TRENDER I DET DIGITALE TRUSSELBILDET FOR NORSKE VIRKSOMHETER

Bacheloroppgave i Digital Forretningsutvikling

20. mai 2019

Bendik Øvstedal
Torstein Kårstad

Veileder: Bjørn Klefstad

Innholdsfortegnelse

Sammendrag

Denne oppgaven undersøker utviklingen av det digitale trusselbildet og angrepsmetoder norske virksomheter har opplevd de siste fem årene. Rapportens bidrag er å kartlegge hvilke trender som kommer å prege trusselbildet de neste fem årene, og med utgangspunkt i denne kartleggingen vil det anbefales sikkerhetstiltak for å imøtekomme truslene.

For å løse oppgaven ble det valgt å gjennomføre en litteraturstudie bestående av rapporter fra ressurssterke organisasjoner og bransjeforeninger som jobber med informasjonssikkerhet og intervju med ressurspersoner med bakgrunn i informasjonssikkerhet.

På bakgrunn av gjennomført studie kommer det frem at trusselbildet preges i stor grad av vinningskriminalitet og etterretning. Trendutviklingen viser at angrepene blir stadig mer målrettede og profesjonaliserte. Norsk grunnsikring har blitt forholdsvis sterk, og de mest effektive angrepene benytter teknologi og utnytter mennesker til å stjele verdier og informasjon fra virksomheter. Med bakgrunn i studiet vil en økning av antall enheter, lovgiving og håndheving av personvern, samt en internasjonalisering av vinningskriminalitet prege det fremtidige trusselbildet.

.

Abstract

This paper looks at the digital threats facing Norwegian organizations and businesses. By analysing changes from 2014 to 2019 and interviewing key people from a variety of backgrounds within information security, this paper aims to predict the most relevant and overarching trends to shape digital threats in the coming five years. Based on these predictions, we have created a simple “how-to” guide to fit most organizations. The guide contains five areas where organizations can improve to keep up with the changing digital landscape, along with our suggested organizational and technical measures.

1. Innledning

1.1. Tema

Informasjonssikkerhet er arbeidet for å sikre systemene som har med informasjonsbehandling å gjøre. De aller fleste norske virksomheter i dag benytter slike system og en stor andel er fullstendig avhengig av slike system. IT-systemer utgjør samtidig et sårbart område for virksomhetene, da ondsinnede aktører kan stjele verdier, informasjon eller ramme virksomheten på andre måter gjennom disse systemene. Utviklingen og bruk av ny teknologi og innovasjoner åpner nye dører for uvedkommende aktører som ønsker en inngang til virksomheten.

1.2. Problemstilling

IT har blitt et sentralt verktøy for de fleste virksomheter i Norge, og som en konsekvens av dette rammes mange av digitale angrep på sine systemer og verdikilder, noen ganger uten at vedkommende engang er klar over at det har skjedd. Mange virksomheter mangler tilstrekkelig kompetanse innenfor informasjonssikkerhet, og på hvilke sikringstiltak som kan innføres for å imøtekomme truslene. Virksomhetene har ikke oversikt over egne sårbarheter og hvilken risiko de er utsatt for. I tillegg blir trusselaktørene mer sofistikerte og benytter stadig mer avanserte angrepsmetoder. «Dei risikoreduserande tiltaka held ikkje tritt med den raske utviklinga i sårbare punkt, spesielt på cyberområdet»[1] Sier Kjetil Nilsen, direktør for nasjonal sikkerhetsmyndighet i NSM sin årsrapport fra 2017. For å hindre konsekvensene av sikkerhetshendelser må den stadig økende digitaliseringen av norske interesser gjøres i takt med økt kompetanse på truslene og sårbarhetene. Vi må ligge ett skritt foran trusselaktørene.

En forutsetning for å gjøre presise risikoanalyser i sikkerhetsarbeidet er at man har en oversikt over trusselbildet og kan vurdere hvilke trusler som skaper risiko for virksomheten. Vi skal derfor i denne oppgaven se nærmere på følgende:

- Utviklingen av trusselbildet og angrepsmetoder norske virksomheter har opplevd de siste fem årene.
- Kartlegge trendene som vil prege trusselbildet for norske virksomheter de neste fem årene basert på dagens situasjon og ressurspersoner som jobber innen informasjonssikkerhet.

[1] Næringslivets Sikkerhetsråd, *Nasjonalt Tryggingsorgan - Årsrapporten 2017*. 2017.

- Lage en oversiktlig «how to guide» over anbefalte sikkerhetstiltak å imøtekomme de framtidige truslene.

1.3. Begrunnelse, motivasjon og gevinstpotensiale

«Kriminaliteten flytter seg til internett» sier Roger Johnsen, tidligere administrerende direktør i NorSIS. Antallet privatpersoner som er på nett er i stadig økende grad og norske virksomheter følger denne veksten. Virksomhetene blir stadig mer avhengig av IKT løsninger og internett-tilgang, og dette åpner nye dører for målrettet kriminalitet. [2] Norske virksomheter har ikke kapasitet til å håndtere dataangrep på det samme nivået som trusselaktørene behersker, og evnen til å oppdage hendelser er av varierende grad.[3]

«For enkeltvirksomheter vurderer NSM at det er høyest IKT-risiko knyttet til digital kriminalitet, særlig fra aktører som er ute etter økonomiske verdier» [4] Hendelser knyttet til IT-sikkerhet koster både private og offentlige virksomheter store summer hvert år. Selv om det er store mørketall på dette området estimerer Næringslivets Sikkerhetsråd at det i Norge er snakk om et økonomisk tap på et titalls milliarder kroner hvert år. [5] Et ferskt eksempel som understøtter estimater i slik størrelsesorden er cyberangrepet mot Hydro i mars 2019. Hydro koblet ut hele datasystemet for å hindre at et krypteringsvirus spredde seg i selskapets IT-infrastruktur, og produksjon måtte dermed fortsette manuelt den første tiden etter angrepet. Tidlige estimater fra selskapet anslo et tap på mellom 300 og 350 millioner tilknyttet hendelsen, på grunn av redusert volum og produksjon. [6]

Etter hvert som virksomheter digitaliseres blir sikkerhetsbildet mer sammensatt og komplekst. Noen av trendene som sammenfaller med digitaliseringen er at flere tjenester settes ut til eksterne, verdikjedene blir lengre og antall avhengigheter til andre systemer og virksomheter øker. Fra et sikkerhetsperspektiv betyr dette flere mulige sårbarheter og flere ledd i forretningsprosessene som kan utnyttes og misbrukes. Målet med oppgaven er å bidra til forebyggende sikkerhetsarbeid ved å rette blikket fremover.

1.4. Avgrensninger

Oppgaven belyser det digitale trusselbildet. Med dette så mener vi trusler, angrepsmetoder, sårbarheter og trender hvor nettverket utnyttes som inngangsportal til virksomheten. Vi

[2] NorSIS, *Trusler og Trender 2015*. 2015.
[3] Nasjonal Sikkerhetsmyndighet, *Risiko 2015*. 2015.
[4] Nasjonal Sikkerhetsmyndighet, *Helhetlig IKT risikobilde 2016*. 2016.
[5] Næringslivets Sikkerhetsråd, *Mørketallsundersøkelsen 2018*. 2018.
[6] Anders Nybakken Kvale, H.H.T., *Hydro: Anslår kostnad på 300 til 350 millioner kroner etter cyberangrepet*, in *E24*. 2019.

inkluderer ikke trusler, metoder og sårbarheter som er knyttet til den fysiske sikringen av virksomhetene. Det vil si at tema som eksempelvis innsidertrusler, personellsikkerhet, fysiske innbrudd og tyveri ikke er en del av denne oppgaven. Fysisk sikkerhet vil behandles ulikt for forskjellige virksomheter, men de aller fleste virksomheter er utsatt for digitale trusler. Ikke alle virksomheter har personell og store lokaler, men alle virksomheter har informasjon som må beskyttes. Trusselbildet og angrepsmetoder, som det fremstår i oppgaven består i hovedsak av tilsiktede hendelser. Utilsiktede hendelser, som menneskelige og tekniske feil, uhell og ulykker er ikke inkludert i beskrivelsen av trusselbildet. Avgrensingen er gjort for å kunne samle inn data som er generaliserbar for norske virksomheter, og som dermed vil være relevant for flest mulig.

2. Bakgrunn

2.1. Kildene

Litteraturen i oppgavens resultatdel består hovedsakelig av rapporter og undersøkelser fra disse kildene. I dette kapitelet vil vi beskrive de viktigste kildene og ressursene som resultatet bygger på.

- **Næringslivets Sikkerhetsråd (NSR)**
    - Mørketallsundersøkelsen
- **Norsk senter for informasjonssikring (NorSIS)**
    - Trusler og Trender
- **Nasjonal Sikkerhetsmyndighet (NSM)**
    - Risiko
    - Helhetlig IKT Risikobilde
- **Mnemonic**
    - Security Report
- **Telenor**
    - Digital Sikkerhet

Mørketallsundersøkelsen (NSR)

Mørketallsundersøkelsen foretas av Næringslivets Sikkerhetsråd (NSR) annen hvert år. NSR har som formål å forebygge kriminalitet mot næringslivet og undersøkelsen skal bidra til opplysning og informasjon som næringslivet og offentlige myndigheter kan få nytte av. Undersøkelsen bidrar til å kartlegge omfanget av datakriminalitet, sikkerhetshendelser og

sikringstiltak hos norske virksomheter. Undersøkelsen har hatt opptil 1500 respondenter og sammensetningen av respondenter har vært ulik for hver undersøkelse.

Trusler og trender (NorSIS)

Norsk senter for informasjonssikring (NorSIS) er en forening som er del av regjeringens satsing på informasjonssikkerhet. De er delvis finansiert av Justis- og beredskapsdepartementet og har som oppgave å bidra til kunnskapsformidling og utvikling av digital sikkerhetskultur. NorSIS er blant annet ansvarlige for Nettvett.no, Slettmeg.no og Nasjonal sikkerhetsmåned. Senteret publiserer årlige rapporter om trusselbilde hvor målgruppen er små- og mellomstore virksomheter og enkeltpersoner.

Risiko (NSM)

Nasjonal sikkerhetsmyndighet (NSM NorCERT) har som oppdrag å oppdage, varsle og bistå ved hendelseshåndtering i forbindelse med angrep mot samfunnsviktig infrastruktur. Rapporten kan beskrives som en generell risikovurdering som setter søkelyset på sikkerhetstilstanden til infrastruktur og objekter av nasjonal betydning, noe som inkluderer flere offentlige og private virksomheter. Rapporten utgis i samarbeid med Etterretningstjenesten, PST og Direktoratet for samfunnssikkerhet og beredskap (DSB).

Helhetlig IKT-Risikobilde (NSM)

Helhetlig IKT-Risikobilde, som også utgis av NSM, har til hensikt å øke bevissthet og motivere for bedre IKT-sikkerhet i offentlige og private virksomheter. Målgruppen er ledere og personell med oppgaver knyttet til sikkerhet på tvers av sektorer. Rapporten tar for seg trusler og praktiske tiltak som er relevant for en virksomhet, og har mindre fokus på samfunnskritisk infrastruktur og verdier.

Security Report (Mnemonic)

Mnemonic er et IT-sikkerhetsselskap med over 180 ansatte som tilbyr tjenester knyttet til rådgiving, risikostyring, detektering, respons og hendelseshåndtering. I deres årlige rapport deler de informasjon fra firmaets operasjonssenter fra året som har gått, tar opp tidsaktuelle endringer i bransjen og kommer med prediksjoner for fremtiden.

Digital Sikkerhet (Telenor)

Rapporten har blitt gitt ut årlig siden 2017 og omhandler trusselforståelse, utvikling i teknologi, angrepsmetoder og sikkerhetskompetanse som er relevant for Telenor, deres

kunder og utenforstående. Rapporten informerer om hvordan Telenor håndterer sikkerhet internt, men også hvordan trusselbildet ser ut for Telenors kunder og spesielt bedriftskunder. Statistikken som benyttes i rapporten er basert på Telenors eget datagrunnlag og deres kunder. Rapporten sees i sammenheng med at Telenor forvalter samfunnskritisk infrastruktur og har et samfunnsansvar til å opprettholde sikkerheten i sin drift.

2.2. Sentrale begreper

I oppgaven benyttes flere sentrale begreper tilknyttet informasjonssikkerhet og IKT. I dette kapitelet forklares betydningen av disse begrepene.

Begrep	Forklaring
Angrepsvektor	Område som er sårbart for angrep og brukes som inngang.
Informasjonssikkerhet	Informasjonssikkerhet handler om å sikre systemene som har med informasjonsbehandling. Det er en tilstrekkelig og balansert sikring av tilgjengelighet, konfidensialitet og integritet på informasjon i virksomhetens informasjonsbehandling. Dette inkluderer alt av IKT-systemer og digitale tjenester.
Inntrengingstest	Et kontrollert forsøk på å bryte gjennom sikkerhetssystemene til en virksomhet. Hensikten med slike angrep er å avdekke sårbarheter og sikkerhetshull i informasjonssystemer, slik at virksomhetene kan forbedre sikkerheten.
IoT (internet of things)	IoT, eller «tingenes internett» er en betegnelse for enheter og gjenstander med mulighet for å koble seg opp mot internett.
On-premise	IKT løsning som blir fysisk plassert innenfor virksomhetens bygninger.
Patching	Patching er en betegnelse på feilretting av kode. Hensikten er ofte å tette sikkerhetshull eller gjøre koden mer effektiv.
Sikkerhetshendelse	Tilknyttet informasjonens tilgjengelighet, konfidensialitet og integritet. En sikkerhetshendelse er et brudd på en eller flere av disse. Dette kan oppstå på flere forskjellige måter, eksempelvis ved virus- og malwareinfeksjon, manipuleringsangrep og hacking.

Sikkerhetstiltak	Arbeidet som utføres for å hindre at sikkerhetshendelser skal oppstå. Kan deles opp i tre hovedkategorier: Personell, teknologi og prosedyrer.
Sårbarhet	Manglende evne til å motstå en uønsket hendelse eller opprette ny stabil tilstand dersom en verdi er utsatt for uønsket påvirkning.
Tjenestutsetting	En organisasjon inngår et samarbeid med en ekstern leverandør for anskaffelse av en vare eller tjeneste.
Trusselbilde	En helhetlig oversikt over ulike trusler mot informasjonssikkerheten.
Trussel	En mulig uønsket handling som kan gi negativ konsekvens for en virksomhet.
Virus/Skadevare	Et program som infiserer andre programmer og reproduserer seg selv.

2.3. Angrepsmetodene

Dette kapitelet består av beskrivelse av vanlige angrepsmetoder norske virksomheter opplever.

Phishing	En betegnelse på en metode for svindel hvor man forsøker å tilegne seg sensitiv informasjon som personopplysninger, brukernavn, passord, kredittkortnummer eller bedriftshemmeligheter som kan brukes i vinnings øyemed. Et eksempel på dette er at en angriper utgir seg for å være fra en stor bank, og sender e-post til mange mottakere i håp om at noen skal la seg lure til å utføre instruksjonene i e-posten. Dette kan være instruksjoner som å oppsøke en webside eller klikke på et vedlegg.
Målrettet e-post (spearphishing)	Målrettet e-post er i motsetning til vanlig phishing rettet mot en spesifikk virksomhet. Angrepet er en metodisk tilnærming hvor angriperen samler informasjon om målet for å kunne personalisere e-posten som sendes for å virke mest mulig troverdig.

Krypteringsvirus	En type skadevare som låser eller krypterer hele eller deler av innholdet på en datamaskin. Målet er å få offeret til å betale løsepenger for at angriperen skal gi tilgang til datamaskinen igjen.
Tjenestenektangrep	Et angrep som overbelaster en server med stor trafikk. Hensikten med angrepet er å hindre brukere tilgang til systemet, informasjonen eller tjenesten som rammes.
Botnets	En samling av datamaskiner og enheter infisert med spesifikk skadevare for fjernstyring. Botnets kan leies ut av kriminelle for å begå kriminelle handlinger som for eksmpel tjenestenektangrep.
Vannhullsangrep	I et vannhullsangrep kompromitteres en nettside og brukes til å spre skadevare. Målet er at trusselaktøren skaffer tilgang til offerets nettverk. For å minimere sjansen for å bli oppdaget kan aktøren «hviteliste» IP-adresser, slik at skadevaren kun spres til den tiltenkte målgruppen.
Avanserte vedvarende trusler	En fellesbetegnelse for avanserte og målrettede angrep, hvor formålet er å etablere bakdører, plante og spre skadevare og hente ut informasjon. Angrepene kjennetegnes av at trusselaktøren er ressurssterk og langsiktig. Et eksempel på en slik trussel kan være etterretning fra statlige trusselaktører.

2.4. Trusselaktørene

Det finnes flere forskjellige trusselaktører med forskjellige mål og motiv. I dette kapitlet vil vi beskrive de mest sentrale aktørene.

Statlig sponsede og organiserte

Dette er cyberangrep som er utført av kontraktører på oppdrag av statlige makter. Det benyttes store ressurser på disse angrepene og de kan foregå over lang tid. Dette er målrettede angrep hvor hensikten er å tilegne seg informasjon eller produkter. Denne gruppen omtales ofte som avanserte vedvarende trusler og forbindes med etterretning og i noen tilfeller sabotasje.

Cyberkriminelle

Dette er kriminelle aktører som begår innbrudd på datasystemene, stjeler informasjon og svindler for økonomisk gevinst. Gruppen forbindes med vinningskriminalitet.

Aktivister og Hacktivister

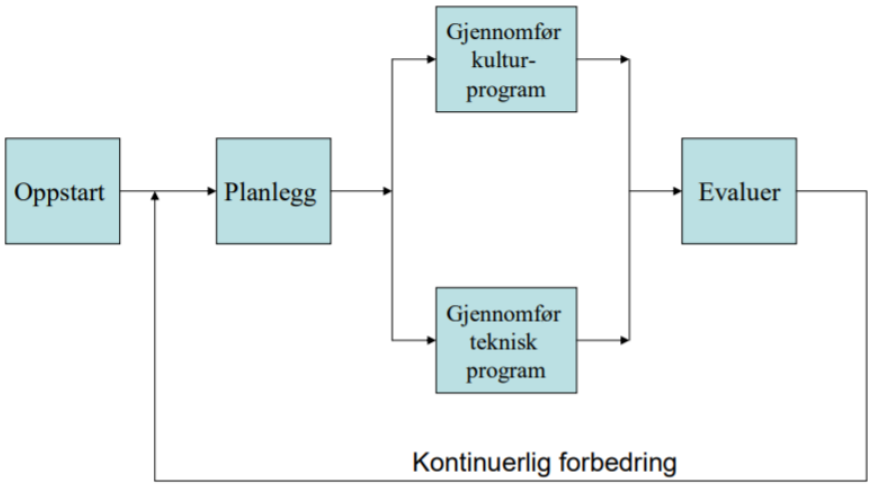
Dette er cyberkriminelle med en politisk agenda. Disse angriper gjerne virksomheter de ikke har et godt forhold til for å få frem sitt politiske budskap. Angrepene skjer ofte som tjenestenektangrep, nettbaserte protestaksjoner eller endring av innhold på nettsidene til virksomheten de angriper.

Vandaler

Nettvandaler er aktørene som saboterer og driver ugagn for moros skyld. Denne gruppen kan beskrives som individer som drives av spenningssøkende eller oppmerksomhetssøkende atferd.

2.5. Styringssystem for informajosnsikkerhet og Demingsirkelen

Hensikten med ISMS er å beskytte informasjon og IT-systemer i organisasjonen med helhetlig sikkerhetsarbeid som tar hensyn til både mennesker og teknologi. ISMS er en del av virksomhetens kvalitetssystem, og i den forbindelse brukes ofte Demingsirkelen, med dens fire faser for kontinuerlig forbedring.



Figur 1 Demingsirkelen for kontinuerlig forbedring. Hentet fra leksjon: Informasjonssikkerhetsstyring. NTNU.

Noen viktige poeng med demingsirkelen er å måle effekten av et tiltak, identifisere forbedringsbehov og å gjennomføre korrigerende tiltak slik at prosessen forbedres kontinuerlig. Denne figuren bygger på de samme prinsippene, men har noen forskjeller. En av de forskjellene er at figuren skiller mellom kulturprogram og teknisk program i gjennomføringen av tiltak for å vise at sikkerheten er avhengig av både tekniske løsninger og menneskene som bruker dem. For å lykkes med sikkerhetsarbeidet må den formelle og den uformelle delen av ISMS samsvare. Det innebærer å gjennomføre tiltak knyttet til kompetanse, sikkerhetskultur og holdninger i organisasjonen samtidig som man gjennomfører tiltak for tekniske løsninger. [7]

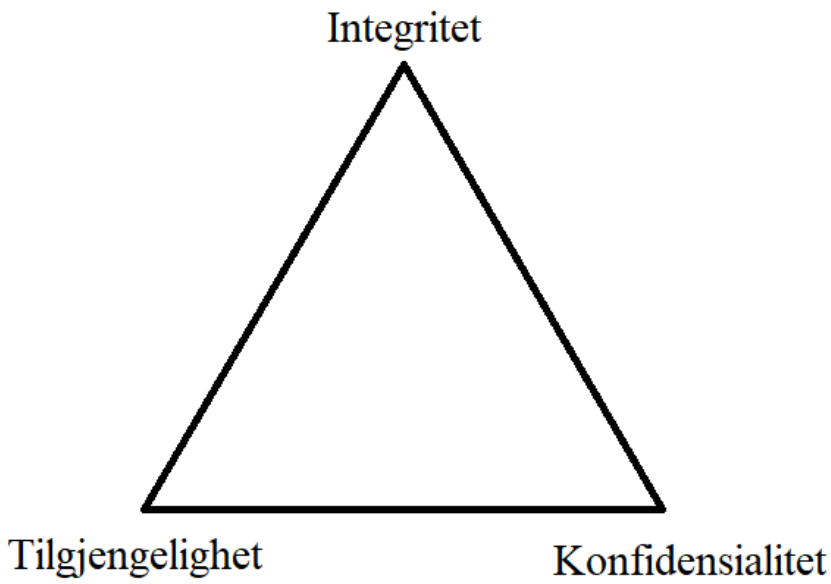
2.6. Risikoanalyse og trusselbildet

En risikoanalyse skal avdekke mulige uønskede hendelser, bedømme sannsynlighet for at hendelsen inntreffer, bedømme hendelsens konsekvens på virksomheten og vurdere tiltak som kan hindre eller redusere skadeomfanget til hendelsen. Man kan skille mellom uønskede hendelser som skyldes utilsiktede menneskelige feil som er forårsaket av egne ansatte og tilsiktede handlinger hvor noen ønsker å misbruke organisasjonens ressurser. En risikoanalyse bør inkludere alle mulige hendelser som har konsekvenser for virksomheten for å få et helhetlig bilde av risikoen man utsettes for. [8, 9]

[7] Greta Hjertø, B. Klefstad. *Informasjonssikkerhetsstyring*. NTNU.
[8] Greta Hjertø, B. Klefstad. *Risikoanalyse*. NTNU.
[9] Bjørn Klefstad, T. Hjelle. *Trusselbildet*. 2018. NTNU

Trusselbildet fokuserer gjerne mer på tilsiktede hendelser, og her skilles det mellom fysiske trusler, digitale trusler og sosial manipulering som kan skje både fysisk og digitalt. Trusselbildet i Norge eller verden er et generelt trusselbilde. For å analysere risikoen knyttet til en konkret organisasjon må truslene ses i sammenheng med og bedømmes ut ifra forhold i organisasjonen. Det skilles derfor mellom det generelle trusselbildet og det spesifikke trusselbildet en organisasjon forholder seg til.

2.7. Sikkerhetstriangelet



Figur 2 Sikkerhetstriangelet

Sikkerhetstriangelet beskriver forholdet mellom tilgjengelighet, konfidensialitet og integritet i informasjon. Tilgjengelighet skal vise hvor enkelt eller vanskelig det er å få tilgang til informasjonen og hvor lang tid det tar. Konfidensialitet handler om hvem som har tilgang og hvordan uvedkommende ikke har tilgang til informasjonen. Integriteten bestemmes av hvor riktig informasjonen er. Når det gjelder integritet finnes det både informasjon som må sjekkes og oppdateres ofte for at den skal være gyldig, og informasjon som må holde seg uendret til enhver tid for at den skal være gyldig. [10]

[10] Mikalsen, A.B. *Brukermiljø og sikkerhet*. 2018. NTNU.

3. Metode

Metode beskriver måten vi har valgt å gå til verks for å fremskaffe eller etterprøve kunnskap. Metode er redskapet vi bruker for å få svar på det vi vil undersøke, og når man velger metode så velger man metoden man mener vil gi data for å belyse problemstillingen på en god måte. [11]

3.1. Forskningsdesign

Etter hvert som problemstillingen ble utarbeidet lagde vi en plan for forskningsarbeidet. Når man velger forskningsdesign står man mellom å velge et ekstensivt og intensivt design. Et ekstensivt design innebærer datainnsamling og forskning i bredden fra mange kilder, med forholdsvis lite informasjon fra hver kilde. Dette er en mer kvantitativ orientert tilnærming til fremskaffing av informasjon. Fordelen med et slikt design er at man får mye strukturert og systematisert kunnskap om temaet, hvor man kan studere kvantitative variasjoner mellom kildene. Man får stor grad av statistisk generaliseringskraft, men det gir lite rom for teoretisk analyse.

Et intensivt design vil gå mer i dybden på temaet for å finne sammenheng og helhet. Ved et slikt design samler man data kun fra et fåtall kilder. Man samler derimot mye informasjon fra hver kilde, og studerer disse innenfor et helhetlig perspektiv. En slik tilnærming fanger opp meninger og opplevelser som ikke lar seg tallfeste eller måle. [11] Slike studier gir bedre muligheter for analytisk generalisering og er godt egnet for komplekse og lite utforskede temaer.

Det viktigste kriteriet for hvilken tilnærming man bestemmer seg for ligger i problemstillingen. Ved en avgrenset formulering vil det være mer hensiktsmessig å velge et ekstensivt design, men dersom problemstillingen er svært kompleks med mange variabler gir det mer mening å velge et intensivt opplegg.[12]

3.2. Valg av metode

Problemstillingen i oppgaven handler om trusselbildet norske virksomheter forholder seg til og utviklingen av denne over et satt tidsperspektiv. Problemstillingen berører blant annet trusselaktører i samfunnet, teknologisk utvikling, menneskelige faktorer og organisasjonelle faktorer. Med et komplekst problem som berører og påvirkes av svært mange variabler har vi

[11] Olav Dalland, *Metode og oppgaveskriving*. 5. utgave ed. 2012: Gyldendal.
[12] Busch, T., *Akademisk skriving - for bachelor- og masterstudenter*. 2013: Fagbokforlaget.

vurdert det som mest hensiktsmessig med et intensivt forskningsdesign. Forskningsprosjektet ble igangsatt uten klare hypoteser eller forhåndssatte svar på problemstillingen. Vi har dermed hatt en induktiv tilnærming til forskningsspørsmålet og vi har undersøkt mulige forklaringer underveis i prosjektet.

Siden problemstillingen omhandler et langt tidsperspektiv vurderte vi det som hensiktsmessig å gjennomføre datainnsamlingen i form av en litteraturstudie. Vi har foretatt en systematisk gjennomgang av litteratur fra de siste fem årene (2014 til 2019) som omhandler informasjonssikkerhet, digitale trusler, sårbarheter, angrepsmetoder og trender tilknyttet dette. Videre har vi analysert og sammenlignet rapporter og undersøkelser innenfor temaet for å hjelpe oss å tilegne nødvendig kunnskap for å gjøre en kartlegging av trusselbildet.

For å supplementere litteraturen har vi valgt å bruke intervju til videre datainnsamling. Dette er valgt for å oppdage og utforske nye temaer som ikke har vært en del av våre forkunnskaper og som ikke har kommet frem i vårt litteratursøk. Intervjuene med respondentene har vært semi-strukturerte, for å sikre en respons på en rekke spørsmål og i tillegg ha mulighet til å utforske nye temaer etter hvert som det har dukket opp. Intervjuene har blitt gjennomført med den hensikt å få eksperters innspill og meninger, spesielt knyttet til andre og tredje del av problemstillingen.

Prosessen for forskningsarbeidet kan beskrives med figur 3.

Figur 3 Prosessen for forskningsarbeidet

3.3. Datainnsamling

Når vi har jobbet med datainnsamling har vi hatt fokus på to spørsmål:

1. Hvilken relevans har data for problemstillingen?
2. Hvor pålitelig er måten data er samlet inn på?

Det er et helt grunnleggende krav at data man samler inn må være relevante for problemstillingen. For oppgaven vår har vi forsøkt å finne kilder som er nært knyttet til fagområdet og som har kunnskap og erfaring som kan belyse problemstillingen.

For å kunne svare på problemstillingen har kvalitative data vært et viktig utgangspunkt for analyse og bearbeiding. Med en kompleks problemstilling som berører mange tema har det vært hensiktsmessig å heller bruke et mindretall relevante kilder og benytte det arbeidet som allerede har blitt gjort på området som datagrunnlag. Mange av kildene inkluderer naturligvis kvantitative data, som undersøkelser og statistikk, som er valgt ut for å kartlegge omfang av fenomener.

3.4. Intervju og utvalg av deltakere

Vi har tatt kontakt med personer med bakgrunn innenfor informasjonssikkerhet, fra privat næringsliv, offentlig sektor, forskningsmiljøer og bransjeforeninger. Personene er valgt basert på følgende kriterium: kompetanse på informasjonssikkerhet som fagområde, type stilling og arbeidserfaring i relevante virksomheter. Med relevante virksomheter menes aktører fra privat og offentlig sektor som arbeider med informasjonssikkerhet til daglig og som vi mener kan være med på å svare på problemstillingen. Utvelgingen har blitt gjort skjønnsmessig basert på overnevnte kriterium og er dermed ikke et representativt utvalg. Likevel er det respondenter fra næringslivet, offentlig sektor og med bakgrunn i forskningsmiljø, slik at det er en viss bredde i representasjonen i utvalget.

Vi har gjennomført fire intervjuer, på respondentenes foretrukne kommunikasjonskanal, det vil si via telefonsamtale, videomøte og over e-post. Respondentene fikk tilsendt intervjuguide, informasjonsskriv og samtykkeerklæring på forhånd. Intervjuguiden er enkel og oversiktlig, og ble tilsendt for å gi respondentene en pekepinn på omfanget og retningen på intervjuet. For å kunne utforske nye temaer med respondentene ble guiden kun brukt som en veiledning under samtalene og ble ikke fulgt absolutt. Intervjuene kan beskrives som dybdeintervju med åpne spørsmål, og samtalene varte i underkant av en time. Etter avtale med respondentene ble det tatt opptak av samtalene.

3.5. Litteraturstudie og utvalg av litteratur

For å kunne svare på problemstillingen på en god måte er det viktig at litteraturstudiet bygger på rapporter med kvalitet som kan brukes til videre analyse og diskusjon. Kilder som arbeider med informasjonssikkerhet knyttet til virksomheter, enten som næring eller fagområde har blitt vurdert.

For å kartlegge utviklingen har vi valgt kilder som gjennomfører jevnlige undersøkelser og rapporter. Blant disse kildene er mer ressurssterke organisasjoner som er konsistente med

publiseringer, noe som gjør det mulig å følge disse rapportene over tid. Kilder fra flere sektorer har blitt vurdert og inkludert for å sikre et dekkende datagrunnlag som tar hensyn til bredden av virksomheter som finnes. Blant kildene vi har vurdert er offentlige myndigheter og organisasjoner, private bedrifter, medlemsorganisasjoner og foreninger.

I oppstartfasen søkte vi bredt i litteraturen for å avdekke hvilke trusler som norske virksomheter forholder seg til. Kildene med årlige eller jevnlige publiseringer er gjennomgått i kronologisk rekkefølge for å danne et så oversiktlig bilde av utviklingen som mulig. Informasjon som var av interesse for problemstillingen ble dokumentert for internt bruk og senere kategorisert. Samme fremgangsmåte er også tatt i bruk for andre kilder med relevant informasjon til problemstillingen.

4. Resultat – litteraturstudie

I dette kapitelet presenterer vi resultatene av litteraturstudiet. Enkelte trusler og hendelser på global basis er inkludert i tilfeller hvor vi har vurdert disse som relevante.

Resultatene fra litteraturstudiet og intervjuene er behandlet med det i tankene for å belyse trender/endringer i utviklingen av trusselbildet og angrepsmetodene norske virksomheter har opplevd de siste fem årene. Truslene og angrepsmetodene vi har vurdert som fremtredende og aktuelle for norske virksomheter kartlegges og eksemplifiseres. Hvor det er funnet endringer eller trender kommenteres denne utviklingen til slutt innenfor hver trussel og metode.

4.1. Trusselbildet

Direktørsvindel

NSM peker ut direktørsvindel som en ny trend og trussel for norske virksomheter som kriminelle benytter i 2016. [13] En av sakene som satte denne typen svindel på agendaen skjedde i januar 2016, da et norsk datterselskap i et internasjonalt konsern ble lurt til å overføre 500 millioner til flere kontoer i utlandet. Svindleren utga seg for å være en topplеder i konsernet og da pengene først var overført ble de flyttet på kryss og tvers over landegrenser. Svindelen ble oppdaget innen kort tid og politiet greide å stanse flesteparten av overføringene. Likevel ser det ut til at rundt 100 millioner ikke kom tilbake til rette eier. [14]

[13] Næringslivets Sikkerhetsråd, *Mørketallsundersøkelsen 2016*. 2016.
[14] Rolf J. Widerøe, K.L., *Bedragere lurte ansatt til å utbetale en halv milliard kroner*, in *VG*. 2016.

Gjerningsmannen undersøker gjerne virksomheten på forhånd og kartlegger økonomiansvarlige og ansatte med ansvar for transaksjoner. Med så mye informasjon som mulig kan gjerningsmannen utgi seg for å være en toppsjef i virksomheten og benytte blant annet spearphishing, falske fakturaer og falsk eller kompromittert epost-adresse til å lure ansatte til å overføre verdier. En forfalsket avsender kan for eksempel være en epost som registreres på et domene som ligner på, og dermed forveksles med virksomhetens eget domene. I perioden juni til august 2016 ble NSM varslet av 45 virksomheter som har blitt utsatt for denne type svindel. [13] I en undersøkelse fra Næringslivets Sikkerhetsråd svarer 13 prosent av virksomhetene at de har blitt utsatt for direktørsvindel og 9 prosent har opplevd tap tilknyttet dette i 2017. [15]

Over tid har direktørsvindel blitt enda mer sofistikert og målrettet. Trusselaktørene bruker mer tid til å kartlegge roller og relasjoner i virksomhetene i tillegg til å skrive på godt norsk. Nordea observerer flere virksomheter som blir rammet og taper penger på grunn av direktørsvindel, men som ikke rapporterer om dette. [5]

Ifølge en rapport fra Trend Micro er direktørsvindel i stadig økning på verdensbasis, med en 28 prosent økning i antall hendelser fra 2017 til 2018. Rapporten viser også at Norge er et av de mest populære målene for denne trusselen i verden. Norge står for 1.9 prosent av alle registrere forsøk på direktørsvindel, som plasserer Norge på en femteplass i verden. [16]

Spionasje

Spionasje er en vedvarende og stor utfordring for norske virksomheter og utgjør en av de største digitale truslene mot det norske samfunnet. Trusselen berører både små og store virksomheter og har vært i sterk økning siden 2014. De fleste dataangrepene NSM håndterte i 2014 handlet om forsøk på å stjele informasjon fra datasystemene til store eller viktige norske bedrifter eller virksomheter. [2, 3]

I 2018 ble Visma ble utsatt for et avansert dataangrep. Hensikten med angrepet var antagelig å nå Vismas kunder for å stjele forretningshemmeligheter eller annen intern informasjon. Visma mener at angriperne var inne i nettverket for kort tid til å ha rukket å hacke seg inn hos

[2] NorSIS, *Trusler og Trender 2015*. 2015.
[3] Nasjonal Sikkerhetsmyndighet, *Risiko 2015*. 2015.
[5] Næringslivets Sikkerhetsråd, *Mørketallsundersøkelsen 2018*. 2018.
[13] Næringslivets Sikkerhetsråd, *Mørketallsundersøkelsen 2016*. 2016.
[15] Næringslivets Sikkerhetsråd, *Kriminalitets- og sikkerhetsundersøkelen i Norge 2017*. 2017.
[16] Trend Micro, *Caught in the Net: Unraveling the Tangle of Old and New Threats*. 2019.

noen av deres kunder. Sikkerhetssjef i Visma, Espen Johansen, understreker at kundedata fra selskapet ikke har kommet på avveie. Sikkerhetskonsulentselskapet Recorded Future gransket hendelsen. De mener angrepet var en del av en større kampanje kalt Operation Cloud Hopper, utført av en aktør med tilknytning til kinesiske myndigheter. HP, IBM og andre leverandører skal også ha blitt rammet gjennom denne kampanjen. [17, 18]

Spionasje preges i stor grad av statlig-sponsede eller statlige organiserte aktører, og konkurrenter. [19] Målet med spionasje er avhengig av motivasjon og bruk. Dette innebærer alt fra økonomisk vinning til sabotasje. Angrepet kan komme fra et ønske om å tilegne seg informasjon og forståelse om en ny teknologi, eller å komme i forkjøpet på konkurrenter. [20] Slike angrep kjennetegnes ved at de har et tydelig mål om å hente ut spesifikk informasjon eller produkter fra en virksomhet samtidig som de kan holde på over lengre perioder. [21]

Spionasje går også mot et stadig bredere spekter av norske virksomheter. Enkelte virksomheter er hovedleverandører innen en nisje, for eksempel teknologi, industri eller produksjon, mens andre virksomheter kanskje utgjør et sårbart element i en verdikjede. Disse faktorene kan gjøre virksomheter til et verdifullt og attraktivt mål. [20] [22] Telenor antar at det sannsynligvis er mange norske bedrifter som blir utsatt for industrispionasje uten at de er klar over det. [5]

Krypteringsvirus

Kypterinsvirus låser eller krypterer hele eller deler av innholdet på en datamaskin, hvor målet er å få offeret til å betale løsepenger for at angriperen skal gi tilgang til datamaskinen igjen. Slike virus kan brukes både som middel for å kreve løsepenger og som middel for å drive sabotasje mot virksomheten. Enkelte virksomheter oppfatter det som mer kostnadseffektivt å betale løsepengene enn å oppsøke hjelp. De føler at prisen de må betale for å få tilgang til systemene sine igjen er rimeligere enn å risikere å miste verdifull informasjon. [20] Nøyaktig hvor mange som betaler løsepengene, og hvor mange cyberkriminelle som tjener penger på det finnes det ingen god statistikk på. [23]

[5] Næringslivets Sikkerhetsråd, *Mørketallsundersøkelsen 2018*. 2018.
[17] Recorded Future, *APT10 Targeted Norwegian MSP and US Companies in Sustained Campaign*. 2019.
[18] Marte Halsør, Ø.B.S., Svein Vestrum Olsson, Åsa Vartdal, Olav Døvik,, *Granskarar: Kina hacka norsk selskap*, in *NRK*. 2019.
[19] NorSIS, *Trusler og Trender 2017-18.* 2018.
[20] NorSIS, *Trusler og Trender 2018-19.* 2019.
[21] Nasjonal Sikkerhetsmyndighet, *IKT-risikobilde 2018 - Et sikkert digital Norge.* 2018.
[22] Nasjonal Sikkerhetsmyndighet, *Risiko 2018.* 2018.
[23] Mnemonic, *Security Report 2019*. 2019.

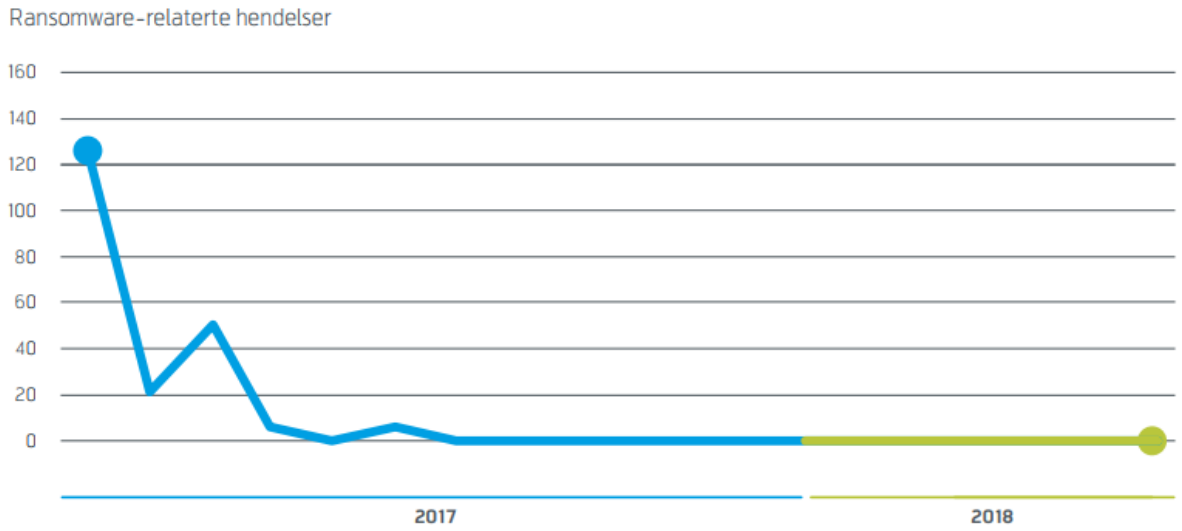
I 2015 var det en kraftig oppgang i utsending av krypteringsvirus på nett og det kommer stadig nye krypteringsvirus på markedet. NSM får daglige rapporter fra samarbeidspartnere om kompromitterte norske nettsider som omdirigerer til sider som er infisert av skadevare. Dette er en vanlig måte å distribuere slike krypteringsvirus. [13] Trusselaktørene blir også flinkere til å bygge på erfaringer fra tidligere krypteringskampanjer, og oppdaterer kontinuerlig sine verktøy og teknikker for å trenge inn i datasystemer. [5] I tillegg er teknologien både enkel å bruke og til salgs, såkalla «ransomeware-as-a-service». [19]

Wannacry

2017 var sterkt preget av denne trusselen. Krypteringsviruset «WannaCry» som først dukket opp i april 2017 spredde seg gjennom svakheter i Microsoft Windows Server Message Block (SMB). Microsoft hadde allerede patchet svakhetene da spredningene startet, men etterslep av oppdatering av programvare førte til at ble spredt til over 90 land og infiserte over 230.000 datamaskiner. Norske virksomheter har relativt god grunnsikring, og de aller fleste patcher i det minste operativsystemet. I tillegg er piratkopiering av Windows lite utbredt. Dette gjorde at Norge stort sett slapp unna de store spredningene av krypteringsvirus, som krypterte og slettet harddisker i 2017 (WannaCry og NotPetya). Dette var kjente svakheter, som Microsoft allerede hadde patchet og dermed var fullt patchede og oppdaterte maskiner immune. Telenor har uttalt at ingen av deres norske kunder ble rammet av disse angrepene. I tillegg sier Telenor at det generelt er mindre infiserte PCer og servere i dag enn tidligere [5]

I 2018 er det en stor nedgang i krypteringsvirus-relaterte hendelser på verdensbasis. I tillegg blir det gjort observasjoner om tilsvarende nedgang i antall nye krypteringsvirus-familier. Til tross for at WannaCry ble oppdaget og patchet tidlig i 2017, var den fremdeles ansvarlig for mer enn halvparten av alle krypteringsvirus oppdagelser i 2018.[16]

[5] Næringslivets Sikkerhetsråd, *Mørketallsundersøkelsen 2018*. 2018.
[13] Næringslivets Sikkerhetsråd, *Mørketallsundersøkelsen 2016*. 2016.
[16] Trend Micro, *Caught in the Net: Unraveling the Tangle of Old and New Threats.* 2019.
[19] NorSIS, *Trusler og Trender 2017-18.* 2018.



Figur 4: Antall Ransomware relaterte hendelser. Hentet fra Telenors årlige sikkerhetsrapport: Digital Sikkerhet 2018 – Sikrere sammen

3.1.3.2 Norsk Hydro utsatt for krypteringsvirus

Hydro ble utsatt for et dataangrep natt til 19. mars. Ifølge kommunikasjonsdirektør, Halvor Molland, opplevde Hydro unormal datatrafikk mot kvelden og de fikk problemer med noen av styringssystemene. Det viste seg utover natten at de var blitt utsatt for et dagangrep med krypteringsvirus. For å forhindre at dette spredde seg videre koblet de ut hele datasystemet og skiftet til manuell drift så langt det var mulig. IT-systemer i de fleste forretningsområdene ble påvirket av dette angrepet og på noen områder ble produksjonen stengt ned for å begrense skader. I perioden etterpå foregikk kommunikasjonen i selskapet kun på telefon, tekstmeldinger og møter, da ansatte fikk beskjed om å ikke skru på datamaskiner eller koble seg på det interne nettverket. Foreløpig er det uklart hvem som står bak hendelsen, og konkret hvordan angrepet ble gjennomført. Dataangrepet fikk omfattende konsekvenser for driften i flere av selskapets forretningsområder og Hydro estimerte et tap på opptil 350 millioner. [24]

3.1.3.3 Hacktivisme

Hacktivistangrep mot norske interesser er i økende grad. I løpet av sommeren av 2014 var en enkelt tenåring i stand til å utføre et omfattende tjenestenektangrep mot flere store virksomheter i Norge. I 2015 og 2016 ble Norge angrepet av hacktivistgruppen Anonymous i

[4] Nasjonal Sikkerhetsmyndighet, *Helhetlig IKT risikobilde 2016*. 2016.
[13] Næringslivets Sikkerhetsråd, *Mørketallsundersøkelsen 2016*. 2016.
[24] Oda Ording, M.K.V., Birger Kolsrud Jåsund, Anders Brekke, Per Kristian Grimeland, Kjartan Rørslett,, *Hydro utsatt for dataangrep: - Ikke opplevd lignende*, *NRK*. 2019.

forbindelse med en kampanje mot hvalfangst. Flere norske nettsider ble delvis tatt ned og ble tvunget til å blokkere utenlands trafikk for å holde nettsidene oppe. [4, 13]

Hacktivistangrep blir vanligere og tilgjengeligheten av teknologi gjør det stadig enklere. Angriperen er ofte motivert av kortsiktig synlighet eller anerkjennelse. Tjenestenektangrep er en veldig populær angrepsmetode blant disse aktørene fordi konsekvensene av det er synlige og får lett medieomtale. 40 prosent av alle tjenestenektangrepene NSM NorCERT observerte i tidsrommet 2015-2016 kunne tilknyttes hacktivisme. [13] Andre vanlige angrepsmetoder innebærer endring av innholdet på nettsiden til offeret, såkalt «defacing», i forsøk på å skade virksomhetens omdømme, eller lekkasje av sensitiv informasjon. [25]

4.2. Angrepsmetodene som brukes

I dette kapitlet beskrives de vanligste metodene trusselaktørene har benyttet for å kompromittere system, forstyrre virksomhetens tjenester og stjele informasjon, verdier eller ressurser fra virksomheter de siste fem årene.

Angrepsmetodene blir mer målrettede

Det har i flere år vært en økning av målrettete angrep mot norske interesser. [26] Ettersom omverdenen blir mer oppmerksom på trusler som krypteringsvirus og annen skadevare vil trusselaktører lete etter nye og effektive måter å tjene penger på. Trusselbildet har endret seg fra den brede generiske spredningen av skadevare, til en økning av flere store målrettede angrep. Denne tendensen er mest synlig blant angrep mot større organisasjoner. [5] Mesteparten av sikkerhetshendelser forekommer i løpet av en vanlig arbeidsdag mellom klokka 08-16. [23] Målrettede trusselaktører kjennetegnes av at de er mer utholdende, og kan utførte gjentatte angrep med nyere teknikker basert på kunnskap fra tidligere angrep. [5]

Spearphishing

> «I 100% av målrettede angrep i 2014 og hittil i 2015, har epost vært brukt som hovedangrepsvektor. Alle angrep har startet med at noen utvalgte ansatte har mottatt en epost som inneholder skadevare» [25]

[4] Nasjonal Sikkerhetsmyndighet, *Helhetlig IKT risikobilde 2016.* 2016.
[5] Næringslivets Sikkerhetsråd, *Mørketallsundersøkelsen 2018*. 2018.
[13] Næringslivets Sikkerhetsråd, *Mørketallsundersøkelsen 2016*. 2016.
[24] Oda Ording, M.K.V., Birger Kolsrud Jåsund, Anders Brekke, Per Kristian Grimeland, Kjartan Rørslett,, *Hydro utsatt for dataangrep: - Ikke opplevd lignende*, in *NRK*. 2019.
[25] Nasjonal SIkkerhetsmyndighet, *Helhetlig IKT-Risikobilde 2015.* 2015.
[26] Næringslivets Sikkerhetsråd, *Mørketallsundersøkelsen 2014*. 2014.

I 2014 var spearphishing den mest populære angrepsmetoden, og til tross for at det har vært en økende bevissthet rundt denne trusselen gjennom årene, omtales spearphishing fremdeles som den vanligste målrettede angrepsmetoden i 2018. [5, 26]

4.2.2.2 Spearphishing er effektivt fordi mennesket lar seg lure

NSM observerer en økning av målrettede e-poster med skadevare til personers private adresser. Egne ansatte beskrives som det svakeste ledd i nettverkssikkerhet, og økningen av spearphishing er én av årsakene til at digital kriminalitet utgjør den største trusselen mot finansnæringen. [27] I Risiko 2016 beskrives en inntrengingstest som NSM utførte hvor de sendte e-post med skadevare til ansatte i en offentlig virksomhet. Halvparten av de som mottok e-posten åpnet vedlegget slik at datamaskinen ble infisert. [28] NSM gjennomførte noen år senere en lignende inntrengingstest mot en virksomhet i norsk statsforvaltning. Av de som mottok e-posten var det 90 prosent av de som trykket på vedlagte lenken, 50 prosent aktiverte den simulerte skadevaren og 30 prosent oppga sine påloggingsdetaljer til virksomhetens systemer. Gjennom inntrengingstestene observerer NSM flere eksempler på «enkle» feil sluttbrukere gjør som kunne vært unngått dersom virksomheten hadde valgt sikre løsninger. Disse feilene er eksempelvis at sluttbrukerne får tildelt for mange rettigheter, det er fritt fram for å bruke private enheter, og brukere blir påtvunget til å bytte passord altfor ofte, som fører til at brukerne velger å lage svake passord. [21] Svake passord er en av det vanligste årsakene for datainnbrudd [21, 29]

4.2.2.3 Skanning og utnyttelse av sårbareheter

> «Et fellestrekk i vellykkede dataangrep i Norge er at trusselaktørene benytter kjente sårbarheter for å få tilgang til ønsket informasjon. Generelt kan vi si at trusselaktørene synes å gå minste motstands vei ved at de utnytter sårbarheter som er kjent av mange. Dette er sårbarheter som i mange tilfeller kunne vært lukket dersom programvaren hadde vært oppdatert.» [4]

Å skanne et nettverk etter sårbarheter kan sammenlignes med å kjenne på dørhåndtaket for å sjekke om døren er låst. Slik skanning foregår i bakgrunnen til enhver tid og kan avdekkes

[4] Nasjonal Sikkerhetsmyndighet, *Helhetlig IKT risikobilde 2016*. 2016.
[5] Næringslivets Sikkerhetsråd, *Mørketallsundersøkelsen 2018*. 2018.
[21] Nasjonal Sikkerhetsmyndighet, *IKT-risikobilde 2018 - Et sikkert digital Norge*. 2018.
[23] Mnemonic, *Security Report 2019*. 2019.
[25] Nasjonal SIkkerhetsmyndighet, *Helhetlig IKT-Risikobilde 2015*. 2015.
[26] Næringslivets Sikkerhetsråd, *Mørketallsundersøkelsen 2014*. 2014.
[27] Nasjonal Sikkerhetsmyndighet, *Helhetlig IKT-risikobilde 2017*. 2017.
[28] Nasjonal Sikkerhetsmyndighet, *Risiko 2016*. 2016.
[29] Europen Union Agency for Network and Informastion Security, *ENISA Threat Landscape 2014*. 2015.

med tilstrekkelig nettverksovervåkning. Dersom virksomheten har mangelfulle rutiner for å oppdatere programvare kan sårbare eller utdaterte versjoner gi angriperen en enkel vei inn.

Utviklingen av ny teknologi oppstår nye sårbarheter og angrepsflaten øker. IKT-angrep som benytter eldre sårbarheter lykkes fortsatt i stor grad, og skanning og utnyttelse av sårbare systemer er en av de mest populære angrepsmetodene. [5]

Manglende segmentering av nettverket vil gjøre at angriperen kan bevege seg mellom ulike deler av IKT-systemet i virksomheten. Det er heller ikke bare sårbare versjoner av programvare som utnyttes, men også sårbare implementasjoner av IKT-system, svakheter i design av en tjeneste eller feilkonfigurering av systemet. Denne typen skanning krever minimalt med ressurser fra trusselaktørens side og heller ikke menneskelig interaksjon for å lykkes. Sårbare nettverk og applikasjoner, virus, feil brukerautentisering, og databasefeil er noen av de viktigste årsakene for datainnbrudd. [5, 29]

Datainnbrudd på Helse Sør-Øst

Helse Sør-Øst opplevde en slik tilnærming i 2018, da de 8.januar oppdaget et datainnbrudd som kunne berørt helseopplysningene til mer enn halvparten av Norges befolkning. Administrerende direktør i Helse Sør-Øst, Cathrine Lofthus forklarte i ettertid at aktøren som stod bak hadde foretatt skanning etter angrepsvektorer i flere dager før selve inntrengningen. Deretter skal det ha blitt utført kartlegging med et lavt aktivitetsnivå for å unngå å bli oppdaget. I innbruddet ble servere kompromittert og etter hvert tatt ned av driftspersonellet. Etter angrepet var pasientsystemet til Helse Sør-Øst nede i flere uker. Nesten et år senere ble saken henlagt av PST, som ikke kunne fastslå om opplysninger ble stjålet eller ikke. [30, 31]

Gjennom årene har NSM tatt del i mange saker hvor utdaterte webserverinstallasjoner har blitt kompromittert, vanligvis hos mindre bedrifter med begrensede IT-ressurser. De kompromitterte serverne blir deretter brukt som mellomledd i angrep mot andre mål, både innenlands og utenlands. [5]

---

[5] Næringslivets Sikkerhetsråd, *Mørketallsundersøkelsen 2018*. 2018.
[29] Europen Union Agency for Network and Informastion Security, *ENISA Threat Landscape 2014*. 2015.
[30] Marthe S. Lien, *PST henlegger etterforskningen av dataangrepet mot Helse Sør-Øst*, in *VG*. 2018.
[31] Brombach, H., *Helse Sør-Øst: Datainnbruddet skjedde ikke hos Sykehuspartner*, in *Digi*. 2018.

Tjenestenektangrep (DDoS)

Hensikten med tjenestenektangrep er å gjøre en tjeneste utilgjengelig. Dersom det blir utført mot kritiske systemer kan denne trusselen true både liv og vår nasjonale beredskap. [22] Tilgjengelighet blir stadig viktigere i vår digitale hverdag, og nedetid kan være svært alvorlig for de som rammes. Det medfører direkte økonomiske konsekvenser dersom en virksomhet ikke klarer å selge, få ut informasjon til kunder eller ikke klarer å levere en forventet tjeneste.

Hensikten med tjenestenektangrep er å gjøre en tjeneste utilgjengelig. Dersom det blir utført mot kritiske systemer kan denne trusselen true både liv og vår nasjonale beredskap. [22] Tilgjengelighet blir stadig viktigere i vår digitale hverdag, og nedetid kan være svært alvorlig for de som rammes av det. Det medfører direkte økonomiske konsekvenser dersom en virksomhet ikke klarer å selge, få ut informasjon til kunder eller ikke klarer å levere en forventet tjeneste. Antall vellykkede tjenestenektangrep er imidlertid i nedgang. Norsk infrastruktur har blitt sterkere i de siste årene, som kan være grunnen til at det oppleves mindre vellykkede tjenestenektangrep. [26]

Større virksomheter blir mer utsatt for tjenestenektangrep

Fire prosent av virksomhetene som deltok i mørketallsundersøkelsen 2016 opplevde tjenestenektangrep. Det påpekes i rapporten at det ikke var noen vesentlig forskjell mellom hvilke bransjer som ble utsatt for DDoS, men at større virksomheter ble i mye større grad offer for denne angrepsmetoden. Av virksomheter med 100 ansatte eller flere var det 12 prosent av disse som opplevde tjenestenektangrep, mens virksomheter med 5-19 ansatte var det kun tre prosent. [13]

Mørketallsundersøkelsen 2018 viser imidlertid at det har vært en økning av DDoS angrep i løpet av kalenderåret 2017. Dette året ble totalt syv prosent av virksomhetene utsatt for DDoS angrep. Det påpekes at utvalget for denne undersøkelsen består av flere større bedrifter sammenlignet med 2016 undersøkelsen, som kan være årsaken til at det ser ut som det er en økning. [5]

[5] Næringslivets Sikkerhetsråd, *Mørketallsundersøkelsen 2018*. 2018.
[13] Næringslivets Sikkerhetsråd, *Mørketallsundersøkelsen 2016*. 2016.
[22] Nasjonal Sikkerhetsmyndighet, *Risiko 2018.* 2018..
[26] Næringslivets Sikkerhetsråd, *Mørketallsundersøkelsen 2014*. 2014

4.2.4.2 Angrep i Telenors nettverk

Fra 2016 til 2017 registrerte Telenor over 8000 DDoS-angrep i deres nettverk og mot deres bedriftskunder, noe som tilsvarer over 650 angrep i måneden. «Omtrent en tredjedel av angrepene var så store at sikkerhetssenteret måtte gjøre tiltak for at angrepene ikke skulle påvirke Telenor Norges tjenester eller våre kunders tjenester.» [32]

Så langt i 2019 (januar-april) har Telenors sikkerhetssenter registrert mellom 250 og 500 DDoS-angrep i måneden, hvor mellom 100 og 200 av disse har blitt mitigert gjennom tiltak fra sikkerhetssenteret.[33]

4.2.4.3 Tjenestenekt som utpressingsmiddel

Det kommer fremdeles bølger med trusler om tjenestenektangrep mot bedrifter i 2017 og 2018. Noen bedrifter forsøkes utpresses til å betale en sum for å forhindre påståtte kommende DDoS-angrep, og ofte kommer det test-angrep samtidig for at trusselen skal bli tatt på alvor. Selv om summen ikke betales er det ikke fullt så ofte at det faktisk kommer angrep som følger opp trusselen. Telenor rapporterer at det totale antallet DDoS-angrep i deres nettverk er noe fallende i 2018, og at de aller fleste av ofrene var privatbrukere. [5]

Nettleverandørene, som Telenor, blokkerer utgående trafikk som benytter falske IP-adresser, noe som gjør det vanskeligere å iverksette DDoS-angrep fra deres nett. I tillegg holder de oversikt over adresser i nettet de mener kan misbrukes til tjenestenektangrep. Innkommende DDoS-angrep kan også til en viss grad filtreres, da trafikken mellom nettleverandørene går gjennom store rutere, som fungerer som knutepunkter. Filtrene begrenser de vanligste angrepstypene og oppdateres etter hvert som det oppdages nye angrepstyper og taktikker. [34]

4.2.4.4 Utnyttelse av underleverandører

Det har blitt vanligere for offentlige og private virksomheter å tjenesteutsette hele eller deler av sine IKT-tjenester. I mange tilfeller er tjenestutsetting av økonomiske grunner, og dette kan føre til at det tas snarveier ved implementeringen, og risikoer forbundet med tjenestutsetting blir dermed ikke tilstrekkelig vurdert. [21]

---

[5] Næringslivets Sikkerhetsråd, *Mørketallsundersøkelsen 2018*. 2018.
[21] Nasjonal Sikkerhetsmyndighet, *IKT-risikobilde 2018 - Et sikkert digital Norge*. 2018.
[32] Telenor, *Digital SIkkerhet 2017*. 2018.
[33] Jan Roger Wilkens, *Oppsummering av nyhetsbildet innen datasikkerhet for janauar-april 2019*. 2019.
[34] Telenor, *Digital Sikkerhet 2018 - Sterkere sammen*. 2018.

Nettverksoperasjoner går i økende grad går mot underleverandører og kontraktører, istedenfor direkte mot primærmålet. Det er ofte snakk om virksomheter med svakere sikkerhetsmekanismer, som bevisst utnyttes som en inngangsdør for å nå primærmålet. [27] NSM har registrert operasjoner hvor hensikten var å oppnå tilgang til IT-tjenesteleverandørers kunder og data. I tillegg har NSM opplevd at trusselaktører kompromitterer tilfeldige systemer, for å benytte disse til nettverksoperasjoner mot tredjeparter. I mørketallsundersøkelsen 2018 kommer det frem at 2% sikkerhetshendelsene var forårsaket av underleverandører. [5]

Botnets

Microsoft omtaler Botnets som en av de største truslene på internett i 2014. ID-tyveri som er forårsaket av Botnets blir i stor grad brukt til industrispionasje og økonomisk svindel. Nesten halvparten av de som blir smittet av ondsinnet kode skyldes av at de gjør en aktiv handling som å klikke på koblinger eller vedlegg i en e-post, eller besøker en infisert web-side [26]

På høsten i 2016 ble skadepotensialet til botnets på mange måter realisert. 21. Oktober ble Dyn, et selskap som har ansvar for mye av DNS-infrastrukturen på internett, offer for et storstilt DDoS-angrep. I motsetning til vanlige botnets bestod det såkalte Mirai-botnettet av mange IoT-enheter, som webkamera og videoopptakere. Nettverket, som man antar bestod av rundt 100 000 enheter, sendte trafikk opptil 1,2 Tbps mot Dyns servere. Angrepet varte mesteparten av dagen og tok ned nettsider som Twitter, Netflix, Reddit, Spotify, Paypal og en rekke andre i USA og Europa.[35] Blant enhetene som ble brukt i angrepet var hackede webkameraer fra det kinesiske firmaet Xiongmai. Angrepet varte mesteparten av dagen og tok ned nettsider som Twitter, Netflix, Reddit, Spotify, Paypal og en rekke andre i USA og Europa.[35] Blant enhetene som ble brukt i angrepet var hackede webkameraer fra det kinesiske firmaet Xiongmai. Kameraene ble levert med standard brukernavn og passord og lot seg ikke oppgradere. Firmaet endte opp med å tilbakekalle disse kameraene i USA. [32]

Det forventes at flere IoT-enheter vil i større grad bli utnyttet ved cyberangrep. IT-selskapet Gartner har estimert at innen 2020 vil 25 prosent av angrep mot virksomheter involvere IoT enheter. I tillegg til antall enheter vil det store antallet ulike versjoner og leverandører

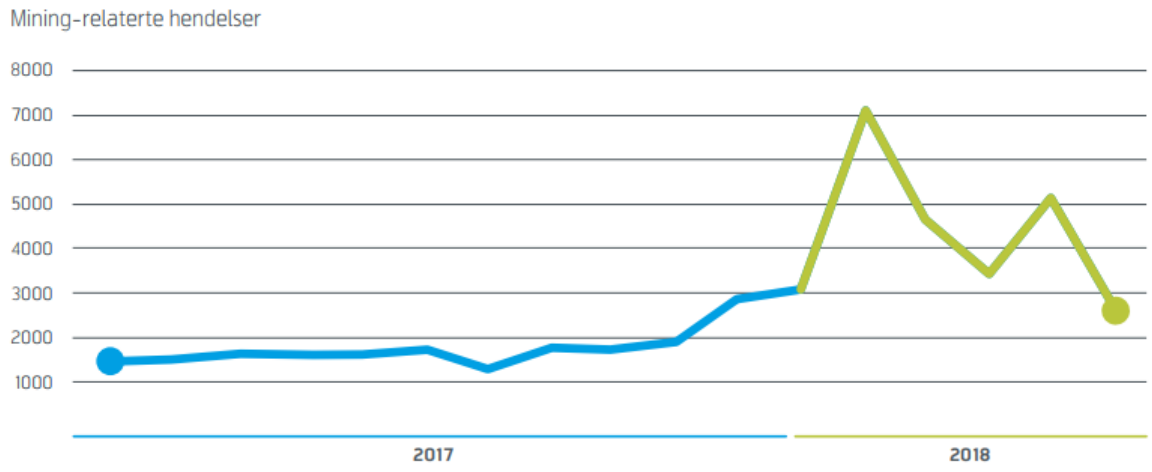
[5] Næringslivets Sikkerhetsråd, *Mørketallsundersøkelsen 2018*. 2018.
[26] Næringslivets Sikkerhetsråd, *Mørketallsundersøkelsen 2014*. 2014.
[27] Nasjonal Sikkerhetsmyndighet, *Helhetlig IKT-risikobilde 2017*. 2017.
[32] Telenor, *Digital SIkkerhet 2017*. 2018.
[35] Nicky Woolf, *DDoS attack that disrupted internet was largest of its kind in history, experts say*, in *The Guardian*. 2016.

komplisere skalerbarheten og hvordan de inkluderes i virksomhetens nettverk. I tillegg til antall enheter vil det store antallet ulike versjoner og leverandører komplisere skalerbarheten og hvordan de inkluderes i virksomhetens nettverk [36].

I februar 2018 ble det oppdaget et botnet som bestod av omtrent en halv million maskiner, flesteparten Windows-servere. Botnettet fikk infiserte maskiner til å utvinne kryptovalutaen Monero fra mai 2017 til februar 2018. Ifølge estimater tjente bakmennene rundt 8900 Monero (1,4 millioner i 2018 USD) i løpet av perioden. [34]

Crypto-jacking

En ny type skadevare som har vært i sterk vekst er illegitim graving etter kryptovaluta, såkalt «crypto-jacking». Hensikten er å bruke maskinkraften til å utvinne og overføre verdiene tilbake til angriper, uten at dette stjeler for mye av maskinens ressurser slik at det blir vanskelig å oppdage. Denne typen skadevare vil ikke ha like store konsekvenser på en virksomhet som eksempelvis et krypteringsvirus, men representerer likevel en trussel. Over tid vil strømforbruk og misbrukt kapasitet utgjøre en kostnad for virksomheten. [5]



Figur 5: Mining-relaterte hendelser i perioden 2017-2018. Hentet fra Telenors årlige sikkerhetsrapport: Digital Sikkerhet 2018 – Sikrere sammen

Tidlig i 2018 fikk denne typen skadevare mye oppmerksomhet. Angripere skannet etter sårbare systemer, og spesielt webservere har blitt infisert av disse. Telenor rapporterer at flere av deres norske kunder også ble rammet av dette. Fordelen for angriperen med denne typen skadevare er at den ofte er vanskelig for offeret å oppdage, ressurser kan dermed misbrukes

[5] Næringslivets Sikkerhetsråd, *Mørketallsundersøkelsen 2018*. 2018.
[34] Telenor, *Digital Sikkerhet 2018 - Sterkere sammen*. 2018.
[36] Nasjonal Sikkerhetsmyndighet, *Risiko 2017*. 2017.

over lang tid, oppfattet skadeomfang er lavt og det er lav risiko for angriper. I tillegg tjenes og overføres verdiene automatisk da det ikke er behov for menneskelig kommunikasjon eller interaksjon for å lykkes. [5]

Exploit kits

Et exploit kit kan infisere maskinen med skadevare kun ved at brukeren besøker en nettside. Trusselaktøren utnytter gjerne svakheter i tredjeparts-plugins i nettleserne, som for eksempel Java, Silverlight og Flash til å infisere maskinen. For å få brukere til å besøke riktig sted kompromitteres gjerne en populær nettside, slik at den omdirigerer trafikken til nettsiden som serverer skadevare. I 2016 observerer NSM at dette har vært en vanlig angrepsvektor for å distribuere krypteringsvirus og andre typer skadevare, og at norske nettsider daglig har blitt kompromittert og blitt brukt til dette formålet.[13]

I Telenors beskrivelse av risikobilde for 2018 blir det nevnt at exploit kits, som tidligere var et stort problem har nesten helt forsvunnet. [5] Noe av årsaken til dette er at nettleserne ble mer aktive med å blokkere tredjeparts-plugins etter hvert som svakheter i slike plugins ble utnyttet. I tillegg har oppdateringer blitt stadig hyppigere og automatisk oppdatering har blitt en norm, både innen nettlesere og annen programvare. Det betyr at det generelt har blitt færre svakheter som kan utnyttes på de fleste bedrifts-PCer. [13]

Vannhullsangrep

Navnet 'vannhullsangrep' kommer fra rovdyr som jakter ved vannhull i ørkenen. I stedet for å oppsøke byttet, så venter rovdyret på at byttet kommer til vannhullet. Trusselaktøren tar kontroll over en dårlig sikret nettside, som de vet at offeret besøker regelmessig og har tillit til. Når offeret besøker nettsiden blir svakheter i nettleseren utnyttet for å infisere eller bryte seg inn på maskinen. [34] For å unngå å bli oppdaget vil trusselaktøren ofte legge til en liste med IP-adresser som de vil infisere. Disse adressene er da «hvitelistet», slik at andre besøkende på nettsiden forblir urørt. Når det kun er en liten andel besøkende som påvirkes kan aktiviteten være vanskelig å oppdage. Metoden tiltrekker seg lite oppmerksomhet og etterlater minimalt med spor. Dersom angrepet oppdages vil sporene kun føre tilbake til den legitime nettsiden som brukeren besøkte. [4, 34]

[4] Nasjonal Sikkerhetsmyndighet, *Helhetlig IKT risikobilde 2016*. 2016.
[5] Næringslivets Sikkerhetsråd, *Mørketallsundersøkelsen 2018*. 2018.
[13] Næringslivets Sikkerhetsråd, *Mørketallsundersøkelsen 2016*. 2016.
[34] Telenor, *Digital Sikkerhet 2018 - Sterkere sammen*. 2018.

I 2015 og 2016 omtales vannhullsangrep som en angrepsmetode som har vokst i flere år.[4, 25] og fortsetter i øke i 2017. [22]

4.3. Dagligdagse og alvorlige hendelser norske virksomheter opplever

I 2015 var virus og skadevare, forsøk på inntrenging og hacking, og phishing og sosiale manipulerings angrep de digitale sikkerhetshendelsene som norske virksomheter opplevde mest. 20 prosent av virksomhetene ble rammet av virus og skadevare, åtte prosent opplevde sosial manipulering og forsøk på datainnbrudd. Av sikkerhetshendelsene var ti prosent av disse forårsaket av egne ansatte. [13] Denne trenden fortsetter i 2018, men med en bemerkelsesverdig økning spesielt for phishing og andre former for sosial manipulerings angrep.[5]

Tapt arbeidstid, tap av data og kostnader er de mest alvorlige konsekvensene

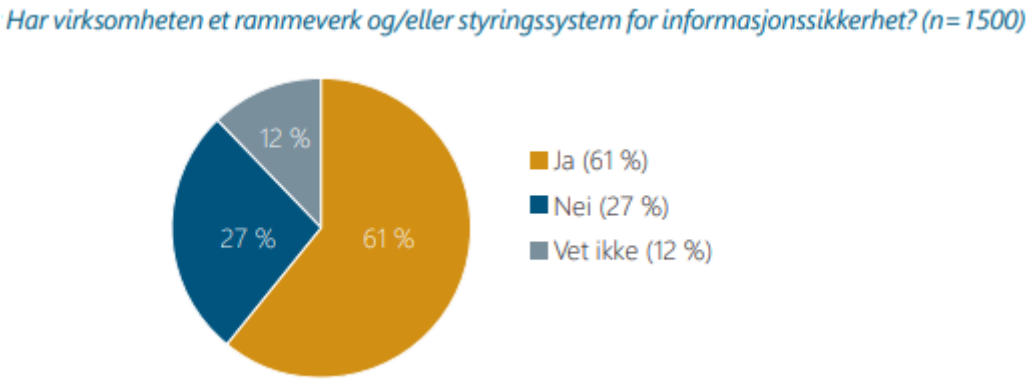
Disse områdene utgjorde også en del av de alvorligste hendelsene, basert på hvilke konsekvenser virksomheten opplevde. For mange var det virus og skadevare som forårsaket de verste hendelsene. Forsøk på innbrudd, systemfeil og virus førte hovedsakelig til tapt arbeidstid. For virksomhetene som ble rammet av krypteringsvirus var tap av data den største konsekvensen. Angrep som bestod av sosial manipulering hadde mer sammensatte konsekvenser for virksomhetene, blant annet oppgis det ekstraarbeid, tapt data og direkte kostnader. Et fåtall av virksomhetene oppga DDoS-angrep og phishing som sin alvorligste hendelse.

Årsaksforhold som bidro til hendelsen

Som medvirkende faktorer til at hendelsen oppstod oppga 74 prosent 'tilfeldigheter eller uflaks'. Dette tyder på at de fleste hendelsene ikke oppfattes som at de er rettet spesifikt mot virksomheten. I 60 prosent av tilfellene gjorde medarbeidere feil som bidro til at hendelsen oppstod, og i 47 prosent av tilfellene var mangel på sikkerhets-bevissthet eller kompetanse en medvirkende faktor. Ellers er utilstrekkelige prosesser, utilstrekkelig teknisk infrastruktur og mangel på teknisk kompetanse medvirkende faktorer til at hendelsen oppstod. Manglende prioritering av og investering i sikkerhetsarbeid er den underliggende årsaken i mange

[4] Nasjonal Sikkerhetsmyndighet, *Helhetlig IKT risikobilde 2016*. 2016.
[5] Næringslivets Sikkerhetsråd, *Mørketallsundersøkelsen 2018*. 2018.
[13] Næringslivets Sikkerhetsråd, *Mørketallsundersøkelsen 2016*. 2016.
[22] Nasjonal Sikkerhetsmyndighet, *Risiko 2018.* 2018.

tilfeller. I mørketallsundersøkelsen 2018 oppgir seks av ti virksomheter at de har rammeverk eller styringssystem for informasjonssikkerhet. Virksomheter med rammeverk eller styringssystem for informasjonssikkerhet mener at det skyldes tilfeldigheter og uflaks i mindre grad enn virksomheter uten slike system. [5]



Figur 6: Virksomheter med rammeverk og/eller styringssystem for informasjonssikkerhet. Hentet fra Mørketallsundersøkelsen 2018

Hendelser blir oppdaget ved tilfeldigheter

I undersøkelsen kommer det fram at 46 prosent oppdaget hendelsen 'ved en tilfeldighet', 34 prosent ble oppdaget etter 'negativ effekt på virksomhetens drift', 32 prosent med intern sikkerhetsmonitorering, 21 prosent med andre interne kontroller og revisjoner og 4 prosent ved varsel fra politi og offentlige myndigheter. Fordi så mange oppdager hendelser tilfeldig eller etter direkte påvirkning på virksomhetens drift tyder det på at de fleste virksomhetene ikke har effektive mekanismer for å oppdage hendelser.[5]

Hva skjer etter hendelsen?

I kjølvannet av den mest alvorlige hendelsen gjorde 44 prosent av virksomhetene endringer i policy eller rutiner, 25 prosent investerte i sikkerhetsutstyr og 20 prosent utviklet sikkerhetsprosesser. I tillegg var det 20 prosent som leide inn en tjenesteleverandør til å håndtere sikkerheten, 13 prosent outsourcet sikkerhetsfunksjoner og 3 prosent av virksomhetene ansatte flere med sikkerhetskompetanse.[5]

[5] Næringslivets Sikkerhetsråd, *Mørketallsundersøkelsen 2018*. 2018.

5. Resultat – intervju

Her presenteres samtaler med fem deltakere gjennom fire intervjuer. Spørsmålsguiden er grunnlaget for disse samtalene. Deltakernes svar er kategorisert etter spørsmål med tilhørende tema og flere av svarene er gjengitt i kortfattet form. Deler av datagrunnlaget vi har vurdert som mindre relevant for problemstillingen har blitt ekskludert.

5.1. Intervjukandidatene

Arild Bjørk, IKT-sikkerhetsleder i Difi, Digitale fellesløsninger, Drift og sikkerhet

Respondent 1, Sikkerhet og drift

Maria Bartnes, forskningssjef i Sintef, Software Engineering, Safety and Security

Respondent 5, respondent ved Nasjonal Sikkerhetsmyndighet

Respondent 4, trusselidentifisering- og vurdering, fra IT-sikkerhetsselskap

Intervju med Arild Bjørk og respondent 1

Hva er de største digitale truslene norske virksomheter møter i dag?

«Den største digitale trusselen er det svakeste lenken i kjedet, og det er da mennesker» Sier Arild Bjørk. Han argumenterer for dette ved å si at man kan enten benytte mangel på kompetanse, eller at noen er lettlurt for å «starte noe».

Videre nevner han teknologi og tilgjengeligheten av det. «DDoS vil alltid være en vinkel, fordi det er noe man kan bestille på nett. Vi har tekniske verktøy for å håndtere disse, men det vil jo alltid være en mulighet. Man kan jo bare *pøse* på så mye man klarer.» Han påpeker at dette også vinkles opp mot mennesker, og balansen mellom sikkerhetstiltak og brukervennlighet. Han refererer til hvordan det var ført i tiden, hvor programvare ikke var tilknyttet nett, og det eneste du trengte å huske på var å vedlikeholde diskettene dine. «Nå er det mer kompliserte forhold, og større forventninger. Det pøser på i markedet med nye løsninger som skal løse både det ene og det andre, og da gjelder det ofte å finne en balanse mellom sikkerhetstiltak og brukervennlighet i bedriftssystem». Han sier videre at det dersom systemene blir for tungvinte vil brukerne av det begynne å lete etter andre veier rundt problemet, og legger ting i andre tjenester som kan skape problemer.

Respondent 1 legger til: «Det handler om å finne en balanse mellom sikkerhet, kompetanse og risikostyring. Det er så mange måter å oppnå ting man vil gjøre digitalt, så dersom brukerne ikke har kompetanse eller mulighet til å gjøre oppgavene på en digital alternativ måte så vil man alltid komme seg rundt sikringstiltak»

Arild trekker også frem at sikkerheten blir mer dynamisk i en tradisjonell forvaltningsorganisasjon hvor det er fastsette rutiner og regler for hvordan ting skal gjøres. «Nye produkt er jo vél og bra, men det er en viss risiko for at man glemmer å vedlikeholde. Produkt man kjøper til seg må fortsatt måles jevnlig, ting må repareres og oppdateres. Det kan fort gå i glemmeboken»

Hvordan vil trusselbildet se ut fremover?

Fremover mener Arild at mennesker vil bli et mer og mer sårbart mål. Han tar opp skillet mellom jobbverden og privatverden, og hvordan disse er på vei inn i skymiljøet «Hvor mange tjenester er det som kommer til å flyttes over i skyen, og hvor godt klarer en bruker selv å ta vare på den privates verden? En person kan selv bli en trusselaktør. Tanken er at trusselaktørene vil alltid gå etter det svakeste punktet»

Videre nevner han kryptering, og hvordan aktører som NSA ønsker bakdører inn i krypteringen. «De (NSA) gir seg ikke, og de skjønner ikke at dette er en dårlig idé». Arild påpeker at dersom andre aktører får tak i denne bakdøren, som kriminelle er flinke til, kan de brukes til å hente verdier, eller i verste fall publisere disse nøklene. «Undergraving av kryptering er noe vi er klar over, men noe som aldri vil få se lys, fordi det ødelegger så mye. Da kan vi ikke ha tillit til noe som helst».

Hvilke sikringstiltak er viktige å vurdere?

«Det blir jo stadig flere system, og flere elektroniske tjenester, og da vil risikoen for sårbare komponenter være i oppgang naturligvis. Ifra en zero day blir publisert, så blir det stadig raskere utnyttet. Man må bli mer *på* for å sikre systemet fremover, og man må bli raskere til å håndtere endringer får å kunne håndtere en sårbarhet» Sier Arild. Han trekker også frem at man må være observant på hvilke system du har, hva de inneholder av teknologi og hva som må gjøres fortløpende ift. Vedlikehold. Arild sier også det er viktig de ansatte er klar over verdiene de sitter på, og hvilken informasjon de har tilgang til.

Hva kan konsekvensene bli dersom virksomhetene ikke tar trusselbildet på alvor?

Arild trekker fram at det er avhengig av hvilken type virksomhet det gjelder. For små virksomheter, eller enkeltmannsforetak så behøver det ikke nødvendigvis å ha noen innvirkning i det hele tatt, men for større kan jo det i verste fall gå under for virksomheten. «De kan gå konkurs. Alt etter hvilken type virksomhet det er, og evnen de har til å håndtere slike hendelser. I den forstand gjenopprette driften, om en i det hele tatt *har* den evnen.» Han sier videre «Om man står på bar bakke uten back-up, og hele ordreboken og alt du skulle fakturere ut har gått tapt, og du har absolutt ingen oversikt over noe du skal arbeide med, og eventuelt bedriftshemmeligheter som du skulle tjene penger på er nå borte og tatt over noen andre. Det sier seg selv at du har sunket millionvis av kroner i satsing og plutselig ryker hele inntektsgrunnlaget» Han nevner også hvordan tillitten til bedriften kan bli vesentlig svekket, slik at man får lavere omsetning og lavere inntjening i en periode.

Respondent 1 trekker frem Hydro saken, og hvordan aksjekursen faktisk gikk opp etter angrepet. «Man kan jo analysere hvorfor det har skjedd, men veldig mange sier at de har håndtert hendelsen på en veldig god måte, i alle fall responsen på hendelsen. Det kunne jo vært noe de kunne gjort bedre for å ha unngått hendelsen, men når den først skjedde, så håndterte de det på en god måte, og kom da positivt ut av det».

Intervju med Maria Bartnes

Hva er de største digitale truslene norske virksomheter møter i dag?

Maria nevner E-post som en mye brukt kanal. «Mange ulike skade-mail sendes. Phishing, falsk avsender, direktørsvindel, diverse vedlegg eller lenker som kan klikkes på, hvorpå skadelig kode installeres/kjøres på datamaskinen». Hun sier at slike e-poster er laget i forsøk på å lure en naiv eller vennligsinnet mottaker. «De mest effektive angrepene utnytter mennesker og samtidig som teknologi brukes som et verktøy». Hun nevner også skadelig kode som mye brukt i en stor andel av angrep i dag.

Videre nevner hun at veldig mye kan kartlegges ved hjelp av åpne informasjonskilder på internett, og er et viktig middel i mange angrep. «Mye informasjon om den enkelte, om prosjekter, om virksomheter, om relasjoner, interesser osv. ligger åpent på nett, godt fordelt mellom mange kanaler, men likevel tilgjengelig for den som målrettet ønsker å samle mye om sitt angrepsmål». Hun påpeker at godt informerte angripere kan få til så mye mer enn den som skyter i blinde.

Hvilke digitale trusler vil vokse frem eller bli mer aktuelle innen fem års tid?

Maria trekker frem IoT og hvordan det vil eksplodere fremover, samtidig som at sårbarhetene i disse er uendelig mange. «Utnyttelse av slike sårbarheter, vil kunne ha alvorlige konsekvenser. Når programvare styrer alle ting vi omgir oss med, må programvare være sikrere, mer robust og mer pålitelig enn i dag». Hun sier videre at dette er en enorm trussel som ligger og venter, som er kjent, og som er nødt til å forebygges med mye større trykk enn det vi gjør i dag. Hun legger til at «Sikker programvareutvikling, reguleringer og krav til sikkerhet i alle produkter som kommuniserer med ting og styrer ting, er en nødvendighet»

Hvilke konsekvenser kan det har for virksomheten dersom den ikke tar trusselbildet på alvor eller lar være å innføre nye sikringstiltak?

Maria nevner økonomiske tap, tap av renomme, kunder og tillit «I noen tilfeller kan konsekvensene være tap av liv og helse – avhengig av hva slags virksomhet der er og hvilke hendelser som inntreffer».

Intervju med respondent fra NSM

Hva er de største truslene norske virksomheter møter i dag?

Respondenten nevner fremmede stater som en av de største truslene. «De er veldig aktive mot norske mål. De er interessert i å stjele informasjon, eksempelvis forretningshemmeligheter og høyteknologi» Videre nevner respondenten at disse er interessert i muligheten for ytterligere operasjoner, og derfor er det nyttig for de å ha fotfeste i samfunnskritiske virksomheter.

Respondenten tar også opp vinningskriminalitet som direktørsvindel, cryptomining og krypteringsvirus som noen av de største truslene. «De følger pengene, der det er mye penger og der det er enkle penger»

Hvilke trusler vil komme i fremtiden?

«Den utviklingen vi ser i kriminaliteten er at de følger pengene. Her er det snakk om mer og mer internasjonalt organisert kriminalitet.» svarer respondenten. Han nevner også hvordan svindleren kan kartlegge målet sitt ved internett, og leie inn nordmenn til å skrive e-poster. «Kriminelle kan da stjele 100 millioner kroner fra en norsk virksomhet uten å engang ha vært i Norge. Vi ser en internasjonalisering og profesjonalisering av økonomisk kriminalitet».

Respondenten trekker også frem fremmede stater, og hvordan de vil være styrt av politikk. «Når det er gnissinger mellom stater så reflekteres dette i cyberdomenet». Videre nevner respondenten at det norske samfunn kommer til å få flere digitale sårbarheter. Kritisk infrastruktur, og ting som medisinsk utstyr, kraft og e-kom kommer på nett, og som vil føre til mer alvorlige konsekvenser dersom en sårbarhet utnyttes.

Hvilke sikringstiltak bør norske virksomheter vurdere å bruke?

Respondenten refererer til listen over 10 enkle tiltak for IKT sikkerhet NSM har laget. «Hvis norske virksomhet hadde fulgt disse tiltakene ville de forhindret 80-90 prosent av uønskede sikkerhetshendelser».

Videre legger respondenten til: «IKT sikkerhet er ikke bare hacking og beskyttelse mot det. Det er helhetlig arbeid i organisasjonen, det er teknologi og folk» legger respondenten til. «Det er ingen magisk formel. Det er kontinuerlig og langsiktig arbeid».

Hva kan konsekvensene være av å bli utsatt for sikkerhetshendelser?

«De to store vil være penger og omdømme» sier respondenten. «Det som er viktig å nevne er at det er veldig positivt når de virksomhetene som blir utsatt for et angrep står fram og forteller om det, og deler informasjon»

Områder i virksomheten

Respondenten påpeker at generelt blir mer og mer av virksomheten digitalisert, og da kan mer bli rammet. Informasjon er veldig relevant her, om det er forretningshemmeligheter eller databaser med brukernavn, passord osv som lagres. Det som er knyttet til pengeoverføring og de som har rettigheter til utbetaling i virksomheten er også utsatt.

«Mange virksomheter kan være mål, selv om de ikke tror det selv og mener at man ikke har store nok verdier. Små virksomheter med manglende sikkerhet blir angrepet og brukt som infrastruktur til videre angrep.»

Intervju med respondent 4 – Trusselidentifisering- og vurdering, fra IT-sikkerhetsselskap

Hva er de største digitale truslene norske virksomheter møter i dag?

«Fra et bredt perspektiv er det sikkerhetshendelsene som har innvirkning på forretningsprosessene som er problemet.»

Respondenten trekker frem vinningskriminalitet som en umiddelbar trussel. Her skilles det mellom optimistisk vinningskriminalitet, hvor aktørene yter lite innsats og går etter lavthengende frukter, og mer målrettet vinningskriminalitet, hvor aktøren bruker tid på identifisering og kartlegging av mål og arbeider mot målet over tid.

I tillegg er det tilsiktede handlinger hvor personlig vinning ikke nødvendigvis er målet, som etterretning, industrispionasje og annen informasjonstyveri. Disse er ikke nødvendigvis store kortsiktige trusler mot forretningsprosessene, men mer langsiktige strategiske trusler for norske virksomheter. «Dersom en virksomhet blir tappet for informasjon over tid mister man konkurransefortrinnet over konkurrentene, det kan være snakk om informasjon om teknologi, intellektuell eiendom, om produksjon, prosesser eller forretningshemmeligheter i virksomheten.»

Den siste trusselgruppen som nevnes er individer og organisasjoner som ønsker oppmerksomhet rundt egne saker, som å fremme et politisk budskap, oppnå dekning fra media eller som rett og slett er ute etter å ødelegge.

Hvilke trusler vil vokse frem eller bli mer aktuelle innen fem års tid?

Respondenten tar opp GDPR og personvernlover. «Dersom personvernlover håndheves strengere fremover og det gis flere bøter kan det bli en økende risiko for virksomheter. Samtidig blir dette en ny type informasjon som vinningskriminelle kan sikte mot. Man kan se for seg at aktører vil stjele informasjon som gir grunnlag for bøter og bruke dette til utpressing mot virksomheter, eller at de skreddersyr en pakke slik at det ser ut som man har den type informasjon. Utpressing kan ta mange former, også med krypteringsvirus hvor filer holdes som ‘gissel’.»

I tillegg påpekes det at kriminaliteten er drevet av muligheter og at hensikten bak handlingene kommer nok ikke til å endre seg drastisk i løpet av fem år. «Hensiktene vil være omtrent som tidligere; økonomisk vinning, etterretning, spenningssøkende atferd og oppmerksomhet rundt egen agenda eller politiske saker. Men mulighetene vil nok endre seg, og som et eksempel på dette nevnes det at selskapet har observert en korrelasjon mellom verdien i kryptovalutaer og uønsket mining. Hvordan virksomheten blir eksponert og hva man ‘henges ut’ i media for vil nok endre seg, men ikke hensikten bak handlingene.

Samtidig som metodene utvikler seg modnes også sikkerheten og tiltakene i virksomhetene. Derfor kommer nok ikke for eksempel direktørsvindel til å være like aktuelt om fem år.»

Hvilke sikkerhetstiltak bør vurderes for å imøtekomme disse truslene?

«Det *riktige* svaret er å innføre tiltak som beskytter forretningsprosessene slik at selskapet går rundt. På et organisatorisk nivå handler det om å stille krav og på et teknisk nivå handler det om å bygge operasjonelle kapabiliteter. Det er altså kapabiliteter som forhindrer, detekterer, responderer og rydder opp i hendelser. Disse fire kapabilitetene må balanseres og det er måten man tilnærmer seg informasjonssikkerhet og imøtekommer truslene.»

«Vi opplever at virksomheter har varierende grad av forståelse for hvordan trusselbilde ser ut og hvilke tiltak som er effektive for å redusere risikoen som trusselen utgjør. Det hjelper lite å kjøpe sikkerhetsprodukter uten å ha en formening om hvordan de faktisk reduserer risiko i et scenario. Når man gjør sikringstiltak bør det reflektere at man ønsker å redusere risikoen knyttet til en trussel som er relevant for selskapet og forretningsprosessene. Det å jobbe systematisk med dette er viktig, hvis ikke blir det tilfeldig i hvilken grad tiltakene reduserer risiko.»

Hvilke konsekvenser kan det ha for virksomheten dersom den ikke tar trusselbildet på alvor eller lar være å innføre nye sikkerhetstiltak?

«Alt som påvirker forretningsprosessene som skaper verdi i virksomheten får konsekvenser. Dermed risikerer du at lønnsomheten til virksomheten går nedover. Hvis organisasjonen leverer en samfunnskritisk funksjon risikeres denne funksjonen. Det kan være en stor belastning å rydde opp i en hendelse, som å finne ut hvilke systemer som er kompromitterte, leie inn ekstern hjelp og bygge opp deler av virksomheten på nytt. Potensielt er det kroken på døra, det finnes selskaper som har gått konkurs etter kompromittering. Dette er da ekstremtilfellene, ellers må man vurdere konsekvensene individuelt.

Konsekvensene kan være sammensatte, det kan også oppstå utilsiktede bieffekter når man blir utsatt for eksempelvis industrispionasje, ved at det oppstår forstyrrelser, avbrudd eller nedetid»

Er det enkelte områder eller avdelinger i virksomheten som vil bli spesielt utsatt i møte med trusler fremover?

«De mest utsatte vil være de som arbeider med teknologi. Det er forskjellige områder som er utsatt, ettersom hva trusselen motiveres av. De som arbeider med transaksjoner er nok mer utsatt for svindel, og de som arbeider med forskning er nok mer utsatt for spionasje og informasjon-tyveri.

Om vi ser fem år tilbake og ser på konkrete tekniske løsninger har vi sett et skifte i trusselaktørenes leveranseplattform, fra web til epost. Det handler om at tilgjengelige sårbarheter i nettleser og nettleser-plugins har gått ned de siste årene. Sammenligner vi med 2012-13 har det vært et skifte. Angrep mot endepunkt-plattform skjer fortsatt, men det skjer i større grad gjennom epost-vedlegg, fordi mulighetsrommet på web er mindre enn før.»

Er skylagring generelt tryggere enn tradisjonell lagring?

«Det er andre fallgruver med skylagring. En positiv effekt med å ta i bruk skylagring er at standard-konfigurasjonen ofte er bedre enn det man ville konfigurert selv, on-premise. Men behovet for kontrollmekanismer forsvinner ikke fordi man går over til skylagring. Man har samme behov for kontroll, men det er ikke alltid skyleverandøren tilbyr støtte for slike funksjoner. Skyleverandørene har ofte ikke forretningsmessige grunner til å støtte den type funksjoner og kontrollmekanismer. Da må man kompensere med tiltak for å ivareta den kontrollen man ønsker. Hvis man tar i bruk skylagring uten å ta stilling til hvordan man ivaretar kontroll, sporbarhet og sikkerhet blir det et lavt nivå av sikkerhet.»

6. Analyse og Diskusjon

I dette kapitlet presenteres analyse- og diskusjonsdelen av resultatene for oppgaven. Resultatene fra litteratursøket og resultatene fra intervjuene blir diskutert hver for seg, henholdsvis «Del 1» og «Del 2».

6.1. Om metode

Å kartlegge fremtiden, spesielt i det digitale domenet hvor nye innovasjoner stadig utvikles er en stor utfordring. Ingen kan med høy nøyaktighet forutse hvordan fremtiden vil se ut, da det er mye som kan forandre seg innen fem år, og oppgaven bør i den grad sees på som en kvalifisert «gjetting» på de trender som vil prege det fremtidige trusselbildet.

Datainnsamling

Å oppsøke kilder som har tilfredsstilt våre kriterier til kunnskap og erfaring innen dette spesifikke tema har vært tidkrevende. Gjennom prosessen for å finne intervjukandidater fikk vi dessverre kun respons på et fåtall av henvendelsene. Det å finne passende intervjukandidater som kunne bidra med ny data har derfor vært en utfordring gjennom prosjektet. Kvantitative data ville vært verdifullt for å belyse problemstillingen, men det var ikke realistisk å finne mange nok respondenter med riktig bakgrunn til å oppnå et substansielt datagrunnlag.

6.2. Del 1 - Litteraturstudiet

Omfanget av direktørsvindel vokser

Gjennom årene har direktørsvindel blitt en av de største truslene for norske virksomheter. Svindel blir stadig mer målrettet, og aktørene mer utspekulerte. Norge viser seg også å være en av de mest populære målene for denne formen for svindel, og flere norske virksomheter har tapt store beløp på dette.

Når virksomheter velger å ikke rapportere at de har blitt lurt av denne svindelformen svindelformen. Det er ingen som liker å innrømme at man har blir lurt, og det kan medføre skam, da det kan gi inntrykk om at virksomheten har et avslappet forhold til regler og rutiner. I mørketallsundersøkelsen 2018 kommer det frem at over halvparten av hendelsene var delvis forårsaket av medarbeidere, og dette skyldes i stor grad på grunn av manglende bevissthet eller kompetanse rundt sikkerhet. Bevissthet og kunnskap på trusler bidrar til nedgang av antall vellykkede hendelser, og når virksomheter velger å ikke rapportere at de blir utsatt for

vellykket direktørsvindel, holdes kunnskap om denne trusselen til en viss grad i et vakuum. Det bidras dermed mindre enn det er mulig til økt forståelse av fremgangsmåten angriperne benytter, samt hvorfor ofrene lar seg lure. Så lenge virksomheter har en slik tilnærming vil det bli utfordrende å hindre denne trusselen i å vedvare.

Som virksomhet kan man innføre både kulturmessige og tekniske tiltak for å hindre denne typen økonomisk svindel. Et viktig tiltak for å stanse direktørsvindel vil være å innarbeide rutiner rundt transaksjoner. Det bør være en tydelig prosedyre på hvordan endring av kontonummer skal foregå i virksomheten. Prosedyren bør minst beskrive hvordan kontoinnhaver skal melde ifra om endringen på en sikker måte og hvor mange og hvem som skal godkjenne for at endringen trer i kraft.

Spionasje må forventes å forekomme

Spionasje vil sannsynligvis alltid være en stor trussel. Så lenge virksomheter innehar verdifull informasjon, vil det alltid være noen som forsøker å tilegne seg det. Det er en trussel som berører både små og store virksomheter samtidig som det går mot et stadig bredere spekter. Virksomheter som behandler verdifull informasjon teknologi, infrastruktur og annen kommersiell informasjon vil være av høy interesse av både fremmede stater og konkurrerende virksomheter. Konsekvensen av å bli utsatt kan være svært kritisk. Private virksomheter mister hele konkurransefortrinnet sitt dersom forretningshemmelighetene deres skulle komme på avveie, og det medføres store økonomiske tap. Dersom en virksomhet med kritisk infrastruktur for det norske samfunn skulle bli kompromittert, har det potensialet til å svekke hele samfunnssikkerheten.

Hvem som helst kan bli en cyberutpresser

Trendutviklingen av krypteringsvirus viser at det er totalt en nedgang i antall hendelser fra 2017 til 2018. Dette kan forklares av at det var mye omtale og saker i pressen vedrørende «Wannacry/petya» hendelsen, som gjorde omverdenen mer oppmerksom på trusselen. Krypteringvirus utgjør likevel en stor trussel da det fortsatt forekommer, og konsekvensene av å bli utsatt for slike angrep kan være svært alvorlige i form av tap av arbeidstid, informasjon og økonomi.

Enkelte virksomheter velger også å betale løsepengene istedenfor å oppsøke hjelp fordi de føler det er billigere og mindre risikabelt. En slik tilnærming er imidlertid ikke optimal. Selv om man betaler løsepengene er det ingen garanti for at angriperen gir tilgang til systemene

igjen. Det kan samtidig oppmuntre angriperne til å gjenta slike angrep, da det gir inntrykk om at trusselen er effektiv.

Teknologien er i tillegg både er enkel å bruke samtidig som den er til salgs. Dette innebærer at hvem som helst med et kredittkort kan kjøpe denne «tjenesten» og bli en cyberutpresser. Det virker rimelig å anta at omfanget av denne trusselen vil komme til å fortsette å øke så lenge det er forholdsvis enkle penger å tjene på dette.

Hacktivisme bør ikke undervurderes

Det er ennå ikke blitt utført angrep av hacktivister som har fått betydelige samfunnsmessige konsekvenser for Norge, men det er likevel viktig å ikke undervurdere denne trusselen. Det oppleves en økende grad av hacktivistangrep mot norske virksomheter og tilgjengeligheten av ressurser og kunnskap som kreves for å gjennomføre omfattende angrep blir stadig bedre. Når en enkelt tenåring er i stand forstyrre flere av Norges største virksomheter, kan man bare tenke seg hvor mye mer omfattende angrepene kan bli dersom angrepene utføres av en organisert og koordinert gruppe.

Spearphishing er vanligste angrepsmetode

Spearphishing har blitt den mest vanlige angrepsmetoden trusselaktørene benytter, og det er tydelig at dette er en effektiv metode. De fleste sikkerhetshendelsene skjer i løpet av en vanlig arbeidsdag, som tyder på at det er en årsakssammenheng mellom brukeraktivitet og sikkerhetshendelser. Inntrengingstestene NSM utfører på norske virksomheter støtter denne påstanden. Det er altfor lettvint å lure ansatte til å trykke på vedlegg og lenker i tilsynelatende troverdige e-poster, som da infiserer datamaskinen og nettverket. Trusselaktørene blir stadig mer målrettet, og rekogniseringsfasen trusselaktøren utfører før angrepet e-postene som sendes mer troverdige, som kan være årsaken til at mange blir lurt. Så lenge mennesket vil være en faktor for virksomhetens sikkerhet virker det sannsynlig at angrep som benytter e-post for å få fotfeste i bedriftene vil være en sentral faktor.

Skanning og utnyttelse av sårbarheter

Dataangrep som ikke avhenger av menneskelig interaksjon og kommunikasjon benytter gjerne sårbarheter i programvare, operativsystem eller maskinvare for å trenge inn i et nettverk. Slike sårbarheter kan utnyttes til å spre skadevare eller oppnå uautorisert tilgang til et nettverk. Dersom programvareleverandøren er aktiv med å patche disse svakhetene etter hvert som de oppdages reduseres mesteparten av den potensielle skaden.

Utfordringen har midlertidig vært at brukerne ikke alltid oppdaterer programvaren, selv når det er kjente sårbarheter som er patchet. Det kan skyldes manglende kunnskap hos den enkelte, mangelfulle rutiner i virksomheten eller designet av programvaren.

Vellykkede tjenestenektangrep er i nedgang, men trusselen vedvarer

Tjenestenektangrep kan gjøre nettsider og andre internett-eksponerte tjenester utilgjengelige og skape forstyrrelser i nettverket. Mørketallsundersøkelsen fra 2016 og 2018 indikerer at DDoS-angrep er en noe økende trussel, men økningen kan skyldes en endret sammensetting i utvalget av respondenter til undersøkelsen. Undersøkelsen fra 2018 hadde flere store virksomheter som respondenter enn tidligere, og det antas at store virksomheter tiltrekker mer oppmerksomhet og blir dermed mer utsatt for slike angrep enn de små virksomhetene.

Telenors datagrunnlag viser derimot en nevneverdig reduksjon i antall DDoS-angrep i deres nettverk fra 2016 til 2019. Årsaksforholdene i denne sammenhengen er komplekse og det er ingen garanti for at nedgangen vil fortsette. En av årsakene til nedgangen kan være at filtrering og andre mottiltak nettleverandørene benytter for å skjerme nettet sitt har blitt mer avanserte og effektive. En annen faktor som spiller inn er i hvilken grad nettilbydere verden rundt klarer å begrense denne typen aktivitet fra deres nettverk. Det kan også være ikke-tekniske årsaker til at norske mål utsettes sjeldnere for denne typen angrep enn før.

Tjenestenektangrep forbindes ofte med aktivisme og vandalisme, men det kan også brukes som middel til vinningskriminalitet. Telenor har opplevd bølger med utpressing de siste årene, hvor noen virksomheter trues til å betale en sum for å unngå DDoS-angrep.

Selv om det er registrert en viss nedgang mot norske mål de tre siste årene er tjenestenektangrep en vedvarende trussel, da det fortsatt kommer vellykkede angrep mot bedrifter og andre virksomheter.

Skadepotensialet til botnets vokser

Som virksomhet er det en risiko for å ufrivillig bli del av et botnet og en annen risiko for å bli utsatt for angrep fra et botnet. Risikoen for å bli en del av et botnet kommer an på sikkerheten og kvaliteten i enhetene man eier, og om de har svakheter som kan føre til infisering eller fjernstyring. Risikoen for å bli utsatt for angrep fra botnets er vanskelig å forutsi, da enhetene et botnet består av kan brukes til mange ulike formål. Tidligere har disse blitt brukt til eksempelvis utvinning av kryptovaluta og til tjenestenektangrep.

En trend knyttet til dette området er den eksponentielle økningen i antall enheter som kobles til internett. Samtidig som det forventes at sikkerhetene i slike enheter gradvis blir bedre kommer det så mange nye enheter at det er vanskelig å holde en oversikt over sikkerheten i alle disse. Både økningen i antallet enheter og den kontinuerlige utvidelsen av oppgaver disse utfører gjør at skadepotensialet til botnets vokser, noe vi mener har blitt demonstrert i stadig større hendelser de siste par årene.

Vekst i illegitim utvinning av kryptovaluta

Et nytt verktøy for vinningskriminelle er skadevare som bruker maskinressurser til å utvinne kryptovaluta. Om vi tar utgangspunkt i statistikken fra Telenor virker denne skadevaren å være knyttet til prisbevegelsene i kryptovaluta-markedet. Når prisene stiger blir det mer lønnsomt å utvikle denne type skadevare og motsatt når prisene reduseres. Sammenligner vi denne typen skadevare med krypteringsvirus er skadepotensialet mot virksomheten mindre. På kort sikt vil skadevaren bruke maskinkapasitet og dermed kan tjenester som driftes av maskinen påvirkes. På lengre sikt vil det utgjøre kostnader for virksomheten i form av strøm og vedlikehold av maskiner.

Den generiske virusspredningen via nettlesere har nesten forsvunnet

Exploit kits og den mer generiske virus-spredningen gjennom nettlesere virker å være redusert til et minimumsnivå, og har omtrent forsvunnet i Norge. Enkelte kilder tolkes som at Exploit kits er en metode som fortsatt anvendes i Asia og andre områder, men at det er for få sårbare systemer i Europa og Nord-Amerika til at metoden blir brukt her.[37]

Vannhullsangrep brukes i målrettede angrep

Vannhullsangrep har i løpet av de siste årene økt i bruk ifølge flere kilder, spesielt til mer målrettede angrep. Denne typen angrep er avhengig av at offeret faktisk besøker en nettside som trusselaktøren klarer å kompromittere, noe som gjør at det er usannsynlig at slike angrep vil lykkes i stort volum. For at trusselaktøren skal lykkes må nettsiden offeret besøker kompromitteres, svakheter i nettleser må utnyttes for å servere skadevaren gjennom nettsiden og i tillegg må det være en verdi i å oppnå tilgang til offerets maskin. Forutsetningene for å lykkes etter at trusselaktøren har valgt et attraktivt offer er nok sjelden tilstede, men om angrepet først lykkes er det veldig vanskelig å spore.

Det er mulig for virksomheter å begrense risikoen for denne type angrep ved å blokkere uønskede nettsider og programmer. Tilstrekkelig bevissthet og sikkerhetskultur rundt PC-

bruk i virksomheten vil nok også begrense risikoen. En risikofaktor for virksomhetene vil i dette tilfelle være private maskiner og enheter som benyttes i arbeidssammenheng, da man ikke har samme kontroll-mekanismer på programvare som man ofte har på bedriftsmaskiner.

Underleverandører blir utnyttet som inngangsportal til virksomheten

Mørketallsundersøkelsen 2018 viste at kun 2 prosent av virksomhetene opplevde sikkerhetshendelser «forårsaket av outsourcingleverandør». Til sammenligning opplevde 21 prosent virus eller malwareinfeksjon. Samtidig har NSM de siste par årene observert at underleverandører i økende grad blir utnyttet som inngangsdør for å nå det egentlige målet.

Mørketallsundersøkelsen bruker begrepet «outsourcingleverandør» og spørreundersøkelsen inkluderte ikke spørsmål om andre leverandører på dette punktet. Her ville det vært interessant å samle data på hvilken grad virksomhetene opplever sikkerhetshendelser knyttet til andre leverandører og samarbeidspartnere, som ikke er i forbindelse med outsourcing. Erfaringsmessig er det også stor variasjon i hvordan ord som «outsourcing» og «outsourcingleverandør» blir tolket, og ulik begrepsforståelse hos respondentene må derfor anses som mulige feilkilder i denne sammenhengen.

Det at underleverandører blir utnyttet for å nå et primærmål betyr at en virksomhet som i utgangspunktet ikke oppfattes som et attraktivt mål i seg selv kan være attraktivt på grunn av dens samarbeidspartnere, bedriftskunder, plassering i verdikjeden eller rett og slett teknisk utstyr. Som virksomhet bør man vurdere risiko i prosessen med å velge leverandører og underleverandører. Leverandører som lagrer data på oppdrag fra virksomheten eller oppbevarer kritisk informasjon i forbindelse med andre forretninger må inkluderes i den totale risikostyringen.

6.3. Del 2 – Intervju

De største truslene i dag

Flere av respondentene nevner vinningskriminalitet som en av de største truslene i dagens trusselbilde, og mer spesifikt direktørsvindel, krypteringsvirus og kryptomining. Den menneskelige faktoren er en fellesnevner som muliggjør disse truslene da mange av angrepene bruker e-post for å fotfeste i virksomhetene ved å lure naive og lettlurte ansatte til å trykke på vedlegg eller lenker som installerer skadelig kode. Det er også en fare for at de som er ansvarlige rett og slett glemmer å oppdatere og vedlikeholde systemene sine da de mest effektive angrepene utnytter mennesker og bruker teknologi som et verktøy.

Vinningskriminalitet kan skilles mellom optimistisk og målrettet. Optimistisk innebærer å angripe virksomheter som er mer sårbare, og som krever mindre innsats for å oppnå gevinst. Målrettet vinningskriminalitet innebærer å bruke tid på å identifisere målet, kartlegge de og arbeide mot de over tid. Informasjon om virksomhetene, ansatte osv. ligger åpent på forskjellige informasjonskilder på nett, og kriminelle er flinke til å tilegne seg denne informasjonen. Informerte angripere kan få til mye mer enn de som skyter i blinde.

Fremmede stater og etterretningsvirksomhet nevnes også som noen av de største truslene i dag. Det observeres mye aktivitet mot norske virksomheter for å stjele forretningshemmeligheter, høyteknologi og annen sensitiv informasjon. Disse truslene er mer langsiktige og strategiske hvor personlig vinning ikke nødvendigvis er målet.

Utsatte områder i virksomhetene

Respondentene påpeker at områdene som er utsatt vil være avhengig av virkeområdet til virksomheten og hvilke verdier og informasjon som forvaltes. I tillegg er det avhengig av hvordan trusselbildet til virksomheten ser ut, og hva trusselen motiveres av. Eksempelvis vil en trussel som motiveres av økonomisk vinning sikte mot andre områder enn en trussel som motiveres av spenningssøkende atferd eller oppmerksomhet. En avdeling med rettigheter til transaksjoner vil være mer utsatt for svindel og en avdeling som arbeider med forskning og teknologi vil nok være mer utsatt for industrispionasje og informasjonstyveri.

Samtidig påpeker respondenten ved NSM at små virksomheter med lavt nivå av sikkerhet angripes og brukes som infrastruktur til videre angrep. Det er ofte snakk om virksomheter som antar at man ikke er et attraktivt mål for trusselaktører. Det kan tyde på at virksomhetene undervurderer egne midler og ressurser i forhold til trusselbildet eller at de ikke har et tilfredsstillende system for risikostyring. Uten slike vurderinger er det vanskelig å vite hvilke områder som er utsatt og hvor man som virksomhet bør rette sikkerhetsinnsatsen for å finne effektive tiltak.

Når det gjelder kanaler som benyttes til å levere skadevare rettet mot virksomheter har det skjedd en endring i løpet av de siste årene. Trusselaktørene bruker i mindre grad nettleseren og i større grad e-post til å levere skadevare. Det skyldes at sårbarheter i nettlesere og nettleser-plugins har gått ned og dermed er mulighetsrommet på nett er smalere enn før. For noen virksomheter kan dette ha en viss betydning for hvilke områder som er utsatt.

Generelt kan utviklingen beskrives med at mer av virksomhetene digitaliseres, noe som betyr at flere områder blir utsatt. Alle som arbeider med teknologi og benytter et nettverk vil være utsatt for digitale trusler.

Fremtidens trusler og faremomenter

Respondentene har svært ulikt syn når det gjelder utviklingen av trusler de kommende årene og trekker frem trusler på en rekke forskjellige områder. Tema som IoT-enheter, strengere håndheving av personvern, den menneskelige faktoren i sosial manipulering og internasjonalisering av økonomisk kriminalitet er sentrale.

IoT – Antallet enheter eksploderer

Ifølge Maria Bartnes er det viktig at programvaren må bli sikrere, siden det styrer alle ting vi omgir oss med. Hun mener at både utilsiktede feil og svakheter som utnyttes bevisst i disse enhetene kan få alvorlige konsekvenser.

Den eksplosive økningen av IoT-enheter som kommuniserer med hverandre, styrer systemer og er koblet til internett vil utgjøre en større trussel de neste årene. I tilfeller hvor slike enheter kompromitteres kan de bli en del av et større botnet og fjernstyres av trusselaktører. Økningen i antall enheter og oppgavene disse utfører gjør at skadepotensialet i en kompromittering vokser. Med stadig flere enheter og mer programvare blir sårbarhetsoverflaten til virksomheten større og det blir viktigere å ha oversikt over enhetene og programvaren som er i bruk.

Selv i kjente produkter med høy kvalitet oppdages det svakheter som utnyttes. For å kunne tette sikkerhetshull så raskt som mulig bør virksomheten etablere en rutine for å oppdatere regelmessig. Virksomheten bør holde oversikt over all maskinvare som brukes og etablere et system med rutiner for å oppdatere programvare, operativsystem og firmware (internprogram).

For å begrense sårbarhetsoverflaten og mulighetsrommet til trusselaktørene bør virksomheter som forvalter kritisk informasjon vurdere risikoen i private enheter som benyttes i arbeidsammenheng. Virksomheten bør avklare hvilke arbeidsoppgaver som tillater bruk av private maskiner.

Personvern – Strengere håndheving av personvern

«Om personvernlover håndheves strengere fremover og det gis flere bøter kan det bli en økende risiko for virksomheter og samtidig en ny type informasjon som vinningskriminelle kan sikte mot. Man kan se for seg at aktører vil stjele informasjon som gir grunnlag for bøter og bruke dette til utpressing mot virksomheter, eller at de skreddersyr en pakke slik at det ser ut som man har den type informasjon. Utpressing kan ta mange former.» sier respondent 4.

En kompromittering av data forbindes ofte med oppmerksomhet i media og svekket omdømme. Fordi personvern blir tatt på alvor i større grad og personvernlover håndheves mer aktivt vil kompromittering av persondata kunne få større økonomiske konsekvenser de neste årene.

Virksomheten bør vurdere om personvernet data bør behandles separat fra annen informasjon som forvaltes. Uansett om virksomheten lagrer data selv (on-premise) eller om denne funksjonen tjenesteutsettes bør informasjonens konfidensialitet, tilgjengelighet og integritet vurderes og prioriteres.

For å tjenesteutsette funksjonen på en trygg måte må virksomheten stille krav til sikkerhet, sporbarhet og kontrollmekanismer i lagringen som leverandør tilbyr. Dersom kravene ikke kan tilfredsstilles av leverandør må en selv implementere kompenserende tiltak.

For on-premise lagring vil en backuprutine være en effektiv måte å sikre informasjonens tilgjengelighet på. Backuprutinen bør inneholde fullstendige og inkrementelle backup og kan lagres over lang tid om man vil ha mulighet til å gå tilbake til tidligere versjoner. En fullstendig backuprutine kan også være et eksempel på et korrigerende tiltak dersom leverandør ikke tilfredsstiller krav til tilbakerulling av dataen. En annen fordel med backuprutinen er at man kan gjenopprette IT-systemene relativt raskt dersom et katastrofalt dataangrep skulle inntreffe, som et krypteringsvirus.

Menneskelig faktor

«Trusselaktørene vil alltid gå etter det svakeste punktet, og uansett hvordan man snur og vender på det så mener jeg at mennesker kan således være det svakeste punktet, og vil kanskje dra det så langt som å si at de *er* det.» sier Arild Bjørk. Ifølge Bjørk vil den menneskelige faktoren vil bli enda viktigere fremover og at det både er og blir det mest sårbare punktet for sikkerheten i en virksomhet. Det kan tolkes som at teknologiske og

organisatoriske faktorer vil forbedres i virksomhetene, men det vil alltid være mulighet for å benytte sosial manipulering og den menneskelige faktoren.

Internasjonalisering og profesjonalisering

«Vi ser en internasjonalisering og profesjonalisering av økonomisk kriminalitet. Kriminelle kan stjele millioner fra norske virksomheter, uten å engang ha vært i Norge.» sier respondent 5. Personen observerer at det blir mer internasjonalt organisert kriminalitet, hvor aktørene arbeider på tvers av landegrenser. Respondenten beskriver hvordan aktører bruker mer målrettede metoder for sosial manipulering:

«For å svindle deg kan de google navnet ditt for å finne ut hva du er interessert i, og leie inn en nordmann til å skrive eposter. Da får du en epost med skadevare som er direkte rettet mot deg. Mye programvare (skadevare) er også tilgjengelig på internett for å gjennomføre slikt.»

I tillegg nevner respondenten at vi generelt legger ut mer informasjon på nett. Denne informasjonen kan benyttes til sosial manipulering og blir lagret av forskjellige selskaper ,f.eks. internettgigantene, slik at de etterhvert kan vite veldig mye om brukerne.

Sosial manipulering går mot menneskene i virksomheten og dermed er det nødvendig å ha mer fokus på den uformelle delen av et styringssystem. Uten sikkerhetsbevisste ansatte vil ikke tekniske løsninger kunne ivareta sikkerheten i virksomheten. Som en del av kulturprogrammet i den kontinuerlige forbedringen vil tiltak som øker ansattes kunnskap og kompetanse knyttet til sikkerhet være relevante. Forslag til tiltak er å informere ansatte om virksomhetens spesifikke trusselbilde, gjennomføre sikkerhetsopplæring og å vedlikeholde sikkerhetsrutiner og prosedyrer blant ansatte. Med kunnskap om det spesifikke trusselbildet virksomheten forholder seg til kan det være enklere å oppdage forsøk på phising og annen sosial manipulering.

Sammen med kulturprogram er det også tiltak knyttet til det tekniske programmet som kan hindre sosial manipulering. Kompromitterte epost-brukere har eksempelvis blitt brukt til sosial manipulering og svindelsaker. For å redusere sannsynligheten for at brukere kompromitteres på epost eller andre plattformer kan man innføre 2-faktor autentisering. Innloggingsprosessen vil ta noe mer tid, men autentiseringen forbedres. Passord blir i mange tilfeller skrevet ned og om de kommer på avveie kan de raskt bli en inngang for uvedkommende. Med et steg til i autentiseringsprosessen økes sikkerheten betraktelig. Et alternativt tiltak er å benytte biometriske data, som fingeravtrykk eller øyeskanning.

Autentiseringsprosessen blir ikke lenger avhengig av passord og blir på mange måter rask og trygg.

Tiltak og endringer virksomheten bør vurdere

Respondentene er i stor grad samstemte om at informasjonssikkerhet handler om kontinuerlig, langsiktig og helhetlig sikkerhetsarbeid som er integrert i virksomheten. Virksomheten må gjøre egne risikovurderinger, verdivurderinger og trusselvurderinger for å finne tiltak som beskytter deres forretningsprosesser på en effektiv måte.

På et overordnet nivå handler det om at virksomheten stiller krav til sikkerheten og bygger operasjonelle kapabiliteter som tilfredsstiller disse kravene, ved å forebygge, detektere, respondere og å rydde opp i sikkerhetshendelser.

Flere av respondentene foreslår tiltak og endringer knyttet til utformingen av virksomhetens eget IT-system. Det er ofte mulig for ansatte å finne en vei rundt interne sikkerhetstiltak og rutiner. Det kan eksempelvis gjelde rutiner knyttet til lagring, passordbytter, brukerrettigheter, oppdateringer og lignende som skal bevare sikkerheten. Derfor er det viktig å finne en balanse mellom sikkerhet og brukervennlighet når man utformer tiltak og rutiner. Her må man også vurdere IT-kompetansen til brukerne, de ansatte, slik at tiltakene tilpasses målgruppen og ikke blir for krevende og vanskelig. Når det gjelder sikkerhetskultur er det viktig at de ansatte er klar over verdiene og informasjonen de har tilgang til.

Angående de tekniske løsningene i IT-systemet er det viktig at man holder oversikt på systemer, komponenter og elektroniske tjenester som er i bruk i virksomheten. En forutsetning for å finne tiltak som reduserer risiko er at man har oversikt over hvilke hvilken teknologi komponentene er bygget på, hvilke avhengigheter som eksisterer og nivået av vedlikehold som kreves i komponentene.

NSMs liste med 10 med tiltak kan anbefales for alle virksomheter, da de er forholdsvis enkle å implementere og vil forebygge de aller fleste digitale og internett-relaterte dataangrep en virksomhet kan oppleve.

Konsekvenser ved mangelfull sikkerhetsstyring

Økonomiske tap, tap av data/informasjon og tap av tillitt eller omdømme er de vanligste konsekvensene ved sikkerhetshendelser. Når forretningsprosessene blir påvirket av hendelser vil lønnsomheten gå nedover, arbeidsoppgavene tar lengre tid, og det kan kreve mye ressurser for å gjenopprette normal tilstand. Mye av konsekvensene knyttes opp mot penger, og i verste

tilfelle kan virksomheten gå konkurs, men dette skjer kun ved ekstremtilfeller. Om det er snakk om virksomheter med samfunnskritiske funksjoner så kan det også stå om liv og helse.

Måten virksomheten velger å håndtere hendelsen på kan også påvirke utkommet av situasjonen. Når virksomheter som blir utsatt velger å stå fram om hendelsen er det fortsatt mulig å komme positivt ut av det. Omverdenen blir mer bevisst på trusselen og vi kan dermed ta lærdom av hverandre. Det kan også øke tillitten folk har til virksomheten, ettersom de ser at virksomheten er i stand til å håndtere sikkerhetshendelsene.

7. Oppsummering og konklusjon

Hensikten med denne oppgaven har vært å kartlegge utviklingen og fremtiden av trusselbildet for norske virksomheter med tilhørige sikkerhetstiltak.

For å kartlegge trendutviklingen gjennomførte vi en litteraturstudie. Kildene har i stor grad bestått av organisasjoner som jobber med informasjonssikkerhet knyttet til norske virksomheter, som publiserer jevnlige undersøkelser og rapporter om trusselbildet. Resultatene fra dette litteratursøket har gitt oss god innsikt i trendutviklingen.

For å avdekke hvilke trender som vil prege trusselbildet om fem års tid har vi gjennomført intervjuer med personer med bakgrunn i informasjonssikkerhet, både fra privat næringsliv, offentlig sektor, forskningsmiljøer og bransjeforeninger. Resultatene fra intervjuene og funnene vi gjorde i litteratursøket gav oss grunnlag for å kartlegge dagens situasjon samt kartlegging av fremtidens trusselbilde.

Med utgangspunkt i disse truslene, har vi basert på teori og innspill fra respondentene laget en kortfattet guide for hvilke sikkerhetstiltak norske virksomheter bør implementere for å imøtekomme truslene.

Foreslåtte tiltak er basert på vår egen analyse av utviklingen og deltakernes innspill. Vi har foreslått kjente tiltak som vi mener passer best for det fremtidige trusselbildet. Tiltakene er generelle og en virksomhet må gjøre egne analyser for å finne ut hvilke områder som bør prioriteres i sikkerhetsarbeidet.

Gyldigheten i oppgavens funn er knyttet til ressurspersonene som deltok. Alle deltakerne hadde forskjellige syn på hvilke trusler som vil bli mer aktuelle. Problemstillingen omhandler et forholdvis stort tema og med flere deltakere ville vi trolig fått enda flere synsvinkler og bedre grunnlag til å besvare problemstillingen.

7.1. Oppsummering

Utviklingen av trusselbildet og angrepsmetoder.

Kartleggingen viser en trend hvor trusselbildet og angrepsmetodene mot norske virksomheter blir stadig mer målrettede og profesjonaliserte. Trusselbildet preges i stor grad av vinningskriminalitet og etterretningsvirksomhet. De mest effektive angrepsmetodene er avhengig av menneskelig interaksjon, og det er en tydelig økning av trusler mot norske virksomheter som tar utgangspunkt i dette. Årsaken er sammensatt, men mye kan knyttes opp

mot mennesker. Informerte trusselaktører kan oppnå mer enn de som skyter i blinde, og ettersom informasjonen om målet ofte ligger tilgjengelig på nett, er det mulig for trusselaktørene å kartlegge angrepet med bedre forutsetninger. Sammenlignet med andre land fremstår norsk grunnsikring og infrastruktur som forholdsvis sterk, og ettersom trusselaktørene har en tendens til å gå minste motstands vei går de derfor i stor grad etter menneskene. Med tryggere nettlesere og bedre grunnsikring har den generiske virusspredningen blitt redusert til et minimumsnivå. Samtidig er det en kontinuerlig utvikling av nye typer skadevare. Det har vært en brå økning i hendelser knyttet til illegitim utvinning av kryptovaluta de siste årene. Når det gjelder mer målrettede metoder har det i de siste årene vært en økning i angrep, eller avdekkede angrep, som går etter underleverandører. Kilder som NSM observerer at underleverandører blir utnyttet som en inngang til primærmålet.

Fremtidens trusler og anbefalte tiltak

Ettersom trusselbildet blir mer målrettet og profesjonalisert og grunnsikringen til norske virksomheter er sterke virker det sannsynlig å anta at den menneskelige faktoren vil bli enda viktigere fremover, og trusler som tar utgangspunkt i sosial manipulering vil vedvare. Innen vinningskriminalitet vil trusselaktørene vil følge pengene, og der det er lette penger å tjene. Direktørsvindel og krypteringsvirus vil derfor sannsynligvis fortsatt utgjøre en del av trusselbildet om fem års tid. Fremmede stater og konkurrerende virksomheter vil alltid ha interesse for høyteknologi og annen verdifull informasjon og derfor er det rimelig å anta at spionasje vil være en stor trussel fremover.

Økningen i antall enheter, og oppgavene disse utfører gjør at skadepotensialet i kompromitteringer vokser og at sårbarhetsflaten til virksomheten blir større. For virksomheten vil det være viktig å holde oversikt over maskinvaren som brukes, lage et system for oppdateringer og å gjøre en bevisst vurdering for hvordan private enheter brukes.

Flere lover for personvern og strengere håndheving av disse stiller høyere krav til oppbevaring og håndtering av personvernet data. I tillegg til andre konsekvenser kan en datakompromittering på dette området også føre til straff, i form av bøter. Enten virksomheten oppbevarer data selv eller benytter en leverandør bør man stille krav til sikkerheten i lagringen og gjøre en bevisst vurdering på hvilken løsning som er hensiktsmessig.

Det blir stadig mer informasjon tilgjengelig på nett og det er lettvint for vinningskriminelle å samarbeide på tvers av land og språk. Vinningskriminaliteten blir mer profesjonell må sees på

i en internasjonal sammenheng. Når trusselaktøren har nok forkunnskaper kan målrettede svindelforsøk fremstå som svært troverdige. Utsatte virksomheter kan forbedre sikkerhetskulturen og kompetansen i virksomheten og fatte tiltak som gjør ansatte i bedre stand til å avsløre svindelforsøk og phishing. For å øke konfidensialiteten i IT-systemene og sikre at avsender er riktig person bør virksomheten vurdere å benytte mer enn kun passord for pålogging, på epost og andre plattformer.

Trusselaktørene med nok ressurser og kapasitet vil i økende grad angripe underleverandører for å bryte seg inn i virksomhetens system eller for å oppnå uautorisert tilgang til informasjon. Generelt blir verdikjeden for virksomhetene stadig lengre og det blir vanligere å tjenesteutsette IT-funksjoner. Virksomheter med underleverandører og leverandører som har tilgang til forretningskritisk informasjon eller annen viktig informasjon bør inkludere disse i den totale risikostyringen.

7.2. Konklusjon

Trusselbildet til virksomhetene preges av vinningskriminalitet og etterretning og angrepene blir mer målrettede og profesjonelle. De mest effektive angrepene benytter teknologi og sosial manipulering for å stjele verdier og informasjon fra virksomheter. Generelt er grunnsikringen og IT-infrastrukturen i norske virksomheter forholdsvis god, og angrepsmetodene blir mer avhengig av sosial manipulering og menneskelige sårbarheter. Økningen i antall enheter, lovgiving og håndheving for personvern og internasjonaliseringen av vinningskriminalitet vil være de mest sentrale trendene som vil prege trusselbildet om fem år. Med hensyn til disse trendene peker vi ut fem viktige områder med anbefalte tiltak norske virksomheter bør vurdere for å imøtekomme fremtidens trusler.

5 OMRÅDER DIN VIRKSOMHET KAN LIGGE FORAN TRUSSELBILDET

MÅLRETTEDE SVINDELFORSØK FREMSTÅR TROVERDIGE

Med nok tid, nok informasjon fra nett og samarbeid på tvers av grenser kan svindlere kartlegge virksomheten nøye og sende troverdige hendvendelser med godt språk.

- ☐ Kartlegg virksomhetens trusselbilde slik at ansatte er bedre rustet til å avsløre svindelforsøk.
- ☐ Ha klare regler og rutiner rundt transaksjoner. Sentrale spørsmål er: Hvordan kan kontonummer endres på en trygg måte? Hvilke kommunikasjonskanaler er trygge nok? Hvor mange og hvem må godkjenne endringen?

USIKRE UNDERLEVERANDØRER

Underleverandører med lavt nivå av sikkerhet benyttes som en inngang til det egentlige målet.

- ☐ Sørg for å vurdere risiko når man velger leverandører som får tilgang til viktig informasjon. Vurder både leverandøren OG landet den opererer i for å sikre deg at informasjonen blir tatt vare på.

NÅR ER DET NOK MAKSINER OG ENHETER?

Det blir stadig flere enheter og selv i kjente produkter oppdages svakheter og sikkerhetshull.

- ☐ Hold oversikt over all maskinvare som brukes i virksomheten og etabler et system for å regelmessig oppdatere programvare, operativsystem og firmware.
- ☐ Utsatte virksomheter bør vurdere risikoen i private enheter som brukes i arbeidsammenheng. Hvilke arbeidsoppgaver kan trygt utføres fra private maskiner? Hvilke oppgaver kan ikke?

DATAKOMPROMITTERING KAN KOSTE MER ENN OMDØMME

Uansett om datalagringen håndteres av virksomheten selv eller en leverandør er det viktig å vurdere sikkerheten i lagringen. Personvernlover håndheves strengere og uansvarlig datalagring kan få enda større konsekvenser enn tidligere.

- ☐ Still krav til skyleverandør og velg en leverandør som tilfredstiller dine krav til tilgjengelighet, sporbarhet og kontrollmekanismer.
- ☐ En komplett backuprutine reduserer risiko på mange områder. Både utilsiktede feil og alvorlige dataangrep kan føre til tap av data og en god backuprutine reduserer konsekvense betydelig. Test at backuprutinen fungerer ved å tilbakerulle IT-systemer jevnlig.

BENYTT MER ENN PASSORD

Mange bruker samme passord på tvers av tjenester, og mange passord blir skrevet ned slik at «nestemann» får logget inn. Her finnes det enkle løsninger som styrker sikkerheten betraktelig.

- ☐ Unngå kompromitterte brukere og e-poster ved å styrke autentiseringsprosessen:
  - Bruk 2-faktor autentisering med mobil eller annen enhet.
  - Bruk biometrisk data, som fingeravtrykk eller øyeskanning."

Figur 7 Anbefalte sikkerhetstiltak for å imøtekomme fremtidige trusler og faremomenter

8. Referanseliste

1. Næringslivets Sikkerhetsråd, *Nasjonalt Tryggingsorgan - Årsrapporten 2017*. 2017.
2. NorSIS, *Trusler og Trender 2015*. 2015.
3. Nasjonal Sikkerhetsmyndighet, *Risiko 2015*. 2015.
4. Nasjonal Sikkerhetsmyndighet, *Helhetlig IKT risikobilde 2016*. 2016.
5. Næringslivets Sikkerhetsråd, *Mørketallsundersøkelsen 2018*. 2018.
6. Anders Nybakken Kvale, H.H.T., *Hydro: Anslår kostnad på 300 til 350 millioner kroner etter cyberangrepet*, in *E24*. 2019.
7. Greta Hjertø, Bjørn Kleftsad. *Informasjonssikkerhetsstyring*. NTNU
8. Greta Hjertø, Bjørn Klefstad. *Risikoanalyse*. NTNU
9. Bjørn Klefstad, Torstein Hjelle. *Trusselbildet*. 2018 NTNU.
10. Mikalsen, A.B. *Brukermiljø og sikkerhet*. 2018.
11. Olav Dalland, *Metode og oppgaveskriving*. 5. utgave ed. 2012: Gyldendal.
12. Busch, T., *Akademisk skriving - for bachelor- og masterstudenter*. 2013: Fagbokforlaget.
13. Næringslivets Sikkerhetsråd, *Mørketallsundersøkelsen 2016*. 2016.
14. Rolf J. Widerøe, K.L., *Bedragere lurte ansatt til å utbetale en halv milliard kroner*, in *VG*. 2016.
15. Næringslivets Sikkerhetsråd, *Kriminalitets- og sikkerhetsundersøkelen i Norge 2017*. 2017.
16. Trend Micro, *Caught in the Net: Unraveling the Tangle of Old and New Threats.* 2019.
17. Recorded Future, *APT10 Targeted Norwegian MSP and US Companies in Sustained Campaign*. 2019.
18. Marte Halsør, Ø.B.S., Svein Vestrum Olsson, Åsa Vartdal, Olav Døvik,, *Granskarar: Kina hacka norsk selskap*, in *NRK*. 2019.
19. NorSIS, *Trusler og Trender 2017-18*. 2018.
20. NorSIS, *Trusler og Trender 2018-19*. 2019.
21. Nasjonal Sikkerhetsmyndighet, *IKT-risikobilde 2018 - Et sikkert digital Norge.* 2018.
22. Nasjonal Sikkerhetsmyndighet, *Risiko 2018*. 2018.
23. Mnemonic, *Security Report 2019*. 2019.
24. Oda Ording, M.K.V., Birger Kolsrud Jåsund, Anders Brekke, Per Kristian Grimeland, Kjartan Rørslett,, *Hydro utsatt for dataangrep: -Ikke opplevd lignende*, in *NRK*. 2019.
25. Nasjonal SIkkerhetsmyndighet, *Helhetlig IKT-Risikobilde 2015*. 2015.
26. Næringslivets Sikkerhetsråd, *Mørketallsundersøkelsen 2014*. 2014.
27. Nasjonal Sikkerhetsmyndighet, *Helhetlig IKT-risikobilde 2017*. 2017.
28. Nasjonal Sikkerhetsmyndighet, *Risiko 2016*. 2016.
29. Europen Union Agency for Network and Informastion Security, *ENISA Threat Landscape 2014*. 2015.
30. Marthe S. Lien, *PST henlegger etterforskningen av dataangrepet mot Helse Sør-Øst*, in *VG*. 2018.
31. Brombach, H., *Helse Sør-Øst: Datainnbruddet skjedde ikke hos Sykehuspartner*, in *Digi*. 2018.
32. Telenor, *Digital SIkkerhet 2017*. 2018.
33. Jan Roger Wilkens, *Oppsummering av nyhetsbildet innen datasikkerhet for janauar-april 2019*. 2019.
34. Telenor, *Digital Sikkerhet 2018 - Sterkere sammen*. 2018.
35. Nicky Woolf, *DDoS attack that disrupted internet was largest of its kind in history, experts say*, in *The Guardian*. 2016.

36. Nasjonal Sikkerhetsmyndighet, *Risiko 2017*. 2017.
37. Jérôme Segura, *Exploit kits: summer 2018 review*. 2018.

9. Figurliste

Vedlegg A - Følgebrev

Hei!

Vi er to studenter som går Digital forretningsutvikling ved NTNU Trondheim og skriver **bacheloroppgave** om informasjonssikkerhet.

I oppgaven skal vi kartlegge det digitale trusselbilde for norske virksomheter i dag, for fem år siden og i tillegg gjøre en prediksjon for hvordan trusselbildet vil se ut om fem år. Vi skal også gi anbefalinger for hvilke sikkerhetstiltak som bør vurderes for å imøtekomme disse truslene. Vi ønsker derfor å komme i kontakt med fagfolk, IT-bedrifter og andre med kompetanse og erfaring med informasjonssikkerhet som kan komme med innspill. Vi håper det er mulig å avtale et kort intervju med deg for å snakke om det ovennevnte. Om det blir vanskelig å få gjennomført et intervju setter vi også pris på svar via e-post eller et kort telefonintervju. Vi har lagt med spørsmålene vi ønsker å få innspill på. Om dere velger å delta vil dere få tilsendt resultatet av oppgaven så snart den står ferdig.

Med digitalt trusselbilde mener vi alle slags trusler og uønskede hendelser som foregår på digitalt nivå i virksomheter. Eksempler på dette er virus, malware, phishing, sosial manipulering og bedrageri, hacking eller forsøk på inntrenging i nettverk eller sikkerhetssystemer, DDoS-angrep eller tjenestenekt-angrep, trusler om angrep, tap av personopplysninger eller annen informasjon, spam, systemfeil og hendelser forårsaket av virksomhetens ansatte.

Mvh Bendik Øvstedal og Torstein Kårstad

Vedlegg B – Intervjuguide

1: Hva er de største digitale truslene norske virksomheter møter i dag?

2: Hvilke digitale trusler vil vokse frem eller bli mer aktuelle innen fem års tid?

3: Hvilke sikkerhetstiltak bør vurderes for å imøtekomme disse truslene?

4: Hvilke konsekvenser kan det ha for virksomheten dersom den ikke tar trusselbildet på alvor eller lar være å innføre nye sikkerhetstiltak?

5: Er det enkelte områder eller avdelinger i virksomheten som vil bli spesielt utsatt i møte med disse truslene?