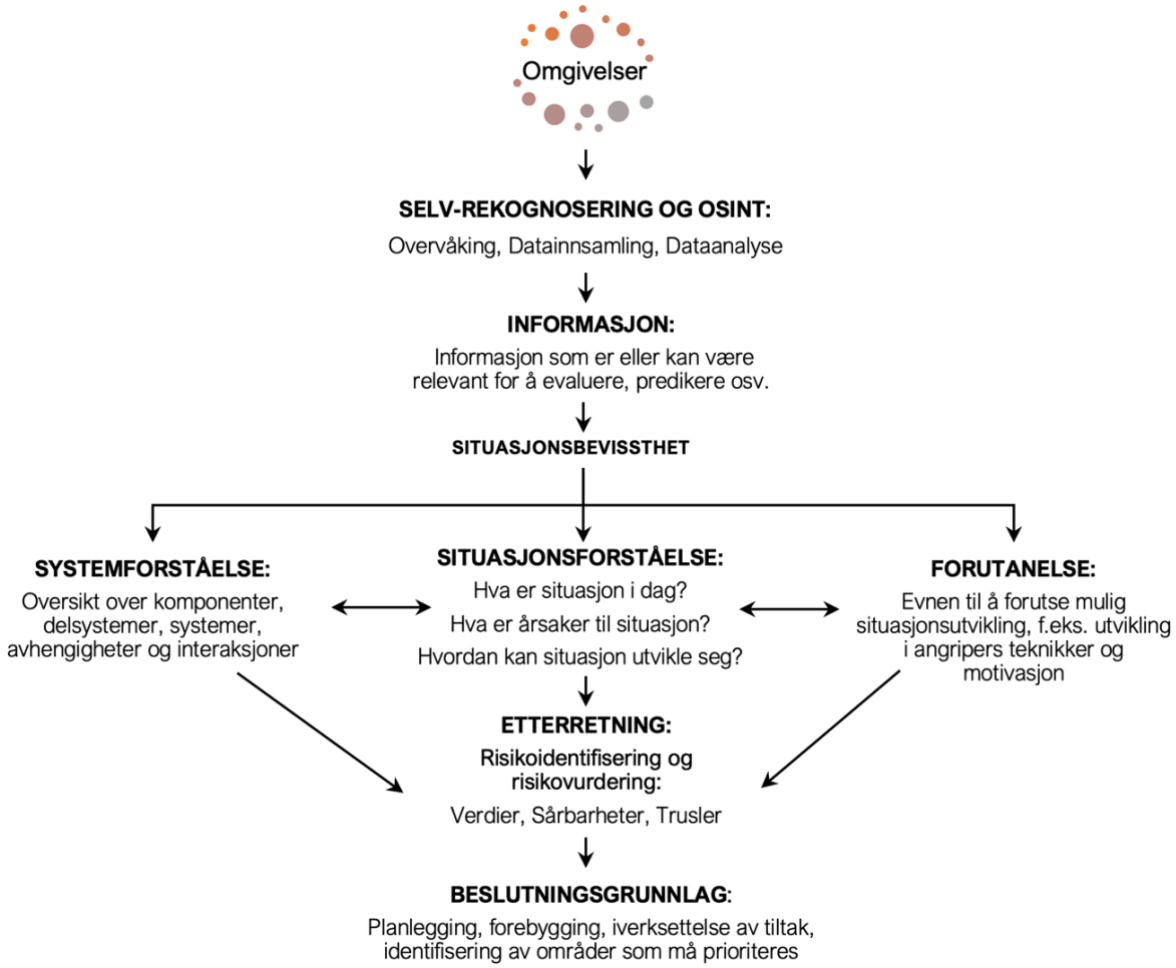
Jeg har allerede nevnt at trusselaktør velger den enkleste vei. Enkleste vei vil være å avdekke sårbarheter som er enkle å utnytte ved bruk av teknikker som ikke er lett å spore. Empirien viser at de lett utnyttbare sårbarhetene først og fremst er brukere, deres digitale fotspor og feilkonfigureringer i nettverket. Kunnskap om dette kan bidra til valg og vurdering av ulike scenarioer.

De kan identifisere eksponerte elementer som kan representere verdi for en trusselaktør og skjerme disse eller fjerne når det er mulig. Eksempelvis kan informasjon om IP-adresser og domener skjermes gjennom betaling av et lite gebyr til myndigheter som registrerte disse. Videre kan organisasjoner overvåke datalekkasjer for å avdekke tidlig hvorvidt sensitive data om ansatte er eksponert. Dette bør selvfølgelig gjøres på en måte som ikke strider med lovverk og GDPR. Eksempelvis kan ansatte informeres om nylig datalekkasje og bes om å sjekke hvorvidt deres data ble kompromittert. Dette kan også bidra til å øke ansattes bevissthet rundt egen eksponering. Også Hayes og Cappa (2018) fremhever at verdien av overvåking av datalekkasjer i sann tid bør ikke undervurderes. Man bør også vurdere å fjerne metadata fra dokumenter og bilder som offentliggjøres. Innhold i jobbannonser bør vurderes opp mot hvilken informasjon om eksempelvis IT-ansvarlig er eksponert og i hvilken grad er det mulig å gi ut minst mulig sensitiv informasjon uten at det går på bekostning av formålet med annonsen. Denne liste av enkle tiltak kan fortsettes og organisasjoner kan selv velge hva de bør og kan inkludere i sitt daglige sikkerhetsarbeid.

NSM (2020c, s. 10) advarer om at overvåking av egne sårbarheter ikke er nok, som følge av økt gjensidig avhengighet. Man må påse sårbarheter som arves av virksomheter som ligger tidligere i verdikjeden. En trusselaktør inngangspunkt kan ramme på et hvert trinn i verdikjeden, og som vist i empiri-del kan trusselaktører bevege seg på tvers gjennom flere ledd på veien mot sitt endelige mål (NSM, 2020c). Dette er kanskje spesielt sårbart i tilfeller hvor organisasjoner tjenesteutsetter hele, eller deler av sine systemer, som Organisasjon B. Herunder mer sårbart ved flere ledd og mindre oversikt. NSM (2020c) fremhever at alle virksomheter som forvalter skjermingsverdige systemer og som velger tjenesteutsetting må gjennomføre risikovurderinger knyttet til verdikjeder de er en del av. I denne oppgaven viser jeg at dette kan gjøres ved bruk av OSINT-verktøy, ved å utvide søk i forhold til hva jeg har gjort i denne studien, til å omfatte underleverandører og tredjeparter.

Figur 19 er forenklet fremstilling av hvordan kan selv-rekognosering ved hjelp av OSINT være redskap i forebyggende informasjonssikkerhetsarbeid og oppsummerer min tankegang.

Figur 19: Hvordan kan selv-rekognosering være redskap i forebyggende informasjonssikkerhetsarbeid



6.2. Utfordringer og nødvendige forutsetninger

6.2.1. Forutsetninger som må være på plass

Bruk av selv-rekognosering og OSINT strider ikke med lovverket og er i tråd med NSMs grunnprinsipper for informasjonssikkerhet (se Figur 6). Men for at selv-rekognosering kan brukes i organisasjoner er det en del forutsetninger som bør være på plass (Breivikås, 2021b).

For det første bør det utarbeides rammeverk og prosessbeskrivelser for aktivitetene. Faglitteratur tilbyr flere ulike forslag for hvordan prosessen kan utformes (se f.eks AlKilani & Qusef, 2021; Brooks & Larson, 2020; Wiradarma & Sasmita, 2019). Rammeverket skal redegjøre for hvordan informasjon innsamles og hvordan informasjonskvalitet vurderes. Her kan man eksempelvis bruke OSINT-hjulet som grunnlag, etterforsknings-hjulet eller såkalt Åttetallet-modellen (Politiet, 2014, s. 18 referert i Gibson, 2016; Paulsen & Simensen, 2019; Ratcliffe, 2016). Gibson (2016, s. 106) argumenterer for at kilder og informasjon skal vurderes mot fem kvalitetskriterier (a) pålitelighet, (b) validitet, (c) objektivitet, (d) gyldighet og (e) relevans.

For det tredje er det viktig å være systematisk, samtidig som man må være fleksibel og oppdatert når det gjelder bruk av verktøy. Som med alle andre metoder for datainnsamling bør man være konsekvent i bruk av måleinstrumenter. Nye verktøy bør testes og vurderes opp mot mål og funksjoner. OSINT som datainnsamlingsmetode byr på flere muligheter og utfordringer ved utforming, planlegging og gjennomføring av prosessen. Mulighetene er mange, sikkerhetsansvarlige kan selv vurdere hvilket rammeverk som passer best til deres forutsetninger. Man må imidlertid huske at ingen rammeverk garanterer fullstendig sikkerhet for organisasjoner som opererer i cyberspace.

Et av de viktigste aspekter er at bruk av metoden skal være juridisk forankret i alle faser, særlig når det gjelder GDPR (Breivikås, 2021b). Sikkerhet vs. personvern-dimensjonen er en stadig voksende problemstilling, som ikke har entydige svar.

6.2.2. Personvern og demokrati vs. sikkerhet-dilemma

Demokrati vs. sikkerhets-dilemmaet er en av nåtidens store utfordringer. Det er viktig at bruk av OSINT for personprofilering ikke nedprioriteres uten videre, til fordel for sikkerhetshensyn

(Cartagena et al., 2020; Rønn & Søe, 2019). På grunn av økende interesse fra både privat sektor og offentlige myndigheter etterlyser Omand, Bartlett og Miller (2012) et etisk rammeverk for bruk av SOCMINT for sikkerhetsrelaterte hensyn. Forfatterne foreslår følgende krav til bruk av metoder:

1) krav til tilstrekkelig forsvarlig årsak,
2) krav til integritet av motivet,
3) krav til proporsjonalitet og nødvendighet av metoder,
4) krav til regelmessig tilsyn av et myndighetsorgan,
5) bruk av metoder må være en siste utvei,
6) krav til informert samtykke (Omand et al., 2012, s. 820–822).

Rønn og Søye (2019, s. 374) uttrykker enighet om at disse prinsippene kan brukes som rettesnor, men mener at begrepet «informert samtykke» er et konsept som kun fungerer på papir. Forfatterne skriver at brukere av sosiale medier i praksis ikke har kontroll over deres personlige informasjon. De argumenterer for at bruk av informasjon innsamlet fra SoMe brukerkontoer kan ha negativ effekt på hvordan vi samhandler og hvordan vi bruker sosiale medier. Til slutt er det samfunnet som helhet og demokrati spesifikt som betaler prisen.

Personprofilering ved hjelp av OSINT brukes i dag for bakgrunnssjekk av potensielle ansatte. Men fra et menneskerettighetsperspektiv krever innsamling av OSINT regulering på statlig nivå. Cartagena et al. (2020) påpeker at dette er spesielt viktig når sikkerhetsmyndigheter og private selskaper bruker og utveksler informasjon. Dette innebærer også at forankring av bruk av metoder hos interessenter og ledelse må være på plass (Breivikås, 2021b).

Prosessen med å redusere risikoen for misbruk av åpen informasjon er kompleks. Demokratiske verdier og lovverk setter begrensninger for hvilke tiltak en kan og bør gjøre. De setter blant annet grenser for i hvilken grad en organisasjon kan føre kontroll med og overvåke sine ansatte, i tillegg til å sette krav til offentlig åpenhet om flere forhold. Derav forblir disse problemstillingene viktige elementer i dagens og fremtidens samfunnsdebatt (NSM, 2020c, s. 19).

7. Konklusjon

Formålet med denne studien har vært å undersøke

Hvordan kartlegger trusselaktører organisasjoner og hvordan kan selv-rekognosering brukes som redskap i organisasjoners forebyggende informasjonssikkerhetsarbeid?

Den første delen av problemstillingen, *hvordan kartlegger trusselaktører organisasjoner,* har vært undersøkt ved hjelp av metoder som brukes av trusselaktører, dokumentstudie samt intervjuer med etiske hackere og cybereksperter. I empiri-delen har jeg demonstrert hvordan trusselaktører opererer og hva som kan være av interesse for de når det gjelder informasjonssikkerhet. For å eksemplifisere har jeg kartlagt to organisasjoner som driver med forskning og utvikling. Dette for å vise hvor mye informasjon er tilgjengelig for uvedkommende og for å demonstrer metoder og teknikker som brukes av trusselaktører.

Funnene indikerer at de aller fleste nettangrep starter med passiv digital rekognosering av organisasjoner. Denne fasen består av kartlegging av infrastruktur og omgivelser, og profilering av nøkkelpersonell ved bruk av OSINT-metode og -verktøy. Mengden åpen tilgjengelig informasjon om individer og organisasjoner på nett har eksplodert i de siste årene, som gjør at en trusselaktør kan samle store mengder informasjon på en effektiv måte. Fragmentert og stykkvis representerer ikke nødvendigvis informasjon særlig stor verdi. Men når informasjonsbiter struktureres og settes i sammenheng kan den imidlertid oppnå større verdi, i slik grad at den kan utnyttes til å forårsake skade på organisasjoner og/eller samfunnet.

Etter passiv rekognosering starter en trusselaktør med aktiv skanning av offerets nettverk og kartlegging av teknisk infrastruktur, brukere og konfigurasjoner. Funnene indikerer at selv ressurssterke trusselaktører med avanserte, tekniske ferdigheter og kapabiliteter foretrekker passiv rekognosering, som er enkleste vei, fremfor mer aggressive teknikker. Dette fordi denne metoden bidrar til at en trusselaktør kan forbli anonym lengst mulig.

Alle disse aktivitetene danner grunnlag for skissering av angrepsflate, som videre brukes i planlegging av et cyberangrep.

Den andre delen av problemstillingen, *hvordan kan selv-rekognosering brukes som redskap i organisasjoners forebyggende informasjonssikkerhetsarbeid,* ble besvart med bakgrunn i empiri og teorier om situasjonsbevissthet og trefaktormodellen for risikovurderinger.

Jeg har argumentert for at organisasjoner ved å bruke selv-rekognosering vil ha bedre forutsetninger for å avdekke, fjerne, minske eller skjule sårbarheter og dermed motvirke potensielle trusselaktører. Selv-rekognosering og OSINT kan være redskap i forebyggende sikkerhetsarbeid ved å etablere systemforståelse, bevissthet om dagens situasjon og mulig situasjonsutvikling. Situasjonsbevissthet er dermed en viktig forutsetning for et effektivt og proaktivt forebyggende informasjonssikkerhetsarbeid, særlig når det gjelder sårbarhets- og trusselvurderinger.

Forståelse av sine sårbarheter er imidlertid ikke tilstrekkelig for å beskytte seg mot en målrettet trusselaktør. God forebygging krever at organisasjoner identifiserer verdier som må beskyttes. Jeg argumenterer for at det ikke bare er organisasjonens verdier som må kartlegges, men at organisasjoner og bør forstå hva er en trusselaktør kan være interessert i. Å vite hvilke verdier som kan være interessante for en trusselaktør er imidlertid en stor utfordring for mange organisasjoner, påpeker NSM (2020c). I denne forbindelse fremheves det to problemer. For det første spesifiserer ikke standardene hvordan man operasjonaliserer verdier. For det andre er mange virksomheter og individer av den oppfatning at de ikke besitter verdier som er av interesse for en trusselaktør. I denne oppgaven har jeg demonstrert hvordan organisasjoner kan se på egen virksomhet gjennom trusselaktørs briller. Vurderinger av hva som kan representere verdi for en trusselaktør, kan med fordel inkluderes i risikovurderinger som et element i sårbarhetsvurdering eller i vurdering av intensjon.

Jeg konkluderer med at selv-rekognosering og OSINT med fordel kan brukes i organisasjoners forebyggende informasjonssikkerhetsarbeid ved å etablere situasjonsbevissthet, identifisere verdier og sårbarheter, og dermed være grunnlag for å vurdere ulike scenarioer og angrepsvektorer. Selv-rekognosering kan midlertid ikke gi absolutte svar eller eliminere all usikkerhet.

OSINT som datainnsamlingsmetode byr på flere muligheter og utfordringer ved utforming, planlegging og gjennomføring av prosessen. Virksomheter må utvise varsomhet og bevissthet ved eksponering av informasjon, som trusselaktører kan utnytte i forberedelser eller utvikling av angrep.

Informasjon som kan brukes for å målrette angrep, er opplysninger om virksomheten, ansatte, funksjoner og brukerroller. Detaljer om hvilke produkt og versjoner som brukes, hvordan de brukes og sikkerhetstiltak, muliggjør undersøkelser av sårbarheter og derav kartlegging av

mulige innganger. Opplysninger om produsenter, leverandører og distribusjonsnettverk kan utnyttes til å kompromittere produkter og forsendelser.

Avslutningsvis vil jeg fremheve viktigheten av deltakelse i ulike faglige fora og nettsamfunn hvor eksperter deler sine erfaringer om både utvikling i trusselaktørers verden og i bruk av metoder for innsamling av åpen tilgjengelig informasjon. Mitt inntrykk er at i andre land er disse miljøene svært aktive og erfaringsdeling er forankret i mange ledd. Enkelte organisasjoner kan ikke ta kampen mot digital kriminalitet alene.

7.1. Forslag til videre forskning

Jeg ser at flere organisasjoner i dag tar i bruk OSINT verktøy. Det er derfor nødvendig å forske på de etiske implikasjoner bruk av metodikken medfører. Å belyse aspekter som feilinformasjon, personvern og lovlighet vil være avgjørende for regulering av OSINT. Det er fortsatt en lang vei å gå i dette området, og til det formålet bør forskere og beslutningstakere diskuterte utfordringene rundt implementering av OSINT i sikkerhetsarbeid.

Mens denne studien rettet søkelys mot to organisasjoner som driver med forsknings og utvikling, bør man også fokusere på bruk av OSINT for risikovurderinger i andre næringer for å øke vår kunnskap om organisasjoners eksponeringsgrad. Jeg etterlyser en komparativ tverrsektoriell studie som undersøker årsaker til forskjellene mellom ulike sektorer og eventuelt på tvers av nasjonale grenser.

8. Litteraturliste

Abello, J., Pardalos, P. M., & Resende, M. G. C. (2013). *Handbook of Massive Data Sets*. New York, NY: Springer.

Akhgar, B., Sampson, F., & Bayerl, S. P. (Red.). (2016). *Open source intellegence investigation*. Cham, Switzerland: Springer International Publishing.

Alhayani, B., Abbas, S. T., Khutar, D. Z., & Mohammed, H. J. (2021). Best ways computation intelligent of face cyber attacks. *Materials Today: Proceedings*, S2214785321016989. https://doi.org/10.1016/j.matpr.2021.02.557

AlKilani, H., & Qusef, A. (2021). OSINT Techniques Integration with Risk Assessment ISO/IEC 27001. *International Conference on Data Science, E-Learning and Information Systems 2021*, 82–86. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3460620.3460736

Anderson, R. (2021, januar 27). Watch Out for the Silent Librarian: An Interview with Crane Hassold. Hentet 9. april 2021, fra The Scholarly Kitchen website: https://scholarlykitchen.sspnet.org/2021/01/27/watch-out-for-the-silent-librarian-an-interview-with-crane-hassold/

Angrosino, P. A., & Coffey, A. (2000). Rethinking observation: From method to context. I N. K. Denzin & Y. S. Lincoln (Red.), *Handbook of qualitative research* (2. utg., s. 673–702). Thousand Oaks, California: Sage.

Anholt, R., & Boersma, K. (2018). *From Security to Resilience: New Vistas for International Responses to Protracted Crises*. IRGC. Hentet fra https://beta.irgc.org/wp-content/uploads/2018/12/Anholt-et-al-for-IRGC-Resilience-Guide-Vol-2-2018.pdf

APWG. (2019). *Phishing Activity Trends Report. Unifying the Global Response To Cybercrime* (s. 13). APWG. Hentet fra APWG nettside: www.apwg.org

Barford, P., Dacier, M., Dietterich, T. G., Fredrikson, M., Giffin, J., Jha, S., … Wang, C. (2010). Cyber SA: Cyber Situational Awareness for Cyber Defense. I S. Jajodia, V. Swarup, S. Jajodia, P. Liu, & C. Wang (Red.), *Cyber situational awareness: Issues and research* (s. 3–13). New York: Springer.

Bazzell, M. (2021). *Open source intelligence techniques: Resources for searching and analyzing online information*. (Sixth Edition).

Bergsjø, H., Windvik, R., & Øverlier, L. (2020). *Digital sikkerhet: En innføring* (1. utg.). Oslo: Universitetsforlaget.

Berman, G. *United States of America v. Rafatnejad et al.*, 1:18-cr-00094-JMF (United States District Court Southern District of New York 2018).

Bertalanffy, L. van. (2003). *General system theory: Foundations, development, applications* (Rev. ed., 14. paperback print). New York: Braziller.

Bharara, P. *United States of America v. Fathi et al.* , (United States District Court Southern District of New York 24. mars 2016).

Bing. (2021). Bing.com [Søkemotor]. Hentet 15. mars 2021, fra Bing website: https://www.bing.com

Blaikie, N. W. H., & Priest, J. (2019). *Designing social research: The logic of anticipation*. Cambridge, UK ; Medford, MA: Polity.

Boin, A., & McConnell, A. (2007). Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience. *Journal of Contingencies and Crisis Management*, *15*(1), 50–59. https://doi.org/10.1111/j.1468-5973.2007.00504.x

Boin, A., 't Hart, P., Stern, E., & Sundelis, B. (Red.). (2005). *The politics of crisis management: Public leadership under pressure*. Cambridge, UK ; New York: Cambridge University Press.

Bowen, G. A. (2009). Document Analysis as a Qualitative Research Method. *Qualitative Research Journal*, *9*(2), 27–40. https://doi.org/10.3316/QRJ0902027

Breivikås, T. A. (2021a). Tabalizer/5W1H [Database]. Hentet fra GitHub.com website: https://github.com/tabalizer/5W1H/blob/b6a40b639c3df7a11b2e987937cf3fdfb447eb2b/5W1H.pdf

Breivikås, T. A. (2021b, mai 27). *Trusler og Etterretning i Andeby*. Presentasjon presentert på Webinar - trussel og etterretningsprosessen i regi av ASIS Norge.

Brombach, H. (2017, mars 16). Studie om nulldagssårbarheter viser at risikoen ved hemmelighold er liten. Hentet 20. mars 2021, fra Digi.no website: https://www.digi.no/artikler/studie-om-nulldagssarbarheter-viser-at-risikoen-ved-hemmelighold-er-liten/377999

Brooke, A., & Anderson, M. (2021, april 7). Social Media Use in 2021. Hentet 2. mai 2021, fra Pew Research Center: Internet, Science & Tech website: https://www.pewresearch.org/internet/2021/04/07/social-media-use-in-2021/

Brooks, C. J., Grow, C., Craig, P., & Short, D. (2018). *Cybersecurity: Essentials*. Hoboken, NJ: SYBEX, Wiley.

Brooks, C., & Larson, S. (2020). *Open Source Intelligence*. Dragos.

Busmundrud, O., Endregard, M., Kiran, J. H., & Maal, M. (2015). *Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger* (s. 149). Kjeller: FFI.

Cartagena, A., Rimmer, G., van Dalsen, T., Watkins, L., Robinson, W. H., & Rubin, A. (2020). Privacy Violating Opensource Intelligence Threat Evaluation Framework: A Security Assessment Framework For Critical Infrastructure Owners. *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*, 0494–0499. Las Vegas, NV, USA: IEEE. https://doi.org/10.1109/CCWC47524.2020.9031172

Chauhan, S. (2015). *Hacking web intelligence: Open source intelligence and web reconnaissance concepts and techniques* (First edition). Amsterdam: Elsevier.

Christensen, L. B., Johnson, R. B., & Turner, L. A. (2015). *Research methods, design, and analysis* (Twelfth edition, global edition). Harlow, England: Pearson.

ClearSky Cyber Security ltd. (2021). *"Lebanese Cedar" APT. Global Lebanese Espionage Campaign Leveraging Web Servers*. Hentet fra https://www.clearskysec.com/wp-content/uploads/2021/01/Lebanese-Cedar-APT.pdf

Coughlan, S. (2017, juni 15). Top university under «ransomware» cyber-attack. *BBC News*. Hentet fra https://www.bbc.com/news/education-40288548

Coville, R. J. *United States of America v. Andrienko et al.* , 20-CR-316 (United States District Court Western District of Pennsylvania (Alleghency County) 19. oktober 2020).

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (Fifth edition). Los Angeles: SAGE.

Crowdstrike. (2021). *Global Threat Report 2021* [Trusselvurdering].

CSIS. (2021). *Significant Cyber Incidents Since 2006*. Center for Strategic & International Studies. Hentet fra https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

CVE Details. (2021). Cisco Aironet Access Point Software: List of security vulnerabilities. Hentet 15. mai 2021, fra Cvedetails.com nettside: https://www.cvedetails.com/vulnerability-list/vendor_id-16/product_id-32537/Cisco-Aironet-Access-Point-Software.html

Dargahi, T., Dehghantanha, A., & Taylor, P. (2019). *Analysis of APT Actors Targeting IoT and Big Data Systems: Shell_Crew, NetTraveler, ProjectSauron, CopyKittens, Volatile Cedar and Transparent Tribe as a Case Study*.

Datatilsynet. (u.å.). Kan arbeidsgiveren lese ansattes private e-poster og filer? Hentet 24. april 2021, fra Datatilsynet nettside: https://www.datatilsynet.no/regelverk-og-verktoy/sporsmal-svar/Arbeidsliv/har-arbeidsgiveren-lov-til-a-lese-de-ansatte-sine-private-e-poster-og-filer/

Dawson, C. (2020). *A-Z of digital research methods*. London ; New York, NY: Routledge, Taylor & Francis Group.

DeHashed. (2021). Dehashed: Compromised Assets. Hentet 12. mars 2021, fra www.dehashed.com

Dekker, S. (2014). *The field guide to understanding «human error»* (Third edition). Farnham, Surrey, England ; Burlington, VT, USA: Ashgate.

Dekker, S. (2016). *Just Culture* (2. utg.). Aldershot: Ashgate.

Denzin, Norman K. (1978). *The research act: A theoretical introduction to sociological methods* (2d ed). New York: McGraw-Hill.

Departementene. (2012). *Nasjonal strategi for informasjonssikkerhet* (s. 32) [Strategi]. Hentet fra https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-informasjonssikker/id710469/

Derbyshire, R., Green, B., & Hutchison, D. (2021). "Talking a different Language": Anticipating adversary attack cost for cyber risk assessment. *Computers & Security*, *103*, 102163. https://doi.org/10.1016/j.cose.2020.102163

DSB. (2019). *Risikostyring i digitale verdikjeder* (s. 41). DSB. Hentet 11. februar 2021 fra https://www.dsb.no/globalassets/dokumenter/rapporter/risikostyring-i-digitale-verdikjeder.pdf

DSTL. (2018, april 5). We cannot ignore what has happened in Salisbury: UN Security Council statement, 5 April 2018. Hentet 18. mai 2021, fra GOV.UK nettside: https://www.gov.uk/government/speeches/we-cannot-ignore-what-has-happened-in-salisbury

DuckDuckGo. (2021). DuckDuckGo—Privacy, simplified. [Søkemotor]. Hentet 15. april 2021, fra DuckDuckGo nettside: https://duckduckgo.com/

Edgar, T. W., & Manz, D. O. (2017). *Research methods for cyber security*. Cambridge, MA: Syngress, Elsevier.

Eisner, E. W. (2017). *The enlightened eye: Qualitative inquiry and the enhancement of educational practice*. New York: Teachers College Press.

ElevenPaths. (2021). ElevenPaths | Intelligence Managed Security Service Provider. Hentet 15. april 2021, fra ElevenPaths | Intelligence Managed Security Service Provider nettside: https://elevenpaths.com/

Endsley, M. R. (2016). *Designing for Situation Awareness: An Approach to User-Centered Design, Second Edition* (2. utg.). Boca Raton, FL: Taylor and Francis Group, CRC Press.

ENISA. (2016). *ENISA threat landscape report 2016: 15 top cyber-threats and trends*. Heraklion, Greece: ENISA. Hentet fra http://dx.publications.europa.eu/10.2824/92184.

Fielding, N., Lee, R. M., & Blank, G. (Red.). (2017). *The SAGE handbook of online research methods* (Second edition). Los Angeles: London : SAGE.

Florin, M.-V., & Nursimulu, A. (2018). *IRGC Guidelines for the Governance of Systemic Risks* (s. 83). Lausanne, Switzerland: EPFL International Risk Governance Center. Hentet fra EPFL International Risk Governance Center nettside: http://infoscience.epfl.ch/record/257279.

Forsvarets etterretningstjeneste. (2020). *FOKUS- 2019: Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer* (s. 104). Hentet 22. februar 2021 fra https://www.forsvaret.no/aktuelt-og-presse/publikasjoner/fokus/Fokus 2019.pdf/_/attachment/inline/893625cd-6223-45dd-b1eb-a534baed8111:aa3a2625fff2154621001ad972ec4e03d73988b6/Fokus 2019.pdf.

Forsvarets etterretningstjeneste. (2021). *Forsvarets etterretningsdoktrine* (s. 110). Oslo: Forsvarets etterretningstjeneste. Hentet 22. februar 2021 fra https://www.forsvaret.no/om-forsvaret/organisasjon/etterretningstjenesten/Etterretningsdoktrine_2021.pdf

Gibson, H. (2016). Acquisition and Preparation of Data for OSINT Investigations. I F. Sampson, S. P. Bayerl, & B. Akhgar (Red.), *Open source intellegence investigation.* (s. 69–92). Place of publication not identified: Springer International Publishing.

Gilchriest, V., & Williams, R. L. (1999). Key Informant Interviews. I B. F. Crabtree & W. L. Miller (Red.), *Doing qualitative research* (2nd ed, s. 71–88). Thousand Oaks, Calif: Sage Publications.

GitHub. (2021). GitHub: Where the world builds software. Hentet 12. mai 2021, fra GitHub nettside: https://github.com/

Goyal, S. (2020, august 9). *iFrame Injection—Attacks and Mitigation*. Secnhack. https://secnhack.in/iframe-injection-attacks-and-mitigation/

Grassegger, T., & Nedbal, D. (2021). The Role of Employees' Information Security Awareness on the Intention to Resist Social Engineering. *CENTERIS 2020 - International Conference on ENTERprise Information Systems / ProjMAN 2020 - International Conference on Project MANagement / HCist 2020 - International Conference on Health and Social Care Information Systems and Technologies 2020, CENTERIS/ProjMAN/HCist 2020*, *181*, 59–66. https://doi.org/10.1016/j.procs.2021.01.103

Guba, E. G., & Lincoln, Y. S. (1982). Epistemological and Methodological Bases of Naturalistic Inquiry. *Educational Communication and Technology*, *30*(4), 233–252. JSTOR. Hentet fra http://www.jstor.org/stable/30219846

Habermas, J., & Shapiro, J. J. (1971). *Knowledge and human interests*. Boston: Beacon Press.

HackerTarget. (2021). DNSdumpster.com—Dns recon and research, find and lookup dns records. Hentet fra https://dnsdumpster.com/

Hacquebord, F. (2020). *Pawn Storm in 2019 A Year of Scanning and Credential Phishing on High-Profile Targets*. Trend Micro Research. Hentet 5. april 2021 fra https://documents.trendmicro.com/assets/white_papers/wp-pawn-storm-in-2019.pdf

Hacquebord, F., & Hilt. (2016, november 9). Pawn Storm Boosts Attacks Before Zero-Days Get Patched. Hentet 7. april 2021, fra Trend Micro nettside: https://www.trendmicro.com/en_us/research/16/k/pawn-storm-ramps-up-spear-phishing-before-zero-days-get-patched.html

Hai-Jew, S. (2018). Beware! A Multimodal Analysis of Cautionary Tales in Strategic Cybersecurity Messaging Online. I Z. Fields (Red.), *Handbook of research on information and cyber security in the fourth industrial revolution* (s. 264–303). Hershey, PA: IGI Global.

Halvorsen, K. (2008). *Å forske på samfunnet en innføring i samfunnsvitenskapelig metode*. Oslo: Cappelen akademisk.

Hassan, N. A., & Hijazi, R. (2018). *Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence* (1st ed. 2018). Berkeley, CA: Apress : Imprint: Apress. https://doi.org/10.1007/978-1-4842-3213-2

Hassold, C. (2018a, mars 26). Silent Librarian: More to the Story of the Iranian Mabna Institute Indictment [Blog]. Hentet 28. april 2021, fra https://info.phishlabs.com/blog/silent-librarian-more-to-the-story-of-the-iranian-mabna-institute-indictment

Hassold, C. (2018b, april 11). *Testimony of Crane Hassold Director of Threat Intelligence Before the U.S. House of Representatives Committee on Science, Space, and Technology Subcommittee on Oversight and Subcommittee on Research and Technology "Scholars or Spies: Foreign Plots Targeting America's Research and Development"*. PhishLabs. Hentet fra https://science.house.gov/sites/democrats.science.house.gov/files/documents/Hassold%20Testimony.pdf

Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. *Computers & Security*, *73*, 102–113. https://doi.org/10.1016/j.cose.2017.10.008

Hayes, D. R., & Cappa, F. (2018). Open-source intelligence for risk assessment. *Business Horizons*, *61*(5), 689–697. https://doi.org/10.1016/j.bushor.2018.02.001

Hollnagel, E., Pariès, J., Woods, D., & Wreathall, J. (Red.). (2011). *Resilience engineering in practice: A guidebook*. Farnham, Surrey, England ; Burlington, VT: Ashgate.

Hubbard, D. W., & Seiersen, R. (2016). *How to measure anything in cybersecurity risk*. Hoboken: Wiley.

Hudson, T. (2021). *Tomnomnom/assetfinder* [Go]. Hentet fra https://github.com/tomnomnom/assetfinder (Original work published 2019)

Hudson, T. (2021). *Tomnomnom/httprobe* [Go]. Hentet fra https://github.com/tomnomnom/httprobe (Original work published 2017)

Hutchins, E., Cloppert, M., & Amin, R. (2011). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. *Leading Issues in Information Warfare & Security Research*, *1*. Hentet 12. januar 2021 fra https://lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

Intelligence X. (2021). Intelligence X. Hentet 12. april 2021, fra https://intelx.io/

Internet Archive. (2021). Wayback Machine [Arkiv]. Hentet 8. april 2021, fra https://web.archive.org/

Internet Live Stats. (2021). Total number of Websites—Internet Live Stats. Hentet 21. mars 2021, fra https://www.internetlivestats.com/total-number-of-websites/

ISO/IEC 27005:2018. (2018). *Information technology, security techniques, information security risk management*. International Organization for Standardization (ISO) and International Electrotechnical Comisson.

Jesson, J., Matheson, L., & Lacey, F. M. (2011). *Doing your literature review: Traditional and systematic techniques*. Los Angeles, Calif. ; London: SAGE.

Johansen, G. (2017). *Digital Forensics and Incident Response*. Birmingham, Mumbai: Packt Publishing. Hentet fra https://www.safaribooksonline.com/library/view/-/9781787288683/?ar

Jore, S. H. (2017). The risk and value nexus in security risk management. I M. Cepin & R. Bris (Red.), *Safety and Reliability—Theory and applications* (s. 1553–1559). Portoroz, Slovenia: Taylor and Francis group.

Jore, S. H. (2019a). The Conceptual and Scientific Demarcation of Security in Contrast to Safety. *European Journal for Security Research*, *4*(1), 157–174. https://doi.org/10.1007/s41125-017-0021-9

Jore, S. H. (2019b). The Multifaceted Aspect of Uncertainty – the Significance of Addressing Uncertainty in the Management of the Transboundary Wicked Problem of Terrorism. *Proceedings of the 29th European Safety and Reliability Conference (ESREL) 22-26 September 2019, Hannover, Germany*, 4044–4051. Hannover: Research Publishing.

Kanta, A., Coisel, I., & Scanlon, M. (2020). A survey exploring open source Intelligence for smarter password cracking. *Forensic Science International: Digital Investigation*, *35*, 301075. https://doi.org/10.1016/j.fsidi.2020.301075

Katos, V., Rostami, S., Bellonias, P., Davies, N., Kleszcz, A., Faily, S., … European Union Agency for Cybersecurity. (2019). *State of vulnerabilities 2018/2019: Analysis of events in the life of vulnerabilities.* Attiki, Hellas: ENISA. Hentet fra https://op.europa.eu/publication/manifestation_identifier/PUB_TP0320014ENN

Kerner, R. (2015, oktober 2). *Reconnaissance: A Walkthrough of the "APT" Intelligence Gathering Process*. EMC Corporation. Hentet fra https://drive.google.com/file/d/0B3tdhdmrVDEwQ3ptdHJKb3N1NjA/view

Kibar, O. (2020, september 2). Justisminister Mæland om hackerangrepene som rammer Norge: – En krisesituasjon. Hentet 21. februar 2021: https://www.dn.no/teknologi/monica-maland/cyberkriminalitet/cybersikkerhet/justisminister-maland-om-hackerangrepene-som-rammer-norge-en-krisesituasjon/2-1-867757

Kruke, B. I., & Olsen, O. E. (2012). Knowledge creation and reliable decision-making in complex emergencies. *Disasters*, *36*(2), 212–232. https://doi.org/10.1111/j.1467-7717.2011.01255.x

Kshetri, N. (2016). *The Quest to Cyber Superiority: Cybersecurity Regulations, Frameworks, and Strategies of Major Economies* (1st ed. 2016). Cham: Springer International Publishing : Imprint: Springer. https://doi.org/10.1007/978-3-319-40554-4

Lande, D. (2017). Analysis of information flows in global computer networks. *Institute for Information Recording of National Academy of Sciences of Ukraine*, (03), 45–53. https://doi.org/10.15407/visn2017.03.045

Lande, D., Kalyan, N., & Matiishin, O. (2019). *Social media aggregation system on cybersecurity*. Presentert på XVII All-Ukrainian scientific-practical conference of students, graduate students and young scientists «Theoretical and applied problems of physics, mathematics and computer science», Kyiv, Ukraine. Hentet fra http://its.iszzi.kpi.ua/article/view/217993

Lande, D., & Shnurko-Tabakova, E. (2019). OSINT as a part of cyber defense system. *Theoretical and Applied Cybersecurity*, *1*(1). https://doi.org/10.20535/tacs.2664-29132019.1.169091

Lande, D., Subach, I., & Puchkov, A. (2020). A System for Analysis of Big Data from Social Media. *Information & Security: An International Journal*, *47*(1), 44–61. https://doi.org/10.11610/isij.4703

Langved, Å., & Kibar, O. (2021, februar 18). Norway's 11179 billion NOK wealth fund affected by the SolarWinds hack. Hentet 21. februar 2021: https://www.dn.no/teknologi/oljefondet/hacking/solarwinds/norways-11179-billion-nok-wealth-fund-affected-by-the-solarwinds-hack/2-1-964180

Lazzarotti, J. J., Dorer, T., & Khetarpal, M. H. (2017). Increasing Ransomware Attacks in Higher Education. Hentet 23. februar 2021, fra The National Law Review nettside: https://www.natlawreview.com/article/increasing-ransomware-attacks-higher-education

Lervik, R. (2018, juni). *Probability and uncertainty. Some things are more uncertain than others*. DNV GL.

Liseter, I. M. (2020). URL. I *Store norske leksikon*. http://snl.no/URL

Lussier, R. N. (2012). *Management fundamentals: Concepts, applications, skill development* (5th ed). Mason, Ohio: South-Western.

Lyon, G. (2021). *Nmap: The Network Mapper - Free Security Scanner* [C++, Lua]. Hentet fra https://nmap.org/

Maltego Technologies. (2021). Maltego—Homepage. Hentet 7. april 2021, fra https://www.maltego.com/

Marion, N. E., & Twede, J. (2020). *Cybercrime: An encyclopedia of digital crime* (First Edition). Santa Barbara: ABC-CLIO.

Martorella, C. (2021). TheHarvester (Versjon 3.2.4) [Python, Kali Linux]. Hentet fra https://github.com/laramies/theHarvester (Original work published 2011)

Matvej, E., Moric, Z., & Papic, S. (2020). Croatian Bank Security Analysis by Publicly Available Data. I B. Katalinic (Red.), *DAAAM Proceedings* (Bd. 1, s. 0184–0188). Vienna: DAAAM International Vienna. https://doi.org/10.2507/31st.daaam.proceedings.024

Mirzaei, O., de Fuentes, J. M., & Lorena González Manzano. (2018). Dynamic Risk Assessment in IT Environments: A Decision Guide. I Z. Fields (Red.), *Handbook of research on information and cyber security in the fourth industrial revolution* (s. 234–263). Hershey, PA: IGI Global.

MITRE. (2021a). ATT&CK for Enterprise Introduction | MITRE ATT&CK®. Hentet 20. februar 2021, fra https://attack.mitre.org/resources/enterprise-introduction/

MITRE. (2021b). Gather Victim Identity Information: Credentials, Sub-technique T1589.001—Enterprise. Hentet 14. februar 2021, fra https://attack.mitre.org/techniques/T1589/001/

MITRE. (2021c). Reconnaissance, Tactic TA0043—Enterprise. Hentet 23. februar 2021, fra https://attack.mitre.org/tactics/TA0043/

Morgan, S. (2020, juni 3). The World Will Store 200 Zettabytes Of Data By 2025 [Tidsskrift]. Hentet 21. mai 2021, fra Cybercrime Magazine nettside: https://cybersecurityventures.com/the-world-will-store-200-zettabytes-of-data-by-2025/

NCSC. (2020). More targeted ransomware attacks on UK education. Hentet 1. mai 2021, fra https://www.ncsc.gov.uk/news/alert-targeted-ransomware-attacks-on-uk-education-sector

NCSC. (2021). Alert: Further ransomware attacks on the UK education sector by cyber criminals. Hentet 4. juni 2021, fra https://www.ncsc.gov.uk/news/alert-targeted-ransomware-attacks-on-uk-education-sector

Neuman, W. L. (2014). *Social research methods: Qualitative and quantitative approaches* (7. ed., Pearson new internat. ed). Harlow: Pearson.

NorSIS. (2018). *Trusler og trender 2018–19: Hvilke digitale trusler møter oss på jobb og i hverdagen?* (Nr. 978-82-93651-03–1; s. 52). Gjøvik: Norsk Senter for Informasjonssikring. Hentet fra Norsk Senter for Informasjonssikring nettside: https://norsis.no/publikasjoner/

NOU 2006: 6. (2006). *Når sikkerheten er viktigst: Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner.* (s. 323) [Norges offentlige utredninger]. Oslo. Hentet fra https://www.regjeringen.no/contentassets/c8b710be1a284bab8aea8fd955b39fa0/no/pdfs/nou200620060006000dddpdfs.pdf

NOU 2015: 13. (2015). *Digital sårbarhet – sikkert samfunn Beskytte enkeltmennesker og samfunn i en digitalisert verden* (s. 331) [Norges offentlige utredninger]. Oslo: Justis- og beredskapsdepartementet. Hentet fra Justis- og beredskapsdepartementet website: https://www.regjeringen.no/no/dokumenter/nou-2015-13/id2464370/?ch=3

NS 5830:2012. (2012). *Samfunnssikkerhet—Beskyttelse mot tilsiktede uønskede handlinger—Terminologi*. Lysaker: Standard Norge.

NS 5832:2014. (2014). *Samfunnssikkerhet. Beskyttelse mot uønskede tilsiktede handlinger. Krav til sikringsrisikoanalyse.* Lysaker: Standard Norge.

NSM. (2017). *Risiko 2017. Risiko og Sårbarheter i en ny tid. En vurdering av sårbarheter og risiko i Norge.* (s. 44) [Risikovurdering]. Sandvika: Nasjonal Sikkerhetsmyndighet.

NSM. (2020a). *Helhetlig digitalt risikobilde 2020* (s. 44). Sandvika: Nasjonal Sikkerhetsmyndighet. Hentet fra Nasjonal Sikkerhetsmyndighet nettside: https://nsm.no/sok/?categoryID=14&tileInstanceId=2597&q=Helhetlig+digitalt+risikobilde

NSM. (2020b). *Håndbok: I beskyttelse av skjermingsverdig ugradert informasjonssystem*. Nasjonal Sikkerhetsmyndighet. Hentet fra https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker-til-sikkerhetsloven/handbok-i-beskyttelse-av-skjermingsverdig-ugradert-informasjonssystem/om-denne-handboken/

NSM. (2020c). *NSM Risiko 2020* (s. 44). Nasjonal Sikkerhetsmyndighet. Hentet fra https://nsm.no/getfile.php/131421-1587034764/Hermans undermappe med bilder/NSM_Risiko_2020_web_0104.pdf

NSM. (2020d, juni 5). Grunnprinsipper for IKT-sikkerhet 2.0. Hentet fra https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/introduksjon-1/

NVE. (2019). *Metode for å finne kraftsensitiv informasjon på Internett*. NVE. Hentet fra https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjbqrLf-uHuAhWxlYsKHYgsAcUQFjAAegQIARAC&url=https%3A%2F%2Fpublikasjoner.nve.no%2Ffaktaark%2F2019%2Ffaktaark2019_11.pdf&usg=AOvVaw1rtRLbgaCBvs4dPRqO62_2

Nyssen, A. S. (2011). From Myopic Coordination to Resilience in Socio-technical Systems. A Case Study in a Hospital. I E. Hollnagel, J. Pariès, D. Woods, & J. Wreathall (Red.), *Resilience engineering in practice: A guidebook* (s. 220–235). Farnham, Surrey, England ; Burlington, VT: Ashgate.

Nätt, T. H., & Heide, C. F. (2021). *Datasikkerhet* (2. utg., Bd. 1). Oslo: Gyldendal Akademisk.

Oliver, R. A., & Shields, N. P. *United States of America v. Park Jin Hyok*. , (United States District Court for the Central District of California 6. september 2018).

Omand, D., Bartlett, J., & Miller, C. (2012). Introducing Social Media Intelligence (SOCMINT). *Intelligence and National Security*, *27*(6), 801–823. https://doi.org/10.1080/02684527.2012.716965

OPCW. (2021). Organisation for the Prohibition of Chemical Weapons. Hentet 18. mai 2021, fra OPCW nettside: https://www.opcw.org/node/2632

Oxford Dictionary. (2021). Data Mining [Online dictionary]. Hentet 26. april 2021, fra www.oxfordlearnersdictionaries.com nettside: https://www.oxfordlearnersdictionaries.com/definition/english/data-mining?q=data+mining

Pariès, J. (2011). Lessons from the Hudson. I E. Hollnagel, J. Pariès, D. Woods, & J. Wreathall (Red.), *Resilience engineering in practice: A guidebook* (s. 9–27). Farnham, Surrey, England ; Burlington, VT: Ashgate.

Pastor-Galindo, J., Nespoli, P., Gomez Marmol, F., & Martinez Perez, G. (2020). The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends. *IEEE Access*, *8*, 10282–10304. https://doi.org/10.1109/ACCESS.2020.2965257

Patton, M. Q. (2015). *Qualitative research & evaluation methods: Integrating theory and practice* (Fourth edition). Thousand Oaks, California: SAGE Publications, Inc.

Paulsen, J. E., & Simensen, T. K. (2019). Generalistens rolle i etterretningsstyrt politiarbeid. *Nordisk politiforskning*, *6*(2), 169–181. Hentet fra https://juridika.no/tidsskrifter/nordisk-politiforskning/2019/2/artikkel/paulsen

Pellissier, R. (2010). The Implementation of Resilience Engineering to Enhance Organizational Innovation in a Complex Environment. *International Journal of Business and Management*. https://doi.org/10.5539/ijbm.v6n1p145

Perez, M. (2019, august 6). What is Web Scraping and What is it Used For? Hentet 27. april 2021, fra ParseHub Blog nettside: https://www.parsehub.com/blog/what-is-web-scraping/

Perrow, C. (1999). *Normal accidents: Living with high-risk technologies*. Princeton, N.J.: Princeton University Press.

Personopplysningsloven. (2019). *Lov om behandling av personopplysninger* (LOV-2018-06-15-38). Lovdata. Hentet fra https://lovdata.no/dokument/NL/lov/2018-06-15-38

POD. (2020). *Etterretningsdoktrine for politiet*. Politidirektoratet. Hentet fra https://www.politiet.no/globalassets/05-om-oss/03-strategier-og-planer/etterretningsdoktrine.pdf

PST. (2020a). Datainnbruddet mot Stortinget er ferdig etterforsket. Hentet 14. februar 2021, fra www.pst.no nettside: /alle-artikler/pressemeldinger/datainnbruddet-mot-stortinget-er-ferdig-etterforsket/

PST. (2020b). *Nasjonal trusselvurdering 2020* (s. 36). Politiets Sikkerhetstjeneste. Hentet fra Politiets Sikkerhetstjeneste website: https://pst.no/globalassets/artikler/utgivelser/2020/nasjonal-trusselvurdering-2020-print.pdf

Ratcliffe, J. (2016). *Intelligence-led policing* (Second Edition). London ; New York: Routledge, Taylor & Francis Group.

Reason, J. (1997). *Managing the risks of organizational accidents*. Aldershot: Ashgate.

Reason, J. (2016). *Organizational accidents revisited*. CRC Press.

Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2019). *Developing cyber resilient systems: A systems security engineering approach* (Nr. NIST SP 800-160v2; s. NIST SP 800-160v2). Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-160v2

Roth, E. M. (1997). *Analysis of decision making in nuclear power plant emergencies: An investigation of aided decision making* (C. E. Zsambok & G. A. Klein, Red.). Mahwah, N.J: L. Erlbaum Associates.

Røise, M. B. (2021, januar 11). Norsk milliard-selskap rammet av dataangrep som lammer en hel næring. Hentet 21. februar 2021, fra Digi.no website: https://www.digi.no/artikler/norsk-milliard-selskap-rammet-av-dataangrep-som-lammer-en-hel-naering/505398

Rønn, K. V., & Søe, S. O. (2019). Is social media intelligence private? Privacy in public and the nature of social media intelligence. *Intelligence and National Security*, *34*(3), 362–378. https://doi.org/10.1080/02684527.2019.1553701

Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet*, *11*(4), 89. https://doi.org/10.3390/fi11040089

Sanghvi, H. P., & Dahiya, M. S. (2013). Cyber Reconnaissance: An Alarm before Cyber Attack. *International Journal of Computer Applications*, *63*(6), 36–38.

Sawakinome. (2021). Hva er forskjellen mellom IP-adresse og vertsnavn. Hentet 28. april 2021, fra Https://no.sawakinome.com/ website: https://no.sawakinome.com/articles/technology/what-is-the-difference-between-ip-address-and-hostname.html#Hostname

SensePost. (2021). Gowitness (Versjon 2.3.4) [Go, Kali Linux]. SensePost. Hentet fra https://github.com/sensepost/gowitness (Original work published 2017)

Settanni, G., Skopik, F., Shovgenya, Y., Fiedler, R., Carolan, M., Conroy, D., … Olli, P. (2017). A collaborative cyber incident management system for European interconnected critical infrastructures. *Journal of Information Security and Applications*, *34*, 166–182. https://doi.org/10.1016/j.jisa.2016.05.005

Shimonski, R. (2015). *Cyber reconnaissance, surveillance, and defense*. Amsterdam ; Boston: Elsevier/Syngress.

Shodan. (2021). Shodan. Hentet 15. april 2021, fra https://www.shodan.io/

Sikkerhetsloven. (2018). *Lov om nasjonal sikkerhet* (LOV-2018-06-01-24). Lovdata. Hentet fra https://lovdata.no/dokument/NL/lov/2018-06-01-24#KAPITTEL_1

Skopik, F. (Red.). (2017). *Collaborative cyber threat intelligence: Detecting and responding to advanced cyber attacks on national level*. Boca Raton, FL: CRC Press.

Skotnes, R. Ø. (2020). Standardization of cybersecurity for critical infrastructures. I O. E. Olsen, K. Juhl, P. H. Lindøe, & O. A. Engen (Red.), *Standardization and risk governance: A multi-disciplinary approach* (s. 166–180).

Smith, C. L., & Brooks, D. J. (2013). *Security science: The theory and practice of security*. Amsterdam: Elsevier, BH.

Snee, H., Hine, C., Morey, Y., Roberts, S., & Watson, H. (2016). *Digital Methods for Social Science: An Interdisciplinary Guide to Research Innovation*.

Spradley, J. P. (1979). *The ethnographic interview*. New York: Holt, Rinehart and Winston.

SRA. (2020). *Society for Risk Analysis Glossary*. SRA. Hentet fra https://www.sra.org/wp-content/uploads/2020/04/SRA-Glossary-FINAL.pdf

Stair, R. M., & Reynolds, G. W. (2018). *Principles of information systems* (Thirteenth edition). Boston, MA, USA: Cengage Learning.

Stor engelsk ordbok. (u.å.). Hashtag [Ordbok]. Hentet 3. april 2021, fra Ordnett.no nettside: https://www.ordnett.no/search?language=en&phrase=hashtag

Stretch, B. J. *United States of America v. Dokuchaev et al.*, (United States District Court for the Northern Distric of California 2017).

Tabatabaei, F., & Wells, D. (2016). OSINT in the Context of Cyber-Security. I B. Akhgar, P. S. Bayerl, & F. Sampson (Red.), *Open Source Intelligence Investigation* (s. 213–231). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-47671-1_14

The United States Department of Justice. (2015, november 24). Cyber and Intellectual Property Crimes Section. Hentet 6. mai 2021, fra https://www.justice.gov/usao-cdca/cyber-and-intellectual-property-crimes-section

Tjørhom, B., & Aase, K. (2011). The Art of Balance: Using Upward Resilience Traits to Deal with Conflicting Goals. I E. Hollnagel, J. Pariès, D. Woods, & J. Wreathall (Red.), *Resilience engineering in practice: A guidebook* (s. 157–170). Farnham, Surrey, England ; Burlington, VT: Ashgate.

Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security*, *72*, 212–233. https://doi.org/10.1016/j.cose.2017.09.001

Turner, B. A. (1976). The Organizational and Interorganizational Development of Disasters. *Administrative Science Quarterly*, *21*(3), 378. https://doi.org/10.2307/2391850

Turner, B. A., & Pidgeon, N. F. (1997). *Man-made disasters* (2nd ed). Boston: Butterworth-Heinemann.

Turton, W., & Mhrotra, K. (2021, juni 4). Hackers Breached Colonial Pipeline Using Compromised Password. *Bloomberg.Com*. Hentet fra https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

Tzu, S. (2009). *The art of war*. Place of publication not identified: Pax Librorum Pub. H.

Ulsch, N. M. (2014). *Cyber threat! How to manage the growing risk of cyber attacks*. Hoboken, New Jersey: Wiley.

Varga, S., Brynielsson, J., & Franke, U. (2021). Cyber-threat perception and risk management in the Swedish financial sector. *Computers & Security*, *105*, 102239. https://doi.org/10.1016/j.cose.2021.102239

Verizon. (2020). *Data Breach Investigations Report* (s. 119). Verizon. Hentet fra Verizon nettside: https://enterprise.verizon.com/resources/reports/dbir/

Virksomhetsikkerhetsforskriften. (2019). *Forskrift om virksomheters arbeid med forebyggende sikkerhet* (FOR-2018-12-20-2053). Lovdata. Hentet fra https://lovdata.no/dokument/SF/forskrift/2018-12-20-2053#KAPITTEL_2

Wappalyzer. (2021). Apps—Wappalyzer. Hentet 15. april 2021, fra https://www.wappalyzer.com/apps/

Weick, K. E., & Sutcliffe, K. M. (2003). Organizing for High Reliability: Processes of Collective Mindfulness. I B. M. Staw & R. M. Kramer (Red.), *Research in organizational behavior: An annual series of analytical essays and critical reviews. Vol. 25* (s. 81–123). Amsterdam; London: JAI.

WiGLE. (2021). WiGLE: Wireless Network Mapping. Hentet 16. april 2021, fra https://wigle.net/

Wilcox, H., & Bhattacharya, M. (2020). A Human Dimension of Hacking: Social Engineering through Social Media. *IOP Conference Series: Materials Science and Engineering*, *790*, 012040. https://doi.org/10.1088/1757-899X/790/1/012040

Wilson, C. (2020). Hva er et digitalt sertifikat? Hentet 5. mai 2021, fra SSL.com nettside: https://www.ssl.com/no/Vanlige-sp%C3%B8rsm%C3%A5l/hva-er-et-digitalt-sertifikat/

Wiradarma, A. A. B. A., & Sasmita, G. M. A. (2019). IT Risk Management Based on ISO 31000 and OWASP Framework using OSINT at the Information Gathering Stage (Case Study: X Company). *International Journal of Computer Network and Information Security*, *11*(12), 17–29. https://doi.org/10.5815/ijcnis.2019.12.03

Yahoo. (2021). Yahoo.com [Søkemotor]. Hentet 15. april 2021, fra https://www.yahoo.com

Yandex. (2021). Yandex.com [Søkemotor]. Hentet 15. april 2021, fra https://yandex.com

Yin, R. K. (2009). *Case study research: Design and methods* (4th ed.). Thousand Oaks, Calif: Sage.

Yin, R. K. (2016). *Qualitative research from start to finish* (Second edition). New York: Guilford Press.

Aakre, S. (2020). Hvilket trusselbilde står norske virksomheter overfor, og hvordan kan åpenhet bidra til å forstå cyberrisiko? *Magma*, (2), 37–45. Hentet fra https://www.magma.no/hvilket-trusselbilde-star-norske-virksomheter-overfor-og-hvordan-kan-apenhet-bidra-til-a-forsta-cyberrisiko

Vedlegg

A. Samtykkeerklæring

Samtykkeerklæring

I forbindelse med min masteroppgave i samfunnssikkerhet ved Universitetet i Stavanger, skal jeg gjennomføre innsamling av åpen tilgjengelig informasjon om organisasjoner. Oppgaven omhandler bruk av OSINT-verktøy for datainnsamling fra åpne informasjonskilder. Formålet med studien er å belyse hvordan trusselaktører kartlegger organisasjoner for å utnytte sårbarheter, og hvordan organisasjoner selv kan ta disse verktøyene i bruk i sine risikoanalyser.

For å sikre konfidensialitet vil all innsamlet informasjon og opplysninger anonymiseres. Organisasjonene som deltar i prosjektet, vil få tilsendt oppgavens analysedel før innleveringsdato for å gi godkjenning. Organisasjonene vil anonymiseres og omtales som "Organisasjon A" og "Organisasjon B". På denne måten sikrer jeg at opplysningene blir behandlet anonymt.

Etter innlevering av oppgaven vil jeg utarbeide to sårbarhetsrapporter som vil utleveres til hver organisasjon. Alle opplysninger og data vil bli slettet etter at arbeidet er avsluttet.

Ved å signere på denne erklæringen godtar du at din organisasjon gir meg tiltalelse til å samle informasjon ved bruk av OSINT-verktøy, og at opplysningene som blir samlet inn kan benyttes videre i oppgaven.

Alyona Oftedahl 11.03.2021

....

Alyona Trach Oftedahl
Masterstudent i Samfunnssikkerhet
Universitetet i Stavanger

Respondent

B: Brukte OSINT-verktøy og deres egenskaper

Tabell 8: Oversikt over brukte verktøy og deres egenskaper

Type	Navn	Funksjonalitet, fordeler og ulemper	Input	Output	OS	Interface	Kostnad
Søkemotor	**Google Dorks**	Innhenting av informasjon fra Google ved hjelp av avanserte søkeord som hjelper brukere å søke i indeksen til et bestemt nettsted. Bruk av Google Dorks kan avdekke informasjon som e-postadresser, påloggingsinformasjon, sensitive filer og finansiell informasjon (f.eks. betalingskortdata).	kombinasjoner av søkeord	Filer, bilder, passord, regneark, osv.	Nettleser		gratis
	DuckDuckGo	En søkemotor som sikrer anonymitet for brukeren. Nettleseren lagrer ikke informasjon om brukeren.	søkeord	diverse	Nettleser		gratis
	Google Street View	En teknologi som gir interaktive panoramaer fra posisjoner langs mange gater i verden. Tjenesten gir mulighet til å vurdere fysiske sikkerhetstiltak og bygningstilstand uten å være til stede.	adresse, GPS-koordinater	Bilder av bygninger og nærliggende infrastruktur	Nettleser		gratis
	DNS dumpster[16]	Et effektivt verktøy ved passiv rekognosering, som gir strukturert informasjon om DNS, IP-adresser, software osv. Optimalisert for visualisering av nettverk. Bruker kun åpne kilder.	domene	nettverkskart	Nettleser		gratis
	CVE Details[17]	Sårbarhets-database	utstyr, programvare, port mm..	liste av assosierte sårbarheter	Nettleser		gratis

[16] https://dnsdumpster.com/
[17] https://www.cvedetails.com/

	Shodan	Søkemotor som lar bruker finne bestemte typer datamaskiner og IoT som er koblet til Internett. Shodan-søk kan gi informasjon om display-meldinger, programvare, internettleverandør, eiere mm. Har flere filter-alternativer. Man kan blant annet filtrere på sted, IP-range, kategorier og portnumre. Enkel å bruke. Svært attraktiv for opportunistiske trusselaktører, da man kan avdekke ikke-sikrede enheter uten å ha spesifikke mål.	IP-adresse, org. navn, domene, sted, utstyr, mm.	Liste av assosierte sårbarheter, åpne porter, IP-adresse, eierskap, internett-leverandør, protokoller,	Nettleser	gratis og betaling, avhengig av omfang av søk
Database	**Doffin.no**	En norsk database hvor anskaffelser i offentlig sektor underlagt EØS-forskriftene blir kunngjort.	org. navn, org. nummer, navn mm.	navn, beskrivelse, kontaktperson, kontakt-informasjon, eksterne lenker, dokumenter mm.	Nettleser	gratis
	Pastebin[18]	Nettside hvor man kan «dumpe» hva som helst.	søkeord	diverse «dumps»	Nettleser	gratis
	GitHub[19]	Utvikler-plattform	navn på programvare, utvikler, eller søkeord	programvare i form av scripts, personer og deres verk, mm.	Nettleser	gratis for vanlig bruk, andre betingelser for utviklere eller akademia
	Vigilante[20]	Database som oppdateres jevnlig og som inneholder oversikt over alle nye lekkasjer	navn på datalekkasje eller kilde av lekkasje	Avhengig av lekkasje: passord, e-postadresser,	Nettleser	gratis

[18] https://pastebin.com/
[19] https://github.com/
[20] https://vigilante.pw/

				navn, brukernavn, IP adresser			
	Intelligence X[21]	Database av datalekkasjer. Søket fungerer med spesifikke søkeord (se input). Den søker på Darknett, dokumentdelingsplattformer, whois, offentlige datalekkasjer mm.. Inneholder historisk dataarkiv med resultater, som ligner på hvordan Wayback Machine fra archive.org lagrer historiske kopier av nettsteder.	domene, url, IP, Bitcoin adresse, IPFS-hashes, CIDR-er mm.	datalekkasjer i ulike formater: bilder, passord, dokumenter, innhold i e-poster mm.	Nettleser		mot betaling, men tilbyr gratis prøveperiode
	Wigle.net[22]	Søkemotor for trådløse nettverk. Brukere kan registrere seg på nettstedet og laste opp hotspot-data som GPS-koordinater, SSID, MAC-adresse og krypteringstype som brukes på hotspots. Viser i tillegg celletårndata. Enkel å bruke.	adresse	GPS-koordinater, SSID, MAC-adresse	Nettleser		gratis for enkelte søk, mot betaling for kommersiell bruk
	Assetfinder[23]	Et verktøy som finner domener og underdomener som potensielt er relatert til et gitt domene. Enkelt å bruke, gir mye ustrukturert informasjon.	domene	domener og underdomener	Linux	script	gratis
Programvare	**SubFinder**[24]	Et verktøy som finner gyldige underdomener for en webside. En enkel modulær arkitektur, er optimalisert for hastighet. Har begrenset funksjonalitet. Bruker åpen kilde, er ikke synlig.	domene, IP-adresse	aktive underdomener	Linux	script	gratis
	OWASP Amass[25]	Utfører nettverkskartlegging av angrepsflater og oppdager eksterne eiendeler gjennom innsamling av	domene, IP-adresse	diverse, avhengig av command	Linux	script	gratis

[21] https://intelx.io/
[22] https://wigle.net/
[23] https://github.com/tomnomnom/assetfinder
[24] https://github.com/projectdiscovery/subfinder
[25] https://github.com/OWASP/Amass

		data fra åpen kilde og aktiv rekognosering. Aktiv skanning, altså synlig.					
	theHarvester[26]	Kraftig og effektivt verktøy designet for de tidlige stadiene av rekognoseringsprosessen. Brukes til innsamling av åpen tilgjengelig informasjon for å kartlegge selskaps eksterne angrepsflate. Samler informasjon fra flere offentlige datakilder. Enkelt å bruke, optimalisert for hastighet, gir mye data, dataene er ustrukturert.	IP-adresse, domene	e-post, navn, underdomener, IP, URL, mm.	Linux	script	gratis
	Maltego[27]	OSINT-verktøy som automatiserer store deler av rekognoseringsprosessen. Optimalisert for visualisering, informasjon er presentert i et lenket grafformat. Kan lenke alt fra profiler på sosiale medier, epostadresser og telefonnumre, til IP-adresser, steder og passord-lekkasjer. Innsamler data fra åpen kildekode. Ofte brukt som verktøy for å risikovurdere organisasjons angrepsflate. Egnet for analyse av lenker og datautvinning.	flere	flere	Mac, Linux, Windows	program-vare	Mot betaling, tilbyr gratis prøve-periode, har gratis tilbud for akademia
	Nmap[28]	Brukes til å oppdage verter og tjenester i et datanettverk ved å sende pakker og analysere svarene. Finner store mengder informasjon, optimalisert for hastighet. Oppdages lett av sikkerhetsbarrierer som brannmurer og servere. Utfordringen er å lære å gjøre det anonymt.	IP-adresser, domener, vertsnavn, mm.	angrepsflate: IP-adresser, OS, programvare, versjoner, porter og status mm.	Linux, Windows, Mac OS X	script	Gratis, men har noen funksjoner som krever betaling.

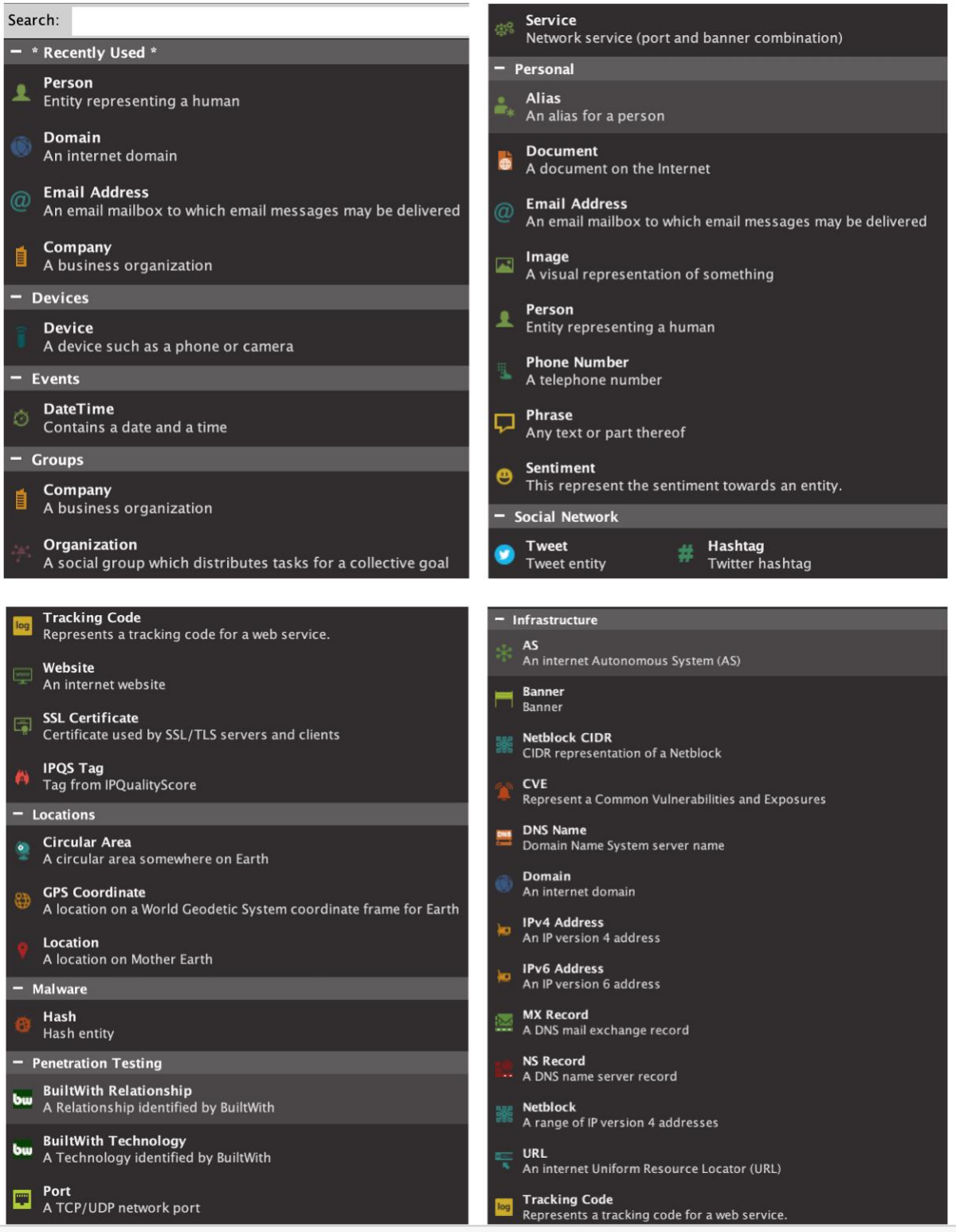
[26] https://github.com/laramies/theHarvester
[27] https://www.maltego.com/
[28] https://github.com/nmap/nmap

	Recon-ng[29]	Rekognoseringsrammeverk som fungerer på samme måte som theHarvester og Nmap. Skanner nettsteder og apper, finner profiler som er registrert eller nevnt. Rask og grundig. Er usikker om den gir fullstendig informasjon når det gjelder søk på brukerkonto.	flere	flere	Linux	script	gratis
	Foca	Finner metadata i elektroniske dokumenter og bilder.	fil	forfattere, lokasjoner, datoer og utstyr	Windows	Program-vare	gratis
	Gowitness	Skanner domener og lagrer skjermbilder	domene	bilder	Linux	script	gratis
Add-on	**Wappalyzer**	Firefox add-on viser all programvare, programmeringsspråk og andre data på en webside. Enkel å bruke.	-	programvarer/ teknologi som kjøres p nettside	Firefox	Pop-up vindu	gratis
	Exif Viewer	Verktøy for utvinning av data fra exif. Fungerer ikke optimalt, da det ikke viser data for bilder som er hostet lokalt.	-	metadata fra bilder	Firefox	Pop-up vindu	gratis

[29] https://github.com/lanmaster53/recon-ng

C: Maltego - input alternativer

Bilde 20: Input alternativer i Maltego



D: Dokumentstudiet - resultater av datainnsamling

Tabell 9: Dokumentanalyse

År	Mål/offer	Hvilke typer informasjon som ble brukt i angrep?	Hvordan informasjonen ble brukt i angrep? (*Modus operandi*)	Formål og/eller konsekvens
United States of America v. Fathi et al. (Bharara, 2016, s. 2-15)				

2011-2013	**Mål/ofre:**
	• USAs finanssektor
	• AT&T - verdens største telecom-selskap
	• NASA
	• tusenvis servere i USA, UK og Israel
		Typer informasjon brukt:
		• nettverksstruktur
		• programvare og versjon i bruk
		• sårbarheter
		• SCADA systemer
		• oppdateringsrutiner
			***Modus operandi*:**
			• gjennomførte teknisk rekognosering herunder
			  ○ nettverksskanning
			  ○ OS fingerprinting
			  ○ sårbarhetskartlegging
			• utviklet botnett
			• gjennomførte DDoS-angrep
			• utviklet og distribuert skadevare
			• infiserte nettverk til flere organisasjoner, bl.a. NASA
			• fikk uautorisert tilgang til SCADA systemer
				Formål:
				• å skape strategisk fordel for Iran
				• å forstyrre USAs grunnleggende kritiske funksjoner
				Konsekvens:
				• forstyrret drift av ca. 46 store finansinstitusjoner
				• tap av titalls millioner dollar

United States of America v. Dokuchaev et al. (Stretch, 2017)				
2014 - 2017	**Mål/ofre:** • Yahoo • journalister • politikere og diplomater • militære ledere	**Typer informasjon brukt:** • personlige opplysninger om ofre og deres familiemedlemmer	***Modus operandi*:** • anskaffet og brukte infrastruktur for å skjule sine aktiviteter, • etablerte flere falske brukerkontoer	**Formål:** • samle informasjon av interesse for FSB[30] • økonomisk gevinst

[30] En intern føderal sikkerhetstjeneste i Russland, tidligere KGB

	• russisk IT-selskap • internett-leverandører • fransk transport selskap • sveitsiske, russiske og amerikanske finansselskap • flere statsråd • embetsmann • sikkerhetseksperter • granskere • andre eksperter • forskere • universitets styremedlem • IMF embetsmann	• private og forretningsrelaterte e-post kontoer • ansatte i organisasjoner • organisasjonsstruktur • ofres sosiale nettverk og relasjoner • aktuelle hendelser • mm	• målrettet passiv og aktiv rekognosering, herunder nettverksskanning • målrettede nettfisking-kampanjer med formål om tilgang til offers data og brukerkonto-opplysninger • «minting» • spam • utviklet skadevare • brukte «log cleaner» • eksfiltrerte data	**Konsekvens:** • fikk tilgang til over 17000 private e-postkontoer og informasjon lagret på kontoene
United States of America v. Rafatnejad et al. - «Silent Librarian»-case (Berman, 2018, s. 3-13)				

2013-2017	**Mål/ofre:**
	• 320 universiteter
	• 47 private selskaper:
	  ○ forlag,
	  ○ medie- og advokatfirma,
	  ○ teknologi-selskaper,
	  ○ konsulentbyråer
	• NGO
		Typer informasjon brukt:
		• navn
		• institusjon
		• forskningsinteresser
		• private og jobbrelaterte e-postadresser
		• publiserte artikler
		• lister med navn og e-postkontoer
		• passord fra datalekkasjer
		• samarbeidspartnere
		• kontakter
			***Modus operandi*:**
			• målrettet rekognosering
			• sosial manipulering
			• målrettede nettfisking-e-poster tilpasset hver enkelt mottaker og/eller organisasjon
			• manipulerte ofre til å bruke et forfalsket domene
			• exfiltrere autentifikatorer ved å manipulere brukere til å tro at de ble logget ut av universitetets datasystem og må logge inn på ny
			• fikk tilgang til offers kontoer ved bruk av stjålne autentifikatorer
			• eksfiltrerte akademiske data og dokumenter
				Formål:
				• økonomisk gevinst
				• skape strategisk fordel for Iran
				Konsekvens:
				• Stjal mer enn 31 terabyte data fra universiteter, private selskaper og offentlige etater over hele verden
				• Dataene ble brukt av Islamic Revolutionary Guard Corps (IRGC) og solgt til Iran

			• såkalt «password spraying» for å kompromittere kontoer tilhørende private selskaper, eksfiltrerte deretter innholdet i ansattes e-postkontoer	• Kostnaden for universitetene alene utgjorde ca. 3,4 milliarder dollar
United States of America v. Park et al. (Oliver & Shields, 2018, s. 18-)				

	Mål/ofre:
	• underholdnings-selskaper
	• finansinstitusjoner i hele verden
	• leverandører/ tjenestetilbydere for militær i USA
	• Bangladesh Bank
	• universiteter
	• teknologi-bedrifter
	• USAs strøm infrastruktur
	• Lockheed Martin
		Typer informasjon brukt:
		• personlige opplysninger om ansatte og involverte i produksjon av «The Interview»
		• informasjon om nettverk, som DNS og IP-adresser
		• informasjon samlet fra offers nettsider
		• e-postadresser tilknyttet spesifikke domener og selskaper
		• informasjon fra forretningsregistre
		• sårbarheter
		• «exploits»
		• hacking-verktøy
		• driftsaktiviteter
		• informasjon om nordkoreansk matforsyning
		• informasjon om nordkoreansk TV
			Modus operandi:
			• anskaffet og brukte infrastruktur for å skjule sine aktiviteter
			• målrettet rekognosering, bl.a.
			  ○ besøkte nettstedene til tiltenkte ofre
			  ○ profilering av personer tilknyttet virksomheter
			  ○ sendte meldinger til ansatte
			  ○ profilerte personlige SoMe kontoer til ansatte
			• sosial engineering
			• målrettede nettfisking-kampanjer med formål å få tilgang til bruk av offers data og brukerkonto-opplysninger
			• utviklet skadevare som ble distribuert til ansatte i SPE
			• fikk tilgang til SPEs nettverk
			• eksfiltrerte konfidensiell informasjon
			• ødela tusenvis PCer
			• cyberangrep på SPE produksjon «The Interview»
			• utviklet «WannaCry 2.0»
				Formål:
				• skape forstyrrelser til strategisk fordel for Nord-Korea
				• samle informasjon av interesse for Nord-Korea
				• økonomisk gevinst
				Konsekvens:
				• stjal 81 million amerikanske dollar fra Bangladesh Bank
				• forårsaket tap på over 1 billion amerikanske dollar
				• «In sum, the scope and damage of the computer intrusions perpetrated and caused by the subjects of this investigation, including PARK, is virtually unparalleled» (Oliver & Shields, 2018, s. 4).

United States of America v. Andrienko et al. - «GRU[31] hackers» rettssak (Coville, 2020, s. 6-42)				
2015 - 2016 (s. 9-11)	**Mål/ofre:** • Ukrainske strømselskaper • andre selskaper i hele verden	**Typer informasjon brukt:** • nettverk • IT-personell • tjenestetilbydere • andre ansatte • oppdateringsrutiner	***Modus operandi*:** • anskaffet og brukte infrastruktur for å skjule sine aktiviteter, • målrettet rekognosering • målrettede nettfisking-kampanjer med formål å få tilgang til bruk av offers data og brukerkonto-opplysninger ○ e-postene imiterte e-poster fra tjenestetilbydere eller kollegaer, oppmuntret til å klikke på hyperlinker eller vedlegg med skadevare som infiserte offers datamaskin • stjal autentifikatorer via nettfisking e-post • utviklet og distribuerte skadevare • brukte skadevaren til å stjele brukerautentifiseringer, som ble brukt for tilgang til selskapenes tilsynskontroll • etablerte skjult kommunikasjon mellom offers datamaskin og tredjeparts-tjeneste brukt av hackerne • brukte skadevaren for å slette data- og hendelseslogger	**Formål:** • skape forstyrrelser til strategisk fordel for Russland **Konsekvens:** • paralyserte flere datasystemer tilhørende ukrainske selskaper, inkludert banker, aviser og strømtilbydere • skadevaren spredde seg til flere andre land og institusjoner • forstyrret strømtilførselen til over 225 000 ukrainske kunder

[31] Tidligere Russlands Hoveddirektoratet for etterretningstjenesten

Des. 2016 (s. 11-15)	**Mål/ofre:** • Ukrainas Finans-departement • Ukrainas Skatteetat	**Typer informasjon brukt:** • nettverk • IT-personell • tjenestetilbydere • andre ansatte • oppdateringsrutiner	***Modus operandi*:** • målrettet rekognosering • sosial manipulering • målrettet nettfisking-kampanje mot Skatteetatens systemadministratorer • distribuerte skadevare til Ukrainas Finansdepartement og Skatteetat • etablerte uautorisert skjult kommunikasjon mellom offers datamaskin og tredjeparts-tjeneste brukt av hackerne • brukte dedikert nettverkstilkobling mellom Ukrainas Skatteetat og Finansdepartement, for adgang til sistnevntes datanettverk • distribuerte oppdatert versjon av KillDisk skadevare, som slettet Windows hendelseslogg på de infiserte datamaskinene	**Formål:** • skape forstyrrelser til strategisk fordel for Russland **Konsekvens:** • Skatteetatens regionale underavdelinger ble avskåret fra nasjonal skatteetats automatiske utbetalingssystem, forhindret ca. 150 000 elektroniske transaksjoner • Finansdepartementets infrastruktur ble avskåret for informasjon og kommunikasjon
2017 (s. 15-16)	**Mål/ofre:** Frankrikes President Macrons valgkampanje	**Typer informasjon brukt:** • personer involvert i valgkampanje • franske politikere og høyt profilerte personer • interne kommunikasjonsmåter • pågående prosjekter • arbeidsrelasjoner • dokumentmaler	***Modus operandi*:** • anskaffet og brukte infrastruktur for å skjule sine aktiviteter, • målrettet rekognosering • syv målrettede nettfisking-kampanjer tilpasset mottakeren • utviklet og testet teknikker for nettfisking, herunder e-poster om fildeling via Google Docs - brukt av partimedlem i En Marchel • utviklet et infisert dokument • brukte avsender-konto som imiterte Macrons pressesekretær for e-poster med infiserte Google Docs lenker til ca. 30 partimedlem	**Formål:** • skape forstyrrelser til strategisk fordel for Russland • påvirke offentlig opinion rett før president valget i Frankrike **Konsekvens:** Uviss

		• «En Marchels»[32] forhold til presse • cybersikkerhets-policyer • andre aktuelle emner	• falsk konto på sosiale medier for å meddele til flere franskmenn at de var villig til å lekke En Marchels interne dokumenter • lekket kompromitterende dokumenter angivelig fra En Marchel valgkampanjes e-postkontoer	
Juni 2017 (s.16-23)	**Mål/ofre:** Ukrainske selskaper, herunder banker, aviser, strømtilbydere	**Typer informasjon brukt:** • nettverk til en familieeid bedrift • navn til bedrifts eiere • organisasjonsnummer • sertifiseringsnummer • IT-personell • andre ansatte • oppdateringsrutiner • EDRPOU[33]-database • dataspråksett som brukt for det ukrainske alfabetet	***Modus operandi:*** • målrettet rekognosering • sosial manipulering • designet skadevare NotPetya • distribuerte skadevaren via et populært ukrainsk regnskapsprogram kalt M.E.Doc • fikk tilgang til programvarekoden til M.E.Doc, som lot dem modifisere og tilføye skadelige funksjoner til filene som inneholdt programvareoppdateringer. NotPetya ble sendt i ettertid til enheter som hadde lastet ned oppdateringen • fikk kommando-og-kontroll over offers enheter som kunne fjernstyres av angriperne	**Formål:** • skape forstyrrelser til strategisk fordel for Russland **Konsekvens:** • NotPetya spredde seg til andre land, herunder f.eks. andre lands sykehus og helsestasjoner og forårsaket betydelige forstyrrelser i grunnleggende kritiske funksjoner i flere land • Sykehuset Heritage Valley rapporterte krypterte harddisker, låste arbeidsstasjoner, bl.a. pasientlister og pasienthistorikk var utilgjengelig, tester måtte derav gjøres på ny. De mistet

[32] Macrons politisk parti

[33] Hver organisasjon som driver virksomhet i Ukraina, har en unik juridisk enhetsidentifikator kalt et EDRPOU-nummer (ЄДРПОУ) som tilsvarer et skatteidentifikasjonsnummer i andre land. Et Sertifiserings Nettsted er brukt til å kontrollere om et selskap har et gyldig sertifikat for verifisering av elektroniske signaturer (Nasjonal Statistisk Sentralbyrå i Ukraina, 2021). Å legge inn et selskaps EDRPOU-nummer på sertifiseringsnettstedet ville avsløre om selskapet hadde et gyldig sertifikat samt navnet på enheten tilknyttet et gitt EDRPOU-nummer.

				tilgang til bl.a. kritiske datasystemer tilknyttet radiologi og kardiologi i ca. en uke. • Heritage Valley brukte over $2 millioner dollar på å bekjempe og hente seg inn fra angrepet.
2017 - 2018 (s. 23-39)	**Mål/ofre:** • Den Internasjonale Olympiske komite (IOC) • Sørkoreanske sports- og olympiske komite • Sørkoreansk kraftverk • Sørkoreansk flyplass • Det Sørkoreanske departement for jordbruk (MAFRA) • Sør-Koreas Nasjonale Antiterroristisk Senter	**Typer informasjon brukt:** • medlemmer av IOC, herunder ledelse, avdelingsdirektører osv. • deltakere og deres kontakter • nettverk, herunder domener og underdomener • partnere og deres ansatte • svakheter i måls nettsider • utøveres bakgrunn, språk	***Modus operandi*:** • målrettet rekognosering av ofre • opprettet falsk infrastruktur, brukt til målrettede nettfisking-e-poster til mottakere, tilpasset til interesse/rolle i arrangementet • målrettede nettfisking-kampanjer mot interessenter, ansatte hos partnere, utøvere - utformet med innhold/språk som fremstod relevant for mottakerne • utviklet skadevare som lastet ned tilleggsinnhold fra et domene angriperne kontroller – template-library.ml. • skannet Korea-basert infrastruktur for sårbarheter • tekniske undersøkelser for svakheter i Sør-Koreas nettsider • «spoofing» - sendte e-poster som imiterte legitime organisasjoner, bl.a. domener som angriperne ikke selv kontrollerte • forfalsket nettsider til MAFRA • målrettet nettfisking ved spoofet e-post – avsender så ut som info@nctc.go.kr – det offisielle domenet til Sør-Koreas Nasjonale Antiterroristisk Senter	**Formål:** • skape forstyrrelser til strategisk fordel for Russland **Konsekvens:** Uviss

			• brukte OSINT-verktøy (sannsynligvis theHarvester) for å samle brukerdata, IP-adresser og server data relatert til all «Remote Desktop Protocol» • brukte det åpent tilgjengelig verktøyet Invoke-PSimage for å etablere kryptert kanal fra mottakers enhet til angripernes server mm.	

2018 (s. 39-41)	**Mål/ofre:**
	• OPCW (Organisation for the Prohibition of Chemical Weapons)
	• DSTL (Defence Science and Technology Laboratory)
		Typer informasjon brukt:
		• OPCWs og DSTLs ansattes e-postadresser
		• informasjon om ansatte i en tysk avis
		• informasjon om et britisk etterforskningsbyrå
		• dokumentmal
		• informasjon om involverte i Salisbury-case
		• personlige opplysninger om britiske og tyske journalister
			***Modus operandi*:**
			• målrettet rekognosering av ofre
			• opprettet falsk infrastruktur
			  ○ e-postkonto med brukernavn som etterlignet navnet til en kjent tysk avis
			  ○ e-postkonto som etterlignet DSTLs e-postadresse
			• målrettede nettfisking-kampanjer mot ca. 60 DSTL e-postadresser, med emne «hendelsen i Salisbury», angivelig fra en tysk journalist
			• sendte e-poster med skadevare, fra tilsynelatende legitim DSTL e-postadresse
			• tre målrettede nettfisking-kampanjer mot OPCW og britiske byrå som var involvert i etterforskningen av Salisbury-case, avsender etterlignet navn til britisk journalist
				Formål:
				• skape forstyrrelser til strategisk fordel for Russland
				Konsekvens:
				Uviss

2018 (s. 41-42)	**Mål/ofre:** • Staten Georgia • georgiske mediehus • andre myndigheter • privat sektor	**Typer informasjon brukt:** • personlige opplysninger om ansatte i et mediehus • e-postadresser • interesser • kontakter	***Modus operandi*:** • teknisk rekognosering av Parlamentet i Georgias offisielle domene • passiv rekognosering av georgiske mediehus, • anskaffet og brukte infrastruktur designet for å etterligne samme mediehus • anskaffet og/eller utviklet skadevare • målrettede nettfisking-kampanje mot mediehus ○ sendte e-poster vedlagt skadevare til 68 e-postadresser tilknyttet samme mediehus sitt domene • forsøkte å få uautorisert tilgang til nettverk • større cyberangrep mot flere enheter i Georgia som ga dem ca. 15000 hjemmesider tilhørende Georgias myndigheter m.fl., og i privat sektor, • Spoofet flere hjemmesider til myndigheter og private organisasjoner	**Formål:** • skape forstyrrelser til strategisk fordel for Russland • skape forstyrrelser av grunnleggende kritiske funksjoner • kompromittere georgiske myndigheter • kompromittere Georgias tidligere president som var kjent for å være anti-russisk **Konsekvens:** • medførte forstyrrelse av tjenester til noen av hjemmesidene de fikk kontroll over
«Pawn Storm» APT-gruppe (Hacquebord, 2020)				
2004 - i dag	**Mål/ofre:** • internasjonale militære organisasjoner • media	**Typer informasjon brukt:** • nettverks-konfigurasjoner • TCP-porter 443, 445, 1433 • e-post kontoer • sårbarheter	***Modus operandi*:** • målrettet passiv og aktiv rekognosering, herunder sårbarhetsskanning – på flere organisasjoner, • sosial manipulering • distribuerte skadevare mot sine mål • distribuerte iFrame-injeksjoner[34]	**Formål:** • påvirke medier og offentlig opinion **Konsekvens:**

[34] iFrame er en komponent i et HTML-element som lar en å legge inn dokumenter, videoer og interaktive medier på en side. Ved å gjøre dette kan man vise en sekundær webside på hoved nettsiden. I utgangspunkt utgjør ikke iFrame-elementet noen sikkerhetsrisiko, men det kan bli brukt for såkalt iFrame-injeksjon. Denne typen angrep omdirigerer besøkende til et ondsinnet nettsted, som deretter vil installere et virus på de besøkendes PC eller forsøke å stjele sensitiv informasjon.

	• politiske organisasjoner • europeiske utdannings-institusjoner • Democratic National Convention (DNC) • Tysklands kristendemokrats union (politisk parti) • Parlamentet i Tyrkia og i Montenegro • WADA		• direkte angrep på nett- og skytjenester • eksfiltrerte informasjon • utnyttet nulldagssårbarheter • brukte kompromitterte e-postadresser for å sende infiserte e-poster med formål å få tilgang til offers passord og andre autentifikatorer	• uviss mengde data ble stjålet fra WADA og DNC
«Lebanese Cedar» APT-gruppe (ClearSky Cyber Security ltd., 2021)				
	Mål/ofre: • privateide selskaper og offentlige organisasjoner over hele verden	**Typer informasjon som har blitt brukt:** • nettverk • sårbarheter • oppdateringsrutiner • brukernavn og passord til web-administratorer • maskinvarer • OS og versjon som er i bruk • IP-adresser • FTP-servere mm.	***Modus operandi*:** • fikk tilgang til systemene ved å utnytte kjente sårbarheter som ikke ble «patchet»	**Formål:** • stjele informasjon **Konsekvens:** Uviss

E: Beskrivelse av noen tidligere cyberangrep som er analysert i denne studien

United States of America v. Rafatnejad et al. - «Silent Librarian» case

United States of America v. Rafatnejad et al. også kjent som «Silent Librarian»-case er tiltalen mot ni iranere som jobbet for en organisasjon ved navn Mabna Institute (Berman, 2018, s.1-2). Ifølge påtalemyndighetene stjal de tiltalte mer enn 31 terabyte data fra 320 universiteter, samt en rekke private selskaper og offentlige etater over hele verden i perioden 2013-2017. Kompromitterte private selskaper tilhørte såkalt «kunnskapsproduserende sektor», herunder forlag, medie- og underholdningsselskaper, advokatfirma, teknologiselskaper, konsulentbyråer og lignende. Kostnaden for universitetene alene utgjorde angivelig omtrent 3,4 milliarder dollar. Informasjonen stjålet fra universitetene ble brukt av Islamic Revolutionary Guard Corps (IRGC) eller solgt til fortjeneste Iran (Berman, 2018, s. 2).

Cyberangrep ble iverksatt rundt 2013 og besto av tre faser. For det første gjennomførte angriperne online rekognosering av universitetsprofessorer. Dette inkluderte profilering av vedkommendes forskningsinteresser og publiserte artikler (Berman, 2018, s. 3, pkt. 4a). Deretter utformet de målrettede nettfisking-e-poster som var tilpasset hver enkelt mottaker og/eller organisasjon. E-postene ble utformet som angivelig å være sendt fra professorer ved et universitet. De ble rettet til professorer ved et annet universitet. Generelt antydet e-postene at avsenderen hadde lest en artikkel som offeret nylig hadde publisert. Videre uttrykket avsenderen interesse av å lese andre artikler. Lenke til slike ønskede artikler ble vedlagt e-postene. Når offeret klikket på lenker, ble de dirigert til et forfalsket domene. Domenet inneholdt en webside designet for å se ut til å være påloggingssiden for offerets universitet. Formålet var å manipulere professorene til å tro at de er blitt logget ut av universitetets datasystem og må logge inn på nytt.

Hvis offeret skrev inn påloggingsinformasjonen (brukernavn og passord), ble autentifikatorer exfiltrert av hackerne. Videre brukte hackerne de stjålne autentifikatorne for uautorisert tilgang til offers kontoer. Derfra eksfiltrerte de akademiske data og dokumenter fra systemene tilhørende kompromitterte universiteter, herunder akademiske tidsskrifter, avhandlinger og elektroniske bøker (Berman, 2018, s. 3-5, pkt. 4a-4c).

For å kompromittere kontoer til ofre i privat sektoren, brukte hackerne en teknikk kjent som «password spraying» (Berman, 2018, s. 7, pkt. 8). Det innebar først innsamling av lister med navn og e-postkontoer tilknyttet offer-organisasjon med hjelp av OSINT-verktøy. Deretter forsøkte de å få tilgang til kontoene ved bruk av ofte brukte passord eller passord som man kan finne i lekkasjer. De fikk tilgang til noen kontoer som de eksfiltrerte informasjon fra og etablerte automatiserte videresendingsregler slik at nye utgående og innkommende e-postmeldinger ble videresendt til e-postkontoer kontrollert av hackerne (Berman, 2018, s. 8, pkt. 8).

Omtrent 31,5 terabyte akademiske data og intellektuell eiendom ble stjålet fra ulike universiteter, og lagret til utenlandske servere som hackerne kontrollerte. I løpet av hacking-operasjonen gjennomførte de målrettet rekognosering og sosial manipulering av over 100 000 professorer og deres kontoer over hele verden. Som et resultat kompromitterte de minst 7998 personlige brukerkontoer (Berman, 2018, s. 5, pkt. 5). De eksfiltrerte dataene og påloggingsopplysningene til professorer ble overlevert til IRGC, og solgt til Iran. Herunder til to nettsteder, Megapaper.ir og Gigapaper.ir (Berman, 2018, s. 6, pkt. 6). Megapaper solgte stjålne akademiske ressurser til andre kunder i Iran, inkludert iranbaserte offentlige universiteter og institusjoner. Gigapaper solgte en tjeneste til kunder i Iran, der innkjøpskunder kunne bruke kompromitterte kontoer for å få direkte tilgang til de digitale biblioteksystemene til bestemte universiteter (Berman, 2018, s. 6, pkt. 6).

United States of America v. Andrienko et al. - «GRU hackers» rettssak

United States of America v. Andrienko et al. eller såkalt «GRU hackers»-case er en ev de mest omtalte hacking-relaterte rettsaker de siste årene. Seks GRU-medlemmer gjennomførte sammen flere målrettede hacking-angrep for å distribuere skadevare og skape forstyrrelser til strategisk fordel for Russland (Coville, 2020). De anskaffet og brukte servere, e-postkontoer, mobilapplikasjoner og tilhørende hackinginfrastruktur til bruk i målrettede nettfisking-kampanjer og andre datainnbrudd. Videre utviklet og distribuerte de skadevare mot offer over hele verden (Coville, 2020, s. 6–7).

Angrepene ble typisk initiert ved rekognosering av blant annet offer-organisasjoners datanettverk og personell (Coville, 2020, s. 8). Rekognoseringen ga omfattende teknisk og biografisk informasjon de brukte til påfølgende innbrudd, ved eksempelvis målrettede nettfisking-kampanjer. Nettfisking e-post ble designet for å lure mottakere til å gi angriperne

tilgang til å bruke offerets data og brukerkonto-opplysninger. E-postene ble utformet for å imitere e-postene fra tjenestetilbydere eller kollegaer, og oppmuntret til å klikke på hyperlinker eller til å åpne vedlegg med skadevare som infiserte offers datamaskin dersom det ble åpnet (Coville, 2020, s. 8).

Angrep mot Ukrainas kraftnett og finanssektor i 2015-2016 og NotPetya i 2017

Angrepet mot Ukrainske strømselskaper i 2015-2016 har fått bølgeeffekt og påvirket stor del av landets kritisk infrastruktur (Coville, 2020). Angrepet startet med målrettede nettfisking e-poster som ble designet for de enkelte IT-personell og systemadministratorene. En grundig rekognosering resulterte i mengder av detaljerte personlige opplysninger om utvalgte individer. For å få tilgang til SCADA-systemene hos de ukrainske energidistribusjonsselskapene brukte hackerne autentifikatorer stjålet ved hjelp av nettfisking e-post (Coville, 2020, s. 10, pkt. 21b).

Angrepet mot Ukrainas Finansdepartement og Skatteetaten i desember 2016 utviklet seg på en lignende måte. Det startet med rekognosering og påfølgende nettfisking-kampanje mot Skatteetatens systemadministratorer. En systemadministrator åpnet en e-post med en Microsoft Excel-fil kalt «MoF[35] critical IT needs_eng.xls» og aktiverte dermed skadevare. Skadevaren ble installert på vedkommendes datamaskin og etablerte skjult kommunikasjon mellom datamaskinen og en tredjeparts-tjeneste brukt av hackerne (Coville, 2020).

NotPetya-angrepet er per i dag en av de mest kostbare og destruktive cyberangrep i historien. NotPetya utnyttet to kjente sårbarheter for eldre Windows-versjoner: EternalBlue og Mimikatz (EH2). For å aktivere og distribuere viruset iverksatte hackerne omfattende rekognosering av en liten, familiedrevet ukrainsk programvarevirksomhet i Kyiv (EH2). Firmaet leverte tjenester til flere virksomheter i alle størrelser over hele Ukraina med programvare M.E.Doc, som ble brukt av nesten alle ukrainske virksomheter og skattemyndigheter. Fra og med april 2017 gjorde hackerne seg kjent med hvordan søk i EDRPOU-database fungerer og med M.E.Doc dataspråksett som er brukt for det ukrainske alfabetet (Coville, 2020, s. 18. pkt. 36).

Via nettverkskanning fikk angriperne informasjon om oppdateringsrutiner, noe de brukte flittig videre (CE2), M.E.Doc-programvaren i kundenettverk var periodisk koblet til oppdateringsserveren for å se etter nye programvareoppdateringer (Coville, 2020, s. 18, pkt. 37). Hackerne fikk tilgang til programvarekoden for M.E.Doc før NotPetya-angrepene, som

[35] MoF er forkortelsen som brukes i Ukrainsk Finansdepartementet (Ministry of Finance)

tillot dem å legge skadevare til filene som inneholder «programvareoppdateringene». Hackerne endret oppdateringsfiler den 14. april 2017; 15. mai 2017; og 21. juni 2017. Datamaskiner som mottok M.E.Doc-oppdateringer lastet ned disse filene, men NotPetya-filen ble ikke aktivert før 27. juni 2017 - Ukrainas Grunnlovsdag. Kvelden 27. juni 2017 paralyserte en serie cyberangrep flere datasystemer tilhørende ukrainske selskaper, inkludert banker, aviser og strømtilbydere (Coville, 2020, s. 19, pkt. 37d). NotPetya ble designet for å spre seg til flere enheter i tilkoblede nettverk, som gjorde at skadevaren spredde seg til flere andre land og institusjoner.

Innblanding i Frankrikes valg i 2017

Hackerne utførte omfattende rekognosering av personer involvert i President Macrons valgkampanje, andre franske politikere og høyt profilerte personer (Coville, 2020, s. 15). De samlet personlige opplysninger og informasjon om interne kommunikasjonsmåter, pågående prosjekter, arbeidsrelasjoner osv. Deretter iverksatt de syv ulik nettfisking-kampanjer, hver enkelt av dem nøye og tilpasset i design. Emnet i kampanjene var offentlige sikkerhetsmeldinger om terrorangrep, programoppdateringer for valgautomater, politiske skandaler, «En Marchels» forhold til presse og anbefalinger om internasjonal cybersikkerhet (Coville, 2020, s. 15, pkt. 27).

En av hackerne utviklet og testet teknikker for nettfisking e-poster omhandlende fildeling via Google Docs, som ble brukt av partimedlemmer i En Marchel (Coville, 2020, s. 15, kt. 28). Deretter utviklet de et infisert dokument med navn «Qui_peut_parler_aux journalists.docx» – «hvem kan snakke med journalister», som påstås å navngi ni medlemmer i En Marchel som kan snakke med journalister om et nylig terrorangrep. De brukte avsender-konto som imiterte navnet til Macrons pressesekretær for å sende e-poster med infiserte Google Docs lenker til ca. 30 partimedlemmer (Coville, 2020, s. 15).

Formålet med alle aktivitetene ble tydelig 12.-26. april 2017, da hackerne brukte en konto på sosiale medier for å kommunisere til flere franskmenn at de var i besittelse av og kunne tilby interne dokumenter fra En Marchel. Rundt 3. mai 2017 begynte uidentifiserte personer å lekke kompromitterende dokumenter angivelig fra En Marchel valgkampanjes e-postkontoer. På denne måten forsøkte gjerningsmennene å påvirke offentlig opinion rett før president valget.

Andrienko et al. utførte flere lignende angrep hvor de brukte de samme teknikkene. Blant annet angrepene mot arrangører av vinter OL 2018 i Pyeongchang, angrepene mot OCWP og DSTL og angrepet mot Staten Georgia (Coville, 2020; DSTL, 2018; OPCW, 2021). For å unngå

deteksjon og dekke over tilhørighet til GRU og sin geografiske plassering, brukte de fiktive navn, persona og digital infrastruktur som servere, domener, kryptovaluta, e-postkontoer, sosiale mediekontoer og andre nettjenester. Infrastrukturen ble brukt til å rekognosere, skanne og sondere offers nettverk, samt sende målrettede nettfisking e-poster (Coville, 2020, s. 6–8).

Gjerningsmennene brukte informasjonen fra rekognoseringsprosessen for å få tilgang til autentifikatorer: Ved å gi fremstilling av andre identiteter fikk de uautorisert tilgang til å bevege seg lateralt til og i offers nettverk. De opprettet domener og lagte URL-er for bruk til hacking, som var designet til å imitere legitime nettsider som ofrene var kjent med, herunder innloggingsider til e-post og andre tjenester, nettsteder for fildeling og fil-lagring, samt sider for passord gjenopprettelse (Coville, 2020, s. 8).

«Lebanese Cedar» APT-gruppe

«Lebanese Cedar»[36] er en APT-gruppe som har operert i nesten et tiår og gjennomført flere cyberangrep på privateide selskaper og offentlige organisasjoner over hele verden (ClearSky Cyber Security ltd, 2021). Det er funnet rundt 250 servere som tilsynelatende ble hacket av «Lebanese Cedar» med formål om å stjele informasjon.

Gruppens hoved angrepsvektor var innbrudd i Oracle og Atlassian WEB-servere. Granskningsrapporten konkluderer med at trusselaktørene brukte OSINT-verktøy, herunder Censys, Shodan og ZoomEye, for å gjennomføre skanning av nettverk. De fikk tilgang til systemene ved å utnytte kjente sårbarheter som ikke ble «patchet» (ClearSky Cyber Security ltd, 2021, s. 8).

Granskning har vist at Volatile Cedar var en svært målrettet og veldig godt administrert kampanje. Det kommer frem av granskningsrapport at målene var nøye valgt og at angriperne gjennomførte omfattende rekognosering for å skreddersy hvert angrep til sitt spesifikke mål. Blant informasjon som ble brukt for å forberede cyberangrep var brukernavn og passord til web-administratorer, generell informasjon om maskinvarer (inkludert PC) og versjon som er i bruk, IIS versjon, IP-adresser, resultater av port-skanning, FTP-servere mm. (ClearSky Cyber Security ltd, 2021, s. 9–10).

«Pawn Storm» APT-gruppe

[36] Også kjent som Volatile Cedar

«Pawn Storm»[37] er en aktiv APT-gruppe som siden 2004 har gjennomført en rekke målrettede angrep mot internasjonale militære-, media- og politiske organisasjoner, samt noen europeiske utdanningsinstitusjoner (Hacquebord, 2020, s. 6). Hovedsakelig driver «Pawn Storm» distribusjon av skadevare mot sine mål, iFrame-injeksjoner, direkte angrep på nett- og skytjenester, samt målrettet passiv og aktiv rekognosering på flere ulike organisasjoner med formål å påvirke medier og offentlig opinion. Trusselaktørene som står bak «Pawn Storm» bruker ulike sosiale manipuleringsteknikker, informasjonstyveri og utnyttelse av nulldagssårbarheter. Gruppen har og brukt kompromitterte e-postadresser for å sende ut infiserte e-poster med formål å få tilgang til offers passord og andre autentifikatorer (Hacquebord, 2020, s. 5).

I 2019 utførte «Pawn Storm» nettverksskanning av flere e-postservere og Microsoft Exchange Autodiscover-servere over hele verden (Hacquebord, 2020, s. 7). Granskning viser at de fleste skanninger var rettet mot TCP-port 443 og flere e-postprotokoller[38]. «Pawn Storm» så i tillegg ut til å gjøre store skanninger på TCP-porter 445 og 1433. Dette fremstår som et forsøk på å finne sårbare servere som kjører Microsoft SQL Server- og katalogtjenester (Hacquebord, 2020, s. 7). Rapporten konkluderer med at vi i fremtid kan forvente enda flere direkte angrep mot e-post- og skytjenester som ikke er avhengige av skadevare, men heller basert på sårbarhetsskanning og utnyttelse av nulldagssårbarheter (Hacquebord, 2020, s. 12).

[37] Også kjent som APT28, Strontium og Fancy Bear
[38] Internet Message Access Protocol (IMAP) [143, 993], Post Office Protocol 3 (POP3) [110, 995], og Simple Mail Transfer Protocol (SMTP) [465, 587] ble skannet.