UiO : Universitetet i Oslo

Cyberangrep mot kritisk infrastruktur

Emnekode: IN2120

Kandidatnumre: 15785, 15721, 15537

Temanummer: T350

Antall ord: 8421

Dato: 3.11.2021

Innholdsfortegnelse

Introduksjon

Angrep mot kritiske systemer og tjenester hos virksomheter, organisasjoner og institusjoner forekommer hele tiden. Slike angrep medfører som regel et eller flere sikkerhetsbrudd som virksomheten eller organisasjonen må håndtere. Et sikkerhetsbrudd er et brudd på et eller flere sikkerhetsmål for verdier. Sikkerhetsmålene består hovedsakelig av konfidensialitet, integritet og tilgjengelighet (Jøsang, 2021).

Selv om ethvert cyberangrep kan ha negative følger for verdier tilhørende offeret, kan verdier rangeres basert på nasjonale sikkerhetsinteresser. Denne artikkelen studerer cyberangrep mot mål som holder på og beskytter verdier som er en del av de nasjonale sikkerhetsinteressene. Nasjonale sikkerhetsinteresser omfatter mye, blant annet kritisk infrastruktur. Mer spesifikt fokuserer denne artikkelen på *hvordan cyberangrep truer kritisk infrastruktur. Artikkelen studerer generelle motiver til trusselaktører, samt hvordan Norge og dets allierte forholder seg til trusselaktører og trusselscenarier.* Kritisk infrastruktur beskrives som en ressurs eller et system som er avgjørende for opprettholdelsen av nødvendige samfunnsfunksjoner. Eksempler på kritisk infrastruktur er blant annet bank- og finanstjenester, matforsyning, helsetjenester, sosiale tjenester og trygdeytelser, nød- og redningsetater, rettsvesen, forsvar og myndigheter. I Norge er også kommunikasjonsnettverk, strømforsyning, olje- og gass infrastruktur, vannforsyning og avløpshåndtering definert som kritisk infrastruktur (NTNU, u.å.).

NSM, *Nasjonal Sikkerhetsmyndighet*, har en oversikt over hva som inngår i de nasjonale sikkerhetsinteressene. Blant annet består de nasjonale sikkerhetsinteressene av "overordnede sikkerhetspolitiske interesser knyttet til samfunnets grunnleggende funksjonalitet og befolkningens grunnleggende sikkerhet". Videre omfatter dette "verdier som er særskilt utsatt for sikkerhetstruende virksomhet" og "infrastruktur og tjenester som er avgjørende for at sivilsamfunnet skal kunne fungere på en måte slik at øvrige nasjonale sikkerhetsinteresser kan ivaretas" (NSM[8], u.å.). Jo flere verdier en virksomhet besitter, jo større vil konsekvensene av en sikkerhetshendelse mot virksomheten være. Trusselaktører ønsker gjerne å angripe mål med flest verdier for størst mulig vinning. Dersom en trusselaktør har kapasitet til og er motivert til å utføre et angrep mot en virksomhet tilhørende kritisk

infrastruktur, er virksomheten særlig eksponert for en eller flere risikoer. Fordi konsekvensene av cyberangrep mot kritisk infrastruktur er høyst negative for samfunnet generelt, er det verdifullt å studere dette i mer detalj.

Som nevnt, innebærer konsekvensene av et cyberangrep et eller flere sikkerhetsbrudd som den som blir angrepet må håndtere. I forbindelse med angrep på kritisk infrastruktur, har vi identifisert tilgjengelighet som det viktigste sikkerhetsmålet som krever beskyttelse. Et brudd på tilgjengelighet hos kritiske systemer og tjenester kan ha enorme konsekvenser for en virksomhet eller organisasjon tilhørende kritisk infrastruktur. For eksempel er nedetid hos systemer og tjenester tilhørende virksomheter innenfor helsesektoren svært kritisk for vellykket pasientbehandling. Dersom nedetiden er forårsaket av et cyberangrep som medfører et brudd på tilgjengelighet til kritiske funksjoner, kan det i ytterste konsekvens sette liv i fare. Brudd på konfidensialitet og integritet kan også sette liv i fare, men ikke i like stor grad. Slike brudd vil i større grad ramme menneskers øvrige behov, som for eksempel sikkerhet, trygghet, beskyttelse, følelsen av tilhørighet og respekt og anerkjennelse fra andre.

Virksomheter og organisasjoner tilhørende kritisk infrastruktur må naturligvis ivareta konfidensialitet og integritet så vel som tilgjengelighet. Dette er man som oftest pålagt gjennom lover og retningslinjer som har i hensikt å ivareta blant annet personvern. I denne sammenheng anser vi derimot brudd på tilgjengelighet som mer katastrofalt ettersom det kan sette menneskers fysiologiske behov i fare. De fysiologiske behovene omfatter blant annet tilgang til vann, mat, husly, søvn og fysisk aktivitet. Alle øvrige menneskelige behov avhenger av at de fysiologiske behovene er tilfredsstilt.

Trusselaktører har ulike motiver bak angrepene sine. Noen angripere fokuserer hovedsakelig på økonomisk vinning eller spionasje, mens andre ønsker å sabotere infrastruktur eller destabilisere det politiske systemet til en nasjonalstat. I den anledning er det nyttig å studere tidligere angrep på kritisk infrastruktur. Videre vil man få en bedre forståelse omkring hvilke konsekvenser cyberangrep kan ha. Studiet av tidligere angrep kan være nyttig i forbindelse med trusselmodellering. For å kunne forsvare seg mot fremtidige cyberangrep er det relevant å ha kunnskap om tidligere måter et system har blitt angrepet på.

Dersom en sikkerhetshendelse først inntreffer, er håndtering av hendelsen avgjørende for å minimere skade og tap hos den som blir truffet av hendelsen. Norge har flere hendelseshåndteringsteam, såkalte CERT-er (*Computer Emergency Response Team)*, som bistår virksomheter i ulike sektorer med håndtering av sikkerhetshendelser. Det er derimot mye som kan gjøres for å minske risikoen for å bli utsatt for angrep. I forbindelse med fokuset på avverging og håndtering av hendelsen, har vi utført et intervju med sikkerhetsekspert Jørgen Bøhnsdalen fra HelseCERT. Intervjuet ga oss innsikt i hvordan HelseCERT hjelper virksomheter innenfor helse- og omsorgssektoren med detektering av trusler og håndtering av sikkerhetshendelser.

Trusselscenarier

For å få en bedre forståelse av risikoer knyttet til kritisk infrastruktur bør man se på trusselscenarier. Dette innebærer å studere hvordan en trusselaktør kommer seg inn i et system og hvilke angrep trusselaktøren er i stand til å utføre. Et trusselscenario beskrives som en sekvens av trinn eller hendelser som må utføres slik at en eller flere trusselaktører kan nå sitt angrepsmål. I denne sekvensen blir sårbarheter i systemer utnyttet. Med andre ord, må det finnes sårbarheter i datasystemer for at et trusselscenario skal være gjennomførbart (Jøsang, 2021).

Sårbarheter

En sårbarhet er "[...] en svakhet i et datasystem, kjent av minst én aktør som er i stand til å utnytte den til å bryte gjennom systemets sikkerhetsmekanismer." (Dvergsdal, 2019). Med andre ord er en sårbarhet noe en trusselaktør kan utnytte for å skape en sikkerhetshendelse. Dersom en virksomhet ønsker å forhindre et angrep mot seg selv, bør de fokusere på sårbarhetene som medfører størst risiko for virksomheten. Det finnes hovedsakelig to kategorier av sårbarheter; kjente og ukjente sårbarheter. Det er imidlertid de ukjente sårbarhetene som utgjør størst risiko. Dette er sårbarheter som enda ikke har blitt oppdaget eller sårbarheter som har blitt feilvurdert (Skar, 2020).

Sårbarheter som medfører størst risiko mot kritisk infrastruktur er såkalte *nulldagssårbarheter*. Dersom en trusselaktør utnytter en nulldagssårbarhet har man null dager til å beskytte seg (Dvergsdal, 2019). Det kan ta flere år før en slik svakhet i systemet blir oppdaget, noe som gjør det vanskelig å forsvare seg mot angrep som utnytter disse sårbarhetene. I forbindelse med dataormen Stuxnet ble det utnyttet fire nulldagssårbarheter. Videre var dataormen i sirkulasjon i ca. et halvt år før den ble oppdaget (Britannica, 2016). Dersom man er bevisst en risiko før en sårbarhet utnyttes av en trusselaktør, kan man redusere sannsynligheten for at en sikkerhetshendelse inntreffer ved å iverksette sikkerhetstiltak. Dette er derimot ikke tilfelle ved nulldagssårbarheter. Den som blir angrepet grunnet utnyttelsen av en slik sårbarhet, vil sannsynligvis være nødt til å bruke alle sine ressurser på å rette opp i konsekvensene av angrepet.

Hvordan sårbarheter oppdages og utnyttes

For å oppdage nulldagssårbarheter i et system bruker trusselaktøren ulike angrepsvektorer som Drive-by-angrep, MITM, og Brute force. De mest brukte angrepsvektorene i dag sikter som oftest ikke til en svakhet i selve datasystemet, men til svakheter som brukerne av systemet besitter. Ifølge statistikk fra The Human Report 2019 krevde over 99% av trusselscenarier som cybersikkerhetsselskapet Proofpoint observerte i 2018 menneskelig interaksjon for å være finne sted (Proofpoint, 2019, s.2). For eksempel må en trusselaktør overtale en bruker til å laste ned en fil med skadevare. For å få til dette må trusselaktøren bruke sosial manipulasjon. Proofpoint er et av verdens ledende cybersikkerhetsselskap, som i 2020 analyserte 2.2 milliarder e-poster daglig (Proofpoint, 2021, s.2).

Ved sosial manipulering forsøker en trusselaktør å påvirke et offer gjennom psykologiske virkemidler for å få tak i informasjon eller utføre handlinger. Et offer kan for eksempel påvirkes ved å påføre offeret en form for tidspress eller "friste" offeret med økonomiske muligheter (Nätt, 2020). Den mest brukte formen for sosial manipulering i dag er phishing, mer spesifikt e-post phishing. Da sender trusselaktøren en overtalende e-post for å få noen til å for eksempel kjøre en fil, laste ned et vedlegg eller følge en lenke. I et intervju med Jørgen Bøhnsdalen fra HelseCERT ble det nevnt at e-post phishing er en av de mest brukte

angrepsvektorene (J. Bøhnsdalen, intervju, 2021 27. oktober). Ifølge statistikk presentert av Verizon ble 94% av skadevare sendt med e-post i 2018 (Verizon, 2019, s.13)

Ettersom phishing e-poster ofte brukes av angripere, er det tenkelig at bedrifter fokuserer på metoder for å forsvare seg mot slike angrep. Det viser seg at dette er tilfelle, men ikke i tilstrekkelig grad. Ifølge 2021 State of Phish Report viste det seg at blant 60 millioner simulerte phishing e-poster fra 2020 var det 12% som ble et offer for lenke-baserte phishing e-poster, 4% som ble et offer for inntastings-baserte phishing e-poster og 20% som ble et offer for vedlegg-baserte phishing e-poster (Proofpoint, 2021, s.9). Det faktum at opp imot 20% av de som mottok en phishing e-post ble et offer angrepet, forteller mye om den digitale sikkerhetskulturen mange er en del av i dag. Modenhet og kognisjon omkring sikkerhet er viktigere enn aldri før. Dette oppnås gjennom blant annet god sikkerhetsstyring og bevissthetstrening. Dette vil utredes i mer detalj senere.

Samtidig som phishing e-poster er en av de vanligste måtene for en trusselaktør å infiltrere et system på, blir også andre angrepsvektorer brukt. Ved angrep på deler av kritisk infrastruktur trenger ikke en trusselaktør å sikte til å infiltrere hele datasystemet. For å bryte ned kritisk infrastruktur kan trusselaktøren angripe kontrollsystemene direkte.

Flere virksomheter tilhørende kritisk infrastruktur krever at kontrollsystemene er tilgjengelig til enhver tid. For eksempel, kan kontrollsystemer hos virksomheter tilhørende energisektoren ha kjørt i flere tiår uten å ha blitt slått av eller gått igjennom en omstart. Dette er et problem ettersom mange sikkerhetsoppdateringer krever at systemet går igjennom en omstart. Som følge av at man unngår å restarte systemer og foreta sikkerhetsoppdateringer, kan systemene innad i kontrollsystemene bli utdaterte og mangle oppdateringer som skal tette sikkerhetshull. Dette gjør kontrollsystemene hos en virksomhet særlig utsatt for angrep (Layne, 2017, s.15). Dette er noe trusselaktører i land som Kina, USA og Russland har utnyttet ved forskjellige anledninger.

Når en trusselaktør har fått tilgang til et system, er det naturlig å tro at trusselaktøren umiddelbart infiserer systemet med skadevare. Dette stemmer derimot ikke alltid. Jørgen Bøhnsdalen fra HelseCERT forklarer at det er mange vinningskriminelle som prøver å få

tilgang til systemer for å selge tilgangen til systemene på såkalte *Initial Access Broker Markets* (J. Bøhnsdalen, intervju, 2021, 27. oktober). Initial Access Broker Markets er et marked hvor vinningskriminelle kan selge tilgang til datasystemer. Initial Access Broker Markets blir ofte brukt av vinningskriminelle i et løsepengeskadevare-angrep. Flere trusselaktører har altså er motiv som innebærer å tjene mest mulig penger på å skaffe og selge tilgang til systemer, fremfor utføre et cyberangrep.

Skadevare

Etter å ha kommet seg inn i systemet på egen hånd eller ved å kjøpe tilgang til systemet, blir resten av cyberangrepet ofte utført ved bruk av skadevare. Skadevare er "[...] et vidt begrep som beskriver ondartet programvare som benyttes av en angriper som har til hensikt å skade eller misbruke virksomhetens IT-systemer for egne hensikter" (NSM, 2021). Det finnes flere typer skadevare. Ulike skadevarer opererer på forskjellige måter og har ulike funksjoner og hensikter.

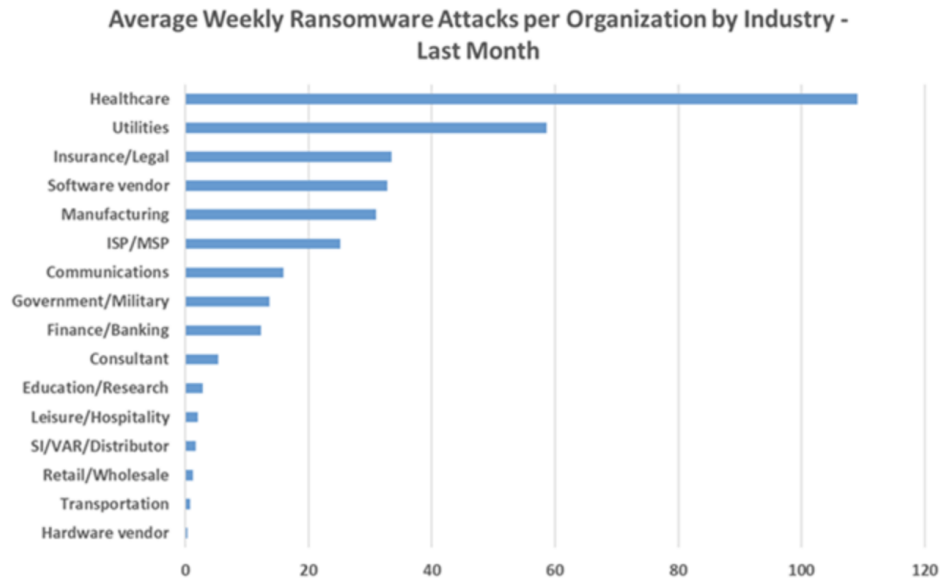
Når det gjelder angrep på kritisk infrastruktur er det viktig å se på hvor destruktivt en skadevare kan være. Som vi allerede har identifisert er tilgjengelighet som regel det viktigste sikkerhetsmålet ved kritisk infrastruktur. Det er fordi brudd på tilgjengelighet vanligvis medfører nedetid hos kritiske systemer og tjenester. Det som tilsynelatende virker mest truende for tilgjengeligheten til kritisk infrastruktur er løsepengeskadevare.

Løsepengeskadevare er "[...] en type skadevare som låser eller krypterer hele eller deler av innholdet på datamaskinen. Målet er å få brukeren til å betale løsepenger til angriperen." (Nettvett, 2021). De som eier dataene, blir som regel bedt om å betale penger til løsepengegruppen for å kunne dekryptere dataene. Dersom en maskin infiseres med løsepengeskadevare, forårsaker det vanligvis et brudd på tilgjengelighet. Jørgen Bøhnsdalen fra HelseCERT forklarer hvordan trusselaktører ofte opererer før de infiserer maskiner med løsepengeskadevare. Bøhnsdalen forklarer at angrepsmønsteret har endret seg betraktelig de siste 4-5 årene. Tidligere var det vanlig at trusselaktører krypterte enkelt-maskiner. I senere tid har man observert at trusselaktører forsøker å kompromittere så mye som mulig og få full kontroll over systemene før de krypterer. Bøhnsdalen nevner at de nye angrepsmetodene gjør trusselaktørene i stand til å utrette mest mulig skade (J. Bøhnsdalen, intervju, 2021, 27.

oktober). Videre forekommer løsepengeskadevare angrep som oftest i slutten av en angrepskjede. Et løsepengeskadevare angrep rammer ofte de som er mest utsatt, i form av sårbarheter og verdier, slik at angriperne kan få størst mulig gevinst. Kritisk infrastruktur holder på mange verdier og er dermed svært utsatt.

MIT Technology Review har beskrevet tiden vi er inne i som en løsepengevirus-krise (O'Neill, 2021). I 2017 estimerte FBI at det kommer til å bli utbetalt opp i mot 1 milliard amerikanske dollar hvert år til vinningskriminelle (Rosenstein, 2017). Dette estimatet har økt betraktelig. Ifølge Alejandro N. Mayorkas, sikkerhets sekretær ved Sikkerhetsdepartementet i USA, økte antall løsepengeskadevare angrep med 300% fra 9. september 2020 til 9. september 2021 (Mayorkas, 2021). Denne utviklingen er kanskje ikke overraskende med tanke på at man har blitt mer avhengig av teknologi under pandemien. For å unngå økonomiske kriser i flere deler av verden, var tilgang til hjemmekontor essensielt. Det er tenkelig at systemer og tjenester ble mer sårbare for angrep etter hvert som flere jobbet hjemmefra. Dette var en særlig risiko for de som arbeider med kritisk infrastruktur.

Systemer og tjenester som er del av kritisk infrastruktur utsettes regelmessig for løsepengeskadevare. I nyere tid har løsepengegrupper vist seg å være svært sofistikerte og målrettet (Norsk Helsenett[1], u.å.). Figur 1 nedenfor er produsert av cybersikkerhetsselskapet, Checkpoint. Figuren viser at helsesektoren var den sektoren som ble mest utsatt for løsepengeskadevare-angrep ved utgangen av april 2021 globalt (Checkpoint, u.å.).



Figur 1. "Gjennomsnitt av løsepengeskadevare angrep ved ulike sektorer april 2021", u.d., av Checkpoint, (https://blog.checkpoint.com/2021/05/12/the-new-ransomware-threat-triple-extortion/). CC BY-NC-ND 2.0.

Virksomheter innenfor helsesektoren behandler menneskeliv, noe av det mest verdifulle i samfunnet. Fordi verdiene som behandles er såpass store, er mulighetene for å kreve enorme summer ved bruk av løsepengeskadevare betydelige. Som følge av store verdier, øker risikoen for å bli utsatt for cyberangrep. Ifølge sjefssikkerhetsforsker ved Cisco, Joseph Carson, er cyberkriminelle villige til å angripe hvem som helst med løsepengeskadevare. Ethvert selskap eller organisasjon kan derfor bli et mål. Dette gjelder til og med sykehus, selv om konsekvensene kan være fatale (Germain, 2021). Dersom systemer blir utilgjengelig hos virksomheter innenfor helsesektoren kan det ha alvorlige konsekvenser for pasientene. Brudd på tilgjengelighet fører til at funksjoner blir mer tidkrevende. I forbindelse med pasientbehandling er tid svært verdifullt. Ved siden av løsepengeskadevare-angrep, finnes det andre eksempler på angrep som kan hindre tilgjengelighet til systemer og tjenester. Et eksempel på dette er DDoS angrep.

DDoS angrep - angrep uten tilgang til datasystemet

Vanligvis må en trusselaktør ha tilgang til et datasystem før de kan utføre sikkerhetshendelser. DDoS angrep kan derimot gjøre trusselaktører i stand til å utføre sikkerhetshendelser uten å ha tilgang til et datasystem. DDoS er en engelsk forkortelse som på norsk står for distribuert tjenestenekt. DDoS beskrives som cyberangrep «hvor angriperen forsøker å hindre at legitime

brukere får tilgang til en tjeneste eller informasjon» (Nettvett[2], 2020). «Den vanligste formen for tjenestenektangrep er å oversvømme nettstedet med trafikk» (Nettvett[1], 2020). Dette blir ofte gjort ved bruk av et botnet. Et botnet er en samling infiserte datamaskiner som blir kontrollert av såkalte gjetere. Eierne av de infiserte maskinene vet som oftest ikke at deres maskin er del av et botnett før gjeteren begynner å angripe. Ved noen tilfeller blir man aldri klar over at ens maskin har vært eller er del av et botnett (Nettvett[1], 2020).

Et DDoS angrep gjør som oftest systemer og tjenester utilgjengelig, noe som har alvorlige konsekvenser i forbindelse med kritisk infrastruktur. I mai 2021 ble den belgiske internettleverandøren *Belnet* hardt rammet av et DDoS-angrep. Over 200 belgiske organisasjoner var helt eller delvis uten internett i et døgn. Organisasjonene som ble rammet var utdannings- og forskningsinstitusjoner, samt en rekke offentlige tjenester. Angrepet resulterte ikke i noe utover tjenestenekt, men det er et eksempel på hvor stor påvirkning et DDoS angrep kan ha på kritiske systemer og tjenester (Knudsen, 2021).

Antall DDoS angrep følger en stigende trend. Ifølge trusselrapporten til sikkerhetsselskapet Netscout, ble det i 2020 ble registrert over 10 millioner DDoS angrep. Dette var en økning på 20% fra året før (Knudsen, 2021). DDoS angrep rammer også Norge. I 2019 ble det gjort 3825 DDoS-angrep mot Telenor. Det tilsvarer over 300 angrep hver måned på Telenor sine tjenester alene (Martinsen, 2020).

Slik som ved løspengeskadevare angrep er det som oftest vinningskriminelle som utfører DDoS-angrep. Angrepene er gjerne politisk motivert. DDoS-angrep er ofte nøye planlagt og blir gjerne utført i kritiske perioder for den som blir angrepet. Tjenestenekt kan kombineres med andre type angrep for å utvide det totale skadeomfanget. I 2015 ble Ukraina utsatt for et cyberangrep mot kontrollsystemene til et strømforsyningsselskap. Angrepet medførte brudd på strømtilførsel i et bestemt område. Da angriperne fulgte opp det første angrepet med et TDoS (*Telephony Denial of Service*) angrep, kunne ikke kundene kommunisere med leverandøren og melde fra om strømbruddet. Som følge av dette varte strømbruddet i opptil seks timer (Zetter, 2016). TDoS ble altså kombinert med andre angrepsmetoder for å forårsake mest mulig skade.

Det finnes flere eksempler på løsepengeskadevare angrep og tjenestenektangrep som har hatt katastrofale konsekvenser for deler av kritisk infrastruktur i ulike verdensdeler. Ved å studere forløp til tidligere cyberangrep, konsekvenser av angrepene og motivasjon hos trusselaktørene, vil man få en bedre forståelse omkring cyberangrep. Forståelsen kan bidra til å identifisere fremtidige trusler. I beste fall kan man forhindre fremtidige angrep ved å studere tidligere angrepsmønstre.

Trusselaktører og tidligere cyberangrep mot kritisk infrastruktur

Cyberangrep har allerede vist seg som svært sofistikerte og nøye gjennomført mot en rekke konkrete kritiske mål. Skadevare har vært i stand til å sette ut atomkraftverk, forstyrre gassrørtransportsystemer og ta kontroll over kontrollsystemer som er del av kritisk infrastruktur, på tvers av kontinenter. Angrep av dette kaliberet krever en enorm kapasitet, kompetanse og gjennomføringskraft, hvor kun noen få grupperinger på verdensbasis har ressursene til å kunne stå bak. Disse angrepene er nærmest utelukkende begått av såkalte APT-er (kort for *Advanced Persistent Threat*) mot mål av nasjonale interesser. En APT er en trusselaktør som ofte tilhører eller er sponset av en nasjonalstat.

Blant nasjoner med gjentakende historikk innen cyberkriminalitet rettet mot transnasjonale mål, finner vi blant annet Kina, Russland og USA. Vi vil i mer detalj se på noen konkrete tidligere angrep mot kritisk infrastruktur.

Kina

Allerede på 90-tallet ble Kina utpekt av det amerikanske energidepartementet som en akutt etteretningstrussel mot USAs atomvåpenprogram, da det ble klart at Kina bedrev cyberspionasje mot USA. Det ble avslørt at en forsker ved Los Alamas National laboratoriet hadde oversendt over tusen dokumenter med klassifisert informasjon om landets atomvåpenprogram til Kinesiske myndigheter (Gerth, Risen, 1999).

Kina, med en befolkning på 1,4 milliarder mennesker, har et unikt taktisk fortrinn ved at de kan gjennomføre cyberangrep i stor skala, fremfor få sofistikerte cyberangrep. Fordi Kina har muligheten til å gjennomføre såpass mange angrep, lykkes de oftere. Vedvarende sårbarheter

i moderne datateknologi hjelper også Kina i å lykkes. Ved siden av dette fremstår de tilsynelatende likegyldige i å bli avslørt. Disse faktorene gjør Kina til en særlig trussel.

Det amerikanske sikkerhetsdepartementet (*Department of Homeland Security*) rapporterte i 2013 at kinesiske hackere hadde klart å hacke 23 amerikanske gasslinjeselskaper over en seks-måneders periode. Fra desember 2011 til juni 2012 sendte kinesiske cyber spioner phishing e-poster til nøkkelpersonell i en rekke utvalgte gasslinje-selskaper. E-postene ble utformet for å lure mottakerne til å klikke på malisiøse lenker eller vedlegg som inneholdt ondsinnet kode som lot angriperne få tilgang til selskapets nettverk (Clayton, 2013).

Mer spesifikt ble det installert skadevare som søkte seg gjennom nettverkets datamaskiner og lette etter filer som inneholdt sekvensen «SCAD» (kort for *Supervisory Control and Data Acquisition* (SCADA). Dette er kontrollsystemer som overvåker og styrer det operasjonelle ved gasslinje-selskapene, som for eksempel gasspumpestasjoner, trykknivåer, ventiler og kommunikasjon. Filene ble deretter stjålet, og angriperne fikk alt de trengte for å få full tilgang til – og kontroll over – gasslinje-selskapenes operasjonelle drift (Clayton, 2013).

Sikkerhetsdepartementet konkluderte i sin endelige rapport om cyberangrepene slik: “The data exfiltrated could provide an adversary with the capability to access US [oil and natural gas industrial-control systems], including performing unauthorized operations” (CISA, 2021). Departementet legger altså ikke skjul på alvorlighetsgraden av sikkerhetshendelsen. William Rush, en pensjonert forsker med ekspertise på gasslinjeteknologi, uttalte seg derimot noe mer nådeløst om de potensielle katastrofale utfallene av angrepene: “Anyone can blow up a gas pipeline with dynamite. But with this stolen information, if I wanted to blow up not one, but 1,000 compressor stations, I could” (Clayton, 2013). De potensielle effektene av dette angrepet, hvis fullt utnyttet, er naturligvis alvorlige for kritisk infrastruktur. Store deler av USAs gassinfrastruktur kunne blitt lammet og holdt gissel, og gitt både staten og den sivile befolkningen store utfordringer i lang tid. I USA står gass for nesten 30 % av landets totale kraftnett. Dette viser viktigheten av solide standarder innen cybersikkerhet for private selskaper, spesielt innenfor kritisk infrastruktur og andre områder av stor nasjonal interesse.

Kinesiske myndigheter på sin side benekter å ha noen som helst tilknytning til cyberangrepene. Likevel er USAs sikkerhetsdepartement sikker i sin sak. CISA og FBI tror

formålet med angrepet var å hjelpe Kina med å utvikle sine evner innenfor cyberangrep mot kritisk infrastruktur, samt for å skade eller forstyrre amerikanske rørtransportsystemer og den operasjonelle driften rundt det (CISA, 2021).

Ekspert og medgrunnlegger av Critical Intelligence, Robert Huber, foreslår at Kina kan ha hatt flere motiver bak cyberangrepene mot de amerikanske gasslinjeselskapene, utover det CISA og FBI konkluderer med. Han sier at Kina kan ha hatt interesse av selskapenes industrihemmeligheter for forskning innenfor naturgassutvinning (Clayton, 2013). Ved å stjele teknologi relatert til hydraulisk frakturering av skifer for utvinning av naturgass, også kalt *fracking*, kan Kina forbedre sine egne teknologier for utvinning av naturgass.

USA

USA har derimot ikke kun vært *offer* for cyberangrep mot gassinfrastruktur. I 1982 eksploderte store deler av Sovjetunionen sitt rørtransportsystem i Sibir som følge av et cyberangrep. Eksplosjonens skadeomfang anslås å tilsvare tre tonn TNT (The Archive, 2013). Angrepet regnes som det første cyberangrepet med betydelige konsekvenser for kritisk infrastruktur.

USA avdekket at Sovjetunionen hadde benyttet stjålet amerikansk teknologi og la dermed en plan for å lure Sovjet til å stjele og ta i bruk programvare infisert med skadevare. I forkant av angrepet hadde USA derfor tillatt Sovjetunionen å stjele programvare for rørtransportkontrollsystemer fra et kanadisk selskap. Den stjålne programvaren inneholdt en trojan som var programmert til å øke trykknivået kraftig ved trykktester. Dette forårsaket til slutt den enorme eksplosjonen (Risidata, u.å.).

Sabotasjen hadde to effekter. Den første var økonomisk. Sabotasjen forstyrret en viktig del av Sovjetunionens gassforsyning og med det en viktig inntektskilde. Det saboterte rørtransportsystemet var forventet å generere 8 milliarder amerikanske dollar i årlig inntekt. Eksplosjonen førte altså til at Sovjetunionen opplevde store økonomiske tap (The Archive, 2013). Den andre effekten var psykologisk. Forholdet mellom USA og Sovjetunionen under den kalde krigen var som kjent svært konfliktfylt. Sabotasjen bidro til å gi USA et psykologisk overtak. Sovjetunionen hadde over en lengre periode stjålet vestlig teknologi. Det var en reell fare for at mye av teknologien de hadde stjålet var infisert av skadevare. De

hadde ikke mulighet til å vite hvilke teknologier som var trygge å bruke og hvilke som var infiserte. Alt kunne potensielt være infisert.

Etter hvert som teknologiverden har blitt stadig mer avansert, har nasjoner forbedret sine evner til å forsvare seg mot og utføre cyberangrep. Analytikere mener USA star bak de mest sofistikerte cyberangrepene hittil, med skadevare som Stuxnet, Duqu, Flame og Gauss (Geers, Kindlund, Moran, Rachwald. 2014). Denne familien av skadelig programvare er helt uten sidestykke i sin kompleksitet og effektivitet.

Stuxnet, den mest kjente av de nevnte skadevarene, var en dataorm som, i motsetning til tradisjonelle dataormer som søker etter å skade så mange datamaskiner som mulig, var svært selektiv når det kom til å utrette skade. Dataormen var programmert til å utelukkende angripe industrielle kontrollsystemer knyttet til Irans atomprogram. Den utnyttet blant annet hele fire nulldagssårbarheter og hadde evnen til å omprogrammere logiske styringer (PLS), samt skjule sine endringer. Man kan skrive mye om Stuxnet sin kompleksitet, men det essensielle er hvordan Stuxnet og andre skadevarer utviklet av USA på mange måter har definert skadevare sitt øvrige potensial for ødeleggelse. Stuxnet var vellykket i sin operasjon og ødela nesten en femtedel av Irans atomsentrifuger (Kelley, 2013).

Cyberoperasjonen var i stor grad politisk motivert. USA ønsket å svekke Irans atomprogram og deres evne til å utvinne uran. Til tross for at USA aldri har innrømmet at de stod bak angrepet, uttalte det Hvite Hus sin koordinator for Arms Control and Weapons of Mass Destruction, Gary Samore, i 2011 følgende i et intervju med det amerikanske TV-programmet *Need To Know*: “We're glad they [the Iranians] are having trouble with their centrifuge machine and that we – the U.S. and its allies – are doing everything we can to make sure that we complicate matters for them” (Broad, Markoff, Sanger. 2011). Samore kommer altså med et tydelig hint hvor han nærmest bekrefter mistanken om at det var amerikanerne som stod bak dataormen som satte ut store deler Irans atomprogram. Å forstyrre Irans atomprogram er for USA et mål i seg selv. Dette gjør de for å styrke sin egen posisjon og svekke Iran sin posisjon.

Russland

Det har vært overraskende lite aktivitet fra Russland på cyberangrepsfronten. Dette kan blant annet forklares med at Russland i større grad begår cyberangrep mot organisasjoner og virksomheter innenfor egne landegrenser, samt mot naboland. Dette er ikke uvanlig blant autoritære styresett (Geers, Kindlund, Moran, Rachwald. 2014).

Russland har stått bak mange av de mest komplekse cyberangrep kampanjene hittil, antakelig kun overgått av USA. Man har sett at russiske hackere har strukket seg uvanlig langt for å forsøke å skjule sin identitet og sine mål. Blant annet har de gjennomført såkalte «false flag»-operasjoner, der de har designet sine angrep for å se ut som de kommer fra Asia (Geers, Kindlund, Moran, Rachwald. 2014).

I 2012 rapporterte det russiske sikkerhetsselskapet Kaspersky Lab om en pågående cyberangrepskampanje. Kampanjen spionerte på millioner av privatpersoner over hele verden, men hovedsakelig på privatpersoner i Russland og land som tidligere hadde vært en del av Sovjetunionen. Mål inkluderte blant annet ambassader, militærbaser, energiforsyning selskaper og annen kritisk infrastruktur (Geers, Kindlund, Moran, Rachwald. 2014). Det regnes som sannsynlig at russiske myndigheter sto bak angrepene. Angrepene kan forklares ved at russiske myndigheter ønsker kontroll over sin befolkning, samt organer som opererer i og rundt Russland.

Da Ukrainas kraftnett ble utsatt for et cyberangrep i 2015, ble rundt 230 000 ukrainere ble uten strøm i flere timer. Cyberangrepet var det første vellykkede cyberangrepet mot et kraftnett, og fant sted under en pågående militær konflikt mellom Russland og Ukraina. Som nevnt hindret tjenestenektangrepet på kraftnettets kundeservice-telefon strømkunder i å få informasjon og melde ifra om situasjonen (Zetter. 2016). Til tross for at cybersikkerheten til kraftnettet i utgangspunktet var av høy standard, klarte angripere å få tilgang til kraftnettets SCADA-nettverk, kraftnettets kontrollsystem, etter flere måneder med kompromittering.

Angrepet startet med en e-post phishing-kampanje rettet mot IT-ansvarlige og systemadministratorer for en rekke ulike selskaper som var ansvarlig for strømdistribusjon i Ukraina. E-postene inneholdt et Word-dokument som ba mottakeren om å tillate macros for

dokumentet når mottakeren åpnet det. Ved godkjennelse ble det installert en bakdør på offerets datamaskin, som ga angriperne adgang til bedriftsnettverket.

Angriperne måtte derimot fremdeles få tilgang til SCADA-nettverket, som var adskilt med en brannmur fra bedriftsnettverket. I løpet av de neste månedene klarte angriperne å få tilgang til Windows Domain Controllers som håndterer brukere på nettverket. Her fanget de opp innloggingsdetaljer tilhørende de ansatte, blant dem innloggingsdetaljer for en VPN brukt for ekstern pålogging på SCADA-nettverket (Zetter. 2016). Kontrollsystemets svake punkt lå i at det ikke krevde to-faktor-autentisering for ekstern pålogging på SCADA-nettverket via VPN. Som følge av dette fikk angriperne full tilgang til kraftnettets kontrollsystem.

Det er verdt å merke seg at kort tid før angriperne utførte cyberangrepet som forårsaket strømbruddet i Ukraina, hadde pro-ukrainske aktivister på Krim-halvøya fysisk angrepet strømforsyningsstasjoner som leverte strøm til det russisk-annekterte området. Angrepet etterlot to millioner innbyggere på Krim-halvøya – samt en russisk militærbase – uten strøm. Man tror derfor, med god grunn, at det påfølgende strømbruddet kan ha vært en gjengjeldelse av det tidligere angrepet.

Det spekuleres mye rundt motivet til angrepet. Det er derimot bred enighet om at angriperne sannsynligvis ikke hadde planlagt å utføre angrepet på det tidspunktet det ble utført, siden de kunne utrette mye mer skade om de hadde ventet og planlagt angrepet i mer detalj. For eksempel hadde ukrainske myndigheter på den tiden planlagt en nasjonalisering av landets kraftnett som på daværende tidspunkt i stor grad var eid av private selskaper. Flere av disse selskapene var eid av mektige russiske oligarker med nære bånd til Vladimir Putin. Det er mulig at et av motivene bak angrepet var å sende et signal til ukrainske myndigheter om å ikke nasjonalisere kraftnettindustrien i landet (Zetter. 2016).

Tjenestenektangrepet mot kundeservice-telefonen kan også ha hatt sitt eget formål utover dets rolle i angrepet mot kraftnettet, nemlig å vekke irritasjon hos ukrainske innbyggere og svekke deres tillit til de ukrainske myndighetene og kraftselskapene.

Diskusjon

Akkurat som at hvert enkelt land har sin egen kultur, historie og politiske system, har statssponsede cyberangrep også sine særtrekk. Dette gjelder motiver bak angrep, strategier og metoder. Man ser for eksempel at Kina i større grad fokuserer på kvantitet fremfor kvalitet i sine angrep, at USA typisk benytter seg av høyt sofistikerte cyberangrep for å oppnå politiske mål og at Russland fokuserer på mål nærme seg selv geografisk.

Cyberangrep mot kritisk infrastruktur er sjeldent uten motiv. Når land står som aktør, utføres angrepene for å oppnå mål som til syvende og sist reflekterer deres bredere strategiske mål; enten det er å sabotere andre land sin atomvåpen utvikling, justere maktbildet eller å svekke noen økonomisk. Statssponsede cyberangrep gjenspeiler dermed på mange måter tradisjonell krigføring.

For å kunne forsvare seg mot cybertrusler er det viktig å ha kompetanse omkring cyberangrep. Utvikling og gjennomføring av cyberangrep mot kritisk infrastruktur har på mange måter en forebyggende effekt. Angrep kan hjelpe med å styrke egen infrastruktur, samt ha en avskrekkende effekt på fiender. Nasjoner utvikler og gjennomfører angrep mot bestemte mål for å vise styrke. Dersom angrepene gjennomføres av land med sterk kompetanse omkring cyberangrep, sender landene et signal til andre land om at de ikke må tro at de kan utføre alvorlige cyberangrep mot kritiske mål uten å forvente en gjengjeldelse. Et eksempel på dette er da pro-ukrainske aktivister angrep Krim-halvøya sin strømforsyning og Russland gjengjeldte handlingen umiddelbart. Cyberangrep er altså en brikke i nasjoner sitt forebyggende cyberforsvar, akkurat på samme måte som et sterkt militært forsvar virker avskrekkende for andre land.

Kritisk infrastruktur er definitivt blant de mest utsatte målene for statlige cyberangrep. Angrep mot slike mål kan ha enorme konsekvenser for de som er avhengige av at infrastrukturen er tilgjengelig. På den annen side er de positive konsekvensene betydelige for aktørene som står bak. Kritiske mål holder gjerne på mye verdier. Altså er inntjeningen stor for trusselaktører som lykkes i sine cyberoperasjoner.

Selv om statene har mange insentiver til å investere i cybersikkerhet, utgjør datasystemer kontrollert av private selskaper og organisasjoner en risiko. Disse selskapene og

organisasjonene setter ofte ikke cybersikkerhet høyt nok på agendaen, noe som utgjør en stor risiko mot statlige organer og kritisk infrastruktur. Den kinesiske hackingen av 23 amerikanske gasslinje selskap i 2011-2012, er et godt eksempel på dette. Selskapene som ble rammet hadde ikke gode nok protokoller for å motstå uautorisert tilgang sine nettverk. Dette resulterte i at gassrørtransportsystemer over store deler av landet ble kompromittert og sårbare for mulige sabotasjeangrep.

Likevel er cyberangrep mot kritisk infrastruktur tross alt sjeldent begått av vinningskriminelle med standard angrepsmetoder, men heller av sofistikerte, statssponsede grupper. Trusselaktøren må vise enorm styrke og kapasitet for å gjennomføre omfattende angrep mot kritiske mål. Det har vist seg at man aldri kan føle seg helt trygg, skulle man bli utsatt for et statssponset cyberangrep. Behovet for håndtering av sikkerhetshendelser dannet en gang i tiden grunnlaget for fremveksten av såkalte CERT-er. CERT står for *Computer Emergency Response Team* og arbeider med å avverge, avdekke og håndtere alvorlige sikkerhetshendelser. Norge har en rekke ulike CERT-er.

Hvordan forholde seg til trusler

CERT – Hendelseshåndteringsteam

For å redusere risikoen for angrep er virksomheter nødt til å implementere sikkerhetstiltak som reduserer sårbarheter. Arbeidet omkring informasjonssikkerhet er et satsningsområde både nasjonalt og internasjonalt. Virksomheter som er en del av kritisk infrastruktur, får kontinuerlig veiledning og oppfølging fra CERT-er. En CERT er en koordinert enhet bestående av sikkerhetseksperter som arbeider med cybersikkerhet og hendelseshåndtering vedrørende en eller flere organisasjoner, virksomheter eller sektorer (Sullivan, 2021). Noen CERT-er jobber med informasjonssikkerheten til en spesifikk sektor, som for eksempel HelseCERT. I tillegg til domenespesifikke CERT-er, har Norge også en nasjonal CERT, NorCERT, som i større grad arbeider med hendelseshåndtering på tvers av sektorer.

NorCERT

NorCERT er en av funksjonene i Nasjonalt Cybersikkerhetssenter (NCSC) og har som formål å styrke Norges forsvar i den digitale verden. Hovedoppgavene til NorCERT er først og fremst å ivareta informasjonssikkerhet og respondere på cybertrusler. Dette oppnås blant annet ved hjelp av gode rutiner for varsling. NCSC arbeider med å opprettholde et nasjonalt sensornettverk som skal detektere dataangrep på kritisk infrastruktur på tvers av sektorer (NSM[1], u.å.) (NSM[2], 2020).

Det nasjonale sensornettverket omtales gjerne som *Varslingssystem for digital infrastruktur* (VDI) og omfatter virksomheter som anses å være en del av norsk kritisk sektor. Det blir plassert ut sensorer hos virksomhetene, som skal detektere og håndtere trusler mot IKT-sikkerheten til virksomheten. Sensorene skal oppdage mistenkelig atferd og rapportere ved behov. VDI er et sammensatt system som er under stadig utvikling (NSM[3], 2020). Det er avgjørende at cyberforsvaret til kritiske funksjoner oppdateres med jevne mellomrom slik at man er forut for ondsinnet cyberaktivitet. En trusselaktør vil alltid prøve å utnytte sårbarheter som enda ikke er oppdaget og utvikle angrepsmetoder som ikke vekker oppmerksomhet. Et godt varslingssystem krever at man har evnen til å tenke som en trusselaktør og definere mistenkelig atferd.

NorCERT er døgnbemannet for å foreta akutt varsling og kontinuerlig oppdatering av det digitale risikobildet. Systemeiere og enkeltpersoner kan følge med på oversikten over varsler som avdekker sårbarheter i systemer og informerer om viktige oppdateringer (NSM[4], u.å.). På denne måten kan virksomheter oppdatere sine systemer basert på råd fra sikkerhetseksperter i Nasjonal Sikkerhetsmyndighet. Fordi tjenesten er lett tilgjengelig, er det enkelt for virksomheter å iverksette de nødvendige tiltakene for å ta hensyn til en eventuell sårbarhet. På den annen side, er det lett for potensielle angripere å utnytte de sårbarhetene som finnes. Dersom en angriper får fatt på slik informasjon før en systemeier har angriperen tid på seg til å utnytte sårbarheten. Forhåpentligvis blir kritisk sektor varslet i god tid før informasjonen om sårbarheter og oppdateringer offentliggjøres.

Mens NorCERT og NCSC har et overordnet ansvar for cybersikkerhet i Norge, finnes det sikkerhetseksperter og hendelseshåndteringsteam som fokuserer på sikkerhetsinteresser angående spesifikke sektorer. Forskjellige sektorer preges gjerne av ulike trusselbilder og risikoer. Kartlegging av sårbarheter, trusler og verdier hos utvalgte virksomheter og sektorer er nødvendig for å utarbeide virksomhet- og sektorspesifikke strategier for hendelseshåndtering.

Cyberangrep mot helse- og omsorgssektoren – trusselbilde og hendelseshåndtering

Ifølge Norsk Helsenett er statsstøttede grupperinger (APT) den prominente trusselaktøren mot norsk helsesektor. APT-er truer tjenester innenfor helse- og omsorgsektoren gjennom blant annet overvåkning og datatyveri. Videre nevner Norsk Helsenett at det er en betydelig risiko for at trusselaktører vil bedrive skadevarekampanjer rettet mot IKT-systemer hos virksomheter innenfor helsesektoren. Det nevnes også at det er mulig at andre nasjonalstater vil angripe norsk e-helseinfrastruktur i et ønske om å destabilisere nasjonale helsesystemer (Norsk Helsenett[1], u.å.).

Basert på risikobildet som beskrives ovenfor, er det tydelig at trusselaktører har et ønske om å svekke tilgjengeligheten til kritiske funksjoner. Som tidligere nevnt, dersom tilgjengeligheten til nødvendige tjenester innenfor helsevesenet svekkes som følge av infiserte maskiner eller systemer, kan det ha fatale konsekvenser for pasientbehandlingen. Jørgen Bøhnsdalen fra HelseCERT nevner at dødsfall, redusert livskvalitet, redusert behandlingskvalitet og lekkasje av sensitiv pasientinformasjon er blant de verst-tenkelige-scenariene for pasienter og virksomheter innenfor helsesektoren (J. Bøhnsdalen, intervju, 2021, 27. oktober). Det er liten tvil om at beskyttelsen av helse- og omsorgssektoren er en svært viktig del av de nasjonale sikkerhetsinteressene. For vellykket pasientbehandling må behandlingstilbudet til helsevesenet være operativt til enhver tid. Altså bør systemer og tjenester hos virksomhetene ha en nedetid tilnærmet 0 %.

Løsepengeskadevare truer oppetiden til systemer og tjenester på maskiner som infiseres. Det er flere eksempler på angrep der løsepengeskadevare har redusert behandlingskapasiteten til sykehus. I september 2020 ble et sykehus i den tyske byen Düsseldorf hardt rammet av et

løsepengevirus. Akuttmottaket på sykehuset ble stengt som følge av at den digitale infrastrukturen på sykehuset ble kompromittert. Systemet som koordinerte leger, senger og behandlinger var nede. Historien om en kvinnelig pasient som mistet livet samme dag har fått flere til å hevde at dataangrepet forårsaket kvinnens død. Kvinnen skulle i utgangspunktet få akutt behandling på sykehuset som ble rammet av angrepet, men måtte sendes til et sykehus lenger unna. Dermed ble pasientbehandlingen utsatt. Det er vanskelig å bevise hvorvidt døden til kvinnen var en direkte konsekvens av dataangrepet (Norsk Helsenett[1], u.å.) (Ralston, 2020). Hendelsen er allikevel en pekepinn på hvor alvorlig konsekvensene av et angrep på helsesektoren kan være. Tilgjengeligheten til digitale systemer og tjenester er svært viktig for et operativt og velfungerende helsetilbud. Det arbeides aktivt med å styrke IKT-sikkerheten til virksomheter innenfor helse- og omsorgssektoren. HelseCERT er et norsk hendelseshåndteringsteam som fokuserer på nettopp dette.

HelseCERT

HelseCERT fokuserer på å detektere, avverge og håndtere truende cyberoperasjoner mot helse- og omsorgssektoren (Norsk Helsenett[2], u.å.). Jørgen Bøhnsdalen fra HelseCERT sier at oppgavene til enheten blant annet består av trussel-etterretning, bistand ved hendelser, sårbarhetsskanning og skadevareanalyse (J. Bøhnsdalen, intervju, 2021, 27. oktober). Enheten arbeider kontinuerlig med å oppdatere trusselbildet som preger det norske helsevesenet og spre kunnskap omkring IKT-sikkerhet til virksomheter innenfor sektoren.

HelseCERT fokuserer stort på forebyggende arbeid angående cybersikkerhet. I 2018 gjennomførte CERT-en inntrengningstester for flere norske kommuner og andre sentrale tjenester. På denne måten får man oversikt over tilstanden til sikkerhetssystemer hos virksomheter. Testene bidro til å avdekke sårbarheter samt nødvendige tiltak for å begrense disse (Regjeringen, 2018). Videre kan virksomheter i helsesektoren få bistand ved behov for hendelseshåndtering gjennom deltakelse i *Nasjonalt Beskyttelsesprogram for helse- og omsorgssektoren* (NBP). NBP sørger også for at deltakere blir informert om trusler, sårbarheter og relevante hendelser (Norsk Helsenett[3]). Sårbarheter i virksomhetenes egne systemer og tjenester avdekkes gjerne ved hjelp av sårbarhetsskanning. Sårbarhetsskanning er et av flere sikkerhetstiltak som anbefales av HelseCERT.

En del av arbeidet til HelseCERT innebærer å informere virksomheter innenfor helsesektoren om hvilke sikkerhetstiltak som bør iverksettes for å redusere konsekvensene av cyberangrep. Ifølge Jørgen Bøhnsdalen er det ikke tilstrekkelig med perimetersikring. I tillegg til å sikre perimeter bør man aktivt identifisere og detektere trusler internt i nettverket. Bøhnsdalen forklarer at HelseCERT har sitt eget sensornettverk som brukes for å oppdage og etterforske cyberangrep. I forbindelse med nettverkstrafikk kan man logge flere typer data som er nyttige ved en hendelse, som IP-adresser og DNS-oppslag, samt kjøre signaturbasert deteksjon som kan oppdage angrep. Bøhnsdalen nevner at skadevare ofte har en unik trafikk som kan identifiseres og fanges opp ved hjelp av sensornettverket (J. Bøhnsdalen, intervju, 2021, 27. oktober).

Utenom sensornettverket, finnes det flere anbefalte sikkerhetstiltak. Et av tiltakene går nærmere inn på *klientsikkerhet*. Tiltakene angående klientsikkerhet er opprinnelig utarbeidet av NSM, og kan ifølge Helsenett hindre 90% av alle dataangrep (NSM[5], u.å.). Tiltakene fokuserer blant annet på viktigheten ved å oppgradere program- og maskinvare regelmessig. Eldre systemer har ofte flere sikkerhetshull enn nyere systemer og er derfor mer sårbare. Altså øker risikoen for å bli utsatt for et dataangrep. Man oppfordres også til å foreta oppdatering av programvare ved varsel om sårbarheter (Norsk Helsenett[4], u.å.). Videre, forklarer HelseCERT hvorfor blokkering av skript og programfiler er et effektivt tiltak for å forhindre at ondsinnet kode eksekveres på maskiner hos virksomhetene. Enkle tiltak som filtrering av filtyper kan beskytte mot flere typer skadevare, som for eksempel løsepengevirus (Norsk Helsenett[5]).

Det er derimot ikke nødvendigvis tilfelle at enhver virksomhet behøver å implementere samme sett med sikkerhetstiltak. Kombinasjonen av verdier og sårbarheter hos en virksomhet samt hvilke trusler virksomheten er eksponert for, avgjør hvilke sikkerhetstiltak virksomheten bør implementere. For at en virksomhet skal vite hvilke tiltak som bør implementeres må det foreligge en eller flere risikovurderinger. Utformingen av en slik vurdering krever at man identifiserer trussel-scenarioer, sårbarheter, verdier og hendelser som kan inntreffe. Kombinasjonen av det man identifiserer sier noe om hvilke konsekvenser sikkerhetshendelsen har. I denne sammenheng er det mest interessant å fokusere på hendelser

med negative følger for virksomheter. Videre bør det gjøres en vurdering av sannsynligheten for at hendelsen inntreffer. Kartlegging av sannsynlighet avhenger av identifisering og analysering av flere faktorer, som motivasjon og kapasitet til trussel-aktør og muligheten til å utnytte en eller flere sårbarheter. Dersom man kombinerer sannsynligheten for at hendelsen inntreffer og konsekvensen av hendelsen får man informasjon angående risikonivået til hendelsen. Risikonivået avgjør hvorvidt virksomheten bør fokusere på tiltak for å minske risikoen (Jøsang, 2021).

HelseCERT er en god pådriver for informasjonssikkerhet hos virksomheter innenfor helse- og omsorgssektoren, men til syvende og sist er det ledelsen og de ansatte i hver enkelt virksomhet som avgjør hvorvidt de anbefalte tiltakene trer i kraft. De ansatte må ha god kunnskap omkring informasjonssikkerhet, samt realistiske tanker og oppfatninger om temaet. Gjennom atferd og handling må hver enkelt ansatt sørge for at sikkerhet ivaretas. Kunnskap, holdninger og atferd hos de ansatte, er derimot et resultat av kvaliteten på sikkerhetsstyringen hos virksomheten. Dette foretas i all hovedsak av ledelsen. Ledelsen må definere klare retningslinjer og prosedyrer som setter standarden for ivaretakelsen av informasjonssikkerhet. Modenhet og kognisjon omkring sikkerhet hos de ansatte er en direkte følge av en motivert og informert ledelse. Ledelsen må være bevisst alle fordelene det medfølger å drive strukturert og målrettet sikkerhetsstyring. Videre må sikkerhetsekspertene i virksomheten sørge for god kommunikasjon med ledelsen og de ansatte. Da blir alle som er en del av virksomheten informert angående trusler og risikoer virksomheten står overfor. Det er også viktig at ledelsen definerer klare ansvarsområder, slik at de ansatte er bevisst sitt ansvar omkring sikkerhetstiltak. De ansatte må gjennomgå regelmessig bevissthetstrening slik at de får økt kompetanse innen sikkerhet og blir oppdatert på trusselbildet og metoder for sosial manipulasjon (NSM[6], u.å.) (Jøsang, 2021).

I løpet av de 10 årene Jørgen Bøhnsdalen har jobbet i HelseCERT hevder han å ha opplevd økt modenhet omkring sikkerhet hos virksomheter innenfor helsesektoren. Han nevner at særlig spesialisthelsetjenesten er bevisst omkring viktigheten av sikkerhet (J. Bøhnsdalen, intervju, 2021, 27. oktober). Fordi større virksomheter er mer ressurssterke enn mindre virksomheter er de i stand til å sette av mer fokus, tid og penger til sikkerhetsarbeid. HelseCERT er derimot en viktig ressurs for ledelsen og sikkerhetseksperter i enhver

virksomhet som er en del av helsesektoren. Enheten opplyser virksomhetene om trusler, risikoer og sårbarheter, og bistår virksomhetene ved behov for hendelseshåndtering. For HelseCERT er samarbeid med andre sikkerhetseksperter en viktig ressurs for å styrke sitt eget arbeid omkring cybersikkerhet.

Bøhnsdalen fra HelseCERT understreker viktigheten av å samarbeide med andre hendelseshåndteringsteam og sikkerhetseksperter. HelseCERT har flere samarbeidspartnere både i Norge og i andre land. Slike samarbeid legger hovedsakelig fokus på informasjonsdeling. Dersom noen har informasjon om konkrete trusselaktører eller trusselscenarier, er det nyttig å videreformidle slik informasjon til samarbeidspartnere (J. Bøhnsdalen, intervju, 2021, 27. oktober). Dette kan bidra til å minske risikonivået til en sikkerhetshendelse hos enkelte virksomheter. HelseCERT både holder og deltar på forumer og seminarer med sikkerhet som tema. På tvers av fagmiljøer og landegrenser utveksles erfaring og kompetanse innenfor sikkerhet og hendelseshåndtering. Verdien av organisert og strukturert samarbeid er stor. Med en felles interesse om å styrke informasjonssikkerhet, kan aktørene drøfte sårbarheter, trusselbilder og tiltak seg imellom.

Internasjonalt samarbeid

Som følge av globalisering, internett og digitalisering har nasjoner og stater blitt mer sammensveiset enn de en gang var. Det finnes en rekke eksempler på dataangrep som har rammet flere land samtidig. Konsekvensene av angrepene varierer selvsagt basert på verdier, trusler og sårbarheter hos hver enkelt virksomhet i hvert enkelt land. Det er allikevel svært verdifullt å sammenlikne hvilke følger et angrep fikk for de som ble utsatt. Det er tenkelig at noen nasjoner eller virksomheter ble hardere rammet enn andre. Hvordan lyktes noen i å forsvare seg mot et angrep, mens andre ble et offer? Å drøfte grunner til disse forskjellene er essensielt i videreutvikling av sikkerhetssystemer. Allerede i 1990 så man et behov for en koordinert samarbeidsplattform. FIRST (*Forum of Incident Response and Security Teams)* ble den gang stiftet, og har siden vokst til å bli en ledende organisasjon innenfor hendelseshåndtering (FIRST[1], u.å.). Både NorCERT og HelseCERT er medlem av FIRST.

Formålet til FIRST er å effektivisere respons og håndtering av sikkerhetshendelser for å minske konsekvensene av et angrep. Organisasjonen fokuserer på viktigheten ved informasjonsutveksling mellom medlemmer og samarbeid om felles interesser (FIRST[2], u.å.). FIRST har over 500 medlemmer bestående av både hendelseshåndteringsteam og enkeltpersoner. Én av tjeneste FIRST tilbyr til sine medlemmer er såkalte tekniske seminarer/konferanser *(eng. "Technical Colloquia and Symposia").* Dette er en begivenhet som arrangeres av FIRST, eventuelt i samarbeid med lokale team eller sponsorer. Det som gjennomgås på seminarene er gjerne mer praktisk-rettet enn teknisk. Seminaret skal tilrettelegge for diskusjon og gjestene skal kunne utveksle informasjon om sårbarheter, hendelser og metoder som påvirker hvordan hendelseshåndteringen i de ulike teamene utføres. Lokale sikkerhetseksperter deltar gjerne seminarene. Deltakerne inndeles i mindre grupper, der de interagerer med hverandre og jobber sammen med en sikkerhetsekspert på ulike tekniske temaer (FIRST[3], u.å.). Jørgen Bøhndalen fra HelseCERT mener organisasjoner som FIRST er nyttige når det gjelder nettverksbygging med andre sikkerhetseksperter (J. Bøhnsdalen, intervju, 2021, 27. oktober).

I 2014 ble cyberforsvar en del av NATO sine hovedoppgaver når det gjelder kollektivt forsvar. NATO har uttalt at organisasjonen ønsker å forsvare seg like godt i cyberdomenet den gjør på andre domener. I likhet med FIRST fokuserer også NATO-medlemsland på betydningen av å utveksle informasjon og erfaring med hverandre og andre allierte. Gjennom øvelser, trening og undervisning har NATO en visjon om å styrke medlemslandenes og organisasjonens cyberforsvar. Det finnes flere sentre og fasiliteter som tilbyr utdanning samt praktiske øvelser angående sikkerhet og forsvar. Organisasjonen tilrettelegger for at medlemsland kan utvikle og vedlikeholde praksiser som de ellers ikke ville hatt kapasitet til på egenhånd. Utover dette, forventes det at medlemmer bistår med hendelseshåndtering og annen assistanse dersom et NATO-medlem utsettes for cyberangrep. NATO har også et eget beredskaps- og hendelseshåndteringsteam som skal hjelpe allierte ved behov. Ved siden av samarbeidet mellom medlemsland, har NATO inngått et samarbeid med EU gjennom *Technical Arrangement on Cyber Defense.* Også dette samarbeidet fokuserer på kompetanse- og informasjonsdeling (NATO[1]).

Samarbeid mellom virksomheter, organisasjoner og nasjonalstater er nødvendig for å styrke digitale forsvar. Gjennom seminarer, forumer og øvelser utveksler deltakere informasjon og metoder for hendelseshåndtering med hverandre. Dette er essensielt i forbindelse med effektivisering av proaktivt og reaktivt sikkerhetsarbeid. Truende cyberaktivitet tar verken hensyn til geografiske eller organisatoriske grenser.

Det fremtidige trusselbildet - kunstig intelligens (KI)

Fremtidens trusselbilde kan endre seg drastisk. Land som Kina og USA har allerede investert milliarder i å utvikle avansert kunstig intelligens. Utviklingen av KI betyr at angrep kan utføres med lite menneskelig innblanding. Med andre ord kan KI bli i stand til å utføre cyberangrep nærmest på egenhånd. KI brukes allerede av trusselaktører for å øke sjansene for at cyberangrep lykkes. For eksempel kan KI brukes til å samle inn data for å lage kvalitetssikre phishing e-poster og metoder som *deepfake* kan brukes til å lure biometriske autentiseringsmekanismer. Fremtidig teknologi kan bety at tradisjonell cybersikkerhet ikke lenger er tilstrekkelig for å avverge, detektere og håndtere cyberangrep. Verdien av å analysere tidligere angrep kan bli mindre, da fremtidige angrep kan ha annerledes hendelsesforløp (Technology Review, 2021). På den annen side er det tenkelig at KI kan brukes for å styrke cybersikkerhet og forsvare seg mot angrep. Bruk av KI i sikkerhetsarbeid er allerede tilfelle.

Konklusjon

Ved å studere tidligere cyberangrep mot kritisk infrastruktur er det tydelig at nasjonalstater evner å oppnå de samme tilsiktede effektene som kunne blitt oppnådd ved bruk av tradisjonell, militær krigføring. Kritisk infrastruktur er av den grunn et populært mål for APT-er som ønsker å oppnå politiske, økonomiske og militære effekter med sine angrep. Cyberangrep mot kritisk infrastruktur skiller seg på mange måter fra ordinær cyberkriminalitet ved at angrepene kan oppfattes som krigshandlinger.

For å redusere risikoen for cyberangrep må sikkerhetseksperter fokusere på hvilke angrepsvektorer og sårbarheter trusselaktører tar i bruk og utnytter. Sårbarhetene som utnyttes

omfatter i stor grad menneskelige svakheter og nulldagssårbarheter. Datasystemer hos kritisk infrastruktur bør designes og videreutvikles med så få svakheter som mulig. Videre er det nødvendig med gode protokoller slik at utnyttelse av menneskelige svakheter ikke utsetter datasystemer for sikkerhetshendelser.

Vi har sett eksempler på undersøkelser der simulerte phishing e-poster har lurt opp imot 20 % av mottakerne. Dette er skremmende statistikk. I forbindelse med datasystemer hos kritisk infrastruktur, er det særlig viktig at systemene utformes på måter som minsker konsekvensene av phishing-kampanjer. Datasystemene bør utformes på en måte som hindrer at ondsinnet, eksekverbar kode kan sendes gjennom e-poster eller e-postvedlegg. E-post phishing kampanjer er den vanligste angrepsvektoren for infiltrering av systemer. Det er nok at kun én ansatt i en virksomhet lar seg kompromittere, for at hele virksomheten rammes av en sikkerhetshendelse.

Med andre ord er det avgjørende at virksomheter, organisasjoner og institusjoner overholder et tilstrekkelig sikkerhetsnivå. For å oppnå og opprettholde god cybersikkerhet, får virksomheter god oppfølging fra CERT-er og andre sikkerhetseksperter. CERT-ene bistår virksomheter med detektering av trusler og håndtering av hendelser. Videre gir CERT-ene kvalitetssikre anbefalinger omkring relevante sikkerhetstiltak. Implementering av egnede sikkerhetstiltak er avgjørende for å tette sikkerhetshull og redusere risikoen for å bli utsatt for cyberangrep. Sensornettverkene til NorCERT og HelseCERT er eksempler på verktøy som kan identifisere og fange opp mistenkelig atferd på et nettverk. Dette kan bidra til å avdekke uvedkommende som har klart å infiltrere nettverket.

Så lenge det finnes sårbarheter i datasystemer, vil trusselaktører forsøke å utnytte sårbarhetene. Og så lenge det utvikles nye datasystemer vil nye sårbarheter oppstå. Dette er en realitet som sikkerhetseksperter må ta stilling til hver eneste dag. Datasystemer hos kritisk infrastruktur er særlig eksponert for risikoer, da kritisk infrastruktur forvalter store verdier. Det er nødvendig å ha informasjon om hvilke trusselaktører man står overfor, sårbarheter som kan bli utnyttet og verdier som kan skades for å forsvare seg mot ondsinnet cyberaktivitet. God risikovurdering og risikohåndtering er avgjørende for å hindre trusselaktører i å nå sine mål.

Referanseliste

- Britannica. (2016, 23. november). Stuxnet. Hentet fra https://www.britannica.com/technology/Stuxnet
- Broad, W. J, Markoff, J, Sanger D. E. (2011). Israeli Test on Worm Called Crucial in Iran Nuclear Delay. *The New York Times*. Hentet fra https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html
- Checkpoint. (u.å.). The New Ransomware Threat: Triple Extortion. Hentet fra https://blog.checkpoint.com/2021/05/12/the-new-ransomware-threat-triple-extortion/
- Clayton, M. (2013). Exclusive: Cyberattack leaves natural gas pipelines vulnerable to sabotage. *The Christian Monitor*. Hentet fra https://www.csmonitor.com/Environment/2013/0227/Exclusive-Cyberattack-leaves-natural-gas-pipelines-vulnerable-to-sabotage
- Cyber Intelligence & Infrastructure Security Agency (CISA). (2021, 21. juli). Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013. Hentet fra https://us-cert.cisa.gov/ncas/alerts/aa21-201a
- Dvergsdal, H., Nätt T., H. (2019, 2. desember). Sårbarhet (IT). *Store Norske Leksikon.* Hentet fra https://snl.no/sårbarhet_-_IT
- FIRST[1]. (u.å.) FIRST history. Hentet fra https://www.first.org/about/history
- FIRST[2]. (u.å.) About FIRST. Hentet fra https://www.first.org/about/
- FIRST[3]. (u.å.). Technical Colloquia & Symposia. Hentet fra https://www.first.org/events/colloquia/
- Geers, K., Kindlund, D., Moran, N., Rachwald, R. (2014). World War C: Understanding nation-state motives behind today's advanced cyber attacks. *California, Estados Unidos: FireEye*.
- Germain, J.M. (2021, 16. februar). The Future of Cybersecurity in 2021 and beyond. Tech News World. Hentet fra https://www.technewsworld.com/story/the-future-of-cybersecurity-in-2021-and-beyond-87018.html
- Gerth, J., Risen, J. (1999, 2. mai). 1998 Report Told of Lab Breaches and China Threat. *The New York Times*.
- Jøsang, A. (2021, 15. oktober). IS-ledelse og sikkerhetskultur. Forelesning presentert ved Universitetet i Oslo.
- Jøsang, A. (2021, 22. oktober). Risikostyring. Forelesning presentert ved Universitetet i Oslo.
- Jøsang, A. (2021, 28. oktober). Risikostyring. Forelesning presentert ved Universitetet i Oslo.
- Jøsang, A. (2021). Informasjonssikkerhet - Teori og praksis (1. utg). Oslo: Universitetsforlaget.
- Kelley, M. B., (2013, 20. november). The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought. *Business Insider.* Hentet fra https://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11
- Knudsen, E. (2021, 6. mai). Massivt DDoS-angrep lammet store deler av Belgia. *Digi*. Hentet fra https://www.digi.no/artikler/massivt-ddos-angrep-lammet-store-deler-av-belgia/509933
- Layne, C. (2017, august). Cyber attacks against critical infrastructure (Del av mastergradsavhandling). *Utica College*. ProQuest.
- Martinsen, H. (2020, 20. februar). Har du råd til at nettsiden din blir utilgjengelig? *Telenor*. Hentet fra https://www.telenor.no/bedrift/blogg/sikkerhet/tjenestenektangrep/

- NATO[1]. (2021, 2. juli). Cyber defence. Hentet fra https://www.nato.int/cps/en/natohq/topics_78170.htm
- Nätt, T. H. (2020, 28. april). sosial manipulering. *Store Norske Leksikon*. Hentet fra https://snl.no/sosial_manipulering_-_datasikkerhet
- Nätt, T. H. (2019, 29. november). Tjenestenekt. *Store Norske Leksikon*. Hentet fra https://snl.no/tjenestenekt
- Nätt, T. H. (2021, 27. oktober). Botnett. *Store Norske Leksikon.* Hentet fra https://snl.no/botnett
- Nettvett[1]. (2020, 13. januar). Botnet. Hentet fra https://nettvett.no/botnet/
- Nettvett[2]. (2020, 13. januar). DDoS-Angrep. Hentet fra https://nettvett.no/ddos-angrep/
- Nettvett. (2021, 19. mai). Løsepengevirus. Hentet fra https://nettvett.no/losepengevirus/
- NHO, (2018, 30. april). Hva er et cyberangrep? Hentet fra https://arbinn.nho.no/Medlemsfordeler/medlemsfordeler-nho/nho-forsikring/sporsmal-og-svar/hva-er-et-cyberangrep/
- Norsk Helsenett[1]. (u.å.). Situasjonsbilde 2021. Hentet fra https://www.nhn.no/Personvern-og-informasjonssikkerhet/helsecert/situasjonsbilde-2021
- Norsk Helsenett[2]. (u.å.). HelseCERT. Hentet fra https://www.nhn.no/Personvern-og-informasjonssikkerhet/helsecert
- Norsk Helsenett[3]. (u.å.). Nasjonalt beskyttelsesprogram (NBP). Hentet fra https://www.nhn.no/Personvern-og-informasjonssikkerhet/helsecert/nasjonalt-beskyttelsesprogram-nbp
- Norsk Helsenett[4]. (u.å.). Klientsikkerhet. Hentet fra https://www.nhn.no/Personvern-og-informasjonssikkerhet/helsecert/anbefalte-sikkerhetstiltak/klientsikkerhet
- Norsk Helsenett[5]. (u.å.). Blokkering av script og programfiler. Hentet fra https://www.nhn.no/Personvern-og-informasjonssikkerhet/helsecert/anbefalte-sikkerhetstiltak/blokkering-av-script-og-programfiler
- NSM[1]. (u.å.). Norwegian National Cyber Security Centre (NCSC) and NorCERT. Hentet fra https://nsm.no/areas-of-expertise/cyber-security/norwegian-national-cyber-security-centre-ncsc/
- NSM[2]. (2020, 24. juni). Hendelseshåndtering. Hentet fra https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/handtering-av-dataangrep/hendelseshandtering
- NSM[3]. (2020, 3. juni). Varslingssystem for digital infrastruktur (VDI). Hentet fra https://nsm.no/tjenester/varslingssystem-vdi/
- NSM[4]. (u.å.). Varsler fra NCSC. Hentet fra https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/varsler-fra-ncsc/
- NSM[5]. (u.å.). Sjekkliste: Fire effektive tiltak mot dataangrep. Hentet fra https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/sjekkliste-fire-effektive-tiltak-mot-dataangrep/
- NSM[6]. (u.å.). Grunnprinsipper for personellsikkerhet. Hentet fra https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-personellsikkerhet/opprettholde-og-oppdage/skape-en-god-sikkerhetskultur/
- NSM[7]. (2021, 30. juni). Tiltak mot skadevare og løsepengevirus. Hentet fra https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/skadevare/tiltak-mot-skadevare-og-losepengevirus

- NSM[8]. (u.å.). Nasjonale sikkerhetsinteresser. Hentet fra https://nsm.no/nasjonale-sikkerhetsinteresser/category1193.html
- NTNU. Critical Infrastructures Security and Recilience (CISR). Hentet fra https://www.ntnu.edu/ccis/cisr#/view/publications
- Mayorkas, N.A (2021, 9. september) Secretary Mayorkas Delivers Remarks at the National Press Club. Hentet fra https://www.dhs.gov/news/2021/09/09/secretary-mayorkas-delivers-remarks-national-press-club
- O'Neill, P. H. (2021, 3. juni). Why the ransomware crisis suddenly feels so relentless. *MIT Technology Review.* Hentet fra https://www.technologyreview.com/2021/06/03/1025679/explainer-is-ransomware-getting-worse/
- Proofpoint. (2019). The Human Factor 2019. Hentet fra https://www.exclusive-networks.com/se/wp-content/uploads/sites/25/2020/12/gtd-pfpt-us-r-human-factor-2019.pdf
- Proofpoint. (2021). The Human Factor 2021. Hentet fra https://proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-human-factor-report.pdf
- Ralston, W. (2020, 11. september). The untold story of a cyberattack, a hospital and a dying woman. *Wired.* Hentet fra https://www.wired.co.uk/article/ransomware-hospital-death-germany
- Regjeringen (2018). Årsrapport 2018. Hentet fra https://www.regjeringen.no/globalassets/departementene/hod/tildeling-oppdrag-og-arsrapporter/2018/arsrapport-nhn2018.pdf
- Risidata. (u.å.). CIA Trojan Causes Siberian Gas Pipeline Explosion. Hentet fra https://www.risidata.com/index.php?/Database/Detail/cia-trojan-causes-siberian-gas-pipeline-explosion
- Rosenstein, R.J. (2017, 4. oktober). Deputy Attorney General Rod J. Rosenstein Delivers Remarks at the Cambridge Cyber Summit. Hentet fra https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-cambridge-cyber-summit
- Skar, K. (2020, 21.august). *Datasikkerhet: Innledning, definisjoner og begreper. Sikkerhetsmål og sikkerhetstiltak.* Forelesning presentert ved Universitetet i Oslo.
- Sullivan, P. (2021, mars). Computer Emergency Response Team (CERT). *TechTarget.* Hentet fra https://whatis.techtarget.com/definition/CERT-Computer-Emergency-Readiness-Team
- Technology review. (2021, 8. april). Preparing for AI-enabled cyberattacks. Hentet fra https://www.technologyreview.com/2021/04/08/1021696/preparing-for-ai-enabled-cyberattacks/
- The Archive (2013). Agent Farewell and the Siberian Pipeline Explosion. *Unredacted*. Hentet fra https://unredacted.com/2013/04/26/agent-farewell-and-the-siberian-pipeline-explosion/
- Verizon (2019). 2019 Data Breach Investigations Report. Hentet fra https://www.phishingbox.com/assets/files/images/Verizon-Data-Breach-Investigations-Report-DBIR-2019.pdf
- Zetter, K. (2016). Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. *Wired*. Hentet fra https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/