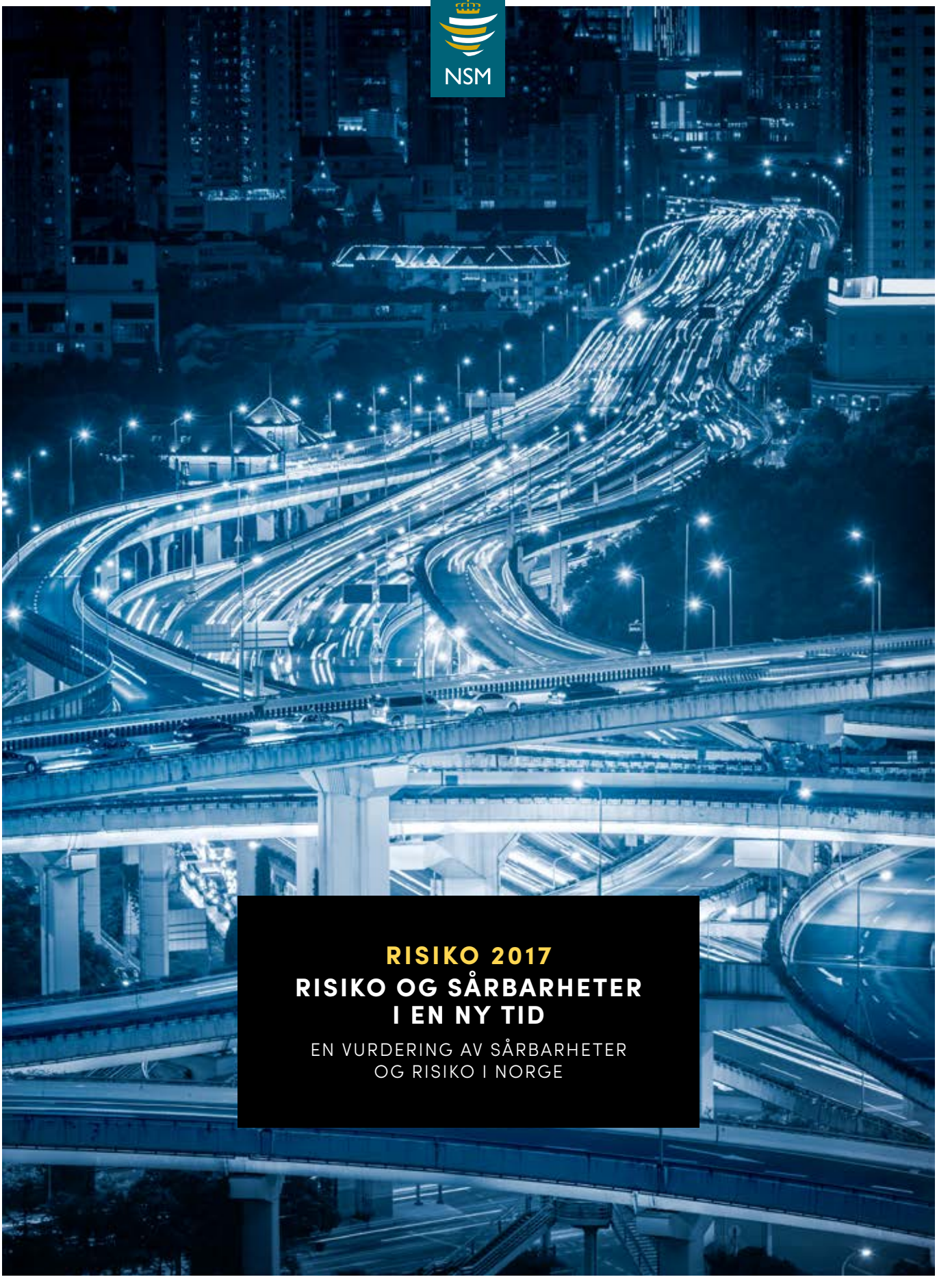


NSM

RISIKO 2017

RISIKO OG SÅRBARHETER I EN NY TID

EN VURDERING AV SÅRBARHETER OG RISIKO I NORGE

NSMs rapport «Risiko 2017» 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 2017» 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 beslutnings¬prosesser med informasjon av spesiell interesse for norsk utenriks-, sikkerhets- og forsvarspolitikk. I årets vurdering «Fokus 2017» 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 tids-horisont på ett år, og utgis i første kvartal.

Direktoratet for samfunnssikkerhet og beredskap (DSB) skal ha oversikt over risiko og sårbarhet i samfunnet. DSB har utgitt scenarioanalyser siden 2011.[1] 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.

Politiets sikkerhetstjenestes (PST) primære ansvar er å forebygge og etterforske straffbare handlinger mot rikets sikkerhet. PSTs årlige trusselvurdering omhandler forhold fortrinnsvis i Norge som kan påvirke norsk sikkerhet og skade nasjonale interesser i det kommende året. Blant disse er trusler fra statlige aktører i form av utenlandske etterretningstjenester, aktuelle etterretningsmål og tjenestenes operasjonsmønster i Norge. Vurderingene tar også for seg trusler fra ikke-statlige aktører, og da særlig trusler om politisk motivert vold fra ekstreme grupper eller enkeltpersoner. Analysen har en tidshorisont på ett år, og utgis i første kvartal.

[1] DSBs scenarioanalyser het t.o.m. 2015 «Nasjonalt risikobilde». F.o.m. 2016 er navnet endret til «Krisescenarioer (årstall) – analyser av alvorlige hendelser som kan ramme Norge».

Innhold

RISIKO 2017

Foto omslag:
SCANPIX

Design:
REDINK

Foto:
ISTOCK, SCANPIX, COLOURBOX

Trykk og distribusjon:
RK GRAFISK

Forord

I RISIKO 2017 vurderer NSM sårbarheter i samfunnet og risiko forbundet med tilsiktede handlinger som kan ramme viktige samfunnsfunksjoner.

Digitaliseringen av samfunnet skaper hele tiden nye verdier og utviklingsmuligheter, men utvider også sårbarhetsflatene til det vi ønsker å beskytte. Utfordringene i det digitale rom er grenseoverskridende og går på tvers av stater, sektorer og virksomheter. Hurtigheten og endringstakten utfordrer også IKT-sikkerhetsarbeidet. Hvilke strategiske valg og tiltak som iverksettes fra myndighetene for å styre utviklingen av samfunnet og redusere risiko, blir avgjørende.

Virksomhetene har primæransvaret for å beskytte sine verdier og bygge robusthet og motstandsdyktighet mot cyberangrep. Myndighetene koordinerer, gir råd og legger til rette for at Norge har tilstrekkelig motstandskraft i det digitale rom. Investering i IKT-sikkerhet er nødvendig, slik at vi skaper tillit til at det er trygt å etablere og drive næringsvirksomhet i Norge.

Sikkerhetstruende hendelser mot skjermingsverdige objekter vil med stor sannsynlighet skje uten forvarsel. Det er derfor viktig å jobbe systematisk med det forebyggende objektsikkerhetsarbeidet, gjennom å legge til rette for en helhetlig tilnærming på tvers av samfunnssektorene når det gjelder utvelgelse, beskyttelse og tilsyn med skjermingsverdige objekter.

Mennesker kan utgjøre et svakt punkt i virksomheter. Innsidere med legitim tilgang har ikke bare tilgang til virksomhet, systemer, informasjon eller prosesser, men kan også kjenne til svakhetene ved tiltak og prosedyrer som skal sikre verdier. Det innebærer en risiko for at tilsiktede uønskede handlinger kan utføres av egne ansatte eller innleide. Bevisstgjøring og holdningsskapende arbeid er sentrale mottiltak.

Hybride trusler visker ut det tradisjonelle skillet mellom fred og krig og utfordrer tradisjonell ansvarsplassering mellom sivil og militær sektor. Bruk av informasjonsoperasjoner for å påvirke demokratiske prosesser og destabilisere samfunn har fått økt oppmerksomhet i den senere tid. Et av virkemidlene som brukes, er fordekt påvirkning av politiske prosesser, noe som har blitt aktualisert gjennom hendelser i den amerikanske valgkampen. I 2017 skal det gjennomføres flere valg i Europa, blant annet i Norge. For å avverge at liknende hendelser skal skje i Norge, er det viktig

å skape motstandsdyktighet og redusere sårbarheter.

For å kunne beskytte verdiene våre må vi ta tak i det vi kan gjøre noe med, og det handler ofte om å redusere samfunnets og virksomheters sårbarheter. Dette oppnås gjennom forebyggende sikkerhetstiltak og etablering av god grunnsikring. I tillegg til dette er det viktig å ha god evne til å oppdage og håndtere hendelser på alle nivåer i samfunnet.

Målet med denne rapporten er at beslutningstakere både i offentlig og privat sektor skal få et bedre grunnlag for å redusere risiko i egen virksomhet og i samfunnet. Gjennom systematisk sikkerhetsarbeid vil det være mulig å redusere sårbarhetene og dermed oppnå bedre sikkerhet.

«Digitaliseringen av samfunnet skaper hele tiden nye verdier og utviklingsmuligheter, men utvider også sårbarhetsflatene til det vi ønsker å beskytte.»

Kjetil Nilsen
Direktør

Sikkerhetstilstanden

NORGE ER ET av verdens tryggeste land, og voldsnivået er lavt. Landets økende velstand og utviklingen av velferdsstaten har ført til at Norge ofte rangerer høyt på oversikter over de beste land å bo i. Befolkningen har høy tillit til myndighetene. Det er samtidig en forventning til at myndigheter og viktige samfunnsaktører sikrer at samfunnsfunksjonene våre fungerer. Dette fordrer blant annet et godt forebyggende sikkerhetsarbeid for å skape et samfunn som er motstandsdyktig mot angrep fra ulike aktører. Forebyggende sikkerhet handler om å sikre verdier i form av informasjon, objekter og viktige samfunnsfunksjoner, både nå og i fremtiden.

NSM vurderer risiko gjennom å analysere forholdet mellom verdier vi ønsker å beskytte, hvilke trusler som kan ramme disse verdiene og sårbarhetene som trusselaktører kan utnytte. Risikobildet er i endring som følge av den generelle samfunnsutviklingen. Nye verdier skapes, nye sårbarheter etableres og trusselbildet er i stadig endring.

OVERORDNET RISIKOBILDE

NSM vurderer at mangelfull planlegging og styring av sikkerhetsarbeidet fortsatt er en utfordring. Dette er alvorlig da god styring av sikkerhetsarbeidet er fundamentet for å gjennomføre sikringstiltak på en måte som er tilpasset den enkelte virksomhets risiko.

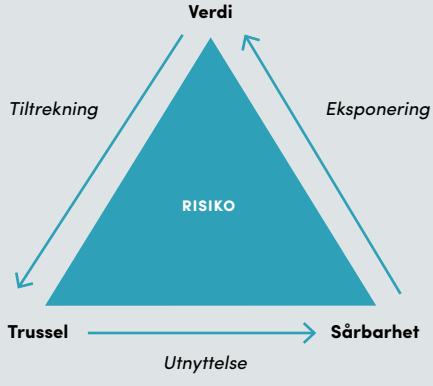
Gjennom flere år har NSM sett en jevn økning av antall målrettede cyberangrep mot norske interesser, både offentlige og private. Disse angrepene utgjør en trussel mot våre verdier. NSM ser tegn på økt bevissthet om tekniske sårbarheter i mange virksomheter, men gjennomføring av sårbarhetsreduserende tiltak skjer ikke med samme takt som utviklingen i trusselbildet.

Også på flere andre områder ser vi en negativ utvikling. Verdikjedene har blitt mer komplekse, og samfunnets avhengighet av ulike tjenester har økt. Fokus er ofte på brukervennlighet fremfor sikkerhet. Vi ser en negativ

FAKTA

RISIKOTREKANTEN

De grunnleggende sammenhengene mellom verdier, trusler og sårbarheter er illustrert i modellen nedenfor.



NSM bruker begrepene verdi, trussel og sårbarhet i sine risikovurderinger. Risiko defineres som forholdet mellom disse tre faktorene. Denne modellen er ofte omtalt som risikotrekanten.

utvikling når det gjelder fragmenterte IKT-løsninger og for mange små drifts- og forvaltningsmiljøer. Heller ikke objektsikkerhet ivaretas i tilstrekkelig grad. Innenfor alle disse områdene kan den negative trenden forsterkes ytterligere, dersom forebyggende tiltak ikke iverksettes.

UTILSTREKKELIG STYRING AV SIKKERHETSARBEIDET

Nøkkelen til å skape motstandsdyktige systemer innen forebyggende sikkerhet ligger i styring av sikkerhetsarbeidet. Mangelfull planlegging og styring av sikkerhetsarbeidet har vært et gjennomgående tema i NSMs vurderinger over flere år. God styring av sikkerhetsarbeidet er grunnlaget for å gjennomføre sikringstiltak på en måte som er tilpasset den enkelte virksomhets risiko. Slike sikringstiltak omhandler blant annet klarering og autorisering av personer som skal jobbe med sikkerhetsgradert informasjon, sikring av informasjonen på IKT-systemene i virksomhetene og fysiske sikringstiltak. NSMs erfaring viser at det er utfordrende for virksomheter å etablere god sikkerhetsstyring.

Den overveiende delen av avvik som er avdekket gjennom NSMs tilsyn, burde virksomhetene selv ha avdekket gjennom interne sikkerhetsrevisjoner. Uten at sikkerhetsrevisjoner er gjennomført, blir også grunnlaget for ledelsens evaluering svakt, noe som igjen kan føre til feil prioriteringer av korrigerende tiltak for å redusere risikoen mot virksomhetens verdier.

ØKNING I CYBERANGREP

Tilsiktede uønskede handlinger er en økende trussel mot våre verdier. Slike handlinger utføres ofte av aktører som er krevende å kartlegge. NSM har gjennom flere år sett en tydelig og jevn økning av antall målrettede cyberangrep mot norske interesser, både offentlige og private. Cyberangrepene er mer avanserte og blir mer profesjonelt utført. Vanlige mennesker blir i økende grad ofre, og store økonomiske verdier går tapt hvert år.

PST skriver i sin trusselvurdering at norske interesser i tiden som kommer vil utsettes for etterretningsvirksomhet fra fremmede stater, spesielt knyttet til mål innenfor forsvars- og beredskapssektoren, politiske beslutningsprosesser og kritisk infrastruktur. NSM registrerer også at statlige aktører forsøker å etablere seg i norske offentlige virksomheters digitale infrastruktur. Dette utgjør betydelig risiko for offentlig forvaltning og for virksomheter som forvalter kritisk infrastruktur, kritiske samfunnsfunksjoner og høyteknologi. Trusselaktører følger med på de mest attraktive målene kontinuerlig, slik at den minste sårbarhet kan utnyttes i det øyeblikk den oppstår. Det har det siste året vært en rekke datanettverksoperasjoner rettet mot statlig forvaltning. Det har vært forsøk på digital spionasje både mot departementer og underliggende enheter. NSM vurderer nettverksoperasjoner fra fremmede stater som den høyeste IKT-risikoen for offentlig forvaltning.

NSM vurderer at økning i alvorlige cyberangrep, kompromittering av

nettverk i mindre virksomheter, bruk av cyberangrep og stjålet informasjon til påvirkning og et stort volum økonomisk motiverte hendelser er trender som vil fortsette i 2017 og videre fremover.

SÅRBARE VERDIKJEDER

Økt digitalisering kan bidra til å gjøre kritiske samfunnsfunksjoner sårbare. Som en følge av digitaliseringen er ofte mange virksomheter knyttet sammen i produksjon av varer og tjenester, noe som skaper lange og uoversiktlige verdikjeder. Disse verdikjedene inkluderer ofte tjenester i andre land. For virksomheter som er avhengig av digitale tjenester, er det derfor vanskelig å ha tilstrekkelig innsikt i, og kontroll over, egne sårbarheter. Samfunnet blir stadig mer avhengig av disse tjenestene, samtidig som det har vært en jevn økning i kompleksitet de senere årene. NSM mener dette må forventes å øke ytterligere i tiden fremover. Digitaliseringstakten er rask, og mange av virksomhetene har god evne til å utvikle og ta i bruk nye løsninger. NSMs vurdering er at virksomhetene ikke har tilsvarende evne til å ivareta sikkerheten, slik at utviklingen kan gjøres på en kontrollert og sikker måte.

NSMs tilsyn med sikkerhet i samfunnsviktige informasjonssystemer og datahaller har blant annet avdekket mangelfull oversikt over hvordan datasentre som er driftet av underleverandører sikres og hvordan eventuelle sårbarheter håndteres og følges opp. NSM har grunn til å tro at disse funnene er representative for virksomheter i mange sektorer.

FRAGMENTERTE IKT-LØSNINGER

I takt med den økende digitaliseringen har vi blitt avhengig av fungerende og pålitelige IKT-systemer. NSM mener det er en stor svakhet at IKT-løsningene i offentlig forvaltning er fragmenterte og at ansvaret er fordelt på mange aktører. Fragmenterte drifts- og sikkerhetsmiljøer medfører kompleksitet og bidrar til unødige variasjoner på nettverk, systemer og tjenester. Dette resulterer i økt antall sårbarheter og mulige angrepsflater.

Ved en samfunnsmessig eller sikkerhetspolitisk krise er det avgjørende at IKT-systemene er tilgjengelige og opererer som de skal. Mange viktige nasjonale funksjoner er avhengig av internett, og bortfall av nettet kan forsterke eller forverre en krise. Generelt har systemer for sikker kommunikasjon liten utbredelse og brukes i for liten grad, noe som kan redusere evnen til krisehåndtering betydelig. I statsforvaltningen innføres nå graderte systemer, og dette reduserer risikoen for digitale angrep.

BEVISSTHET OM TEKNISKE SÅRBARHETER

Nye sårbarheter i programvare oppdages daglig. Tidsrommet fra en sårbarhet er kjent til den blir lukket gjennom en sikkerhetsoppdatering er en gyllen mulighet for en trusselaktør til å trenge inn i et datanettverk. En trusselaktør vil benytte de sårbarhetene som gir maksimal gevinst med minimal risiko for å bli oppdaget. Dette betyr at avanserte aktører ofte utnytter sårbarheter og metoder som

er kjent av mange. I mange tilfeller er dette sårbarheter som kunne vært lukket dersom for eksempel programvare hadde vært oppdatert.

Gjennom NSMs arbeid med inntrengingstesting i virksomheter som forvalter viktige, offentlige funksjoner, har vi de senere år erfart at virksomhetene har blitt bedre til å erkjenne at tekniske sårbarheter finnes og at virksomhetenes eget arbeid med å lukke disse vil bidra til å bedre sikkerhetstilstanden.

UTILSTREKKELIG SIKRING AV OBJEKTER

Gjennom NSMs tilsynsaktivitet på objektsikkerhet og fysisk sikring er det avdekket store mangler. Flere av virksomhetene har ikke oppdatert risikovurdering eller gjennomført sikkerhetsrevisjoner. Mange virksomheter som forvalter skjermingsverdige objekter, har ikke planer for å oppskalere sikkerheten ved økt risiko. Funn fra tilsyn viser også at det sjelden foreligger resultater fra kartlegging av avhengigheter i egen sektor og tverrsektorielt. NSM vurderer at de ulike funnene påvirker sikkerhetstilstanden negativt.

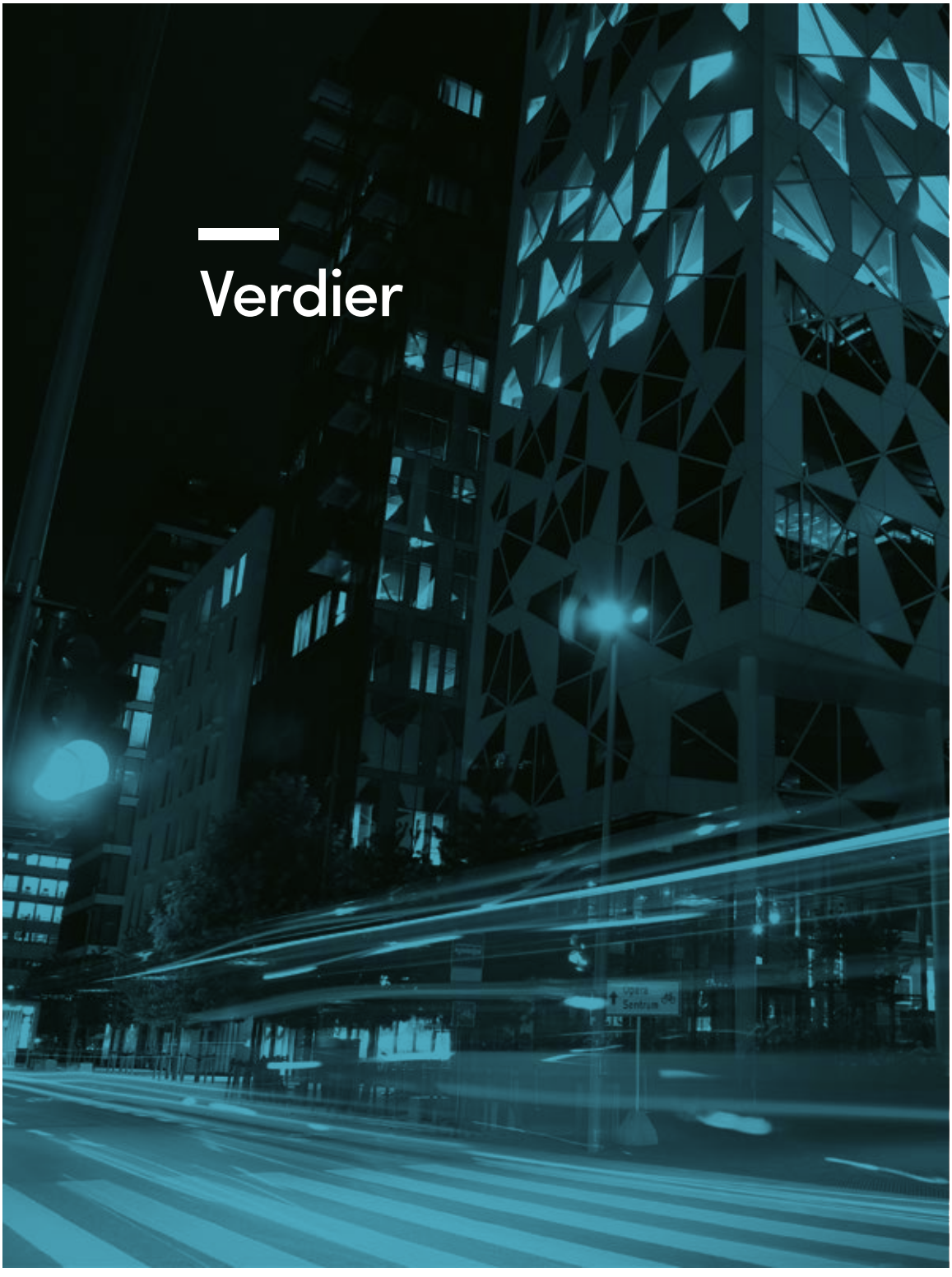
HYBRIDE TRUSLER OG PÅVIRKNINGSOPERASJONER

Bruk av informasjonsoperasjoner til å påvirke demokratiske prosesser og destabilisere samfunn har fått økende oppmerksomhet i den senere tid. Digitale medier brukes for å påvirke opinionen gjennom informasjonskampanjer. Informasjonen som benyttes i slike kampanjer, er i noen tilfeller innhentet gjennom ulovlige metoder. Kampanjene kan inneholde informasjon som er ekte, informasjon som er endret og falsk informasjon for å påvirke befolkningen i en bestemt sak.

Et av virkemidlene som brukes innenfor såkalte hybride trusler, er politisk påvirkning, noe som har blitt aktualisert gjennom hendelser i den amerikanske valgkampen. Russiske myndigheter demonstrerte her evne og vilje til å påvirke politiske prosesser i andre land. I 2017 skal det gjennomføres flere valg i Europa, blant annet i Norge. For å avverge at liknende hendelser skal skje i Norge, er det viktig å skape motstandsdyktighet og redusere sårbarheter.

Et annet element i hybride operasjoner er digitale sabotasjehandlinger. Dette vil si å utnytte IKT-systemer for å skade eller ødelegge sivile eller militære verdier, som for eksempel kritisk infrastruktur. Det antas at statlige aktører i en langsiktig strategi vil kartlegge sårbarhetene i den digitale infrastrukturen som eventuelt kan utnyttes til slike formål. ⊙

«Gjennom NSMs tilsynsaktivitet på objektsikkerhet og fysisk sikring er det avdekket store mangler.»



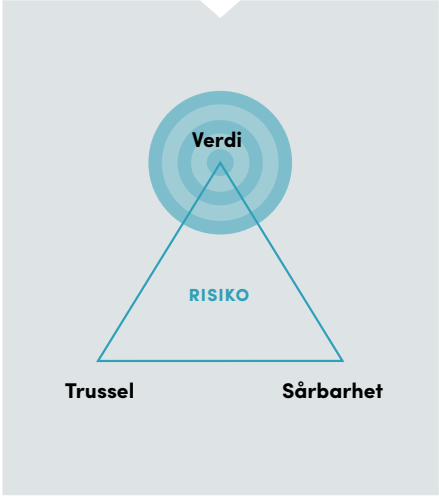
Verdier

SIKKERHETSTILSTANDEN påvirkes av hvilken innsats vi legger i å sikre verdiene våre. Kunnskap om egne verdier og sårbarheter, og forståelse for at verdiene er attraktive for ulike trusselaktører, er avgjørende for egen risikoerkjennelse. Slik kunnskap er også viktig for å fatte gode beslutninger om hvilke sikringstiltak som må implementeres eller hvilken risiko en virksomhet er villig til å akseptere.

Formålet med en virksomhets sikkerhetsarbeid er å sikre egne verdier. I et større perspektiv er formålet å sikre samfunnsverdier mot alvorlige, tilsiktede uønskede handlinger for å ivareta rikets selvstendighet og sikkerhet og andre viktige nasjonale sikkerhetsinteresser. For at staten skal kunne sikre rikets selvstendighet, må den nasjonale styringsevnen fungere, ved hjelp av konstitusjonelle organer, forvaltningen og beredskaps- og kriseledelse.

Demokratiet i Norge gir oss grunnleggende frihet og rettigheter. Rettsstaten og Forsvaret beskytter oss. Naturressursene og teknologien gir inntekter og livsgrunnlag, og velferdsstaten og helsevesenet bistår oss ved behov. Vi tar ofte disse verdiene for gitt, men de er grunnleggende for vårt levesett. Ivaretagelse av vår suverenitet og sikkerhet er avgjørende for at vi skal kunne ha disse verdiene også i fremtiden.

Tap eller reduksjon av verdier har negative konsekvenser både på kort og lang sikt. Alle er avhengig av sikker strømforsyning, sikre elektroniske kommunikasjonstjenester og sikre finans- og banktjenester. I tillegg bruker vi daglig mange støttetjenester av ulike slag. Disse



støttetjenestene eller funksjonene kan være verdier som forvaltes av andre. Vurdering av verdier og sårbarheter har dermed betydning utover den enkelte virksomhet.

I 2016 så vi en økning i bruk av metoder for å påvirke demokratiske institusjoner og verdier. Tilliten til at demokratiske prosesser kan foregå fritt og upåvirket og i henhold til befolkningens forventninger, kan være truet. Digitaliseringen av samfunnet skaper hele tiden nye verdier og utviklingsmuligheter, men kan også utvide sårbarhetsflaten til verdier og interesser vi ønsker å beskytte.

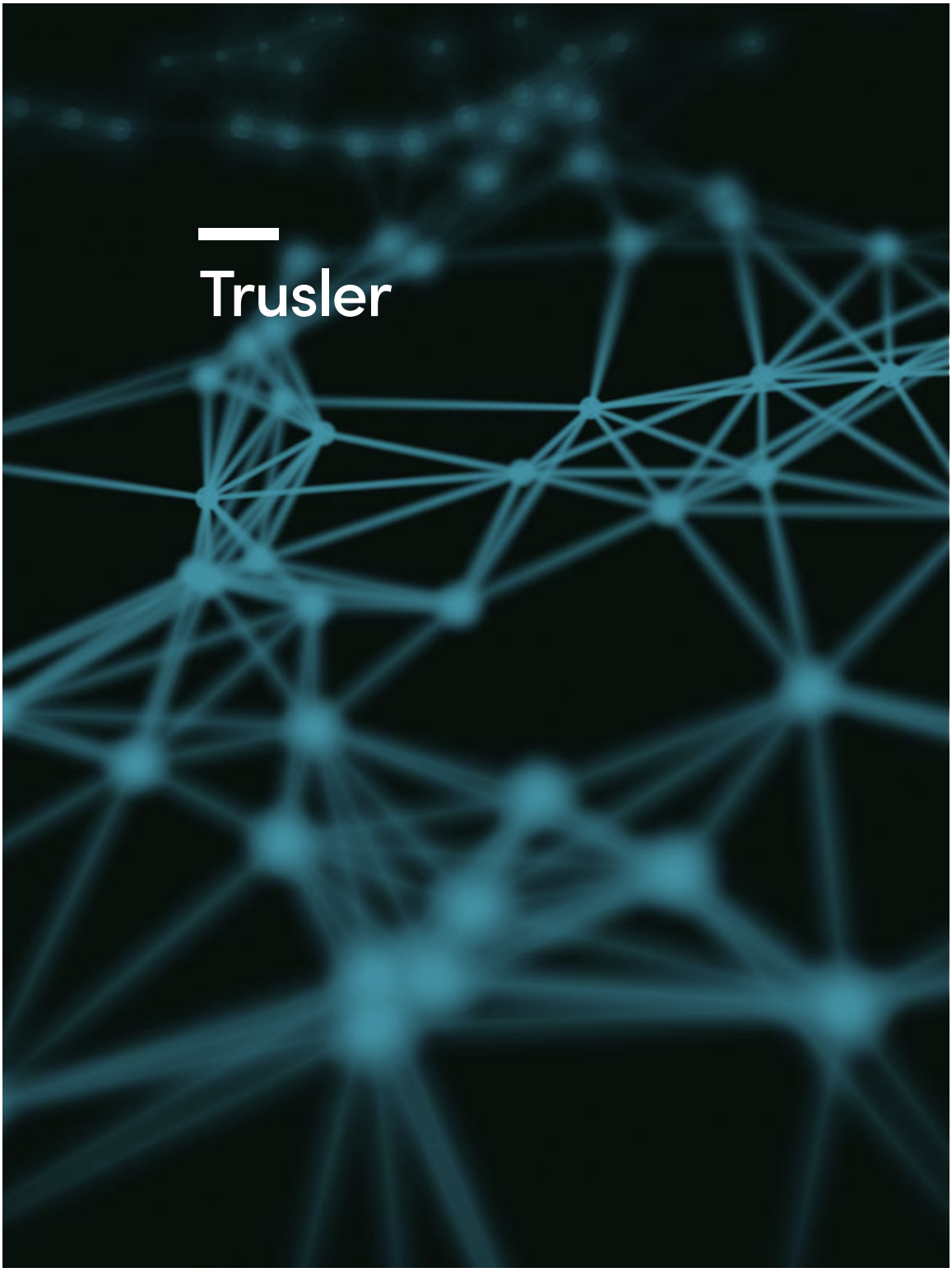
I et stats- og samfunnsperspektiv er det definert et sett med overordnede verdier, kalt kritiske samfunnsfunksjoner. Kritiske samfunnsfunksjoner omfatter blant annet:

«Alle er avhengig av sikker strømforsyning, sikre elektroniske kommunikasjonstjenester og sikre finans- og banktjenester.»

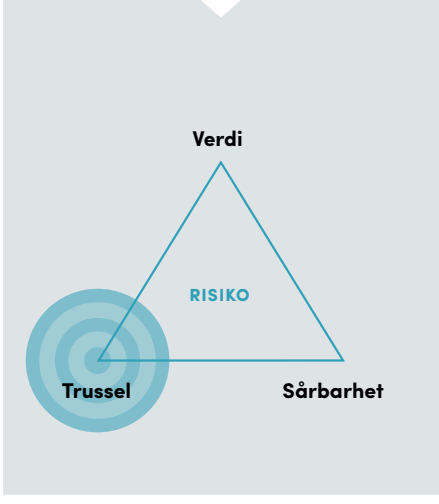
- Styringsevne og suverenitet
  - Styring og kriseledelse
  - Forsvar
- Befolkningens sikkerhet
  - Lov og orden
  - Helse og omsorg
  - Redningstjeneste
  - IKT-sikkerhet i sivil sektor
  - Natur og miljø
- Samfunnets funksjonalitet
  - Forsyningssikkerhet
  - Vann og avløp
  - Finansielle tjenester
  - Kraftforsyning
  - Elektroniske kommunikasjonsnett og -tjenester
  - Transport
  - Satellittbaserte tjenester

Mange av disse funksjonene forvaltes av virksomheter på vegne av samfunnet. Virksomhetene må selv vurdere hvilke konsekvenser det kan få dersom verdiene skulle rammes av en uønsket hendelse. Slike verdier kan for eksempel være:

- informasjon, eksempelvis virksomhetskritisk informasjon, som patenter, anbud, produksjonsplanlegging, budsjetter og produksjonsbeskrivelser
- digital infrastruktur, som nettverk og servere
- programvare, for eksempel industrielle kontrollsystemer (SCADA-systemer) som styrer produksjon
- økonomiske verdier
- ansatte og personopplysninger
- organisasjonsstrukturer
- aktiva, som produksjonsutstyr


Trusler

VERDIENE VÅRE er attraktive for ulike trusselaktører, og verdiene trues av deres handlinger. Trusselaktørene benytter et bredt spekter av virkemidler for å nå sine mål.



TRUSSELAKTØRER OG MÅL

Norske verdier og interesser utsettes for fremmed etterretningsvirksomhet som kan ha et stort skadepotensial. Blant annet er forsvars- og beredskapssektorene, politiske beslutningsprosesser og kritisk infrastruktur utsatt. Datanettverksoperasjoner og utnyttelse av personer med tilgang til sensitiv informasjon og teknologi er blant metodene som benyttes.

Både statlige og ikke-statlige grupperinger utgjør en digital trussel mot Norge. Etterretningstjenesten og Politiets sikkerhetstjeneste (PST) sier i sine årlige ugraderte rapporter at de mest alvorlige truslene mot digitale systemer i Norge i 2017 fremdeles vil komme fra Russland og Kina.[1] Økt spenning mellom Russland og Vesten kan gi høyere antall forsøk på å trenge inn i datasystemene til myndigheter og virksomheter for å innhente informasjon. De synes spesielt interessert i politiske og militære mål. Kinesiske grupper forventes å fortsette med operasjoner mot norske myndigheter og teknologiselskaper innenfor flere områder. Av scenarioene Nasjonal kommunikasjonsmyndighet (Nkom) vurderer i rapporten EkomROS, knyttes det høyest risiko til at utenlandsk etterretning kartlegger kritisk elektronisk kommunikasjonsinfrastruktur og kritisk personell knyttet til denne.

Avanserte datanettverksoperasjoner mot norske myndigheter, IKT-tjenestetilbydere, teknologimiljøer og virksomheter med ansvar for kritisk infrastruktur ventes å fortsette også i 2017.

CYBERANGREP

I løpet av 2016 var det særlig to trender i risikobildet for IKT-hendelser som bekymrer NSM. Den ene er at de mest alvorlige og ressurskrevende sakene fra avanserte trusselaktører øker i omfang. Den andre er at nettopp disse aktørene har begynt å angripe mindre norske virksomheter med sårbare IKT-systemer for å utnytte de kompromitterte nettverkene videre som infrastruktur i angrep mot andre, tilsynelatende mer attraktive mål. Denne trenden er en viktig påminner om at god grunnsikring

[1] Etterretningstjenesten: Fokus 2017. Etterretningstenesta si vurdering av aktuelle tryggingsutfordringar, og PST: Trusselvurdering 2017.

av nettverk og servere er viktig selv om man ikke anser egen virksomhet å være et attraktivt mål i seg selv.

Datanettverksoperasjoner og digital spionasje fra statlige aktører utgjør betydelig risiko for offentlig forvaltning og for virksomheter som forvalter kritisk infrastruktur, kritiske samfunnsfunksjoner og høyteknologi. Trusselaktører overvåker de mest attraktive målene kontinuerlig, slik at den minste sårbarhet kan utnyttes i det øyeblikk den oppstår. Det har det siste året vært en rekke datanettverksoperasjoner rettet mot statlig forvaltning, blant annet gjennom forsøk på digital spionasje både mot departementer og underliggende etater. PST rapporterer i sin årlige trusselvurdering at kinesiske og russiske grupper har stått bak mange av disse og andre hendelser mot datasystemer hos virksomheter som forvalter grunnleggende nasjonale verdier og store kommersielle interesser.

NSM registrerte om lag 22.000 uønskede hendelser mot informasjonssystemer i Norge i 2016. Ca. 5.000 av disse ble prioritert for oppfølging i NSM. Den generelle tendensen er at antall hendelser er stigende. NSM vurderer cyberangrep fra fremmede stater som den høyeste IKT-risikoen for offentlig forvaltning. Det antas å være store mørketall når det gjelder det årlige totale antall cyberhendelser i Norge. Mange virksomheter avdekker og håndterer slike hendelser selv, uten at dette rapporteres til NSM eller til andre myndigheter. I tillegg antas det å være mange hendelser som av tekniske eller kapasitetsmessige årsaker ikke blir oppdaget.

Det store volumet av IKT-hendelser i Norge er imidlertid kriminalitet med økonomisk vinning som formål. To eksempler på dette er tjenestenektangrep og løsepengevirus med kryptolåsing av systemer. Slike angrep kan forårsake stor skade for kritisk infrastruktur og samfunnsviktige funksjoner. Løsepengevirus vil kunne sette ut hele virksomheter i dager eller uker. En tredje angrepstype som jevnlig registreres i Norge, er såkalt hacktivisme, det vil si cyberangrep med idealistiske målsettinger. For eksempel har hvalfangstmotstandere gjennomført slike angrep.

Økonomisk cyberkriminalitet utgjør en betydelig belastning for samfunnet. Det kompliserer bildet ytterligere at både tjenestenektangrep og løsepengevirus benyttes av avanserte (og antatt statlig

FAKTA

HVA ER TAP AV KONFIDENSIALITET, INTEGRITET, AUTENTISITET OG TILGJENGELIGHET?

Cyberangrep truer særlig informasjonens *konfidensialitet*, når uvedkommende hacker seg inn og får tak i informasjon.

Cyberangrep kan også true informasjonens *integritet*, ved for eksempel å endre data eller tjenester. I tillegg utfordrer dette *autentisitet*, ved å introdusere falske data eller tjenester. Informasjonens *tilgjengelighet kan også være et mål*, for eksempel ved et tjenestenektangrep som gjør en tjeneste eller informasjon utilgjengelig.

Kombinasjoner av disse aspektene er også mulig, for eksempel ved at en trusselaktør blander reell og korrekt informasjon sammen med en liten mengde manipulert informasjon.

støttede) aktører som avledningsmanøver eller ren sabotasje. Ifølge Næringslivets sikkerhetsråds (NSR) Mørketallsundersøkelse og Norsk senter for informasjonssikring (NorSIS) koster cyberkriminalitet norske virksomheter årlig betydelige beløp. I en undersøkelse gjennomført av PricewaterhouseCoopers (PwC) i samarbeid med Finans Norge og NorSIS sier 58 prosent av 200 respondenter fra næringslivet at de er blitt utsatt for cyberkriminalitet siste år. En fjerdedel sier at dette har kostet dem mer enn 1 million kroner. Mørketallsundersøkelsen til NSR viser at mer enn en fjerdedel av 1500 respondenter ble utsatt for en «uønsket hendelse» og at 14 prosent av dem har blitt utsatt for løsepengevirus. Utviklingen i sammenlignbare land er negativ, og det antas at denne trenden vil gjelde også i Norge.

Den dominerende angrepsmetoden for målrettede angrep er infiserte vedlegg i e-poster sendt til utvalgte personer, såkalt *spearphishing*. Trusselaktørens intensjon er å få mottakeren til å klikke på vedlegget, som er infisert med skadevare for å ta kontroll over den aktuelle klienten. Angrepet er skreddersydd til offeret, med innhold det er lett å la seg lure av. Eksempelvis kan e-posten se ut som om den kommer fra en kollega. Angrep mot norske myndigheter og teknologivirksomheter er typisk i denne kategorien.

En annen vanlig angrepsmetode er å infisere websider som en gitt kategori personer ofte besøker, såkalte *vannhull*. En trusselaktør som ønsker å minimere sjansen for å bli oppdaget, vil legge inn en liste med IP-adresser som de ønsker infisert i vannhullet, såkalt hvitelisting av IP-adresser. Alle ikke-attraktive mål vil forbli uberørt, og på den måten kan operasjonen gjennomføres svært målrettet og skape lite støy. Dette øker sannsynligheten for at vannhullet og aktiviteten ikke oppdages og dermed også sannsynligheten for at trusselaktøren kan nå sine mål.

Innbrudd i datasystemer forbindes ofte med spionasje og tap av konfidensialitet. Kompromittering av informasjonssystemer med sensitiv eller gradert informasjon kan imidlertid også brukes til å endre, slette eller plante informasjon eller gjøre et

FAKTA

EKSEMPLER PÅ LØSEPENGEVIRUS

> NSM har i løpet av vinteren 2017 observert flere angrepsbølger med løsepengeviruset TorrentLocker. For eksempel advarte Telenor i februar om et løsepengevirus i vedlegg til e-poster som utga seg for å være en betalingspåminnelse fra dem. Siden da har Telenor informert bredt og innført mottiltak. Etter mottiltakene har angriperne gått over til å bruke andre domener enn Telenor.

TorrentLocker blir lastet ned til offerets maskin enten ved at mottakeren blir lurt til å åpne en Zip-fil og Javascript i denne eller ved at mottakeren har åpnet et Word-dokument hvor mottakeren lures til å aktivere makroer som igjen muliggjør nedlasting av skadevaren. Det er så langt ingen kjente løsninger for å dekryptere data som er rammet av denne varianten av TorrentLocker. NSM er kjent med at bølgen treffer flere europeiske land, blant annet Sverige, Spania, Frankrike og Tyrkia. Det er ikke noen tegn på at angrepene mot norske mål er målrettet.

> I februar i år ble Oppland fylkeskommune utsatt for et datavirusangrep og krevd for løsepenger. En ansatt fikk en e-post fra det man antok var en trygg avsender. Da vedlegget som inneholdt viruset ble åpnet, ble nettverkets dokumenter og bilder kodet. Fylkeskommunen vet ikke hvem som står bak angrepet. For å få tilgang til koden ble det krevd løsepenger i bitcoin. Ifølge NorSIS er årsaken til at utpresserne ber om betaling i bitcoin at de da ikke kan spores. Filene er ikke mulige å gjenopprette uten koden. Det eneste man kan gjøre er å ta backup.

> Både Schibsted og Posten opplevde også hendelser med løsepengevirus i 2016.

informasjonssystem eller andre tilknyttede systemer utilgjengelig. Slik kompromittering kan derfor brukes for å påvirke, undergrave, sabotere eller legge til rette for sabotasjeaksjoner i en konfliktsituasjon. På verdensbasis har man sett mange eksempler på slik bruk av cyberangrep i løpet av 2016.

NSM vurderer at økning i alvorlige cyberangrep, kompromittering av nettverk i mindre virksomheter, bruk av cyberangrep og stjålet informasjon til påvirkning og et stort volum økonomisk motiverte hendelser er trender som vil fortsette i 2017 og videre fremover.

HYBRIDE TRUSLER OG PÅVIRKNING

De senere års hendelser i Ukraina har aktualisert trusler som utføres ved sammensatte virkemidler. Når en motpart søker å oppnå sine mål med sammensatt bruk av militære og ikke-militære virkemidler, har dette fått navn som hybride trusler eller hybrid krigføring, med bruk av hybride taktikker eller hybride operasjoner.

Hybride trusler er altså sammensatte operasjoner med mulig bruk av alle tilgjengelige virkemidler. Voldsbruk på lavt nivå, utpressing, sabotasje og terror, diplomatisk press, propaganda, økonomiske og kulturelle sanksjoner kan være blant disse. Hybride operasjoner gjennomført av statlige aktører vil ha trusselen om bruk av militærmakt som et bakteppe. Virkemidlene i hybride operasjoner kan kobles sammen med, og brukes til å forsterke, konvensjonelle militære virkemidler.

Ofte vil hybride operasjoner være utført slik at det ikke er åpenbart hva som er målsettingen, hvem som står bak eller om de er sentralstyrt. Operasjoner kan utføres som en del av en kapasitetsbygging, der intensjonen om bruk av disse kapasitetene kan oppstå på kort varsel.

Et sterkt virkemiddel innenfor hybride trusler vil være å påvirke opinionen i befolkningen og politikerne. Det kan beskrives som en kamp om å definere sannheten eller narrativet, der informasjon og desinformasjon er viktige elementer. Trusselaktører kan utnytte globaliseringen og nettbasert medietilgang for å oppnå strategisk effekt. Trusselbildet presentert i langtidsplanen for forsvarssektoren beskriver hvordan strategisk kommunikasjon brukes i fredstid av en motpart for å berede grunnen for potensielle kriser og væpnet konflikt. Imidlertid har erfaringer fra blant annet Ukraina vist at også kritisk infrastruktur, som for eksempel kraftforsyning eller andre kritiske samfunnsfunksjoner, kan være viktige mål.

Utviklingen av den digitale konfliktareaen har gitt nye muligheter for å påføre skade. Selv om målene en trusselaktør søker å oppnå er ukjente, kan virkemidlene de bruker for å nå dem være synlige for oss. Cyberoperasjoner er et eksempel på dette. De siste årene har vi på verdensbasis sett eksempler på tyveri og offentliggjøring av sensitiv informasjon, potensiell planting av informasjon og bruk av blant annet sosiale medier for å oppnå stor spredning av usannheter og informasjon som bare er delvis sann.

Informasjonens tilgjengelighet kan også saboteres ved hjelp av andre typer digitale angrep, som tjenestenektangrep.

Eksempelvis ble georgiske myndigheter utsatt for massive tjenestenektangrep i forbindelse med konflikten med Russland i 2008. Dette ga russiske myndigheter muligheten til å formidle sin versjon av hendelsene uten konkurranse. Et annet eksempel er Ukraina-konflikten i 2014. Virkemidlene som brukes i formidlingen av Russlands versjon av historien, er blant annet bruk av medier rettet mot utlandet, manipulasjon gjennom sosiale medier, politisk kommunikasjon og diplomati.

I 2017 skal det som nevnt gjennomføres flere valg i Europa, blant annet i Norge. Fordekte digitale angrep for å påvirke forvaltningsapparatet, politiske beslutningstakere og befolkningen, kan potensielt ramme alle faser av stortingsvalget, eksempelvis partienes valgkamp, mediedekning og faktisk gjennomføring, inkludert håndtering av stemmeantall. I hele denne kjeden finnes det IKT-systemer med potensielle sårbarheter. Både avanserte og mindre avanserte metoder kan benyttes. For å avverge at liknende hendelser skal skje i Norge, er det viktig å skape motstandsdyktighet og redusere sårbarheter.

Hybride strategier er designet for å være uhåndgripelige og sette motparten ut av balanse. Dette kan gjøre det vanskelig å finne effektive mottiltak. Der cyberangrep benyttes som et virkemiddel innenfor en hybrid operasjon, vil god IKT-grunnsikring og redusering av sårbarheter være avgjørende for å minimere risikoen. ⊙

EKSEMPLER PÅ HENDELSER

> Hackingen av det amerikanske demokratiske partiets nasjonale komité førte til at flere sentrale personer i partiet trakk seg. De amerikanske etterretningsmiljøene har samlet formidlet at stjålne e-poster ble publisert for å påvirke den amerikanske valgkampen og at de er sikre på at russiske myndigheter står bak. Hackingen er et eksempel på en informasjonsoperasjon som saboterer for et politisk parti i en valgkamp. Sabotasjen medførte i dette tilfellet at sensitiv informasjon om interne prosesser i Det demokratiske partiet ble avslørt og dermed påvirket og undergravde partiets omdømme midt i presidentvalgkampen. Dette rammet derfor en viktig del av selve valgprosessen, som er en kjernefunksjon i et demokratisk samfunn. Aktørene benyttet særlig spearphishing, som i de fleste angrep mot norske mål.

> I rapporter fra amerikanske myndigheter hevdes det at angrepet mot Det demokratiske partiet stammer fra to ulike aktører innen det sivile og militære russiske etterretningsapparatet. Dette er basert på tekniske indikatorer fra Department of Homeland Security, FBI og andre. Rapporten sier videre at informasjonen som ble hentet ut, ble lekket til pressen og offentliggjort.

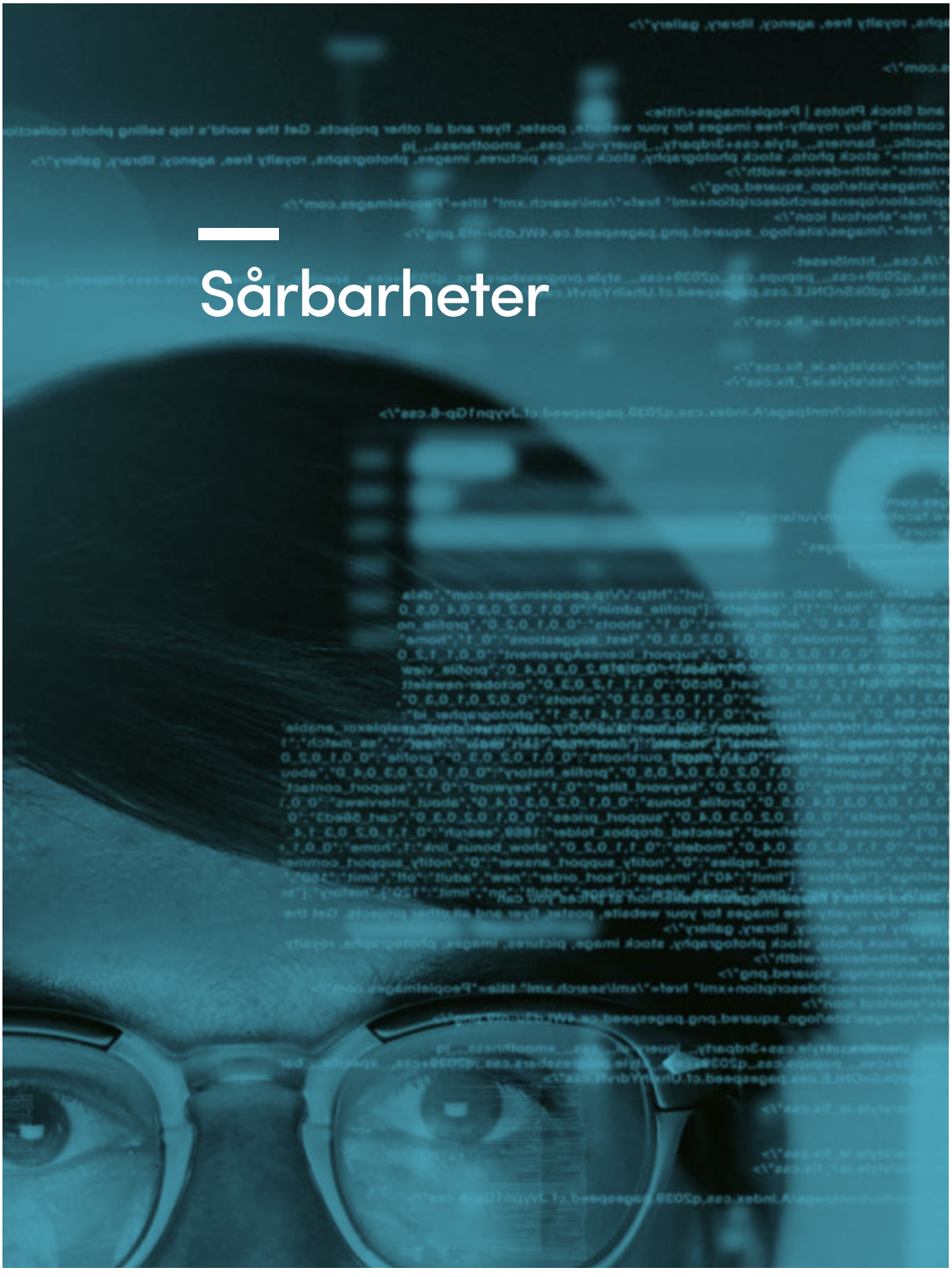
> Russiske digitale operasjoner er avdekket i flere land. Den tyske innenriksetterretningstjenesten Bundesamt für Verfassungsschutz (BfV) uttalte i mai 2016 at russiske hackere fra gruppen Sofacy (APT28) sto bak angrep mot blant annet det tyske parlamentet i 2015, der målet skal ha vært person- og virksomhetsopplysninger fra Angela Merkels parti Christlich Demokratische Union (CDU). Angriperne skal ikke ha lykkes i å hente ut informasjon fra CDUs systemer. De russiske angrepene BfV har avdekket, skal i hovedsak ha handlet om spionasje.

> Angela Merkel og BfV har nylig advart mot russiske cyberangrep og russisk desinformasjon og påvirkning i forbindelse med valget i Tyskland i 2017. Den tyske opinionen kan allerede ha blitt påvirket av russerne og tyske myndigheter er bekymret for at dette kan skje også i forbindelse med valget.

> I februar 2015 dukket det opp en nyhetssak som hevdet at Sverige skulle eksportere våpen til Ukraina. Saken var basert på et fiktivt brev på departementets brevpapir som ble spredt på Twitter, der forsvarsminister Peter Hultqvist gratulerte sjefen for BAE Systems Bofors med våpenavtalen. Brevet skal ha blitt sporet opp til St. Petersburg. Senere samme år ble det opprettet en falsk Twitter-konto i Hultqvists navn, og det samme skjedde på nytt i april 2016.

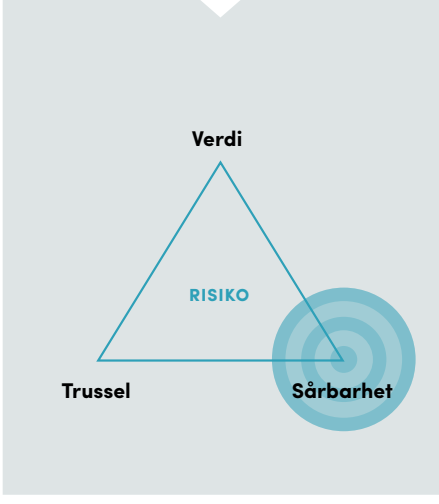
> I februar i år ble den svenske utenriksministeren Margot Wallström utsatt for et russisk twitterangrep der falske uttalelser ble spredt i forkant av hennes møte med den russiske utenriksministeren i Moskva.

> Det er eksempler på at også politiske partier i Norge er forsøkt infiltrert med digitale midler. Både Miljøpartiet De Grønne og Sosialistisk Venstreparti opplevde innbrudd i sine nettverk i løpet av 2016. Et resultat av dette var at medlemslistene til De Grønne ble offentliggjort. Arbeiderpartiet og Stortinget ble utsatt for et forsøk på datainnbrudd senere på året. Slike hendelser kan åpne opp for manipulasjon av informasjon om partienes politikk.



Sårbarheter

FOR AT TRUSSELAKTØRENE skal nå sine mål er de avhengig av sårbarheter som kan utnyttes. Sikkerhetsmessige sårbarheter kan ha organisatoriske, menneskelige eller tekniske årsaker. NSM mener det er bekymringsfullt at så mange kjente sårbarheter fremdeles kan utnyttes.



PLANLEGGING OG STYRING AV SIKKERHETSARBEIDET

Både offentlig forvaltning og private virksomheter har verdier som må beskyttes mot spionasje, sabotasje, terrorisme og andre sikkerhetstruende hendelser. God styring av sikkerhet er det viktigste virkemiddelet og en nødvendig forutsetning for å identifisere og iverksette effektive, helhetlige sikringstiltak. Departementene har et særlig ansvar for sikkerheten innenfor egen sektor.

NSM utfører hvert år tilsyn med både private og statlige virksomheter som er utsatt for både industrispionasje og tradisjonell informasjonsinnhenting. Det vi ofte ser, er at mange store foretak og forvaltningsinstitusjoner sliter med å implementere de fire store hovedtiltakene innen sikkerhetsstyring: verdivurdering, risikoanalyser, internrevisjon og ledelsesevaluering. Dette har vært et gjennomgående tema i NSMs vurderinger over flere år. Den overveiende delen av avvik som er avdekket gjennom NSMs tilsyn burde virksomhetene selv ha avdekket gjennom interne sikkerhetsrevisjoner. Uten at sikkerhetsrevisjoner er gjennomført, blir også grunnlaget for ledelsens evaluering svakt, noe som igjen kan føre til feil prioriteringer om korrigerende tiltak for å redusere risikoen mot virksomhetens verdier. God sikkerhetsstyring krever at virksomhetene tar grunnleggende styringsmessige grep, som det å etablere skriftlige målsettinger og planer for utførelse og evaluering av sikkerhetsarbeidet. Det finnes ofte mye sikkerhetsfaglig kompetanse i virksomhetene, men den blir ikke alltid systematisk utnyttet. Det finnes også tegn som tyder på at underordnede etater i en del tilfeller ikke får tilstrekkelige styringssignaler om og oppfølging av sitt arbeid med forebyggende sikkerhet fra overordnet departement.

LEDERFORANKRING OG LEDELSENS EVALUERING

NSMs tilsyn viser hvorfor det er viktig å styre sikkerhetsarbeidet og bidrar til

forbedret forebyggende sikkerhet. En tredjedel av virksomhetene NSM har ført tilsyn med fra og med 2015, hadde ikke evaluert sitt eget sikkerhetsarbeid. Under halvparten hadde gjennomført dokumenterte interne undersøkelser av status for sikkerhetsarbeidet. En fjerdedel hadde ikke gjennomført risikovurdering. Tilsynelatende gjøres risikovurderinger i større grad for IKT-sikkerhet enn for fysisk sikkerhet eller personellsikkerhet. Likevel mener de fleste av virksomhetene at egen sikkerhetstilstand er «god». Grunnlaget for å fremsette den påstanden er ikke alltid like solid.

Rapportering av sikkerhetstilstand i seg selv kan føre til økt bevissthet i den enkelte virksomhet, og slik sett bidra til å bedre sikkerheten. NSM ser at rapportering kan fremtvinge en økt grad av lederevaluering i virksomhetene. Dersom sikkerhetstilstanden ikke er kjent for virksomhetsledelsen, kan det føre til at sikkerhetsmessige tiltak ikke sees i sammenheng og at nødvendige tiltak for å lukke sårbarheter ikke blir iverksatt. Konsekvensen kan være at virksomheten blir utsatt for høyere risiko enn den har bevissthet om.

EVNE TIL LÆRING

NSM har ved mange anledninger funnet at virksomheten formelt har opprettet et register for sikkerhetstruende hendelser, men at ingen hendelser er registrert. Det gjør det vanskelig å lære av tidligere hendelser, og kan tyde på lav bevissthet rundt sikkerhet generelt og særlig rundt læringsbehov.

OPPFØLGING ETTER TILSYN

I en del tilfeller gjennomfører NSM oppfølgende tilsyn. Erfaring fra disse viser at virksomhetene iverksetter tiltak på bakgrunn av tidligere påviste mangler. For eksempel kan flere virksomheter vise til at de har igangsatt arbeid med årlige risikovurderinger og ledelsesevalueringer.

MENNESKER KAN UTNYTTES

Politiske påvirkningsoperasjoner, blant annet digital påvirkning, misbruker og angriper sentrale verdier i det demokratiske samfunnet. Disse sentrale verdiene er blant annet fri og åpen meningsdannelse og en fri og uavhengig presse. Disse kanalene kan misbrukes til å spre desinformasjon, løgn og undergraving. Når usannheter spres med stor kraft og i stort omfang, må det brukes mye energi og ressurser på å imøtegå dette.

I et samfunn med stor grad av ytringsfrihet kan slike virkemidler være vanskelige å identifisere når de skjuler seg i annen informasjon. Når det til stadighet spres drypp av undergravende informasjon, vil det være utfordrende å vite hva som bare er ufarlige enkeltutspill og hva som er en del av en større, koordinert operasjon. Det kan være vanskelig å vite om det finnes en større hensikt bak og hva som er beste handlemåte for å beskytte seg. Situasjonen er derfor det som i andre sammenhenger kalles asymmetrisk, det vil si spillereglene er ulike for den som angriper og den som angripes.

Siste linje mot spredning av falsk og stjålet informasjon i mediene er journalister og redaksjoner. Et eksempel fra Dagbladet belyser dette. En e-post som

utga seg for å være en pressemelding fra Justis- og beredskapsdepartementet med e-postadresse fra Departementenes sikkerhets- og serviceorganisasjon, ble sendt til Dagbladet den 25. oktober 2016. Innholdet i den falske pressemeldingen og måten den var forsøkt publisert, var oppsiktsvekkende nok til at det aldri var snakk om å publisere dette fra Dagbladets side. Forsøk på påvirkning skjer på mange måter, og dette viser en av metodene. Tilfellet illustrerer hvordan trusselaktører kan bruke ulike metoder for å forsøke å utgi lett forfalskede budskap og dermed undergrave tilliten til offentlig, strategisk kommunikasjon.

I forbindelse med den amerikanske valgkampen fremkom det at Russland delvis har brukt sosiale medier, russisk-kontrollerte redaksjonelle medier og andre medier for å spre saker. Det har også skjedd en forsterkning av budskap og saker gjennom ukritisk deling på nett, bruk av nettroll og diverse mediers egeninteresse av å fremheve spektakulære saker.

Menneskene som er gitt fysisk eller logisk tilgang til et arbeidsområde, kan svekke effekten av sikringstiltak som er innført for å ivareta konfidensialitet, integritet og tilgjengelighet til informasjon, system, objekt og prosedyrer. Det innebærer en risiko for at tilsiktede uønskede handlinger kan utføres som følge av plassering eller utnyttelse av personell, såkalte innsidere.

Innsidere med legitim tilgang har ikke bare tilgang til virksomhet, systemer, informasjon eller prosesser, men kan også kjenne til svakhetene ved tiltak og prosedyrer som skal sikre verdier.

Innsideren kan dessuten bruke sine legitime tilganger til å spre desinformasjon eller manipulere beslutningstakere. Innsideren kan også sabotere eller påvirke beslutningsprosesser og informasjonsflyt. Fordi innsiderens rolle i beslutningsprosessen er akseptert, vil aktiviteten kunne fremstå som lovlig. Det kan derfor være svært vanskelig å skille illegitim påvirkning fra legitime beslutningsprosesser som innsideren deltar i.

LANGE VERDIKJEDER – MANGE AVHENGIGHETER

Økt digitalisering kan bidra til å gjøre kritiske samfunnsfunksjoner sårbare. Digitaliseringen gjør det mulig at mange leverandører er involvert i produksjon av gitte varer og tjenester og skaper dermed lange verdikjeder. Dette kan føre til tap av oversikt. Feil ett sted gir uventede og uforutsigbare feil andre steder. Disse verdikjedene inkluderer ofte tjenester i andre land. For virksomheter som er avhengig av digitale tjenester, er det derfor vanskelig å ha tilstrekkelig innsikt i, og kontroll over, egne sårbarheter. Dette skyldes ikke minst at man arver sårbarhetene til øvrige ledd i de digitale verdikjedene.

Mesteparten av utviklingen av IKT-produkter og -tjenester foregår internasjonalt. Andre, større land enn Norge utvikler fortløpende strategier og handlingsplaner for å møte utviklingen sikkerhetsmessig. Hastigheten på utviklingen og muligheten til å ligge i forkant for å utvikle sikkerhetsmessige løsninger på ny teknologi er en utfordring. NSM mener det er en stor svak-

het at IKT-løsningene i offentlig forvaltning er fragmenterte og at ansvaret er fordelt på mange aktører. Flere av departementene er autonome virksomheter som tar selvstendige beslutninger om hvordan de vil løse sine oppgaver, deriblant forvaltning, drift og vedlikehold av IKT-løsninger. Fragmenterte drifts- og forvaltningsmiljøer medfører økt kompleksitet og bidrar til unødige variasjoner på nettverk, systemer og tjenester. Dette kan resultere i økt antall sårbarheter og mulige angrepsflater og skape utfordringer rundt etablering av sikkerhetsløsninger.

En annen kompliserende faktor er at antall enheter som er koblet til internett, vokser raskere og raskere for hvert år. Innen 2020 kan mer enn tre ganger så mange enheter være tilkoblet internett som ved inngangen av 2016. Gjenstander som klokker, biler, termostater og hele styringssystemer for hus er i økende grad koblet til internett. Dette gjelder for virksomheter, så vel som privatpersoner. IKT-enheter som ikke nødvendigvis var tiltenkt å fungere inne i en virksomhets nettverk, kan utgjøre en angrepsvektor, og antallet tekniske sårbarheter i et nettverk øker.

I takt med den økende digitaliseringen har vi i stor grad blitt avhengig av fungerende og pålitelige IKT-systemer. Ved en samfunnsmessig eller sikkerhetspolitisk krise er det avgjørende at IKT-systemene er tilgjengelige og opererer som de skal. Mange viktige nasjonale funksjoner er avhengig av internett, og bortfall av nettet kan forsterke eller forverre en krise.

Systemer for sikker kommunikasjon har liten utbredelse og brukes i for liten grad. Dette utgjør en sårbarhet som kan redusere evnen til krisehåndtering betydelig. Risiko i forbindelse med digitale angrep reduseres nå gjennom innføring av graderte systemer i statsforvaltningen.

TJENESTEUTSETTING AV IKT – SKYTJENESTER

Tjenesteutsetting betyr at virksomheten velger å anskaffe varer eller tjenester, eksempelvis skytjenester, fra en ekstern leverandør i stedet for å levere dem selv. Tjenesteutsetting benyttes i økende grad for leveranse av virksomhetenes IKT-tjenester, hovedsakelig fordi det er økt fokus på primæroppgaver og kostnader. Tjenesteutsetting er for mange virksomheter en effektiv måte å profesjonalisere tjenester og oppnå bedre sikkerhet.

En skytjeneste innebærer som regel at mye informasjon konsentreres i store datasentre. Dette kan innebære økt risiko i forbindelse med både sabotasjehandlinger og brann eller andre ulykker. Det kan også være lettere for innsidere eller innbruddstyver å få tilgang til mye sensitiv informasjon. Et datasenter kan utgjøre et større og mer fristende mål for hackere, men også etterretningstjenester.

Det finnes hendelser i andre land som belyser farer ved å samle mye informasjon i store datasentre. Tjenestenektangrepet som rammet den store amerikanske nettleverandøren Dyn høsten 2016, er et eksempel. En rekke basistjenester på deler av internett ble påvirket og angrepet fikk ringvirkninger i flere land, blant annet i Norge. Dette gjør at det ikke er vanskelig å se for seg et tjenestenektangrep mot skytjenester som igjen kan resultere i at

tjenesten blir utilgjengelig.

Bruk av skytjenester kan føre til at større mengder sensitive data vil overføres over offentlige nettverk. Tilgangen til viktig informasjon eksponeres for feil i disse nettverkene eller for bevisste tjenestenektangrep mot dem. Virksomheten risikerer at virksomhetskritisk informasjon blir utilgjengelig. Skytjenester krever at nett er tilgjengelig mellom klient og skyleverandør. Går nettet ned, blir tjenesten utilgjengelig. Dersom skyleverandørens datasenter ligger i et annet land eller transporten mellom leverandøren og kunden går via et annet land, kan det gi økt risiko både for konfidensialiteten og tilgjengeligheten til kundens informasjon.

I mange tilfeller kan bruk av skytjenester medføre lavere risiko fordi sikkerhetsfunksjonene og tiltakene profesjonaliseres i større grad enn virksomhetene klarer selv. Skytjenester krever at det er en tilstrekkelig drifts- og sikkerhetsorganisasjon både hos tjenesteleverandøren og hos brukervirksomheten og at disse er omforent om ansvarsfordeling for sikkerhet. Dersom dette ikke er på plass, risikerer virksomheten å øke sine sårbarheter.

NSMs tilsyn med sikkerhet i samfunnsviktige informasjonssystemer og datahaller har avdekket svakheter. Ved flere virksomheter har det manglet gyldig sikkerhetsgodkjenning for informasjonssystemene. Andre funn har vist at sentrale IKT-systemer ikke var utpekt som skjermingsverdige objekter, til tross for kritiske avhengigheter til disse systemene. Tilsyn har også avdekket mangelfull oversikt over hvordan datasentre som er driftet av underleverandører sikres, og hvordan eventuelle sårbarheter håndteres og følges opp.

TEKNOLOGISKE SÅRBARHETER UTNYTTES

Nye sårbarheter i programvare oppdages daglig. Tidsrommet fra en sårbarhet er kjent til den blir lukket gjennom en sikkerhetsoppdatering (patching) eller andre kompenserende tiltak, er en gyllen mulighet for en trusselaktør til å trenge inn i et datanettverk. En trusselaktør vil utnytte de sårbarhetene som gir maksimal gevinst, med minst mulig risiko for å bli oppdaget. Dette betyr at avanserte aktører ofte utnytter sårbarheter og metoder som er kjent av mange. I mange tilfeller er dette sårbarheter som kunne vært lukket dersom for eksempel programvare hadde vært oppdatert. Noen ganger benyttes også ukjente sårbarheter, såkalte 0-dags-sårbarheter.

Gjennom NSMs arbeid med inntrengingstesting i virksomheter som forvalter viktige, offentlige funksjoner, har vi de senere år erfart at virksomhetene har blitt bedre til å erkjenne at tekniske sårbarheter finnes og at arbeid med å lukke disse vil bidra til å bedre sikkerhetstilstanden.

NY TEKNOLOGI I IKT

INTERNET OF THINGS

Vi kobler stadig flere enheter til internett. Disse enhetene, fra bilen og kaffetrakteren vår til virksomhetens styringssystemer, tas inn i varmen for å forbedre kommunikasjon, automatisere komplekse industriprosesser og gjøre livene våre enklere. Sikkerhetsutfordringer knyttet til populariteten og utbredelsen av produkter innen samle-

Sårbarheter som utnyttes i cyberangrep

Gjennom sin virksomhet har NSM avdekket svært mange sårbarheter i systemene til norske virksomheter. Disse sårbarhetene kan utnyttes av trusselaktører i flere faser.

1

UNDERSØKELSER

Trusselaktører kan begynne å gjøre undersøkelser om virksomheter eller personell gjennom åpne kilder, sosiale medier eller data fra tidligere innbrudd.

2

INNLEDENDE TILGANG

Innledende tilgang til systemet kan oppnås gjennom tre inngangsporter:

3

A. FOTFESTE PÅ BRUKERENS KLIENT

De vanligste sårbarheter som utnyttes for å skaffe fotfeste i et nettverk er gjennom en bruker. Dersom klienten tillater kjøring av ikke-autoriserte programmer, vil ondsinnet kode levert gjennom epost eller vannhull kunne kjøres.

Forutsigbare passord vil gjøre det mulig å gjette passordet til brukere. Mange har ofte klare likheter i oppbygging, ved at de består av et vanlig ord med stor forbokstav, og gjerne slutter med et tall på 1-4 siffer. Tidligere passord blir gjerne gjenbrukt med et løpenummer til slutt, for eksempel «Sommer56».

B. SÅRBARE NETTJENESTER

Sårbare tjenester eksponert på internett kan utnyttes for å få tilgang innenfor virksomhetens nettverk. Alle standardpassord bør byttes før enheter settes i system i nettverket.

C. FYSISK TILGANG TIL NETTVERKSPORT

En trusselaktør kan finne tilgjengelige nettverkspunkter og koble seg til avgrensede eller lukkede nettverk i virksomhetens lokaler. Slike nettverkspunkter kan ofte finnes på utsiden av adgangskontrollert område, for eksempel i resepsjonsområder.

4

REKOGNOSERING

I denne fasen vil en trusselaktør søke etter systeminformasjon, andre nettverkssoner, sårbare tjenester og nyttige datafiler. Nettverk med mangelfull filtrering av trafikk mellom maskiner internt gir et stort mulighetsrom for en trusselaktør. Et dårlig segmentert nettverk gir manglende kontroll på trafikk som flyter på tvers av sonene.

5

UTVIDE TILGANG

I denne fasen vil en trusselaktør søke etter å overta viktige brukerkontoer, administratorkontoer og tjenester. For å hindre en trusselaktør i å utvide sin tilgang er det derfor svært viktig at det ikke tildeles administratorrettigheter til sluttbrukere. Svake passord vil hjelpe en trusselaktør også her.

Tjenester som glemmes kan i fremtiden bli sårbare, og kan brukes som en del av et angrep mot andre tjenester i nettverket. Mye gammelt og utdatert utstyr kjører i norske virksomheter uten at noen har oversikt over det. Et godt prinsipp er at servere og tjenester stenges straks behovet opphører. Alle tilganger for ansatte som forlater virksomheten bør straks sperres, men ikke slettes. Program- og maskinvare bør oppgraderes til nyere produktversjoner, og sikkerhetsoppdateringer bør installeres så fort som mulig.

6

OPPRETTHOLDE TILSTEDEVÆRELSE

I denne fasen vil en trusselaktør søke å opprettholde sin tilstedeværelse i nettverket ved å etablere bakdører for fremtidig bruk. Manglende rutiner for logging og analyse av trafikk på nettverket vil gjøre det vanskeligere å oppdage slik aktivitet.

7

TRUSSELAKTØREN OPPNÅR SITT MÅL

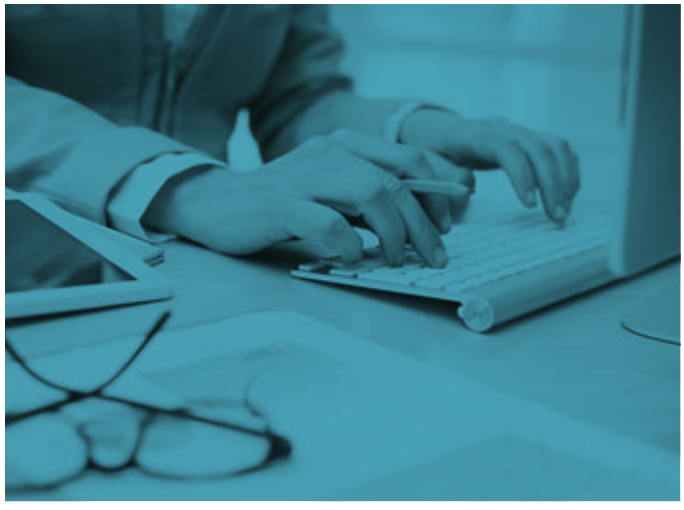
For en virksomhet kan dette bety at informasjon taper konfidensialitet, integritet, autentisitet eller tilgjengelighet. Trusselaktøren kan for eksempel hente ut sensitiv informasjon, endre viktig informasjon eller gjøre kritiske tjenester utilgjengelige.

begrepet Internet of Things (IoT) er en økende bekymring hos flere nasjonale myndighetsorganer rundt i verden. IoT er fysiske gjenstander som bearbeider eller overvåker noe og som kan kommunisere over internett. IoT kan bestå av nettverk, web-applikasjoner, mobile applikasjoner og sky-komponenter, ofte satt i sammen med fokus på funksjonalitet og maksimal tilgjengelighet heller enn på sikkerhet. Utfordringene omfatter blant annet:

- utilstrekkelig autorisasjon
- mangel på transportkryptering
- usikre webgrensesnitt
- mangelfull programvarebeskyttelse

Det gjør at enhetene er sårbare for direkte angrep mot enheten, enten ved at informasjon stjeles eller manipuleres eller ved at tjenesten enheten leverer, blokkeres. Det forventes at IoT-enheter også i større grad vil bli utsatt for og utnyttet ved cyberangrep. Det anerkjente IT-selskapet Gartner har estimert at innen 2020 vil 25 prosent av angrep mot virksomhetene involvere IoT, men sikring av disse enhetene vil ikke utgjøre mer enn 10 prosent av budsjettet for IT-sikkerhet.

Sikkerhetsutfordringene med IoT strekker seg også utover svakheter i enkeltkomponentene. I tillegg til antallet enheter som skal inkluderes, vil også det store antallet versjoner og leverandører av enheter komplisere skalerbarheten og hvordan de inkluderes i virksomheters nettverk. Standardisering og en helhetlig tilnærming til hvordan enhetene integreres vil være avgjørende for å ivareta det økende antall enheter som kobles på internett.



BLOCKCHAIN

Blockchain-teknologien er noe som flere sikkerhetsselskaper ser på som en ny mulighet til å forbedre sikkerheten i blant annet digitale økonomiske transaksjoner. En blokk inneholder et sett med informasjon samt tidsstempel og kode som sikrer at blokken (informasjonen) ikke kan endres uten at dette oppdages. Gartners estimater for 2017 tilsier at initiativene, til tross for økende interesse, fortsatt vil være alfa- og beta-versjoner med store sikkerhetsutfordringer.

SIKRING AV OBJEKTER

Sikkerhetstruende hendelser som terrorisme, sabotasje og spionasje er i sin natur trusler som ikke forventes å ha et forvarsel. Mot denne type trusler er det derfor hensiktsmessig å fokusere på det forebyggende objektsikkerhetsarbeidet. Formålet med objektsikkerhetsarbeidet er å legge til rette for en helhetlig og

overordnet tilnærming på tvers av samfunnssektorene når det gjelder utvelgelse, beskyttelse og tilsyn med skjermingsverdige objekter. Et skjermingsverdig objekt kan for eksempel være en bygning, en dataserver, en operasjonssentral eller et varslingssystem. I sikringen av et objekt inngår både elementer av fysisk sikring, informasjonssikkerhet og personellsikkerhet.

Mange virksomheter kan ha sårbarheter knyttet til objektsikkerhet. Avhengigheter mellom virksomheter er ofte ikke kartlagt. Balansen mellom fysiske sikringstiltak, tiltak for å oppdage hendelser og reaksjonstid er ofte utilstrekkelig. Gjennom NSMs tilsynsaktivitet på objektsikkerhet og fysisk sikring er det avdekket store mangler i gjennomføring av forebyggende sikkerhetstiltak. Flere av virksomhetene hadde heller ikke oppdatert risikovurdering og hadde ikke gjennomført sikkerhetsrevisjoner. Mange virksomheter som forvalter skjermingsverdige objekter, har ikke planer for å oppskalere sikkerheten ved økt risiko. Funn fra tilsyn viser at det sjelden foreligger resultater fra kartlegging av avhengigheter i egen sektor og tverrsektorielt. NSM mener det er nødvendig å legge til rette for bedre kartlegging og rapportering av avhengigheter. Dette vil bidra til å gi myndighetene bedre oversikt over alvorlige sårbarheter.

DRONER

Droner har blitt brukt i militær sammenheng i flere tiår, blant annet i forbindelse med etterretning, overvåkning og innhenting av informasjon om potensielle militære mål. I de senere år har det imidlertid vært en betydelig økning i sivil bruk av droner, både kommersielt og for hobbybruk. Den økte tilgangen på billige, velfungerende droner reiser spørsmål om droner kan bli brukt til ondsinnede handlinger.

I Norge er det ulovlig å bruke droner til fotografering eller filming i nærheten av militære installasjoner eller restriksjonsområder. Utenfor militære restriksjonsområder er det i utgangspunktet tillatt å fly og fotografere fra droner så lenge de er innenfor operatørens synsvidde.

I vinter har Forsvarets øvelser blitt overvåket av ukjente droner. Både i november og i februar ble et tosifret antall ukjente droner observert over militære øvingsområder. Droner er også observert over flere svenske øvelser det siste året.

Det nye elementet som droner introduserer er muligheten for å omgå en rekke sikringssystemer og adgangskontrollmekanismer. Et godt eksempel er fengsler og flyplasser, der det eksisterer strenge systemer for sikring av områder, men hvor det er relativt enkelt å omgå disse ved å fly over eksisterende sikringstiltak. Der noen sikringstiltak har vært innrettet mot trusler på bakkenivå, bør sikringstiltak også vurderes i høydedimensjonen. Dette fjerner ikke behovet for god perimetersikring eller gjør eksisterende sikringstiltak virkningsløse.

Kommersielt tilgjengelige droner blir stadig mer utbredt, billigere og enklere å betjene. Samtidig øker rekkevidden, og de kan bære med seg flere kilo nyttelast i tillegg til egenvekt og kamera. Droner som er tilgjengelig i Norge i dag, kan relativt enkelt utstyres med last som kan brukes

til tilsiktede, skadelige hendelser. Så langt er ikke NSM kjent med at slike angrep er gjennomført i Vesten.

Kommersielt tilgjengelige droner vil bli enda enklere å betjene de neste årene. Droner kan allerede nå settes opp slik at de flyr til et forhåndsprogrammert GPS-koordinat uten styring fra bakken, og de neste årene vil vi se en økning i dronenes rekkevidde, løfteevne, pålitelighet, flyegenskaper og muligheter for avansert programmering av styringssystemer. Dersom utviklingen i kapasiteter går raskere enn utviklingen i mottiltak, vil risikoen droner utgjør, øke.

NY INFRASTRUKTUR, NYE AVHENGIGHETER

Det er økende muligheter og vekst innenfor romsektoren. Kostnader reduseres og teknologier miniatyriseres. Dette muliggjør et større antall kommersielle aktører og små satellitter med gode ytelser.

Satellitter leverer tjenester som navigasjon, presise tidsangivelser, værovervåking, overvåking av skipstrafikk, forskning og mye annet. Sektorer som luftfart, skipsfart og meteorologi er avhengige av disse tjenestene. Fremtidige selvstyrte transporttjenester vil ikke kunne eksistere uten dem. Noen tjenester, som GPS, kan brukes av den enkelte gjennom håndholdte enheter, andre krever store bakkestasjoner. Sektoren er i ferd med å bli av kritisk betydning for samfunnet på linje med kraftproduksjon og elektronisk kommunikasjon. Utnyttelse av sårbarheter kan få konsekvenser for en rekke andre kritiske samfunnsfunksjoner.

Norge har egne satellitter for blant annet telekommunikasjon og skipsovervåking. Vi deltar i europeiske satellittsamarbeid som navigasjonssystemet Galileo og jordobservasjonsprogrammet Copernicus. Vi har bakkestasjoner for å hente ned data fra satellittene, korrigere dem og for å bedrive atmosfærisk forskning.

Denne veksten kan gjøre romsektoren til et mer attraktivt mål for de som vil stjele informasjon og teknologi, blant annet for å utvikle sin egen romsektor eller å utnytte norsk romsektor for sine egne formål. Det kan også finnes aktører som er interessert i å sabotere norsk romvirksomhet i gitte situasjoner. Utviklingen innen romsektoren kan tiltrekke seg statlige etterretningstjenester.

Det er særlig gjennom bakkestasjonene at romvirksomheten kan være lett tilgjengelig for uønskede handlinger, blant annet gjennom personer som kan være infiltrert i virksomheten. Cyberangrep mot bakkestasjoner og brukerterminaler som er koblet mot nett, har den samme sikkerhetsmessige utfordringen som hvilken som helst annen IKT-infrastruktur. Fra sommeren 2013 til høsten 2016 ble det avdekket flere alvorlige cyberangrep mot virksomheter i romsektoren.


«Satellitter leverer
tjenester som navigasjon,
presise tidsangivelser,
værovervåking, overvåking
av skipstrafikk, forskning
og mye annet.»

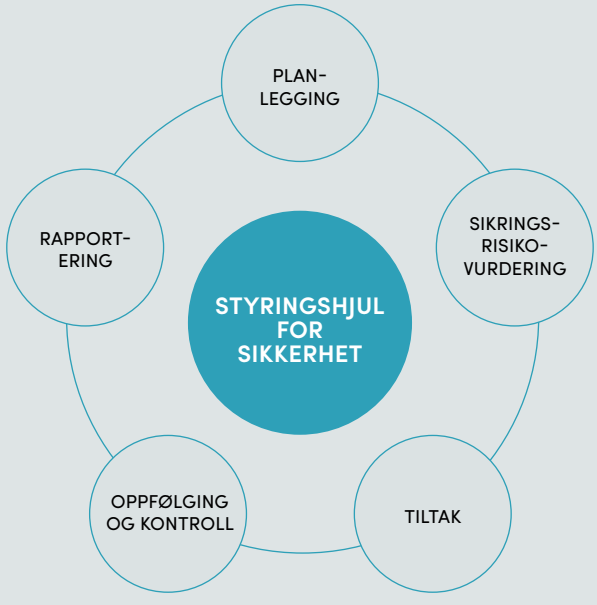
Tiltak som reduserer risiko

NSM ANBEFALER en helhetlig tilnærming til tiltak for å beskytte risikoutsatte verdier. Dette inkluderer både forebyggende tiltak og tiltak for å håndtere hendelser dersom de inntreffer. Forebyggende sikkerhetsarbeid skal bidra til å beskytte viktige verdier og skape motstandsdyktighet. God styring av risiko i virksomhetene er en forutsetning for å beskytte de riktige verdiene med tilstrekkelige sikringstiltak. Virksomhetene må fokusere på de sårbarhetene de selv kan gjøre noe med og skaffe seg tilstrekkelig sikkerhetsfaglig kompetanse til dette. Sikkerhet og risikostyring bør være en integrert del av virksomhetens kjerneprosesser. Behovet for god forebyggende sikkerhet har fått økt oppmerksomhet i blant annet digitalt sårbarhetsutvalg, forsvarssektorens langtidsplan, samfunnssikkerhetsmeldingen og gjennom arbeidet med ny sikkerhetslov.

ETABLERE SYSTEM FOR KONTINUERLIG STYRING OG FORBEDRING AV SIKKERHETSARBEIDET

Et styringshjul som setter sikkerhetsarbeidet inn i et system for kontinuerlig forbedring og utvikling av arbeidet, kan bidra til å gjøre virksomhetenes sikkerhetsarbeid mer systematisk og lettere å følge opp. Det er viktig at styring av sikkerhetsarbeidet blir en integrert del av den øvrige virksomhetsstyringen. Fasene i et styringshjul kan være: planlegging, sikringsrisikovurdering, tiltak, oppfølging og kontroll samt rapportering.

Risikovurderinger vil bidra til å gjøre virksomheten klar over hvilke utfordringer man står overfor. I tillegg gir risikovurderinger grunnlag for å beslutte hvilke tiltak som bør iverksettes. Man unngår mer eller mindre tilfeldige tiltak som mangler faglig fundament og risikerer å bli prioritert bort. Hvis enkelte tiltak ikke gjennomføres, vil dette i praksis si at beslutningstaker vurderer at en identifisert sårbarhet medfører en akseptabel risiko. Eksterne krav, interne føringer, risikovurderinger, hendelser og revisjoner gir grunnlag for å beslutte tiltak som reduserer risikoen. Det kan bety nye tiltak eller



NSM ga ut veileder i sikkerhetsstyring i 2015 og håndboken Risikovurdering for sikring i 2016.

forbedring av eksisterende tiltak for å redusere tekniske, menneskelige og organisatoriske sårbarheter. Tiltakene bør ikke være mer inngripende enn nødvendig.

Virksomhetene bør gjennomføre sikkerhetsrevisjoner jevnlig og minst én gang i året. Resultatet må dokumenteres. Resultatene bør kunne måles over tid, slik at det kan etableres kosteffektive tiltak. Kontinuitet og tilgjengelighet til dokumentasjonen vil bidra til økt forståelse av egen risiko, redusere personavhengighet og forenkle arbeidet med senere revisjoner. NSM anbefaler at virksomhetene registrerer hendelser og avvik for å få oversikt over mulige sårbarheter i virksomheten. Det kan gjøre det mulig å se trender og synliggjøre forbedringspotensial i interne sikkerhetsrutiner, lære av tidligere hendelser og bidra til at riktige sikringstiltak iverksettes.

Det må være kultur for å melde fra om avvik og hendelser. Den som rapporterer, skal ikke utsettes for negative konsekvenser, men heller oppmuntres til å rapportere. Luftfarts- og olje- og gassindustrien er eksempler på sektorer hvor dette lenge har vært etablert.

STYRKE SIKKERHETSBEVISSTHETEN

BEVISSTHET MOT PÅVIRKNINGSOPERASJONER

Med erfaringene fra det amerikanske presidentvalget i 2016 og andre hendelser i verden har mange fått øynene opp for begrepet informasjonsoperasjoner. Myndighetsorganer, politiske partier, medier og andre virksomheter med høy grad av tillit i samfunnet bør forsterke sikkerheten i og kontrollen med egne kommunikasjonskanaler, som nettsider, e-post og kontoer på sosiale medier.

Gode passordrutiner og tofaktorautentisering er tiltak som kan bedre sikkerheten og redusere risikoen for at virksomhetens kanaler blir misbrukt av aktører som ønsker å påvirke mediebildet eller opinionen. Det er også viktig å øke bevisstheten i virksomhetene om slike fenomener.

Virksomhetene er selv ansvarlige for å sikre egen informasjon og for å kartlegge og tette sårbarheter. NSMs råd er å innføre tiltak for IKT-grunnsikring for å redusere et bredt spekter av sårbarheter. NSM gir eksempelvis bistand til partiorganisasjonene for å styrke deres informasjonssikkerhet foran stortingsvalget. Hoved-

FAKTA

TILTAK MOT PÅVIRKNINGSOPERASJONER I ANDRE LAND

I EU er det opprettet en «task force» som har som oppgave å kontre russisk desinformasjon ved effektiv kommunikasjon og promotering av EUs politikk og ved å styrke medieforholdene i EUs østlige naboland og EUs medlemsland. Initiativet skal samtidig øke EUs kapasitet til å forutsi, håndtere og svare på desinformasjon fra eksterne aktører. Tsjekkiske myndigheter har besluttet å opprette en anti-propaganda-enhet for å kontre russisk desinformasjon. Også finske myndigheter følger med på russiske påvirknings- og informasjonsoperasjoner, under ledelse av regjeringens kommunikasjonsavdeling. I Sverige gjennomfører Myndigheten för samhällsskydd och beredskap (MSB) «påvirkningsanalyse» for å øke kunnskapen om påvirkningsforsøk mot svenske myndigheter og samvirker med medieforetakene om medieberedskap.

fokus for rådgivningen er å øke sikkerhetsbevisstheten, i tillegg til å gi anbefalinger om tekniske tiltak for å bedre sikkerheten i organisasjonene.

I Norge har vi et etablert system for å fange opp hendelser i cyberdomenet og mulighet for å se dem i sammenheng. Vi mangler imidlertid en tilsvarende funksjon for å fange opp desinformasjon og forsøk på påvirknings- og informasjonsoperasjoner, for eksempel i sosiale medier, tilsvarende det man har i enkelte andre land.

NORMATIVE BARRIERER MOT INNSIDERE

Det finnes ingen enkle tiltak mot spionasje eller lekkasjer forårsaket av innsidere, men det finnes mottiltak som gir effekt over tid. Gode sikkerhetsbarrierer for å håndtere innsidere handler om enkle prinsipper med tydelige mål.

Virksomhetene må vite hvilke informasjonsverdier de forvalter. Denne informasjonen må tilgangsreguleres, for eksempel gjennom en tydelig kommunisert fysisk og logisk regulert soneinndeling og informasjonsautorisering. Det må utarbeides oversikt over hvilke sårbarheter virksomheten har som potensielle trusselaktører kan utnytte. Det bør utarbeides scenarioer for hvordan en mulig innsider kan tilegne seg og misbruke virksomhetens verdier.

Hvis disse tiltakene blir godt forankret i organisasjonen over tid, vil det også bygges normative barrierer hvor hver enkelt medarbeider blir en integrert del av sikkerhetsarbeidet. Gjennom opplæring og øvelser må målet være at alle virksomhetens ansatte blir bevisste på avvikende oppførsel og hendelser og rapporterer disse. Nøkkelen til å stoppe innsidere ligger i å ha bevisst hendelseshåndtering, med gode rapporteringsprosedyrer samt hendelsesregister. Oppnås en slik sikkerhetskultur, er sannsynligheten for å fange opp utro tjenere eller ubevisste medarbeidere mye større.

SIKKERHETSKULTUR OG KOMPETANSE

Sikkerhetskultur er summen av de ansattes kunnskap, motivasjon, holdninger og adferd. God sikkerhetskultur er, sammen med teknologiske og organisatoriske sikringstiltak, en forutsetning for effektiv forebygging av risiko og håndtering av sikkerhetstruende hendelser.

Ensidig tilnærming til tekniske tiltak gir liten effektiv beskyttelse om ikke ansatte har kunnskap og adferd som støtter opp om tiltakene. På samme måte gir ikke ensidig fokus på ansattes kunnskap og adferd knyttet til teknologibruk og prosesser god nok helhetlig sikkerhet. Evnen til en helhetlig tilnærming til sikkerhetsarbeidet er i seg selv en faktor av stor betydning for hvor god sikkerhetskultur en virksomhet kan ha.

I et samfunnsmessig perspektiv bør samfunnet fokusere ytterligere på digital kompetanseutvikling og å bevisstgjøre sine innbyggere slik at den enkeltes evne til å vurdere digital risiko forbedres.

Nasjonal sikkerhetsmåned, som gjennomføres i oktober måned under ledelse av Norsis, er et viktig tiltak for å forbedre sikkerhetskulturen i norske virksomheter. Det er imidlertid viktig å påpeke at sikkerhetsarbeidet er en kontinuerlig prosess som bør være en naturlig del av hverdagen.

Norske virksomheter bør arbeide

målrettet og langsiktig for å forbedre sin sikkerhetskultur. Samtidig er det viktig at virksomhetene gjør seg i stand til å måle hva tilstanden er i egen virksomhet, før forbedringstiltak iverksettes.

FYSISK SIKRING AV OBJEKTER

Objektsikkerhetsforskriften omhandler grunnsikringstiltak med mulighet for påbygningstiltak hvis risikoen endrer seg. Den som eier skjermingsverdige objekter skal derfor utøve risikostyring. Det vil si å fastsette og gjennomføre sikringstiltak basert på kontinuerlige risikovurderinger. Virksomheten må derfor jevnlig vurdere sine verdier og sårbarheter og håndtere endringer i risiko. Nye utviklinger innen teknologi og andre samfunnsforhold har gjort fysiske sikringstiltak relevante på nye måter. I mange tilfeller har utviklingen hatt forsterkende virkning på allerede eksisterende tiltakskategorier innen fysisk sikring. Nye former for trusler innen spionasje og terrorisme gir nye utfordringer også innen fysiske sikringstiltak. En risikovurdering bør også inneholde en vurdering av hvilke sårbarheter man står overfor eksempelvis når det gjelder droner. Dette betyr at man med stor sannsynlighet må se på supplerende tiltak for å motvirke slike trusler.

Risikovurderingen vil være grunnlag for fysiske sikringstiltak. Disse tiltakene må virke i helhet med hverandre, være effektive og ikke være for inngripende. Trusler kan oppstå relativt raskt, og virksomheter kan som følge av dette få avdekket uforutsette sårbarheter. Ved en hendelse kan virksomheten avgrense eller forhindre skade gjennom gode og effektive grunnsikringstiltak som er på plass og virker til enhver tid.

En god risikovurdering og en god grunnsikring av et objekt vil fortsatt være viktig for å kunne håndtere dagens trusselbilde og for å håndtere fremtidige endringer i trusselbildet. Viktigheten av en god grunnsikring som har fundament i en sikringsrisikosanalyse, er basis for alle videre tiltak som kan gjennomføres ved endret trusselsituasjon. Grunnsikringen innebærer alle organisatoriske, administrative, fysiske og tekniske tiltak mot kjente sårbarheter. En god grunnsikring vil også i mange tilfeller hindre eller redusere konsekvenser ved hendelser som ikke er vurdert av forskjellige grunner.

SIKRING AV IKT-SYSTEMER

DE GRUNNLEGGENDE TILTAKENE

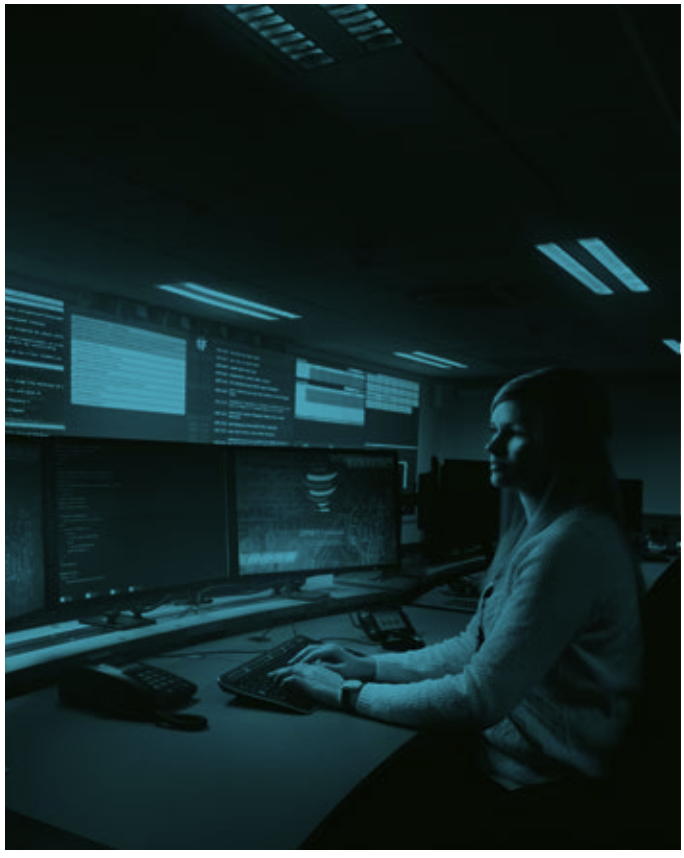
Alle virksomheter, uavhengig av størrelse og om virksomheten er statlig eller privat, bør så langt det lar seg gjøre implementere fire effektive sikringstiltak mot internettrelaterte cyberangrep. Tiltakene blokkerer inntil 90 prosent av kjente cyberangrep og reduserer sårbarheter som er enkle å utnytte. Tiltakene er effektive mot angrep via e-post (phishing) fordi de reduserer muligheten angriperen har for å få kontroll over brukerens maskin.

Fire effektive tiltak

- Oppgrader program- og maskinvare
- Installere sikkerhetsoppdateringer så fort som mulig
- Ikke tildel administrator-rettigheter til sluttbrukere
- Blokker kjøring av ikke-autoriserte programmer

De fire tiltakene er effektive, men er ikke tilstrekkelige for å sikre et informasjonssystem. Dette er fordi tiltakene er begrenset til å beskytte mot angrep på maskinen til brukeren. Nettverkssikkerhet er et annet viktig område. Godt sikrede nettverk vil redusere muligheten for at en angriper får tilgang til virksomhetens verdier, dersom en brukers klient blir kompromittert eller en angriper får fysisk tilgang til nettverket. NSM har derfor publisert *«Ti grunnleggende tiltak for sikring av egne nettverk»*, som har følgende fire hovedkategorier:

- Redusere skadepotensialet ved en kompromittering gjennom nettverksdesign som hindrer angriperen i å få tilgang til hele nettverket
- Hindre angrep ved å få kontroll på nettverkets utstrekning og inngangsdører (fysiske og logiske porter)
- Redusere risiko for avlesning av nettverkstrafikk
- Øke evne til å oppdage og etterforske et angrep



HELHETLIG TILNÆRMING

Virksomhetene er selv ansvarlige for å sikre egen informasjon og bør derfor kartlegge og tette sårbarheter. NSM anbefaler å basere sikringsarbeidet på anerkjente standarder, eksempelvis ISO27000-serien. ISO/IEC 27001:2013 stiller krav til etablering, vedlikehold, implementering og kontinuerlig forbedring av styringssystem for informasjonssikkerhet. ISO/IEC 27002:2013 knytter utforming av sikringstiltak opp mot virksomhetens risikostyring. Dette utgjør en helhetlig tilnærming til tiltak for å beskytte risikoutsatte verdier.

Et tiltak for ytterligere å bedre sikkerheten er å bruke sertifiserte produkter der hvor det er behov for pålitelige og robuste sikkerhetsfunksjoner. Sertifisering etter eksempelvis ISO/IEC 15408 (Common Criteria) innebærer at kunden kan ha tillit til at de aktuelle sikkerhetsfunksjonene oppfyller spesifiserte krav. En økt etterspørsel etter sertifiserte produkter vil

kunne bidra til at markedsaktørene i større grad tar hensyn til sikkerhetskravene allerede i designfasen av produktutviklingen. Bruk av solide komponenter og produkter er et bedre utgangspunkt for å etablere sikre IKT-systemer.

Flere land har iverksatt tiltak for å løse utfordringene knyttet til kravene om en mer effektiv statsadministrasjon og for å imøtekomme behovet for økt digitalisering. Tiltakene er initiert på bakgrunn av behovet for å beskytte kritiske samfunnsfunksjoner og kritisk infrastruktur, i tillegg til å sørge for nødvendig tillit hos virksomheter og innbyggere i bruken av digitale offentlige tjenester. Etablering av en robust felles infrastruktur tilrettelagt for samhandling og kobling av data anses som helt nødvendig.

NSM mener det er behov for færre IKT-miljøer (utviklings- og forvaltningsorganisasjoner) i offentlig sektor, noe som vil gi stordriftsfordeler med mer robuste kompetansemiljøer og kostnadseffektive sikkerhetsløsninger. Felles og større IKT-løsninger vil styrke sikkerhetsnivået ved behandling av sensitiv informasjon sammenlignet med å opprettholde mange spredte og små systemer. Større IKT-miljøer har lettere for å tiltrekke seg og bygge opp sikkerhetsfaglig kompetanse og annen spesialkompetanse. Felles IKT-løsninger vil medføre reduksjon i antall variasjoner på nettverk, systemer og tjenester. Dette gir et potensial for reduksjon av sårbarheter og mulige angrepsflater. Færre variasjoner gir også mindre kompleksitet. Felles IKT-løsninger og infrastruktur er viktig for sikker samhandling både innen sektorer og mellom sektorer.

FAKTA

GRUNNPRINSIPPER FOR IKT-SIKKERHET

NSM er i ferd med å etablere et helhetlig og systematisk sett med de viktigste tiltakene for sikring av samfunnsviktige IKT-løsninger gjennom grunnprinsipper for IKT-sikkerhet. Grunnprinsippene vil legge til rette for gjenbruk i og på tvers av ulike sektorer ved å bygge på etablerte internasjonale standarder. Prinsippene skal gjøre det enklere for sektorer og virksomheter å oppfylle krav i ulike regelverk og på den måten legge til rette for felles tekniske løsninger.

NSM vil i 2017 prioritere de viktigste anbefalingene som gjelder for både ugraderte og graderte løsninger. Hensikten er å gi beslutningstakere i offentlige og private virksomheter en policyfokusert tiltakspakke for sikring av sin virksomhet og sine informasjonssystemer. Den første tiltakspakken er under arbeid og vil omfatte tjenesteutsetting, drift og forvaltning, aksesskontroll, kommunikasjonssikkerhet, herding, logging og hendelseshåndtering.

Tiltakene prioriteres ut fra NSMs og andre relevante miljøers kunnskap og erfaring og vurderes opp mot etablerte standarder og relevante lovverk. Sikringstiltakene skal være dynamiske og i tråd med den teknologiske utviklingen og samtidig støtte opp under digitaliseringen i samfunnet.

GJØRE TJENESTEUTSETTING SIKRERE

For å ivareta sikkerheten ved tjenesteutsetting må virksomheten etablere tilfredsstillende styring og kontroll med leveransene av tjenestene fra leverandører og eventuelle underleverandører. Dette omfatter også hvordan leverandøren håndterer de informasjonsverdiene den er satt til å behandle på virksomhetens vegne. Tjenesteutsetting medfører ikke at ansvaret til virksomheten reduseres eller forenkles. Bruk av tjenesteutsetting vil for virksomheten ofte innebære et betydelig ansvar for å kontrollere og sikre at tjenestene leveres som avtalt og at informasjonsverdier sikres. For virksomheten er kompetanse og

organisering viktig for å kunne utøve tilfredsstillende styring og kontroll.

Virksomhetene anbefales som et minimum å gjennomgå følgende områder før igangsetting av tjenesteutsettingen:

- Kartlegg hvilke lover og regler som gjelder for sektoren virksomheten tilhører – både nasjonalt og internasjonalt.
- Utfør en risikovurdering av virksomhetens verdier som eksponeres ved tjenesteutsetting. Risiko, samt krav til konfidensialitet, integritet og tilgjengelighet, bør vektlegges i vurderingen.
- Utarbeid et detaljert kravdokument for alle faser av tjenesteutsettingen, det vil si selve anskaffelsen, forvaltnings- og driftsfasen samt ved avslutning av kontrakten.

En tjenesteutsetting er inngåelse av en kommersiell avtale som virksomheten skal forholde seg til over år. Det er derfor viktig at leveransene fra det som tjenesteutsettes er tett integrert med virksomhetens daglige operasjon og inngår i realiseringen av dens strategi. Konfidensialiteten og integriteten til informasjon som lagres og formidles via en skytjeneste eller i et datasenter, må sikres gjennom kryptering.

EVNE Å OPPDAGE OG HÅNDTERE IKT-HENDELSER

Evnen til å oppdage alvorlige cyberhendelser må styrkes, både på nasjonalt plan, gjennom sektorvise responsmiljøer og i virksomhetene. Nasjonalt må sensornettverket Varslingssystem for digital infrastruktur (VDI) styrkes for å

FAKTA

RAMMEVERK FOR DIGITAL HENDELSESHÅNDTERING

NSM jobber med å utvikle et nasjonalt operativt «rammeverk for digital hendelseshåndtering». Rammeverket skal styrke Norges evne til å håndtere cyberhendelser som rammer offentlige og private virksomheter i enkeltsektorer og på tvers av sektorer. Rammeverket beskriver en tverrsektoriell og systematisk tilnærming til digital hendelseshåndtering slik at alle relevante aktører effektivt kan utøve sitt ansvar i en koordinert nasjonal respons. Rammeverket skal blant annet bidra til å:

> Tydeliggjøre myndighet, ansvar og roller

> Tydeliggjøre forventninger til virksomheter i privat og offentlig sektor

> Kommunisere hva virksomhetene selv må være forberedt på å håndtere og hva slags støtte og koordinering som kan forventes fra det nasjonale responsmiljøet (NSM NorCERT)

> Styrke samarbeid mellom virksomheter, sektorvis responsmiljø (SRM), NSM, politiet og EOS-tjenestene

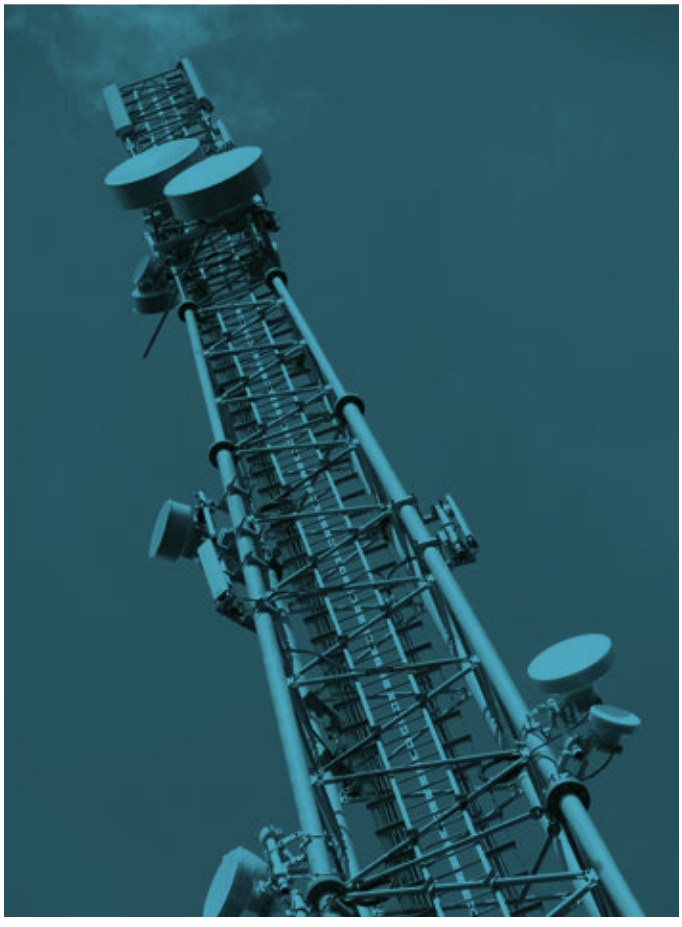
> Videreutvikle evnen til å rapportere cyberhendelser og dele relevant informasjon

> Tydeliggjøre kontaktpunkter mot andre land og organisasjoner

Digital hendelseshåndtering er en prosess for å oppdage og respondere på en cyberhendelse. Rammeverk for digital hendelseshåndtering vektlegger tiltak fra forberedelse og planlegging, deteksjon og rapportering, vurdering, respons og utarbeidelse av læringspunkter.

kunne gi et tilstrekkelig situasjonsbilde av den nasjonale IKT-sikkerhetstilstanden. Virksomhetene bør legge til rette for rapportering av hendelser til sektorvise responsmiljøer, som igjen videreformidler til det nasjonale kontaktpunktet, NSM NorCERT.

Det er viktig at evnen til å oppdage hendelser ivaretas dersom virksomheten velger å sette ut tjenester, også ved bruk av skytjenester. Sikker hendelseshåndtering og gjenoppretting er en viktig del av informasjonssikkerhetsarbeidet. Dette innebærer at hendelser må analyseres og kontrolleres, skadeomfanget begrenses, årsaken til hendelsen identifiseres og elimineres og sikker drift reetableres. Det er sentralt at virksomhetene etablerer, eller har tilgang til, tilstrekkelig evne og kapasitet til å håndtere cyberhendelser. NSM har etablert en kvalitetsordning for leverandører som tilbyr tjenester for håndtering av cyberhendelser. Hensikten er å gjøre det mulig for virksomheter å velge leverandører som etter NSMs vurdering har tilfredsstillende tjeneste-kvalitet. Ordningen skal også bidra til å heve kompetansen til leverandører av hendelseshåndteringstjenester i Norge.



«Evnen til å oppdage alvorlige cyberhendelser må styrkes, både på nasjonalt plan, gjennom sektorvise responsmiljøer og i virksomhetene.»

NASJONAL SIKKERHETSMYNDIGHET

Postboks 814, 1306 Sandvika

Tlf. 67 86 40 00
post@nsm.stat.no
www.nsm.stat.no