



## RISIKO 2018

Verdifulle individer  
Verdifulle virksomheter  
Verdifull infrastruktur





NSMs rapport «Risiko 2018» er én av fire trussel- og risikovurderinger som utgis årlig. De øvrige tre utgis av Etterretningstjenesten (E-tjenesten), Politiets sikkerhetstjeneste (PST) og Direktoratet for samfunnssikkerhet og beredskap (DSB).

**Nasjonal sikkerhetsmyndighet (NSM)** er Norges fagmyndighet for forebyggende nasjonal sikkerhet. NSM gir råd om og fører tilsyn med blant annet sikring av informasjon, objekter og infrastruktur av nasjonal betydning. Videre har NSM et nasjonalt ansvar for å detektere, varsle og koordinere håndtering av alvorlige IKT-angrep. I rapporten «Risiko 2018» vurderer NSM risikoen for at samfunnet skal rammes av spionasje, sabotasje, terror og andre alvorlige handlinger. Vurderingen utgis i første kvartal.



**Etterretningstjenesten (E-tjenesten)** er Norges utenlandsetterretningstjeneste. Tjenesten er underlagt forsvarssjefen, men arbeidet er ikke avgrenset til militære problemstillinger. E-tjenestens hovedoppgaver er å varsle om ytre trusler mot Norge og prioriterte norske interesser, støtte Forsvaret og forsvarsallianser Norge deltar i, samt understøtte politiske beslutningsprosesser med informasjon av spesiell interesse for norsk utenriks-, sikkerhets- og forsvarspolitik. «Fokus 2018» gir E-tjenesten sin analyse av status og forventet utvikling innenfor geografiske og tematiske områder som tjenesten vurderer som særlig relevant for norsk sikkerhet og nasjonale interesser. Etterretningsvurderingen har en tidshorisont på ett år, og utgis i første kvartal.



**Politiets sikkerhetstjeneste (PST)** er Norges nasjonale innenlands etterretnings- og sikkerhetstjeneste. PSTs hovedoppgave er å forebygge og etterforske alvorlig kriminalitet mot nasjonens sikkerhet. PSTs årlige trusselvurdering er en analyse av forventet utvikling innenfor PSTs hovedansvarsområder.



**Direktoratet for samfunnssikkerhet og beredskap (DSB)** skal ha oversikt over risiko og sårbarhet i samfunnet. DSB har utgitt scenarioanalyser siden 2011. Analysene omhandler risiko knyttet til katastrofale hendelser som kan ramme det norske samfunnet og som det bør være forberedt på å møte. Analysene omfatter både naturhendelser, store ulykker og tilsiktede handlinger. De har en lengre tidshorisont enn de årlige vurderingene til de øvrige tre etatene.



# Sunt sikkerhetsvett

1

## IDENTIFISERE OG KARTLEGGE

### Gjør risikovurdering

- Kjenn dine verdier
- Kjenn dine avhengigheter og hvem som avhenger av deg
- Kjenn dine sårbarheter
- Kjenn ditt kompetansebehov
- Kjenn dine ansatte

2

## BESKYTTE

### Sikre dine verdier

- Gjør sikkerhetsstyring til en del av virksomhetsstyringen
- Etabler grunnsikring
- Tenk helhetlig sikring – fysisk – digital – personell
- Foreta sikre anskaffelses- og utviklingsprosesser
- Ha kontroll på IKT-infrastruktur og dataflyt

3

## OPPRETTHOLDE OG OPPDAGE

### Vær bevisst

- Legg til rette for en god sikkerhetskultur
- Ha gode rutiner for å oppdage avvik
- Ivareta daglig sikkerhetsmessig ledelse
- Sett sikkerheten din på prøve – gjennomfør øvelser
- Gjennomfør sikkerhetsrevisjoner
- Meld fra om sikkerhetstruende hendelser

4

## HÅNTERE OG GJENOPPRETTE

### Lær av dine utfordringer

- Forbered virksomheten og håndtering av hendelser
- Vurder og kategoriser hendelser
- Kontroller og håndter hendelser
- Evaluer og lær av hendelser



# Innhold

---

- 7 Forord
- 8 Risikobildet
- 12 Verdifulle individer
- 13 Din digitale angrepsflate
- 15 Du som virksomhetens angrepsflate – offer og angriper
- 18 Verdifulle virksomheter
- 19 Har vi gjennomføringskraft? Fra idé til tiltak
- 22 Flinke nok? Norsk kompetanse
- 24 Verdifull infrastruktur
- 25 Hvem tar vare på våre verdier?
- 27 Små tuer kan velte store lass

## RISIKO 2018

---

**Design:**  
Redink

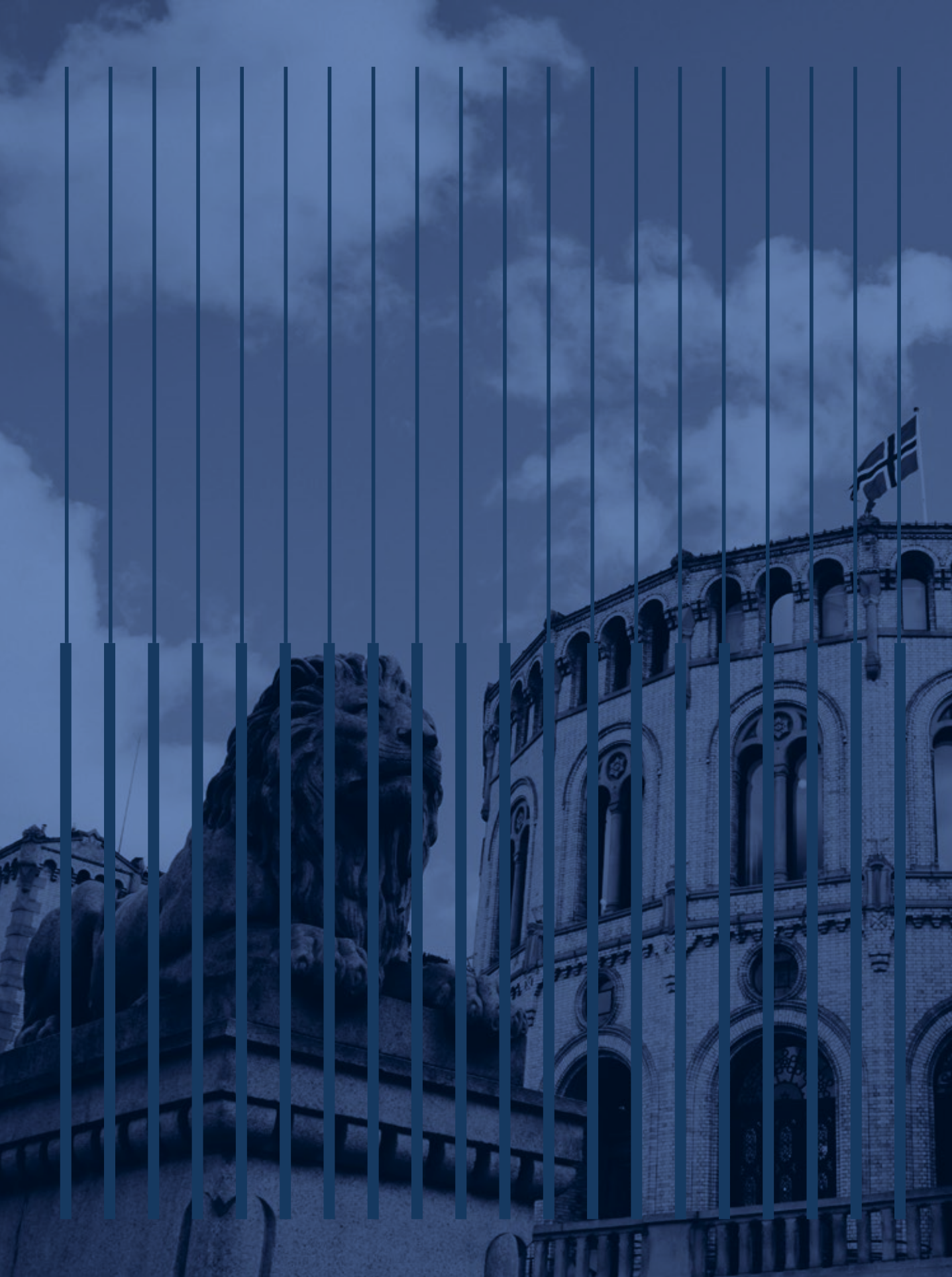
**Forsidefoto:**  
Knut Ove Hillestad/  
Norges vassdrags- og energidirektorat

**Foto:**  
Colourbox, NVE og NSM

**Trykk og distribusjon:**  
RK grafisk







# Forord

---

VI LEVER I et av verdens tryggeste samfunn. Likevel viser en fersk undersøkelse fra DSB at nordmenn blir stadig mer bekymret for egen sikkerhet. Cyberangrep, terrorangrep, kapring og flom topper listen over det vi engster oss for. Alle virksomheter som bidrar til å opprettholde viktige samfunnsfunksjoner, og hver enkelt av oss som bor, lever og arbeider i Norge, har sårbarheter. Samtidig står vi overfor en rekke trusler som kan ha både individ, ulike virksomheter og den overordnede infrastrukturen som mål.

Bevisstheten om risikoen som eksisterer i samfunnet, i de ulike virksomhetene og hos hver enkelt av oss, er knyttet til vår kunnskap om at vi alle forvalter verdier vi ønsker å beskytte, det være seg liv og helse, økonomiske forhold, styrings- evne, livsmiljø eller omdømme. God

sikkerhetsstyring handler om å kunne ta opplyste beslutninger om hvilke tiltak vi bør prioritere, og hvilken risiko vi kan akseptere.

De fleste er kjent med historien om Alle, Noen, Ingen og Enhver som ender med at «Alle bebreidet Noen da Ingen gjorde det Enhver kunne ha gjort». Moralen i denne fortellingen kan også gjøres gjeldende for sikkerhetsarbeidet: alt henger sammen med alt og det hjelper ikke hvor godt sikkerhetsarbeidet er et sted i verdikjeden, hvis det er mangelfullt andre steder. Gjennom påvirkningsoperasjoner og kompromittering av digitale verktøy kan enkeltindivider og den enkelte virksomhet utnyttes for å nå mål andre steder i verdikjeden. Derfor hviler det et ansvar på oss alle. Trusselaktører leter systematisk etter det svakeste ledd. Liten tue kan velte stort lass. ●

Foto: Cicillie S. Andersen



Kjetil Nilsen  
Direktør NSM

# RISIKOBILDET

## Norge står overfor økende risiko

Norge står overfor økende risiko for å bli rammet av sikkerhetstruende hendelser. Dette skyldes vedvarende, nye og et raskt økende antall sårbarheter, særlig innenfor det digitale domenet. Samtidig ser vi en negativ utvikling i trusselbildet. Dette kan medføre at samfunnskonsekvensene av hendelser som skyldes ondsinnede handlinger øker.



### **Etterretningsoperasjoner utgjør fremdeles en fremtredende trussel.**

NSM ser gjennom EOS-samarbeidet med Etterretningstjenesten og PST at etterretningstrusselen mot et stadig bredere spekter av norske virksomheter og interesser er betydelig. Fremmede stater retter nettverksoperasjoner også mot norske virksomheter og systemer som ikke selv forvalter tradisjonelt skjermingsverdig informasjon, og som tidligere har vært mindre aktuelle etterretningsmål. Dette utfordrer norske myndigheters og norske virksomheters sikkerhetsarbeid. Det er også et godt eksempel på hvordan det tradisjonelle skillet mellom stats- og samfunnssikkerhet viskes ut.

### **Konsekvensene kan bli store.**

NSM ser gjentatte forsøk på å etablere digital kontroll over og å innhente sensitiv informasjon fra virksomheter

som forvalter viktige og til dels kritiske samfunnsfunksjoner. Vår vurdering er at slik aktivitet kan få alvorlige og til dels uoverskuelige konsekvenser for stats- og samfunnssikkerhet. NSM har i løpet av det siste året koordinert håndtering av større og mer alvorlige digitale hendelser enn i tidligere år. I lys av disse hendelsene fremstår norske virksomheter som lite motstandsdyktige overfor denne typen nettverksoperasjoner.

### **Teknologiutviklingen skaper sårbarheter.**

Stadig flere enheter, prosesser og tjenester kobles sammen og til internett. Tjenesteutsetting er en attraktiv løsning for mange virksomheter. Denne utviklingen skaper digitale verdikjeder som er lange, komplekse, uoversiktlige og ofte internasjonale og til dels utenfor norske myndigheters kontroll. Den totale digitale angrepsflaten øker. Elementer som i utgangspunktet er godt

NSM ser gjentatte forsøk på etablering av digital kontroll over og innhenting av sensitiv informasjon fra virksomheter som forvalter viktige og til dels kritiske samfunnsfunksjoner.

sikret, eksponeres av sårbarheter hos svakt sikrede elementer i den samme verdikjeden. Risikoen Norge står overfor, øker som følge av at sårbarhetene blir flere og vanskeligere å kontrollere.

#### **Mennesket er en risikofaktor.**

En ansatt kan utnyttes eller uforvarende være en vei inn til virksomhetens verdier, ettersom vedkommende har tilgang til verdiene og fordi mennesket i seg selv i større eller mindre grad har sårbarheter en trusselaktør kan utnytte. I tillegg er mangel på tilstrekkelig kompetanse, både når det gjelder sikkerhetsbevissthet, generell IKT-kompetanse og spesialistkompetanse, en sårbarhet på nasjonalt plan og for mange virksomheter. Norske virksomheter

må i mange tilfeller se utenlands for å få tak i nøkkelkompetanse, noe som kan gi sikkerhetsmessige utfordringer. Kompetanseunderskuddet utgjør i økende grad en sårbarhet.

#### **Effektiv risikostyring og hendelses- håndtering er mangelvare.**

NSM har sett alvorlige eksempler på manglende kontroll over risiko i offentlige virksomheter, blant annet i svært komplekse informasjonssystemer uten tilstrekkelig planlegging, risikostyring og hendeshåndtering. Dette utgjør en alvorlig sårbarhet og illustrerer behovet for grundige verdi- og risikovurderinger, slik at ledelsen settes i stand til å iverksette de riktige tiltakene. ●

En ansatt kan utnyttes eller uforvarende være en vei inn til virksomhetens verdier.

---



# Verdifulle individer

Hvordan kan du som individ og ansatt rammes, og hva bør du tenke på for å sikre deg og verdiene du forvalter?

Enkeltindivider og deres aggregerte kunnskap utgjør en av de mest verdifulle ressursene en virksomhet forvalter. Samtidig utgjør de den virksomhetsressursen det er forbundet mest sårbarhet med. NSM ser at mange virksomheter ikke anerkjenner at deres ansatte kan utgjøre en vesentlig risikofaktor. En ansatt har eller vil kunne få tilgang til verdier, og enkeltindividene har i større eller mindre grad sårbarheter en trusselaktør kan utnytte.

# DIN DIGITALE ANGREPSFLATE

## «BreachCompilation» passorddump avslører 1,4 milliarder passord knyttet til brukernavn, deriblant en halv million norske

Mandag 4. desember 2017 ble en datapakke med 1,4 milliarder brukernavn og passord tilgjengeliggjort i fildelingstjenester. Svært mange nordmenn er rammet av denne lekkasjen. Lekkasjen omfatter også påloggingsinformasjon tilknyttet arbeidsgiver. Ved bruk av samme passord for flere typer kontoer og bruk av løpenumre og andre forutsigbare passord-systemer er man svært eksponert etter en slik lekkasje. Samtidig eksponerer du andres verdier som du har tilgang til.

## Treningsapp avslører lokasjoner som ikke er ment for offentligheten

Treningsappen Strava genererer kart som angir hvor det blir foretatt løpeturer i hele verden. I slutten av januar ble det offentlig kjent at kartet kan brukes til å identifisere både kjente og mindre kjente militære installasjoner i øde områder. Data fra treningsappen kan også identifisere personene som befinner seg i disse områdene. Elektroniske spor du personlig legger igjen gjennom mobiltelefon eller annet utstyr, kan innebære at du eksponerer sensitiv informasjon du ikke har rett til å dele.

## Varmeanlegget i et boligkompleks rammet av angrep mot tredjepart

I oktober 2016 ble automasjonssystemet for varmeanlegget i et boligkompleks i Finland utnyttet til å gjennomføre et DDoS-angrep mot en tredjepart. Hendelsen resulterte i at varmen skrudde seg av over en periode. Alle enheter med tilkobling til internett vil kunne utnyttes direkte eller indirekte dersom de ikke er sikret godt nok. Selv der angrepet ikke er ment å ramme deg, kan uventede følgeeffekter true funksjonaliteten til utstyret ditt.

EKSEMPLENE over er vidt forskjellige, men har én ting til felles: Informasjon og tilganger som blir tilgjengelig gjennom personlig digitalt utstyr og personlige kontoer kan brukes til å ramme både deg og andre.

Det digitale avtrykket en person i Norge legger igjen, blir stadig større. Flere tjenester fra det offentlige tilbys på nett, og ny programvare og nye apper som kan forenkle og berike livene våre, tas i bruk. Antall enheter tilkoblet internett, enten det er mobiler, klokker, gjenstander i husene våre, helseteknologi eller industrielle

enheter, øker eksponentielt. Det er positivt at gevinstene ved digitalisering realiseres, men uten tilstrekkelig sikring av internettilkoblede enheter og god sikkerhetsbevissthet hos brukerne vil denne utviklingen samtidig utfordre oss på måter vi bare ser konturene av.

Det siste halve året har NSM observert et mer nyansert bilde av de ulike teknikkene angriperne tar i bruk. Økonomisk motiverte aktører har tatt i bruk avanserte verktøy som har blitt lagt tilgjengelig på nettet. Samtidig, for å holde kostnadene nede og gjøre attribusjon vanskeligere,

velger avanserte angripere velkjente verktøy og enkleste vei inn, ikke den mest avanserte. Dette betyr at dersom en angriper ønsker tilgang til nettverket til din arbeidsgiver, eller til en virksomhet som din arbeidsgiver er underleverandør for eller samarbeider med, så kan dine passord, selv til personlige kontoer, være starten på veien inn. Dersom din konto er blant de hundretusener som har blitt frastjålet påloggingsinformasjon i løpet av de siste årene,<sup>1</sup> er en grundig sikkerhetssjekk av innstillinger og endring av passord på sin plass. Det er også observert at det settes opp videresending av all e-post på kompromitterte kontoer. Dette er lett å overse og gir tilgang til informasjon på kontoen, selv etter at passord er endret. NSM har i lengre tid registrert og understreket risiko forbundet med svak passordsikkerhet i norske virksomheter. Inntrengingstester NSM har gjennomført det siste året, viser ingen tegn til at denne sårbarheten reduseres.

Passordbeskyttelse av egne e-post-kontoer styrer vi selv, men mye av vårt digitale fotavtrykk er også representert ved teknologien, «dingsene», vi omgir oss med. Flere av de internettilknyttede produktene som tilbys på markedet nå, preges av svak passordsikkerhet og kode med fremtredende sårbarheter. Dette kan medføre at en angriper utnytter dine enheter og ditt nettverk som angrepsinfrastruktur.

Som eksempelet fra Finland viser, kan styringssystemer for hus, men også rutere, kameraer og mye annet, utnyttes ved å innlemme dem i såkalte «botnets», der enheten utfører operasjoner på vegne av en ondssinnet aktør. Enheten kan settes opp til å sende ut e-poster eller delta i såkalte tjenestenektangrep, DDoS,<sup>2</sup> mot en tredjepart. DDoS vil, på samme måte som kryptolåsning, bidra til at en tjeneste



blir utilgjengelig over en periode. Slike angrep kan true liv, helse og vår nasjonale beredskap dersom det blir utført mot kritiske systemer.

Sikkerhetsforskere oppdaget i oktober 2017 en ny type IoT<sup>3</sup>-skadevare som er langt mer potent enn det som er sett tidligere.<sup>4</sup> Det tar kort tid fra publisering av nye sårbarheter til skadevare som benyttes til å ta kontroll over IoT-enheter, utvides for å utnytte dem. En gjentagende spådom det siste året er at sikkerhetsproblemer knyttet til IoT vil øke, og at det vil dannes nye store botnet som er langt kraftigere enn de vi har sett hittil.

Totaliteten av det man må tenke gjennom og beskytte seg mot i det digitale domenet, kan virke overveldende. Svært mye løses imidlertid ved å bli bevisst på verdien man utgjør selv og verdiene man forvalter tilganger til. Ved å benytte sterke og oppdaterte passord, tofaktorautentisering<sup>5</sup> der det er mulig, installere oppdateringer til enheter man har anskaffet, og ellers aktivt styre graden av informasjonsdeling i apper, vil man ha langt bedre kontroll over sitt digitale fotavtrykk og den mulige angrepsflaten dette representerer. ●

Giovanni Domenico Tiepolo – Den trojanske hest blir dratt frem (omkring 1760). Er du med og trekker trehesten innenfor bymuren?

<sup>1</sup> Du kan selv undersøke om dine e-post-kontoer er berørt i store, kjente datalekkasjer på tjenesten «havebeenpwned.com».

<sup>2</sup> Et angrep der det dirigeres så mye trafikk mot en tjeneste at denne går ned og blir utilgjengelig for dem som trenger den. På engelsk: Distributed Denial of Service (DDoS).

<sup>3</sup> Internet of Things, og IIoT, Industrial Internet of Things. På norsk brukes begrepet «tingenes internett».

<sup>4</sup> Fra før av kjenner vi blant annet botnettet Mirai, som ble benyttet i angrepet mot Dyn-DNS i 2016.



# DU SOM VIRKSOMHETENS ANGREPSFLATE – OFFER OG ANGRIPER

## NSM «angrep» offentlig virksomhet – ni av ti ansatte lot seg lure

I 2017 utførte NSMs inntrengingstestere et «e-postangrep» mot en virksomhet i norsk statsforvaltning. En e-post utformet for å fange de ansattes oppmerksomhet og nysgjerrighet ble sendt til virksomhetens ansatte. E-posten inneholdt en simulert skadevare og en lenke som – hvis klikket på – dirigerte brukerne til en tilsynelatende legitim nettside som etterspurte brukerens påloggingsdetaljer.



- ▶ ni av ti klikket på den tilsynelatende legitime lenken
- ▶ fem av ti aktiverte den simulerte skadevaren
- ▶ tre av ti oppga sine påloggingsdetaljer til virksomhetens systemer

TRUSSELAKTØRER vil systematisk identifisere og utnytte det sikkerhetsmessig svakeste leddet. Økt fokus på digital sikring av verdier innebærer at trusselaktører i større grad innretter seg med andre metoder og mot andre sårbarheter. En ansatt utgjør en sårbarhet, en potensiell insider, fordi vedkommende har eller forventes å få tilgang til verdier og fordi mennesket i seg selv i større eller mindre grad har sårbarheter en trusselaktør kan utnytte. Menneskelige egenskaper som forlegenhet, hevn-gjerrighet, grådighet, begjær, takknemlighet, lojalitet, nysgjerrighet og naivitet kan alle utgjøre sårbarheter en trusselaktør kan utnytte til å presse, overtale, smigre, forføre, belønne og lokke ansatte til å eksponere sin virksomhets verdier.

Etterretningsoperatører kan bruke personopplysninger til forberedelse og gjennomføring av sine operasjoner.

De benytter seg effektivt av blant annet sosiale medier til å innhente slike opplysninger. Informasjon i sosiale medier kan sammenstilles til å gi et fylldig bilde av menneskelige sårbarheter og personlige og arbeidsrelaterte forhold som kan utnyttes. Sosiale medier utgjør også en arena hvor en trusselaktør med minimal risiko kan opprette initial kontakt med potensielle kilder og innhente sensitiv informasjon fra etablerte kilder.

I tillegg til tilsynelatende ufarlige opplysninger vi frivillig deler med kjente og ukjente i sosiale medier, kan lojalitetsbånd til eller personlige verdier lokalisert i andre stater utnyttes av en trusselaktør. *Tilknytning til andre stater* er derfor en potensiell sårbarhet som kan medføre at en ansatt utgjør en risiko. NSM observerer at omfanget av denne typen risiko øker i takt med blant annet økende internasjonalisering og behov for

<sup>5</sup> Tofaktorautentisering er å bekrefte din identitet med to ulike faktorer samtidig, det vil si med noe du vet, for eksempel passord, og noe du har, for eksempel kodebrikke eller mobiltelefon.



Vincenzo Camuccini:  
La morte di Cesare  
(omkring 1806). Caesar  
tas av dage av en  
insider i senatet.  
En insider kan være  
den beste inngangen  
til skjermingsverdige  
verdier for en trussel-  
aktør.

utenlandsk kompetanse. *Arbeidsrelaterte konflikter* er en tredje utfordring i ansettelsesforhold. Slike konflikter kan motivere en forulempet ansatt til å fremme eller hevne et gitt utfall ved å kompromittere, sabotere eller manipulere virksomhetens verdier.

Utnyttelse av en ansatt forutsetter ofte at trusselaktøren er kjent med *personlige, gjerne sensitive, opplysninger* om vedkommende. Personlige helseopplysninger er et eksempel på sensitiv informasjon som kan utnyttes. Slik informasjon som kommer på avveie, er både en personvernutfordring og en sikkerhetsutfordring.

En ansatt kan opptre som insider uten selv å være klar over det. Eksempelet over illustrerer hvordan en ansatt uforvarende kan eksponere virksomhetens verdier ved å aktivere skadevare på eller lekke påloggingsdetaljer til virksomhetens systemer. NSMs inntrengingstester og hendelser NSM har koordinert håndteringen av, vitner om at uforvarende innsidervirksomhet av denne typen utgjør en reell risiko.

Anerkjente internasjonale studier har avdekket at innsidesaker ofte oppstår tre til fem år inn i et arbeidsforhold. NSM observerer imidlertid at i mange virksomheter avtar sikkerhetsbevisstheten og sikkerhetsoppfølgingen av den ansatte samtidig med at ansettelsesforholdet modnes. Dette misforholdet understreker behovet for sikkerhetsrutiner som anerkjenner menneskelige sårbarheter som en vesentlig risikofaktor og som legger til rette for virksomhetsstyrt, helhetlig, integrert, vedvarende og inkluderende forebyggende innsats i alle virksomhetens ledd. NSM registrerer at for store ulikheter i risikoerkjennelsen mellom virksomhetens fag- og sikkerhetsansvarlige i noen tilfeller utfordrer forebyggende sikkerhetsaktivitet på virksomhetsnivå. Problemstillingen er særlig fremtredende i forbindelse med rekruttering av nøkkelpersonell. Dersom behovet for rask rekruttering av kompetent personell i slike prosesser trumfer hensynet til personellsikkerhet, påfører virksomheten seg vesentlig risiko for innsidervirksomhet og påfølgende tap av verdier. ●

NSMs inntrengingstestere utførte i  
2017 et «e-postangrep» mot en virksomhet  
i norsk statsforvaltning



9 av 10 klikket på den tilsynelatende legitime lenken



5 av 10 aktiverte den simulerte skadevaren



3 av 10 oppga sine påloggingsdetaljer  
til virksomhetens systemer

# Verdifulle virksomheter

Som ansatt, bruker av tjenester eller som kunde er vi alle tilknyttet én eller flere virksomheter. Sammen danner virksomhetene et nettverk av verdier som er viktige for samfunnet vårt. Hvordan kan vi best ivareta sikkerheten i dette komplekse nettverket og ha oversikten over helheten? Verdivurderinger og oversikter over sårbarheter danner grunnlaget for effektivt forebyggende sikkerhetsarbeid.

# HAR VI GJENNOMFØRINGSKRAFT? FRA IDÉ TIL TILTAK

## Fikk ikke ryddet opp i tide

Hos en virksomhet i norsk offentlig sektor har NSM ved tilsyn funnet avvik knyttet til sikkerhetsstyring og virksomhetens IKT-infrastruktur:

- ▶ Enkelte av avvikene gikk på helt grunnleggende prinsipper for IKT-sikkerhet (rettighetsstyring) nevnt i NSMs «Fire effektive tiltak mot dataangrep».
- ▶ En annen sårbarhet som ble observert, var *manglende patching*<sup>6</sup> og oppdatering av virksomhetens IKT-verktøy, noe som er en gjenganger i NSMs tilsynsfunn.
- ▶ Det var ikke tilstrekkelig skille mellom virksomhetens eksterne og interne nett, noe som kan gjøre det enklere for en trusselaktør å få 'en fot innenfor'.

Senere tilsyn med tre ulike leverandører av sikkerhetsgraderte anskaffelser til virksomheten har avdekket til dels alvorlige og grunnleggende mangler i leverandørenes sikkerhetsstyring, samt i den overordnede virksomhetens oppfølging av sikkerhetsgraderte anskaffelser.

Ved flere anledninger er sårbarhetene i IKT-infrastrukturen hos virksomheten siden blitt utnyttet av en trusselaktør som har plantet skadevare og forsøkt å få en fot på innsiden av systemet. Verdier hos virksomheten har blitt eksponert for trusselaktøren, og det har også vært fare for kompromittering av tilgrensende nettverk og servere.

Til tross for til dels alvorlige avvik og lang rettetid har tilsynet satt i gang et lovende initiativ hos tilsynsobjektet for å bedre arbeidet med forebyggende sikkerhet.

EN GJENGANGER blant NSMs tilsynsfunn er avvik som kan knyttes til sikkerhetsstyring og helhetlig tenkning om sikkerhet. Rutiner og instruksjoner mangler og daglig sikkerhetsmessig ledelse svikter. Sikkerhetstruende hendelser rapporteres bare sporadisk, og sporbarhet og logging er ofte ikke ivaretatt. NSM finner også avvik knyttet til sikkerhetsgodkjenning av graderte informasjonssystemer, og det gjennomføres i liten grad sikkerhetsrevisjoner. I mange tilfeller ville gode rutiner og sikkerhetsrevisjoner ha avdekket avvikene som oppdages ved tilsyn. At sikkerhetsstyring blir et svakt punkt,

bunner ofte i at den ikke er integrert i den generelle virksomhetsstyringen.

NSM har ved flere anledninger sett at man ved å bryte en fysisk barriere oppnår tilgang til skjermingsverdige eller graderte informasjonssystemer. Informasjonssystemet blir sårbart for et angrep dersom angrepet skjer i et område som i utgangspunktet var ment å beskytte systemet mot tilgang fra uvedkommende. Når risikovurderinger er gjort, blir ofte fysisk sikring og informasjonssystemets sikkerhet vurdert hver for seg, men det vil være en gjensidig avhengighet mellom fysiske sikringstiltak

<sup>6</sup> Patching av programvare vil si at brukerne laster ned et ekstra program som modifiserer en liten del av den originale koden, typisk for å rette sårbarheter som er oppdaget. Dette utføres ofte som en regelmessig rutine med oppdateringer fra programvareleverandør.

og informasjonssystemer. På den ene siden må informasjonssystemene sikres fysisk. Samtidig er de fysiske sikringstiltakene ofte avhengig av informasjonssystemer for tilgangsstyring. Ved kun å fokusere på ett av disse elementene, er faren stor for at man ikke oppnår en helhetlig og god sikkerhetstilstand.

I mange tilfeller gjøres det mye godt arbeid for å sikre enkelte verdier i en virksomhet. NSM ser imidlertid eksempler på at ulike sikringstiltak settes i verk uten at det foreligger grundige risikovurderinger. Sikringstiltak kan oppleves som inngripende og medføre store økonomiske utgifter. Det blir derfor avgjørende at det er de viktigste tiltakene som faktisk blir prioritert og implementert. For å kunne gjøre en reell prioritering må risikovurderinger ligge til grunn. På denne måten kan verdiene, truslene og sårbarhetene identifiseres, og samlet risiko vurderes.

I vår nettverksbaserte verden er det også viktig å ikke miste andre virksomheter av syne i en slik prosess. Den enkelte bedrift

er avhengig av og er en del av nettverket til andre bedrifter. Slik representerer ulike virksomheter verdier for hverandre. Sikringstiltak som er basert på gode verdi-, sårbarhets- og risikovurderinger vil kunne gi god lønnsomhet. Dette fordi de bidrar til å holde virksomhetens aktiviteter trygt på rett spor, samtidig som de gjør virksomheten til en sikker og attraktiv samarbeidspartner for de øvrige virksomhetene i en verdikjede.

I tillegg til å integrere sikkerhetsstyring i virksomhetsstyringen, bør det legges til rette for god sikkerhetskultur i virksomheten. Beslutninger om sikringstiltak er ikke bare avhengig av sikkerhets- og risikoforståelse, men vil også påvirkes av den rådende sikkerhetskulturen. Sikkerhetskultur preger også hvordan virksomhetens innførte sikringstiltak etterleves av virksomhetens medarbeidere. Det er viktig at ikke bare de som jobber dedikert med sikkerhet, er årvåkne og sikkerhetsbevisste. Alle medarbeidere må bevisstgjøres, og alle må være med å trekke lasset. ●



Ved å integrere sikkerhet i tidlig planlegging kan barrierene være i stil med øvrige omgivelser. Disse blomsterpottene markerer både en grense og er effektive mot kjøretøy. (Foto: NSM)



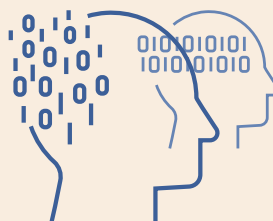


Ikke alle barrierer er like effektive, og kan gi falsk trygghet. Det er viktig å vite hva barrierene dine kan motstå og hva de er til for. (Foto: NSM)

# FLINKE NOK? NORSK KOMPETANSE

## Dagens kryptering står for fall – verdier er truet

Hos Shakespeare tillegges Richard III uttalelsen «en hest, en hest, mitt kongerike for en hest». Mye tyder på at ledere om kort tid vil rope «En kryptolog! En kryptolog! Mitt rike for en kryptolog!». Kvantedatamaskinene vil snart være over oss og med dem mister dagens krypto sin kraft. Norge sliter med å utdanne kryptologer som kan være med å skape fremtidens kryptosystemer som er helt avgjørende for å sikre landets verdier. Richard III tapte slaget ved Bosworth. Er vi i ferd med å tape slaget mot kvantedatamaskinene?



DET ER ikke alltid tilstrekkelig at vi vet at noe må gjøres. Riktig kompetanse er også nødvendig, og tiltak må implementeres på riktig måte. Gjennom tilsyn og annen aktivitet hos NSM fremgår det at det er betydelige svakheter innen sikkerhetsbevissthet og sikkerhetskompetanse generelt. Mangelfull kompetanse har konsekvenser blant annet for hvordan IKT-systemer og -programmer er designet og koblet sammen, og hvordan rutiner og styringssystemer er utformet og fulgt opp sikkerhetsmessig. Det økende gapet mellom tilgjengelighet og behov for sikkerhetskompetanse utgjør en nasjonal sårbarhet.

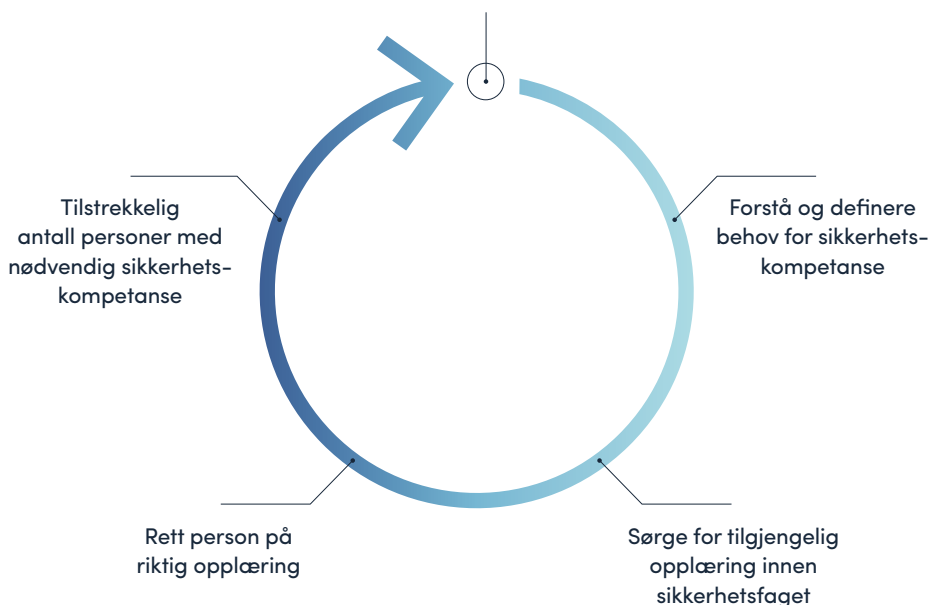
Uten sikkerhetskompetanse vil det være vanskelig for en virksomhet å forstå den risikoen man utsetter verdiene sine for. Får man i det hele tatt med seg at IKT-systemene ble kompromittert? En trusselaktør kan bevege seg rundt i et

nettverk uten å bli oppdaget. Da kreves fagkompetanse og gode mekanismer for å oppdage angrepet. Når en kompromittering har funnet sted, enten det har skjedd i det fysiske eller i det digitale rom, så kreves det kunnskap om

Ved NSMs kurscenter tilbys en rekke kurs innen forebyggende sikkerhetsarbeid.



## Fokus på sikkerhet



hendelseshåndtering.

Riktig fokus på sikkerhet i en virksomhet fordrer at man forstår og kan definere behovet for sikkerhetskompetanse i den enkelte bedrift. Her er kartlegging av allerede eksisterende kompetanse samt av kompetansegap viktig. Deretter er det viktig å utvikle et relevant utdanningstilbud som ansatte med behov kan delta på, slik at virksomhetene til slutt sitter igjen med nok personer med nødvendig sikkerhetskompetanse.

Både NSM og andre har de siste årene påpekt at det utdannes for få med IKT-sikkerhetskompetanse i Norge. IKT-sikkerhet bør ikke bare være en spesialisering, men en obligatorisk del av alle IKT-utdannelse, allerede fra grunnskolen. For å sikre den kompetansen vi trenger i fremtiden, er det også viktig å tenke langsiktig og legge et godt grunnlag så tidlig i et utdanningsløp som mulig. Grunnleggende IKT-sikkerhetskompetanse

bør også vurderes i en rekke andre utdannelse slik at flere har forståelse for og kompetanse om hvordan IKT kan brukes på tryggest mulig måte.

I en medlemsundersøkelse om IT-kompetanse gjennomført av Abelia er det avdekket at halvparten av de spurte virksomhetene vil trenge mer kompetanse innen dataanalyse og IT-sikkerhet fem år frem i tid. Også IKT-Norge viser i sin kompetanseundersøkelse til at det er et økende behov for IT-sikkerhet. Det er opprettet studieplasser i den senere tid, men utviklingen innen IKT skjer raskt, og mye tyder på at opprettelsen av nye læringsplasser tar for lang tid. For å bidra til økt sikkerhetskompetanse generelt har NSM etablert et kurscenter for forebyggende sikkerhet. Her tilbys en rekke kurs knyttet til sikkerhetsloven og forebyggende sikkerhetsarbeid. Vi samarbeider dessuten med Forsvaret om sikkerhetsutdanning. ●



# Verdifull infrastruktur

Nettverk, digitale og fysiske, kjennetegner vår verden.  
Verdiene vi ønsker å beskytte, er knyttet sammen.  
Gjennom ansettelsesforhold kobles den enkeltes verdier  
til ulike virksomheters verdier. Virksomhetene er igjen  
knyttet til hverandre gjennom komplekse verdikjeder.  
Mange virksomheter forvalter verdier som utgjør kritiske  
samfunnsfunksjoner. Slik er den enkeltes verdier knyttet  
sammen med samfunnets verdier i det store bildet.

# HVEM TAR VARE PÅ VÅRE VERDIER?

## Nødnettet i krise

I februar 2017 ble det kjent at Nødnett i lengre tid hadde vært driftet fra utlandet av IT-arbeidere uten sikkerhetsklarering. Nødnettet er samfunnskritisk infrastruktur og sentralt i all nød-, krise- og beredskapskommunikasjon. Blant andre er politiet, andre nødetater og Forsvaret brukere av Nødnett. I sine undersøkelser fant Nasjonal kommunikasjonsmyndighet at deler av Nødnett potensielt kunne blitt satt ut av drift via fjernpålogging fra utlandet.



DET ER EN økende trend at private og offentlige virksomheter velger å tjenesteutsette hele eller deler av sine IKT-tjenester. Ofte skjer dette til utlandet. Tjenesteutsetting er i mange tilfeller økonomisk motivert. Eksempelvis vil visse typer IKT-tjenester kunne leveres rimeligere via fjerndrift fra lavkostland. I andre tilfeller velges det å benytte sentraliserte spisskompetansemiljøer i utlandet, fremfor å bygge opp kompetanse nasjonalt.

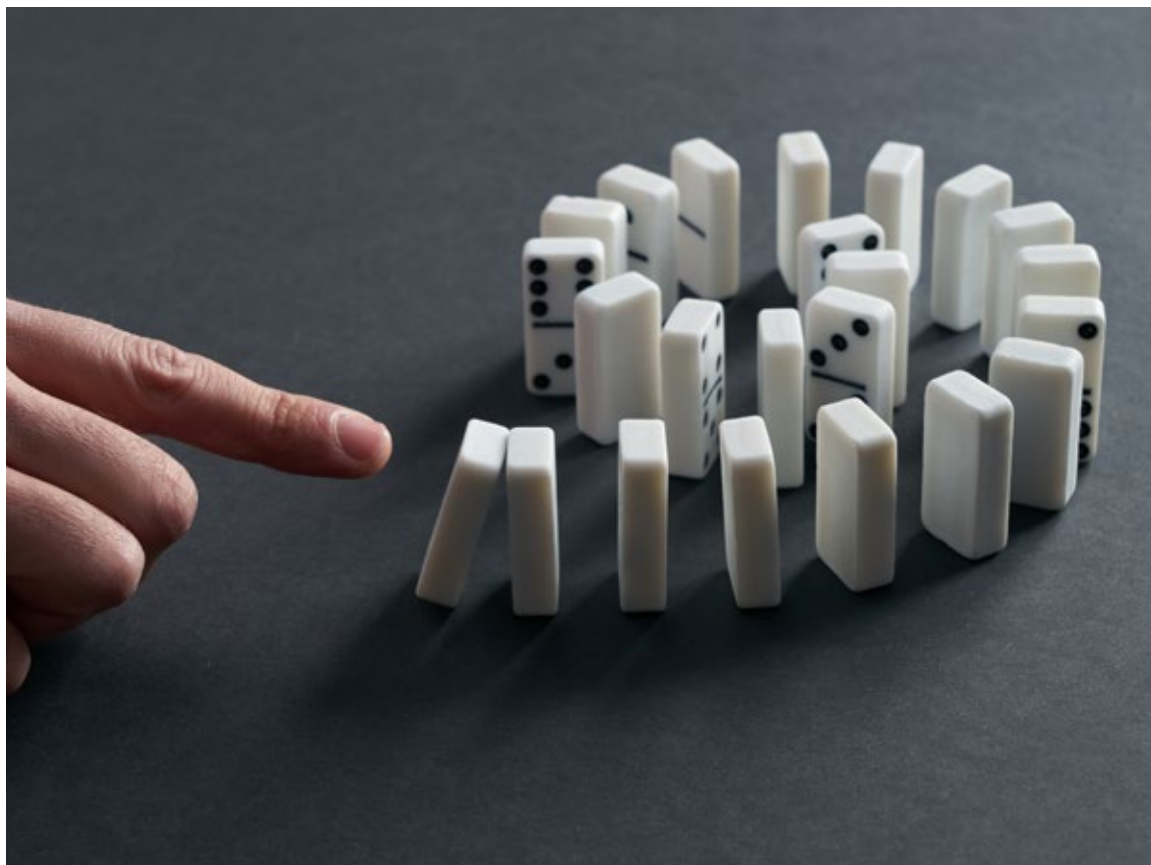
Økende bruk av tjenesteutsetting gjelder også for virksomheter som leverer tjenester som understøtter samfunnets beredskap og krisehåndtering. Dette er leveranser som må være mer robuste og tilgjengelige enn vanlige kommersielle løsninger, fordi de skal fungere i situasjoner hvor mye annet er utilgjengelig. Dette må tas hensyn til når tjenesteutsetting vurderes. Det blir stadig mer krevende å ha oversikt over allerede komplekse verdikjeder ved økende digitalisering av samfunnet. Tjenesteutsetting kan bidra

til å øke risikoen ved ytterligere å øke kompleksiteten i verdikjeden.

Erfaringer fra NSMs operative virksomhet og andre statlige tilsynsorganer viser at det er lav bevissthet rundt krav til og oppfølging av informasjonssikkerhet ved tjenesteutsetting av IKT-tjenester. Risikovurderinger og konsekvensutredninger som utføres ved tjenesteutsetting, er ofte mangelfulle. NSM er bekymret for at samfunnskritiske IKT-tjenester tjenesteutsettes uten tilstrekkelige risikovurderinger og sikringstiltak, og at data flyttes til utlandet uten tilstrekkelige sikkerhetsfaglige vurderinger.

Tjenesteutsetting av IKT-tjenester til profesjonelle aktører kan gi bedre sikkerhet og mer stabile og tilgjengelige tjenester. Samtidig må virksomheter være bevisst hvilken risiko en tjenesteutsetting medfører. En tjenesteutsetting stiller store krav til egen virksomhet og krever annen kompetanse enn om tjenesten leveres av egen organisasjon.

En eventuell tjenesteutsetting av IKT-



tjenester krever grundig verdivurdering. Tre prinsipper for informasjonssikkerhet er alle like viktige å ta hensyn til: å hindre at uvedkommende får tilgang til informasjonen (*konfidensialitet*), å sikre at det er uforfalsket informasjon (*integritet*) og å sikre at den som skal ha informasjonen, faktisk har tilgang til den (*tilgjengelighet*). Tradisjonelt har hensynet til uautorisert tilgang fått mest oppmerksomhet, men alle tre prinsippene er like viktige og må vurderes helhetlig.

For å ivareta IKT-sikkerheten ved tjenesteutsetting, anbefaler NSM at virksomheten er bevisst behovet for:

- 1 God bestillerkompetanse
- 2 Oversikt og kontroll på hele livsløpet for anskaffelsen
- 3 Gode risikovurderinger for å kunne ta riktig beslutning
- 4 Riktige og gode krav til IKT-tjenesten og til leverandør
- 5 Riktig beslutning på riktig nivå



Komplekse verdikjeder gjør godt sikkerhetsarbeid og god sikkerhetsstyring ekstra viktig. En nøkkel på avveie eller et tastetrykk kan potensielt gjøre stor skade.



# SMÅ TUER KAN VELTE STORE LASS

## NSMs OBSERVASJONER

### Fysisk tilgang gir trusselaktør mange muligheter

- 1 NSM fikk fysisk tilgang til lokalene til en offentlig virksomhet ved diskret å ta seg inn en dør som på grunn av treghet i dørpumpen sto åpen forholdsvis lenge etter at en person med legitim tilgang hadde gått inn. Testpersonellet gjemte seg på virksomhetens toalett inntil alle ansatte hadde gått hjem for dagen, og sto dermed fritt til å koble fordekte digitale enheter til virksomhetens nettverk.
- 2 NSM fikk fysisk tilgang til en offentlig virksomhet ved å ta seg inn en åpen kantinedør de ansatte brukte for å trekke frisk luft. Vel inne i lokalene fant teamet fysiske tilkoblingsmuligheter på taket. Virksomheten var trolig ikke klar over tilkoblingsmuligheten,

og det var liten sannsynlighet for at kompromittering kunne bli oppdaget.

- 3 NSM fikk ulegitimert tilgang til et møterom i resepsjonen til en offentlig virksomhet. Møterommet hadde fysiske tilkoblingsmuligheter som ble utnyttet til å «kompromittere» virksomheten.

### Digital tilgang kan komme fra uventet hold

En offentlig virksomhet ble «kompromittert» av NSM i en inntrengingstest. Inngangsporten til hele nettverket var i dette tilfellet plassert på virksomhetens kjøkken; det var en IoT-enhet som drev kjølesystemet.

TILSYNELATENDE små hendelser og banale detaljer kan utløse store, alvorlige sikkerhetstruende hendelser. En trusselaktør trenger kun å identifisere og utnytte én enkelt sårbarhet i ett enkelt domene for å få en fot innenfor. Du må kjenne alle dine sårbarheter, enten de handler om virkelighetsforståelse og samhandling eller befinner seg i det fysiske eller digitale rom.

I 2017 ble det rapportert inn 14712 digitale sårbarheter til en felles, global referansedatabase som fikk et såkalt CVE-nummer (Common Vulnerabilities and Exposures). Det er mer enn en dobling siden 2016 da det ble rapportert

inn 6447 sårbarheter. NSM må daglig vurdere varsling om nye sårbarheter som kan være relevante for norske virksomheter. Man må alltid være på utkikk etter sårbarheter som blir aktivt utnyttet kort tid etter at leverandøren har publisert sikkerhetsoppdateringer. Flere av angrepene og hendelsene beskrevet i rapporten, muliggjøres nettopp av en gitt sårbarhet i ett eller flere produkter. En av de største og mest alvorlige hendelsene i 2017, spredningen av krypteringsviruset WannaCry, ble muliggjort av en sårbarhet i Windows. Denne sårbarheten ble adressert og rettet av Microsoft (MS17-010) to måneder før angrepet fant sted.

## INTERNASJONALE EKSEMPLER

### Omfattende påvirkningsoperasjon startet med Gmail-login på avveie

Et samlet amerikansk etterretningsmiljø vurderer det som sannsynlig at en fremmed makt forsøkte å påvirke den amerikanske presidentvalgekampen høsten 2016. Påvirkningsforsøket ble iscenesatt med utgangspunkt i sensitiv informasjon innhentet fra en kompromittert privat e-postkonto.

### Eksisterende sikkerhetsoppdatering kunne hindret tidenes største datavirus

En av de største og mest alvorlige cyberhendelsene i 2017, som i utlandet fikk konsekvenser for kritiske samfunnsfunksjoner, var ormen som spredte krypteringsviruset WannaCry. Ormen utnyttet en sårbarhet i Windows. Microsoft hadde to måneder tidligere utviklet en sikkerhetsoppdatering som lukket sårbarheten som ville hindret spredning av viruset dersom brukerne hadde installert oppdateringen. Stort etterslep på sikkerhetsoppdateringer hos virksomhetene fører likevel til at slike angrep får store konsekvenser.

### Tjenestenekt forsinket svensk jernbane i flere dager

Onsdag 11. september 2017 ble det svenske Trafikverket (tilsvarende Bane NOR i Norge) og flere andre virksomheter tilknyttet svensk jernbane utsatt for tjenestenektangrep mot noen av sine web-baserte tjenester. Blant disse tjenestene var systemene for overvåking og dirigering av tog. Dette skapte varierende grad av forsinkelser i en og en halv dag, da togene måtte over på manuell kontroll. Det ble aldri klart hvem som utførte disse angrepene. Det kan ha vært guttestreker eller noen som testet det svenske jernbanenettets krisekapabiliteter.


Etterslep på sikkerhetsoppdateringer hos virksomhetene fører likevel til at slike angrep får store konsekvenser.

NSM har i 2017 håndtert og koordinert håndtering av et høyere antall sikkerhetstruende hendelser og flere nasjonale og internasjonale kriser i det digitale rom enn i tidligere år. NSM registrerte rundt 22.000 uønskede hendelser mot informasjonssystemer i 2017. Ca. 5200 av disse ble fulgt opp videre av NSM NorCERT.

NSM observerer flere utviklingstrekk blant de mer alvorlige digitale hendelsene – de som omhandler etterretningsvirksomhet eller som truer viktige samfunnsfunksjoner. NSM registrerer at trusselaktører nå i stor grad krypterer data som hentes ut fra kompromitterte systemer i motsetning til foregående år, da krypterte kommunikasjonskanaler mellom trusselaktør og kompromitterte ble observert ved et fåtall tilfeller. Dette gjør det ressurskrevende og i noen tilfeller urealistisk å identifisere informasjonen som kommer på avveie eller i det hele tatt å avdekke at data hentes ut. Antallet hendelser som dreier seg om at trusselaktører etablerer kontroll over og utnytter nettverk og servere i Norge til å utføre nettverksoperasjoner mot andre mål i og utenfor Norge, er økende. NSM registrerer totalt sett et noe høyere antall alvorlige digitale hendelser enn i foregående år.

Angrepsmetodene skiller seg i noen grad fra foregående år. Særlig fremtredende er nedgangen i antall tilfeller av kompromittering som følger av målrettet e-post (spearphishing). Utnyttelse av legitime påloggingsdetaljer og vannhullsangrep er blant angrepsmetodene som har økt noe.

Gjennom disse hendelsene og gjennom



Tilsynelatende små hendelser  
og banale detaljer kan  
utløse store, alvorlige  
sikkerhetstruende hendelser.

---

NSMs tilsyn, inntrengingstester og øvrige oppgaver som sikkerhetsmyndighet ser vi stadige eksempler på små og store hull i gjerdene til viktige norske virksomheter. Enkelte steder sitter vi igjen med et inntrykk av at virksomhetens ledelse ikke har kontroll over hvilke hull som finnes, eller hvor gjerdet går. En slik mangel på kontroll over sikkerhetsrisiko kan være alvorlig nok for ens egen virksomhet, men kan bli langt mer alvorlig dersom virksomheten forvalter en viktig samfunnsfunksjon.

I en verden som er i ferd med å gjennomdigitaliseres, er mange av de viktigste barrierene som beskytter oss, våre virksomheter og vår infrastruktur, digitale. Samtidig er vi blitt avhengige av at digitale tjenester er konstant tilgjengelige og tilkoblet nett for å opprettholde viktige samfunnsfunksjoner. Konsekvensene kan bli alvorlige og er til dels uoverskuelige. Vi har sett eksempler på trafostasjoner som blir slått av gjennom digitale angrep og at valg kan påvirkes ved at små sårbarheter utnyttes. Anledningen til å kunne stjele sensitiv informasjon, svindle virksomheter for penger eller i verste fall skru av knappen til en viktig samfunnsfunksjon handler om tålmodighet og målrettet jakt etter hullene i gjerdet.

Dette blir spesielt utfordrende når virkemidler koordineres, for eksempel gjennom kombinasjoner av virkemidler som nettverksoperasjoner, sabotasje, etterretningsvirksomhet og påvirkningsoperasjoner. Bruken av fordekte virkemidler gir en trusselaktør taktiske og strategiske fortrinn, og gjør det vanskelig for den angrepne parten å oppdage og verifisere at den er

**Trusselaktørene blir stadig mer profesjonelle, målrettede og kompetente, og for å stoppe dem må vi ha kontroll på våre egne sårbarheter og oversikt over vår egen risiko.**

---

utsatt for sammensatt virkemiddelbruk. Hensikten med slike operasjoner kan blant annet være å undergrave politiske beslutningsprosesser i nasjonale eller internasjonale fora, eller langsiktig svekkelse av et samfunn. Norge har sikkerhetsmekanismer som kan motvirke slike virkemidler isolert sett. Spørsmålet som melder seg er om vi har en tilstrekkelig nasjonal evne til å se bruken av sammensatte virkemidler i sammenheng.

Som nylige hendelser har vist, og som Etterretningstjenesten og PST beskriver i sine trusselvurderinger, er ikke spørsmålet om det finnes aktører som systematisk leter og finner de minste hullene i våre gjerdet, men *hvor* og *når* de slår til og hva de er i stand til å utrette av skade når de er på innsiden. Trusselaktørene blir stadig mer profesjonelle, målrettede og kompetente, og for å stoppe dem må vi ha kontroll på våre egne sårbarheter og oversikt over vår egen risiko. Sammenkoblingene og avhengighetene mellom systemer, infrastrukturer, virksomheter og samfunnsfunksjoner gjør oss stadig mer sårbare for at en liten feil eller sikkerhetshull ett sted kan gi store konsekvenser et annet sted. Selv små tuer kan velte store lass. ●

Som nylige hendelser har vist, og som Etterretningstjenesten og PST beskriver i sine trusselvurderinger, er ikke spørsmålet om det finnes aktører som systematisk leter og finner de minste hullene i våre gjerder, men *hvor* og *når* de slår til og hva de er i stand til å utrette av skade når de er på innsiden.

**NASJONAL SIKKERHETSMYNDIGHET**

Postboks 814, 1306 Sandvika

Tlf. 67 86 40 00

[post@nsm.stat.no](mailto:post@nsm.stat.no)

[www.nsm.stat.no](http://www.nsm.stat.no)

