Hvilket trusselbilde står norske virksomheter overfor, og hvordan kan åpenhet bidra til å forstå cyberrisiko?

SILJE AAKRE er nærings-ph.d.-kandidat i NC-Spectrum AS og tilknyttet handelshøgskolen ved Nord universitet. Hun forsker på cybersikkerhet i kraftbransjen.

SAMMENDRAG

Formålet med artikkelen er å formidle hvilke cybertrusler som dominerer, og hvordan trusselbildet kommuniseres og bør kommuniseres for å gi bedre grunnlag for styring av cyberrisiko. Artikkelen presenterer en definisjon av cyberrisiko og går gjennom aktuelle trusselvurderinger for norske virksomheter. Den anvender teori om kjente og ukjente risikoer og presenterer en modell for hvordan kommunikasjon og åpenhet om risiko kan forstås og bidra til økt situasjonsforståelse. Trusselvurderingene er hentet fra fire myndighetsaktører og to organisasjoner. Analysen viser de mest framtredende cybertruslene og slår fast at cyberrisiko også blir viet betydelig oppmerksomhet i de generelle trusselvurderingene.

INNLEDNING

Samfunnet går fra analogt til digitalt på mange arenaer. Dette gjelder blant annet kjøp og salg av tjenester, offentlig administrasjon, kommunikasjon og kriminalitet. Digitalisering, kunstig intelligens, maskinlæring, smarte løsninger, skytjenester, tingenes internett og stordata skal gi utallige muligheter for økt innovasjon, effektivitet og velferd.

Medaljens bakside er sårbarheter knyttet til teknologi og bruk. Hver gang en ny digital løsning tas i bruk, manifesteres tilhørende risiko. Selv om digitaliseringen kan være en døgnflue, «noe man må skrive om fort, før det blir gammeldags igjen» (Andersen & Sannes, 2017, s. 18), har utfordringene knyttet til cyberrisikoer kommet for å bli. Uønskede cyberhendelser har et bredt spekter og innebærer alt fra nettverksskanninger og datainnbrudd som ikke blir avdekket, til e-post med sensitiv informasjon sendt til feil adresse og omfattende løsepengevirus.

Når «alt skal ha en app» og «alle går over i skyen», følger det med nye sårbarheter og risikoer. Innsamling, lagring, bearbeiding og tilgjengeliggjøring av informasjon er sjelden risikofritt. Da Rema 1000 ønsket å samle og behandle kunders kontaktinformasjon, kjøpsvaner og lokasjon i appen Æ, var det en risiko for at informasjonen kunne komme på avveier. Kort tid etter lanseringen av Æ meldte en forbruker at kundebasen lå åpent tilgjengelig (Gundersen, 2017). Myndigheter og forbrukere forutsetter at sikkerhet er ivaretatt. Dette, kombinert med virksomheters bruk og avhengighet av digitale arbeidsverktøy, kommunikasjonskanaler og tjenester, fordrer at tilhørende cyberrisiko blir en naturlig del av virksomheters risikostyring.

Styring av cyberrisiko kan være krevende fordi risikoene ikke er observerbare og håndfaste som de fleste risikoer i det fysiske rom. Like fullt trengs kompetanse om risiko og kunnskap om trusler for å håndtere risikoen. En forutsetning for å håndtere risiko er informasjon. Gjennomgang av relevant informasjon kan betegnes som første ledd i risikostyring (Aven & Renn, 2010, s. 121). Én lett tilgjengelig kilde til informasjon om cyberrisiko er myndighetenes trusselvurderinger og risikorapporter.

Formålet med artikkelen er å formidle hvilke cybertrusler som dominerer, og hvordan trusselbildet kommuniseres i rapportene. I artikkelen blir det bygget videre på teori om kjente og ukjente risikoer og utviklet en modell for å illustrere hvordan informasjonsutveksling og kommunikasjon kan redusere det ukjente og gi bedre grunnlag for styring av cyberrisiko.

KJENTE OG UKJENTE RISIKOER

Kategoriseringen av hendelser som *kjente kjente, kjente ukjente* eller *ukjente ukjente* ble lagt merke til under en pressekonferanse med USAs daværende forsvarsminister, Donald Rumsfeld, i 2002. Temaet var krigen i Irak. Ordleggingen har fått både pepper og skryt. Han formulerte at det eksisterer kjente kjente – ting vi vet at vi vet. Det eksisterer kjente ukjente – ting vi vet at vi ikke vet. Sist, men ikke minst, eksisterer ukjente ukjente – ting vi ikke vet at vi ikke vet. Det er ifølge Rumsfeld sistnevnte kategori vi bør bekymre oss for (Rumsfeld, 2002). I denne kategorien faller hendelsene vi ofte kaller sorte svaner. Dette er hendelser som er utenkelige for de fleste før de inntreffer, som massakren på Utøya 22. juli 2011. Det har senere blitt argumentert for at ukjente kjente – ting vi ikke vet at vi vet, beskrevet som underbevisstheten – også bør inkluderes (Žižek, 2006, s. 137). De fire kategoriene framstilles ofte som et vindu med fire ruter. Selv om modellen fort ble populær, har flere påpekt utfordringer – blant annet hvorvidt kjente ukjente og ukjente kjente kan eksistere samtidig, eller om den ene leder til den andre (Marshall, Ojiako, Wang, Lin, & Chipulu, 2019, s. 647).

På bakgrunn av dette foreslås en modell (figur 1) som illustrerer hvordan to parter sammen har et bilde av en situasjon, et fenomen, en risiko eller lignende. Modellen skal bidra til å forklare samspillet mellom to parter som har mulighet for informasjonsutveksling. Feltene kan behandles som vinduer hvor vinduets størrelse angir andelen kjent og ukjent kunnskap av totalbildet.

FIGUR 1 Enkel framstilling av kjent og ukjent kunnskap for to parter.

		A	
		Kjent	*Ukjent*
B	*Kjent*	*KJENT (kjent kjent)*	*FORDEKT (ukjent kjent)*
	Ukjent	*FORDEKT (kjent ukjent)*	*UKJENT (ukjent ukjent)*

Informasjonsutveksling kan være ett tiltak for å utvide det kjente vinduets størrelse samtidig som det helt eller delvis ukjente reduseres. Dette bygger på grunntanken om at læring er mulig. Siden partene har ulik kunnskap om totalbildet (feltene for det kjente og ukjente), er problemstillingene knyttet til om alle fire felt kan eksistere samtidig, mindre relevant.

Inkluderingen av hva som er kjent og ukjent for en motpart, kan minne om Joharis vindu. Joharis vindu viser feltene (og trekkene) åpen, skjult, blind og ukjent (Luft & Ingham, 1955, referert i Zahl-Begnum & Begnum, 1990, s. 140). Trekkene beskriver ulike sider ved vår kommunikasjon. Et stort åpent felt vil gi bedre kommunikasjon og mindre sjanse for misforståelse og feiltolkninger. Jo mindre åpne vi er, desto fattigere blir kommunikasjonen, og den stopper gjerne opp etter kort tid (Myrseth, 2013).

Videre i artikkelen benyttes begrepene kjent, fordekt og ukjent, som i figur 1. Fordekt representerer det som er kjent for den ene og ukjent for den andre. Eksempelvis kan en sårbarhet i eget IT-system være kunnskap som er kjent for den ene (A) og ukjent for den andre (B).

UTVALG OG METODE

Datamaterialet består av totalt sju rapporter (tabell 1) som omhandler trusselbilde og risikovurdering. Alle rapportene som analyseres, er ugraderte, gratis og offentlig tilgjengelig.

Norske myndigheter utgir fire trussel- og risikovurderinger årlig. Rapportene utgis av Etterretningstjenesten (E-tjenesten), Politiets sikkerhetstjeneste (PST), Direktoratet for samfunnssikkerhet og beredskap (DSB) og Nasjonal sikkerhetsmyndighet (NSM). Vurderingene fra E-tjenesten, PST og NSM utgis årlig. DSB utgir nye krisescenarioer årlig og har så langt utgitt samlerappor-

TABELL 1 Analyserte risiko- og trusselvurderinger.

UTGIVER	REFERANSE	TITTEL	ÅR	SIDETALL
Etterretningstjenesten (E-tjenesten)	(E-tjenesten, 2019)	Fokus 2019	2019	101
Politiets sikkerhetstjeneste (PST)	(PST, 2019)	Trusselvurdering 2019	2019	27
Direktoratet for samfunnssikkerhet og beredskap (DSB)	(DSB, 2019)	Analyser av krisescenarioer 2019	2019	221
Nasjonal sikkerhetsmyndighet (NSM)	(NSM, 2019)	Risiko 2019	2019	32
Norsk senter for informasjonssikring (NorSIS)	(NorSIS, 2018)	Trusler og trender 2018–19	2018	52
Næringslivets sikkerhetsråd (NSR)	(NSR, 2018)	Mørketallsundersøkelsen 2018	2018	63
Næringslivets sikkerhetsråd (NSR)	(NSR, 2019a)	Hybridundersøkelsen	2019	59

ter i 2014 og 2019. I DSBs samlerapport er kun de generelle delene og scenarioer om cybertrusler analysert.

Myndighetenes trusselvurderinger er supplert med tre rapporter fra andre aktører med særskilt satsing på blant annet informasjonssikkerhet og cyberkriminalitet. *Trusler og trender* utgis årlig av Norsk senter for informasjonssikring (NorSIS) og retter seg spesielt mot små og mellomstore virksomheter og privatpersoner. Næringslivets sikkerhetsråd (NSR) har gitt ut to relevante rapporter som bygger på undersøkelser gjennomført i norske virksomheter og bidragsytere som Forsvarets forskningsinstitutt, Visma og Telenor. *Mørketallsundersøkelsen* har blitt utgitt i en årrekke og omhandler temaene informasjonssikkerhet, personvern og datakriminalitet. *Hybridundersøkelsen* ble utgitt for første gang i 2019. Hybride angrep defineres ved at aktørene har et større mål, at flere ulike virkemidler brukes samtidig, og at det er vanskelig å se dem i sammenheng. Eksempler er cyberspionasje, påvirkningsoperasjoner, sabotasje og terrorisme (NSR, 2019a, s. 6). Det er ventet at hybride angrep vil ta i bruk digitale/teknologiske virkemidler. Artikkelen skiller derfor ikke spesielt mellom cyberangrep og hybride angrep utover at det er spesifisert når det snakkes spesifikt om funn fra hybridundersøkelsen.

Det er gjort en kvalitativ innholdsanalyse av alle rapportene. Rapportene er i tillegg gjennomgått for å identifisere cybertrusler som omtales. Cybertruslene fra rapportene er samlet i kategorier av ulike trusler. Kun cybertrusler som er nevnt i flere enn halvparten av rapportene (minimum fire av sju), framgår i tabell 2. Cybertruslene er oppgitt i rekkefølge, med trusselen som er omtalt i flest rapporter, først. Det gis eksempler på trusler fra rapportene i hver kategori.

Videre anvendes modellen i figur 1 for å studere betydningen av åpenhet gjennom hvordan ukjente trusler kan gjøres kjente. Det benyttes eksempler med en myndighetsaktør og en virksomhet inspirert av funn i rapportene. Modellen viser effekten av informasjonsutveksling mellom to parter.

HVA ER CYBERRISIKO, OG HVILKE CYBERTRUSLER ER DE MEST FRAMTREDENDE?

Trusselvurderingene benytter ulike begreper for cyberrisiko og cybertrusler. Begreper som digital, IKT og cyber har nyanseforskjeller, men blir ofte behandlet som synonymer. Både nasjonalt og internasjonalt blir begrepet cybersikkerhet stadig oftere brukt. På bakgrunn av dette anbefaler NSM (2015, s. 11, 25, 40) at begrepet cybersikkerhet bør erstatte IKT-sikkerhet og benyttes i politiske og strategiske dokumenter. Videre i denne artikkelen benyttes primært prefikset cyber- for trusler og risikoer som blir drøftet.

Det finnes få formelle definisjoner på cyberrisiko. Cyber kan forklares som «det som er relatert til datamaskiner, IKT og nettverk, både digital informasjon og fysiske objekter» (Norsk utenrikspolitisk institutt, 2019). Det er ikke enighet om én definisjon av risiko, men flere vektlegger ventet tap eller skade på verdier, eventuelt sannsynligheten for skade hvor usikkerhet er involvert. Denne artikkelen benytter følgende definisjon: *Cyberrisiko er verdier satt på spill gjennom digitalisering. Verdiene kan være både materielle og immaterielle, og risikoen kan oppstå både tilsiktet og utilsiktet.*

Gjennom digitaliseringen har kjente former for risiko tatt skrittet over i cyberdomenet, som svindel og informasjonstyveri. Vi åpner også for nye risikoer

TABELL 2 De mest framtredende cybertruslene.

CYBERTRUSSEL	EKSEMPEL
Nettverksoperasjoner	Nettverksangrep, hacking
Kompromitteringer	Informasjonslekkasje, overvåking av e-postkorrespondanse, kompromittering f.eks. via utdaterte webservere, adgangssystem på internett, minnepinner
Kartlegging	Skanninger (ofte automatiserte) for å lete etter sårbarheter, kartlegging av ansattes e-poster, rolle og funksjon i virksomheten, brukerprofiler i sosiale medier, innsamling av data gjennom falske henvendelser
Svindel	Nettfiske (*phishing*), direktørsvindel, fakturasvindel, investeringssvindel
Etterretning fra fremmede stater	Rekruttering og føring av hemmelige kilder, nettverksbaserte etterretningsoperasjoner, plassering av studenter og forskere
Skadevare	Virus- og skadevareinfeksjoner, e-post med infiserte vedlegg eller lenke til «vannhull» (nettside med skadevare)
Sabotasje	Skader på maskin- og programvare, sletting av informasjon, endring av konfigurasjon på system, *defacing* (vandalisme mot en nettsides utseende og/eller innhold)
Spionasje	Industrispionasje, digital spionasje
Utnytte sårbarheter	Utnytte kjente sårbarheter, utnytte nulldagssårbarheter (ikke kjente), utnytte sårbarheter i digital infrastruktur og verdikjeder
Løsepengevirus	Krypteringsvirus for økonomisk utpressing, kryptolåsing
Tjenestenektangrep	DDoS-angrep, trusler om DDoS-angrep, overbelaste systemer
Misbruk av ressurser	Graving etter kryptovaluta, *kryptojacking*, misbruk av ressurser til nye angrep, utnyttelse av tredjeparts infrastruktur
Påvirkningsoperasjoner	Påvirkningsforsøk og informasjonskampanjer, falske nyheter, innhentingsoperasjoner og forsøk på påvirkning
Innsidere	Utro tjenere, kan være plassert, utsatt for press eller operere på eget initiativ

ved å koble utstyr til internett. Et akvarium koblet til internett for å overvåke fôring, temperatur og renhold, ble misbrukt som veien inn i et amerikansk kasino for å stjele data (Schiffer, 2017). Dagbladet publiserte i 2013 en rekke artikler i serien «null ctrl» som avdekket alt fra private videokameraer til sensitiv kundeinformasjon og alarmsystemer som lå åpent på nett. Problematikken er med andre ord verken ny eller utdatert.

Sammenkobling av teknologi, aktører og systemer i lange verdikjeder øker risikoen for at virksomheter mister kontrollen på hvor verdifull informasjon er lagret, og hvem som eventuelt har tilgang til den (NorSIS, 2018s. 35). Selv myndighetene vedgår at det nærmest er umulig å holde oversikt over avhengigheter og sårbarheter i en uoversiktlig og kompleks digital infrastruktur (NSM, 2019, s. 15).

NSM NorCERT registrerte i 2018 cirka 20 000 saker der kun nær en fjerdedel ble undersøkt nærmere (NSM, 2019, s. 10). Visma beskriver enkelte typer cyberangrep som så vanlige at de anses som «normal bakgrunnsstøy» fordi de foregår i stort omfang. Det henvises her primært til automatiserte skanninger. Beregninger viser at angrep og angrepsforsøk mot de tjenestene Visma leverer, ville gitt grunnlag for 1 800–3 000 anmeldelser i måneden (NSR, 2018, s. 51).

Av datamaterialet framgår det tydelig at cybertrusler er noe virksomheter må forholde seg til. Alle myndighetsaktørene har bredere ansvarsområder enn cybersikkerhet. Likevel preger cybertrusler og -risikoer samtlige av rapportene. Dette gjelder både som definerte utfordringsområder og som verktøy eller virkemidler i andre trusler.

Gjennomgangen av rapportene identifiserte 177 cybertrusler. Enkelte cybertrusler går igjen i flere av rapportene, men er kun registrert én gang per rapport. Truslene er deretter kategorisert. Tabell 2 viser de 14 mest framtredende cybertruslene fra de sju analyserte rapportene. Kolonnen for eksempler viser noen av cybertruslene som ligger innunder kategorien.

Enkelte cybertrusler er ikke nødvendigvis ulovlige, men ofte i en gråsone fordi aktivitetene gjerne brukes som ledd i et framtidig cyberangrep. Ett eksempel på dette er skanninger. Visma illustrerer skanninger i Mørketallsundersøkelsen med at en ukjent person tester utgangsdører for å se om de er åpne eller låst (Visma i NSR, 2018, s. 51).

Angrep benytter gjerne flere virkemidler i kombinasjon. For eksempel kan en trusselaktør bruke tid på å skanne nettverket og kartlegge bedriftens ansatte og relasjoner. Informasjonen kan brukes til å iverksette mer målrettet nettfiske for å manipulere til handling. Målet kan være å kryptere virksomhetens filer for å kreve løsepenger.

Det rapporteres også om tilpasset svindel. Tilpasset svindel kan være falske e-poster fra en tjeneste du har et kundeforhold til, eller sesongbasert, som «henting av pakke» i desember. Selv utpressingsbeløp kan være tilpasset. I praksis betyr det at virksomheter blir presset for høyere beløp enn privatpersoner (NorSIS, 2018, s. 36–37).

Det er krevende å skille mellom eller finne ut av om angrep er økonomisk kriminalitet, statlige angrep, uhell og feil eller «jente- og guttestreker» (NSR, 2019a, s. 44). I det praktiske arbeidet spiller kanskje dette uansett mindre rolle. Hovedforskjellen antas å være at statlige aktører har «ubegrenset» med ressurser og tid, mens vinningskriminelle vil gå over til andre mål dersom virksomheten er «sikker nok».

HVORDAN KOMMUNISERER AKTØRENE TRUSSELBILDET OG TILTAK?

Flere av aktørene legger fram et trusselbilde som karakteriseres av endring. Noen beskrivelser er «sammensatt og i rask endring og utvikling» (E-tjenesten, 2019, s. 9), «dynamisk» (NSM, 2019, s. 5) og «i kontinuerlig endring» (DSB, 2019, s. 9). Dette er stikk i strid med PSTs (2019, s. 3) vurdering «stabile og relativt varige utviklingstrekk». NorSIS (2018, s. 29) rapporterer også at årets trusler ikke divergerer stort fra året før. NorSIS peker i tillegg på en nyanse her: Selv om metodene er de samme som tidligere, oppfattes trusselaktørene og angrepene som mer avanserte og målrettede.

Ulike vurderinger av risikobildet kan også skyldes at myndighetene har ulike instrukser og mandat. Likevel kan de tidvis vage beskrivelsene av trusselbildet føre til at nytten av rapportene går ned. Informasjonen kan oppleves som intetsigende og lite pålitelig når det gis motstridende vurderinger. Av virksomhetene oppgir kun 17 prosent å ha lest PSTs risikovurdering og kun 10 prosent å ha lest NSMs risikovurdering (NSR, 2019b, s. 16). Dette kan indikere at rapportene ikke blir oppfattet som relevante for virksomhetene. Dersom myndighetene ønsker å være primærkilden for norske virksomheter i framtiden, må det gis informasjon som virksomhetene faktisk forstår og kan bruke i risikostyringsarbeidet.

Mange trenger hjelp til å omsette kunnskap i tiltak (NSR, 2018, s. 61). Rapportene viser en rekke punkter hvor sikkerheten bør bedres, men gir få konkrete tiltak. Eksempelvis anbefales det å arbeide med «sikkerhetsstyring», «risikovurderinger» og å «redusere sårbarheter» uten at det nødvendigvis gis gode svar på hvordan dette kan gjøres. E-tjenestens trusselvurdering skiller seg ut ved å ikke anbefale ett eneste tiltak for å redusere risiko. PST, NSM og DSB kommer med anbefalte tiltak, men er ikke i nærheten av å være like grundige som NorSIS og NSR. Her bør det nevnes at særlig NSM har gitt ut en rekke veiledninger og temarapporter i tillegg til den årlige trusselvurderingen. Eksempler er *Grunnprinsipper for IKT-sikkerhet* og *Håndtering av digital spionasje*. Begge presenterer en rekke tiltak.

ÅPENHET ER INTENSJONEN, MEN IKKE PRAKSISEN?

Økt åpenhet kan bidra til at angrep blir avverget. Når færre angrep lykkes, blir cyberangrep en mindre lønnsom forretningsmodell. På sikt kan dette kanskje gi færre angrep. I rapportene er det bred enighet om at samarbeid, åpenhet og informasjonsutveksling er nødvendig for å møte cybertruslene (NSR, 2018, s. 50, 2019a, s. 44; NSM, 2019, s. 50; NorSIS, 2018, s. 41).

Den nye sikkerhetsloven (i kraft fra 01.01.19) legger opp til bedre samhandling og mer informasjonsdeling mellom myndigheter og virksomheter som er underlagt loven. Det pekes på at myndighetene også har behov for mer innrapportering av hendelser (NSM, 2019, s. 25). Selv om svært få rapporterer og anmelder hendelser, svarer hele 92 prosent av virksomhetene at de ønsker å dele informasjon med myndighetene (NSR, 2019a, s. 39).

Hybridundersøkelsen understreker at økt åpenhet fra myndighetene er ønsket. Over halvparten svarer at de mener norske myndigheter bør bidra med mer informasjon, klarere retningslinjer, veiledning og åpenhet om hybride hendelser som myndighetene vet om (NSR, 2019a, s. 29).

Rapportene viser derimot manglende åpenhet som går begge veier. Av virksomheter som opplevde sikkerhetshendelser, rapporterte kun ni prosent til politiet, og fem, tre og to prosent til andre myndighetsaktører, Nor-CERT eller sektor-CERT og lignende. Det vanligste er å rapportere til administratoren av det aktuelle systemet

(72 prosent). En del melder også til antivirusleverandør (24 prosent) og ISP (internettleverandør) (10 prosent). (NSR, 2018, s. 28) En av grunnene til at få anmelder, kan være manglende bevissthet rundt hva som er en kriminell handling. Det råder også en oppfatning om at en anmeldelse vil gi merarbeid for virksomheten, og at politiet ikke har ressurser til å følge opp (NSR, 2018, s. 50). Med Vismas beregninger av grunnlag for 1 800–3 000 anmeldelser i måneden er det klart at dette vil gi betydelig merarbeid – og mange henleggelser.

Noen virksomheter ønsker ikke at kunder, leverandører og konkurrenter skal få vite om eventuelle hendelser. Dette fører til at de dysses ned (NorSIS, 2018, s. 30). Årsakene kan være at virksomheten ikke ønsker å framstå som et enkelt mål eller svekke tilliten i aksjemarkedet (NSR, 2019a, s. 44). Sikkerhetshendelser kan også virke stigmatiserende dersom allmennoppfatningen er at virksomheten burde gjort mer for å unngå hendelsen (NorSIS, 2018, s. 29). I utpressingssaker oppfatter ofrene det ofte som mer attraktivt å betale enn å søke hjelp eller melde fra (NorSIS, 2018, s. 29). Dette kan gi uheldige ringvirkninger. Det viser at virksomheten er et mulig offer for framtidige angrep. I løsepengevirussaker er det ingen garanti for at filer blir dekryptert, eller at aktøren ikke har installert en bakdør for framtidige angrep. I tillegg bidrar løsepenger til å opprettholde den kriminelle forretningsmodellen.

I trusselvurderingens innledning skiver sjef for E-tjenesten at det er utfordrende å ikke kunne dele gradert informasjon. Som en følge vil enkelte områder ikke være dekket av trusselvurderingen (E-tjenesten, 2019, s. 6). Det kan spørres om det alltid er forsvarlig å være åpen om sårbarheter og angrep. Informasjonen kan i verste fall forstås som en oppskrift til vinningskriminelle og etterretning. Funn som at «ved sikkerhetsbrudd har industri-, overnattings- og serveringsvirksomheter samt tjenesteytende næringer lavest modenhet for oppdagelse» (NSR, 2018, s. 37), gir en pekepinn om i hvilke bransjer det kan være større sjanse for å lykkes med cyberangrep.

DILEMMAET TAUSHET ELLER ÅPENHET – TO EKSEMPLER

Equifax-skandalen illustrerer både den økonomiske konsekvensen og stigmatiseringen som et cyberangrep kan føre til. I 2017 ble det kjent at personopplysninger som kredittovervåkingsbyrået Equifax lagret, var på avveier. Denne typen informasjon kan misbrukes til blant annet identitetstyveri. Datalekkasjen rammet over 146 millioner individer, primært amerikanere (U.S. Government Accountability Office, 2018, s. 1). I løpet av dager falt aksjeverdien med en tredjedel (MarketWatch, 2019). I 2019 ble det besluttet at Equifax må betale opptil 700 millioner dollar i oppgjør etter hendelsen (Schroeder, 2019). I ettertid har det kommet fram at Equifax hadde sårbarheter som kunne vært eliminert eller redusert. Oppdatering av programvaren ville tettet sikkerhetshullet som ble utnyttet. Databasene var ikke segmentert (isolert), slik at angriperne lettere fikk tak i mer informasjon. Angriperne fikk tilgang til databaser hvor brukernavn og passord lå ukryptert. Det var heller ikke tak på antall spørringer som kunne gjøres mot databasen. (U.S. Government Accountability Office, 2018, s. 15–16)

En aktør som håndterte en cyberhendelse ganske annerledes enn Equifax, er Hydro. Når denne artikkelen trykkes, er det cirka ett år siden nyheten kom om at Hydro var utsatt for et omfattende cyberangrep. Selve inntrengningen skjedde ved at et vedlegg i en e-post fra en kunde til en ansatt i Hydro ble kapret og utstyrt med skadevare. Vedlegget var del av en reell og ventet korrespondanse i legitim kommunikasjon i en kunderelasjon (Briggs, 2020). Skadevaren var fordekt som en legitim fil, altså en trojansk hest. Dette skjedde tre–fire måneder før selve angrepet. I denne perioden arbeidet angriperen(e) med å skaffe tilganger for å gjennomføre angrepet (Moberg & Lekanger, 2019). Da krypteringen av servere og datamaskiner begynte, var Hydro tidlig ute med pressekonferanse, anmeldelse og informasjon til media. For dette mottok Hydro Kommunikasjonsforeningens åpenhetspris 2019 (Mellum, 2019).

I ettertid har det blitt kjent at Hydros åpenhet, og særlig bevismaterialet som ble delt med myndighetene, var nyttige for andre formål enn kun etterforskning. Ved hjelp av bevismaterialet kunne det spores opp angrep med samme virus fra de samme hackerne på et tidlig stadium. Dette gjorde det mulig å varsle virksomhetene og avverge angrep. Flere norske og utenlandske virksomheter var blant de utsatte. (Klevstrand, 2019)

De færreste av oss er i særlig grad selvforsynte, verken privat, på virksomhetsnivå eller på samfunnsnivå. Istedenfor benyttes kjøp av varer og tjenester – også innen cyber. Dette skaper et avhengighetsforhold hvor sårbarheter og cyberangrep hos én virksomhet, én person eller ett system kan få følgehendelser og konsekvenser for flere i verdikjeden. Angrepet mot Hydro

var ikke en IT-krise, men en virksomhetskrise som fikk store konsekvenser for hele driften – fra aluminiumsproduksjon til utbetalinger av lønn.

Tiltak koster, i det minste i tid: Det er knappe ressurser, og det må prioriteres. NorSIS (2018, s. 31) antar at mange virksomheter iverksetter tiltak først *etter* hendelser. I slike tilfeller sitter virksomheten med kostnaden både for tapt inntekt under angrepet, opprydningsarbeid og investeringer i sikkerhet. Kostnadene kunne derimot vært langt lavere, kanskje til og med avverget hendelsen, om de ble gjort tidligere. Hydro (2019) anslår selv at cyberangrepet som rammet dem, kostet 550–650 millioner kroner. Kostnader for virksomheter flest er ifølge Mørketallsundersøkelsen i snitt drøyt 54 000 kroner for den mest alvorlige hendelsen. De som er hardest rammet, estimerer en kostnad på to millioner kroner. Merk at tallene inkluderer de som oppgir at hendelsen ikke har hatt noen kostnad. (NSR, 2018, s. 28)

HVORDAN GJØRE UKJENTE RISIKOER KJENTE?

Modellen som ble introdusert innledningsvis (figur 1), er benyttet for å illustrere to parters kunnskap om trusselbildet (figur 2). Eksempler på informasjon i figuren er hentet fra analysen av rapportene. Både virksomheten og myndighetsaktøren kjenner til hendelser som blir delt, og de åpne trusselvurderingene. Videre har virksomheten kunnskap om angrep som ikke er rapportert, og som myndighetsaktøren derfor ikke kjenner til. Myndighetsaktøren har på sin side kunnskap om gradert informasjon og hendelser som ikke er delt i åpne kilder. Partene deler et ukjent felt, for eksempel kartleggingsangrep som ingen av dem har oppdaget.

Feltene som er kjent for den ene parten, men ukjent for den andre, utgjør et potensial for informasjonsutveksling og økt kunnskap. Dersom myndighetsaktøren eksempelvis deler informasjon utover den offentlige trusselvurderingen, vil virksomhetens kjente felt øke. Dette er illustrert i figur 3. Myndighetsaktøren har i dette eksempelet ingen endring i sin andel av kunnskap som er kjent eller ukjent. Figur 4 illustrerer endring i myndighetsaktørens kjente felt som resultat av informasjonsdeling fra virksomheten.

Når myndighetsaktøren deler informasjon, øker virksomhetens kjente felt, og vice versa. Som resultat blir andelen kjent og felles kunnskap større.

FIGUR 2 Eksempler på kjent og ukjent informasjon om cyberrisiko for en virksomheten og en myndighetsaktør.

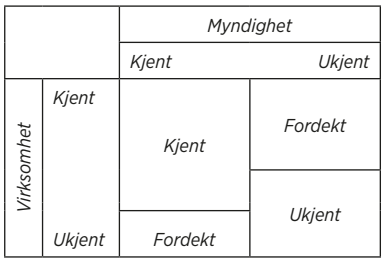
		Myndighet	
		Kjent	*Ukjent*
Virksomhet	*Kjent*	*Hendelser som blir delt, åpne trusselvurderinger*	*Angrep som ikke blir registrert eller anmeldt*
	Ukjent	*Gradert trusselvurdering, det som ikke deles i trusselvurderingene*	*Risiko/angrep ingen av aktørene er klar over, f.eks. kartleggingsangrep*

Figur 5 illustrerer antatt effekt dersom begge partene deler informasjon med hverandre. Her har det kjente feltet også økt på bekostning av det ukjente feltet. Dette baseres på at det å se informasjon i sammenheng kan gi grunnlag for å trekke nye slutninger og gi ny kunnskap. Et eksempel som er beslektet med artikkelens tema, er Cambridge Analyticas bearbeiding av informasjon. De benyttet informasjon fra Facebook-profiler til å finne korrelasjoner mellom liker-klikk og karaktertrekk. Dette muliggjorde at de på bakgrunn av lite informasjon om en enkeltperson kunne danne seg et større og treffsikkert bilde av individets personlighetstrekk og dermed interesser, preferanser og politiske ståsted (NSR, 2019a, s. 46–47). Ved hjelp av stordata kunne et liker-klikk til «Hello Kitty» på Facebook gi sterke indikasjoner om et individs politiske ståsted (Cadwalladr & Graham-Harrison, 2018).

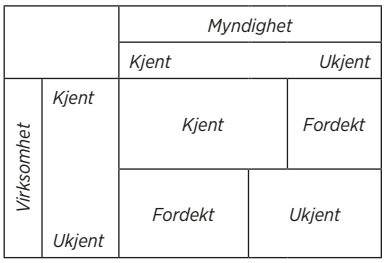
Modellen illustrerer hvordan informasjonsutveksling og ny kunnskap kan minimere feltene som er helt eller delvis ukjente. I hvor stor grad dette kan oppnås, avhenger blant annet av partenes kunnskap om situasjonen og kvaliteten på kommunikasjonen. Det kan være utopisk å anta at hele situasjonsbildet kan gjøres kjent. Målet bør heller være å benytte informasjonsdeling for å redusere de helt eller delvis ukjente feltene så langt det lar seg gjøre, og der dette er til alles fordel. Informasjonsutveksling kan dessuten betraktes som «lavthengende frukt» både organisatorisk og kostnadsmessig.

Åpenhet er ikke synonymt med førstesideoppslag i alle landets aviser. Det bør ved ulike hendelser avgjøres hvilken grad av åpenhet som er konstruktiv. Alternativer omfatter rapportering til myndighetene, inkludert lovpålagt rapportering; deling i lukkede fora som bransjefora og sektor-CERT; informasjon til berørte parter

FIGUR 3 Resultat av informasjonsdeling fra myndighetsaktør til virksomhet illustrert ved endring i vinduenes størrelse.



FIGUR 4 Resultat av informasjonsdeling fra virksomhet til myndighetsaktør illustrert ved endring i vinduenes størrelse.



(kunder, leverandører, samarbeidspartnere, ansatte); eller åpen deling på nettside, i media eller lignende.

Rapportene viser at både virksomheter og myndighetene har forbedringspotensial innen informasjonsdeling. Det bør vurderes om det er behov for å tilpasse eksisterende rapportering, kanaler eller fora for å dele. Videre er det viktig å unngå stigmatisering som kan hemme åpenhet. Mediene har ofte skarpt søkelys på person og virksomhet, noe som kan være belastende for dem som befinner seg i en allerede krevende hendelse. Basert på Hydro-saken kan det se ut til at virksomheter kan unngå spekulerende og negativ omtale ved å informere om en cyberhendelse selv.

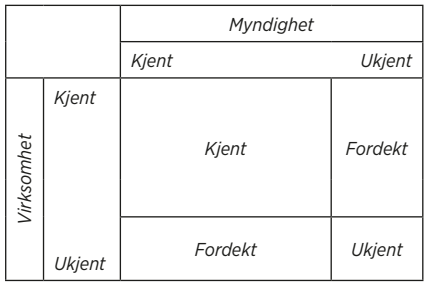
Modellen er, i likhet med alle andre modeller, en forenkling. I praksis er vi omgitt av flere aktører og situasjoner vi har svært ulikt kunnskapsnivå rundt. I tillegg kan kunnskapen vi har, være usikker. Likevel viser modellen hvordan åpenhet kan bidra til at ukjente risikoer gjøres kjente. Når alle deler, blir ukjent kjent. Både myndighetene og virksomhetene etterlyser mer informasjonsutveksling. Dette tyder på at det er et stort potensial for økt kunnskap gjennom informasjonsutveksling.

KONKLUSJON

Kunnskap om trusler og risiko er grunnleggende for risikostyringen. Datagrunnlaget er basert på sju rapporter om risikovurderinger og trusselbilde. Cyberrisiko defineres som verdier satt på spill gjennom digitalisering. Ut fra rapportene identifiseres 14 cybertrusler som de mest framtredende. Det vises også at organisasjonene, i større grad enn myndighetene, bistår med konkrete tiltak for styring av cyberrisiko i trusselvurderingene.

Åpenhet er et gjennomgående tema i innholdsanalysen av rapportene. Både myndighetene og virksomhetene er enige om at informasjonsutveksling og åpenhet er

FIGUR 5 Effekt av informasjonsdeling fra og til begge aktørene.



ønskelig og nødvendig for å møte cybertrusler. På tross av dette er noen av rapportene preget av tidvis vage formuleringer om trusler og tiltak. Informasjonen som deles, er i noen tilfeller begrenset. Fra virksomhetenes side vises det at svært få varsler eller anmelder cyberangrep, til tross for at de ønsker mer informasjon og åpenhet. I noen tilfeller ønsker virksomhetene å dysse ned hendelser fordi det kan gi store konsekvenser for økonomi og omdømme og føre til stigmatisering og merarbeid om hendelsen blir kjent (slik som i Equifax' tilfelle). På den andre siden ser vi at informasjonsdeling og åpenhet, spesielt på et tidlig stadium, kan bidra til å avdekke og avverge ytterligere angrep (slik som i Hydro-saken).

Denne artikkelen har presentert en modell for kjent og ukjent kunnskap. Modellen belyser hvordan to parter kan utveksle informasjon. Informasjonsutvekslingen kan øke andelen kjent kunnskap og minimere helt eller delvis ukjent kunnskap. Dette gjelder også ved at sammenstilling av informasjon kan bidra til å danne ny kunnskap som tidligere var ukjent for begge parter. Åpenhet er sentralt for å realisere informasjonsutveksling, oppnå kunnskap og gjøre ukjente risikoer kjente. M

REFERANSER

Andersen, E., & Sannes, R. (2017). Hva er digitalisering? *Magma*, *20*(6), 18–24. Hentet fra https://www.magma.no/hva-er-digitalisering

Aven, T., & Renn, O. (2010). *Risk management and governance: Concepts, guidelines and applications*. I J.L. Mumpower & O. Renn (Red.), *Risk, governance and society. Volum 16*. Berlin, Heidelberg: Springer.

Briggs, B. (2019, 16. desember). Hackers hit Norsk Hydro with ransomware. The company responded with transparency. *Microsoft Transform*. Hentet 31.01.2020 fra https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/

Cadwalladr, C., & Graham-Harrison, E. (2018, 17. mars). How Cambridge Analytica turned Facebook 'likes' into a lucrative political tool. *The Guardian*. Hentet 02.02.2020 fra https://www.theguardian.com/technology/2018/mar/17/facebook-cambridge-analytica-kogan-data-algorithm

Direktoratet for samfunnssikkerhet og beredskap. (2019). *Analyser av krisescenarioer 2019*. Hentet 05.08.2019 fra https://www.dsb.no/globalassets/dokumenter/rapporter/p1808779_aks_2018.cleaned.pdf

Etterretningstjenesten. (2019). *FOKUS 2019*. Hentet 15.08.2019 fra https://forsvaret.no/fakta_/ForsvaretDocuments/fokus2019_web.pdf

Gundersen, I. (2017, 2. februar). Kundeinfo lå åpent i Rema 1000s Æ-app. *Stavanger Aftenblad*, s. 12.

Hydro. (2019). Cyberangrep på Hydro. Hentet 12.02.2020 fra https://www.hydro.com/no-NO/media/pa-dagsorden/cyberangrep-pa-hydro/

Klevstrand, A. (2019, 8. september). Stoppet hackerangrep mot flere norske selskaper. *Dagens Næringsliv*. Hentet 15.11.2019 fra https://www.dn.no/bors/hydro/datasikkerhet/hacking/stoppet-hackerangrep-mot-flere-norske-selskaper/2-1-666418

MarketWatch. (2019). Equifax Inc. Hentet 24.10.2019 fra https://www.marketwatch.com/investing/stock/efx/charts

Marshall, A., Ojiako, U., Wang, V., Lin, F., & Chipulu, M. (2019). Forecasting unknown-unknowns by boosting the risk radar within the risk intelligent organisation. *International Journal of Forecasting*, *35*(2), 644–658. https://doi.org/10.1016/j.ijforecast.2018.07.015

Mellum, M. (2019). Kommunikasjonsforeningens Åpenhetspris 2019 til Hydro. Hentet 28.10.2019 fra https://www.kommunikasjon.no/fagstoff/nyheter/kommunikasjonsforeningens-apenhetspris-2019-til-hydro

Moberg, J. M., & Lekanger, K. (2019, 5. november). Offer for omfattende dataangrep – slik kan næringslivet ta forholdsregler. *Digi.no*. Hentet 05.11.2019 fra https://www.digi.no/artikler/intervju-offer-for-omfattende-dataangrep-slik-kan-naeringslivet-ta-forholdsregler/477063

Myrseth, H. (2013). Joharis vindu. Hentet 15.11.2019 fra https://ndla.no/subjects/subject:18/topic:1:193544/topic:1:82776/resource:1:116760

Næringslivets sikkerhetsråd. (2018). *Mørketallsundersøkelsen 2018: Informasjonssikkerhet, personvern og datakriminalitet*. Hentet 22.10.2019 fra https://www.nsr-org.no/getfile.php/1311303-1537281687/Bilder/Mørketallsundersøkelsen/Mørketallsundersøkelsen 2018 low.pdf

Næringslivets sikkerhetsråd. (2019a). *Hybridundersøkelsen: Hybride trusler og hendelser mot norsk næringsliv*. Hentet 19.08.2019 fra https://www.nsr-org.no/getfile.php/1312167-1553166117/Dokumenter/NSR publikasjoner/Hybridundersøkelsen/Hybridundersøkelsen_web.pdf

Næringslivets sikkerhetsråd. (2019b). *Kriminalitets- og sikkerhetsundersøkelsen i Norge (KRISINO) 2019*. Hentet 06.11.2019 fra https://www.nsr-org.no/getfile.php/1312949-1568794843/Bilder/Krisino/KRISINO rapport 2019 low.pdf

Nasjonal sikkerhetsmyndighet. (2015). *Sikkerhetsfaglig råd*. Hentet 05.11.2019 fra https://www.nsm.stat.no/globalassets/rapporter/nsm-sikkerhetsfaglig_raad_2015_web.pdf

Nasjonal sikkerhetsmyndighet. (2019). *RISIKO 2019 Krafttak for et sikrere Norge*. Hentet 23.08.2019 fra https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2019_final_enkeltside.pdf

Norsk senter for informasjonssikring. (2018). *Trusler og trender 2018–19: Hvilke digitale trusler møter oss på jobb og i hverdagen?* Hentet 15.08.2019 fra http://norsis.no/upload/trusler og trender 2018–19 web.pdf

Norsk utenrikspolitisk institutt. (2019). Cyber. Hentet 27.10.2019 fra https://www.nupi.no/Vaar-forskning/Temaer/Forsvar-og-sikkerhet/Cyber

Politiets sikkerhetstjeneste. (2019). *Trusselvurdering 2019*. Hentet 15.08.2019 fra https://www.pst.no/globalassets/artikler/trusselvurderinger/psts-trusselvurdering-2019.pdf

Rumsfeld, D. (2002, 12. februar). DoD News Briefing – Secretary Rumsfeld and Gen. Myers. Hentet 24.10.2019 fra https://archive.defense.gov/Transcripts/Transcript.aspx?TranscriptID=2636

Schiffer, A. (2017, 21. juli). How a fish tank helped hack a casino. *The Washington Post*. Hentet 25.10.2019 fra https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/

Schroeder, P. (2019, 22. juli). Equifax's $700 million data breach settlement spurs criticism, calls for new rules. *Reuters*. Hentet 25.10.2019 fra https://www.reuters.com/article/us-equifax-cyber-settlement/equifax-to-pay-up-to-650-million-in-data-breach-settlement-idUSKCN1UH16Y?feedType=RSS&feedName=technologyNews

U.S. Government Accountability Office. (2018). *DATA PROTECTION: Actions taken by Equifax and federal agencies in response to the 2017 breach. GAO-18-559*. Hentet 24.10.2019 fra https://www.gao.gov/assets/700/694158.pdf

Zahl-Begnum, O.H., & Begnum, S. (1990). *Arbeids- og organisasjonspsykologi* (2. utgave). Oslo: NKS-forlaget.

Žižek, S. (2006). Philosophy, the «unknown knowns,» and the public use of reason. *Topoi*, *25*(1–2), 137–142. https://doi.org/10.1007/s11245-006-0021-2