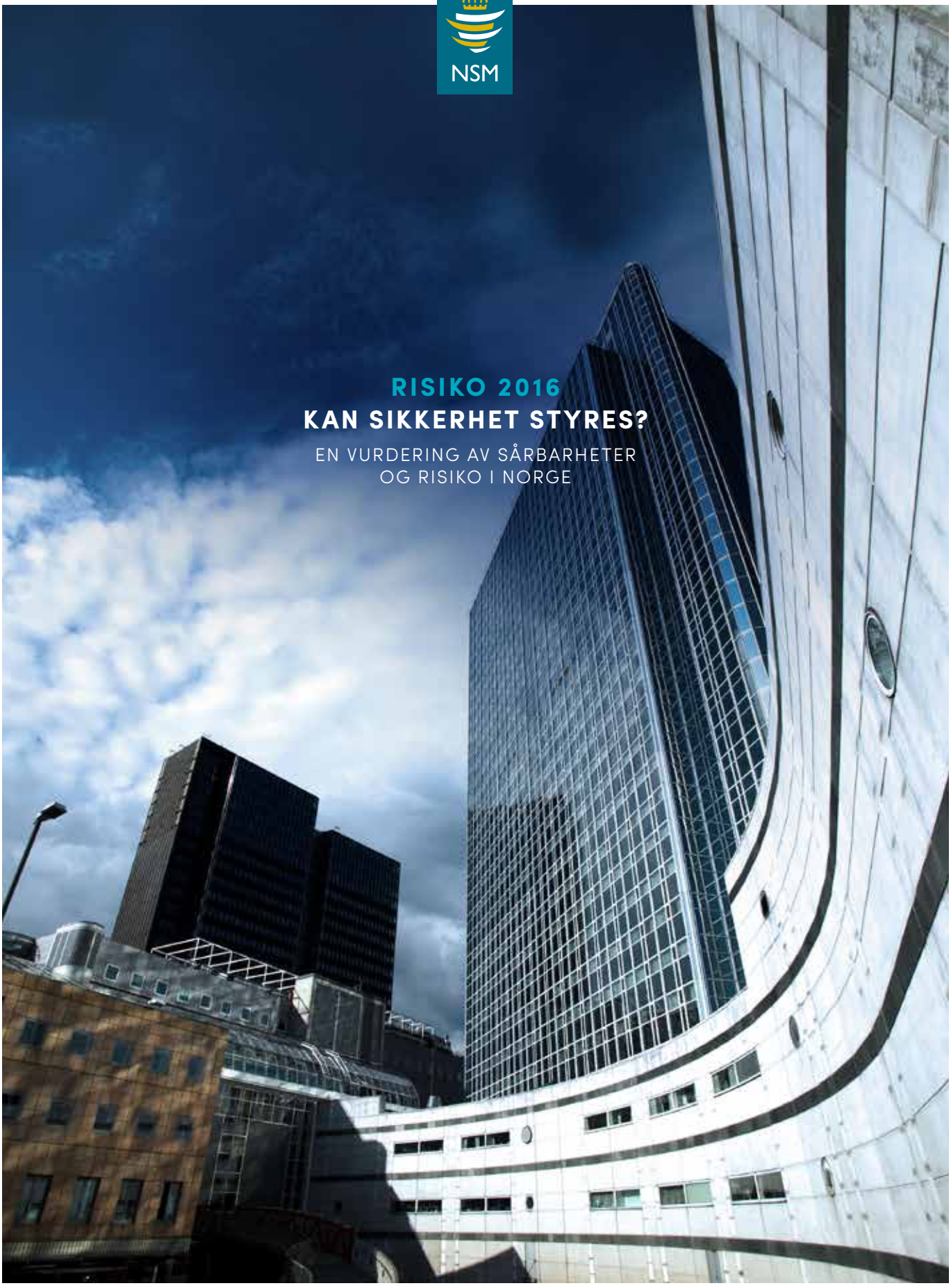
NSM



RISIKO 2016

KAN SIKKERHET STYRES?

EN VURDERING AV SÅRBARHETER
OG RISIKO I NORGE

Nasjonal sikkerhetsmyndighet (NSM) er Norges ekspertorgan for informasjons- og objektsikkerhet. Direktoratet er det nasjonale fagmiljøet for IKT-sikkerhet og varslings- og koordineringsinstans for alvorlige dataangrep og IKT-sikkerhetshendelser.

Innhold

RISIKO 2016

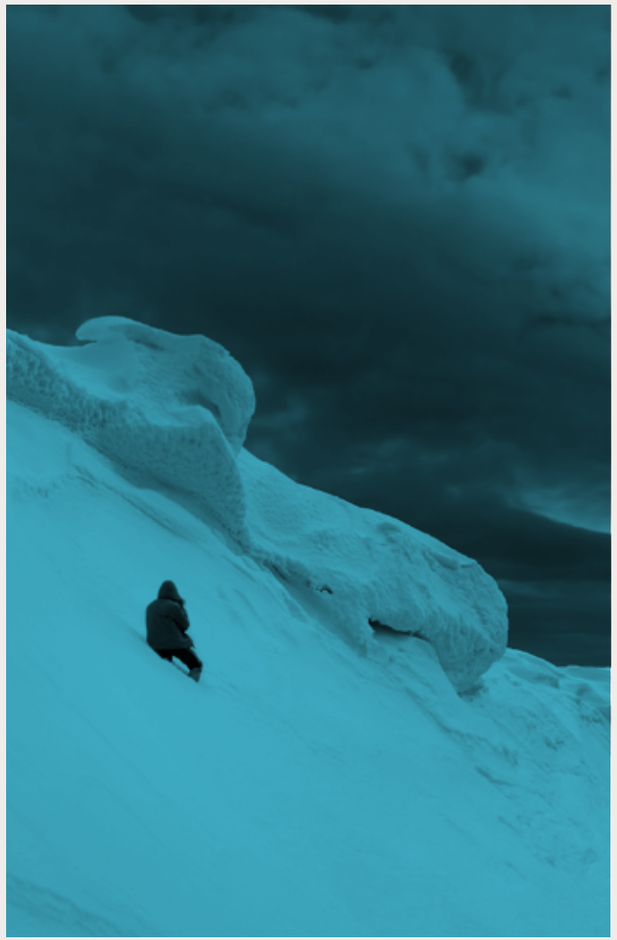
Foto omslag:
SCANPIX

Design:
REDINK

Foto:
ISTOCK, SCANPIX

Trykk og distribusjon:
RK GRAFISK

Forord



NASJONAL SIKKERHETSMYNDIGHET (NSM) har som oppgave å vurdere risiko innen forebyggende sikkerhet og foreslå sikkerhetsfremmende tiltak. Risiko 2016 er årets rapport om sikkerhetstilstanden.

I 2015 utarbeidet NSM Sikkerhetsfaglig råd (SFR) til forsvarsministeren og justis- og beredskapsministeren. I tillegg produserte vi rapporten Helhetlig IKT-risikobilde 2015. Begge er tilgjengelige på NSMs hjemmesider.

I SFR er det utviklet mange forslag til tiltak for å forbedre sikkerhetsarbeidet. Dette inkluderer forbedring av overordnet styring av sikkerhet og styrking av evnen til å oppdage og håndtere IKT-angrep.

Funnene og vurderingene i Risiko 2016, SFR og Helhetlig IKT-risikobilde vil i stor grad være overlappende, ettersom de tre rapportene kommer såpass tett i tid og omhandler i hovedsak samme tematikk.

«Nasjonal sikkerhets-myndighet (NSM) har som oppgave å vurdere risiko innen forebyggende sikker-het og foreslå sikkerhets-fremmende tiltak.»

Sammendrag

RISIKO 2016 er Nasjonal sikkerhets-myndighets (NSM) vurdering av risiko-bildet innen forebyggende sikkerhet i Norge. Vurderingen bygger på funn fra virksomheter underlagt sikkerhetsloven og andre utvalgte kilder. Risikobildet er relevant for offentlige og private virksomheter.

Samfunnet produserer kontinuerlig nye verdier som kan være attraktive for ulike trusselaktører. Disse aktørene tar med økende grad av suksess i bruk mer avanserte verktøy for å tilegne seg denne informasjonen, og de utvikler sine teknikker raskere enn vi utvikler mot-tiltak. Dette kan sammenliknes med et våpenkappløp.

Det er stor risiko forbundet med IKT-angrep og annen spionasje i 2016 og årene fremover. Det kan også være betydelig risiko knyttet til sikkerhetsklarering av personer med tilknytning til fremmede stater.

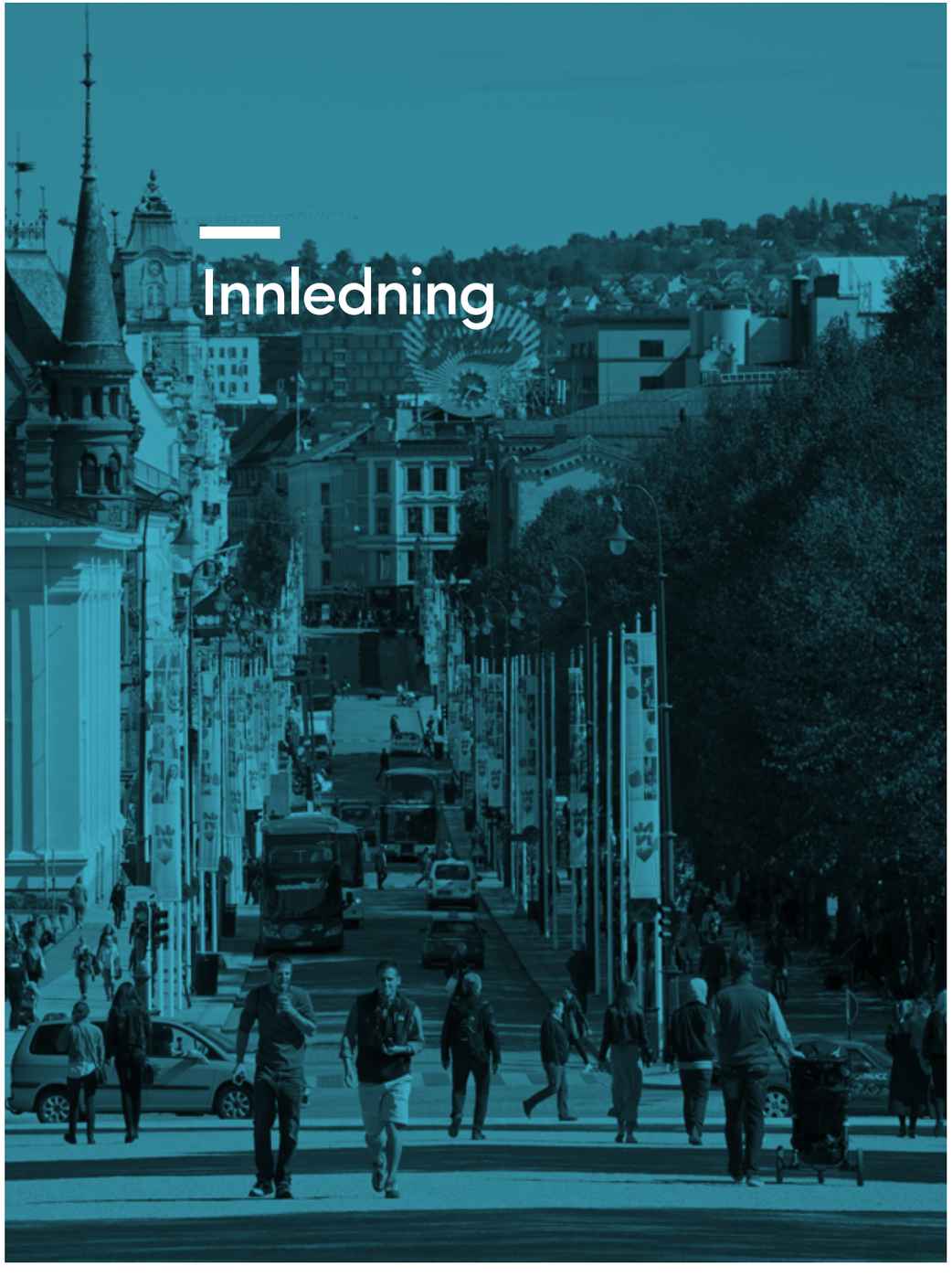
Vi anser svakheter i styring av forebyggende sikkerhet på alle nivåer som den mest vesentlige utfordringen. Svakheter i lederforankring og styring av sikkerhetsarbeidet i et stort antall virksomheter kan få konsekvenser for virksomhetene og for nasjonal sikkerhet. Dette påvirker informasjonssikkerhet generelt, IKT-sikkerhet, personell-sikkerhet og objektsikkerhet.

«Det er stor risiko forbundet med IKT-angrep og annen spionasje i 2016 og årene fremover.»

Evnen til håndtering av IKT-hendelser er under sterkt press. Virksomhetenes egenevne til hendelseshåndtering er liten, og den samlede nasjonale evnen til å oppdage og håndtere uønskede hendelser i IKT-systemer er heller ikke tilstrekkelig utviklet for fremtidens utfordringer.

Det utdannes for få personer med relevant kompetanse om forebyggende sikkerhet på IKT-området, og det er stor konkurranse om de som er tilgjengelig. Det utdannes heller ikke nok spesialister på skadevareanalyse og angrepsanalyse innen hendelseshåndtering på IKT-området for å dekke dagens og fremtidens behov.

Det er lite sannsynlig at risikobildet vil endre seg i positiv retning i løpet av det neste året. Dagens trender vil fortsette og mest sannsynlig føre til økende sikkerhetsmessig risiko. Den omfattende arbeidsinnsatsen fra mange aktører innen forebyggende sikkerhet gir effekt, men ikke i tilstrekkelig grad i forhold til trusselutviklingen.



Innledning

RISIKO 2016 er Nasjonal sikkerhetsmyndighets NSM vurdering av risikobildet i Norge. Her vurderer vi risikoen for at sentrale kritiske funksjoner, samfunnsviktig infrastruktur og skjermingsverdig informasjon kan bli rammet av IKT-angrep eller andre alvorlige handlinger. I hovedsak ligger våre egne observasjoner til grunn for vurderingene i rapporten. Grunnlaget for vurderingen er blant annet våre egne tilsyn, erfaring fra konkrete hendelser, inntrengningstesting av IKT-systemer og opplysninger fra andre.

Risiko 2016 må ses i sammenheng med Helhetlig IKT-risikobilde 2015 og Sikkerhetsfaglig råd, som ble levert til Forsvarsdepartementet og Justis- og beredskapsdepartementet høsten 2015. Disse rapportene er produsert over en kort tidsperiode og har i stor grad sammenfallende informasjonsgrunnlag.

Risiko 2016 fokuserer på svakheter i styring av forebyggende sikkerhet på alle nivåer. Svakheter i lederforankring og styring av sikkerhetsarbeidet i et stort antall virksomheter kan få konsekvenser for virksomhetene og for nasjonal sikkerhet. Dette påvirker informasjonssikkerhet generelt, IKT-sikkerhet, personellsikkerhet og objektsikkerhet.

Forsvarets forskningsinstitutt (FFI) peker dessuten i en studie på at de fleste sikkerhetsbrudd skyldes organisatoriske sårbarheter, og mange av disse har med styring å gjøre.[1] Gode organisatoriske sikkerhetstiltak er en forutsetning for å kunne etterspørre, gjennomføre og få full effekt av teknologiske tiltak og tiltak for å redusere menneskelige sårbarheter. Et styringssystem for sikkerhet[2] bidrar til å beskytte viktige verdier og til kontinuerlig forbedring og utvikling i sikkerhetsarbeidet. Styring av sikkerhet bør integreres i den øvrige virksomhetsstyringen.

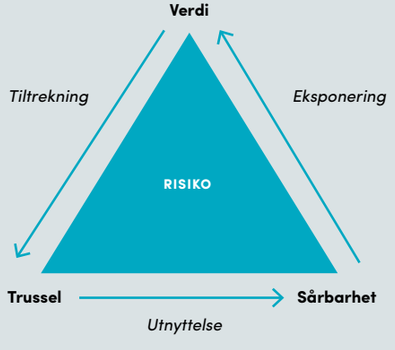
Alle virksomheter må leve med en viss risiko, men det er avgjørende at virksomhetene vet hva de må beskytte og på hvilken måte dette bør gjøres. For å kunne beskytte samfunnets verdier må hver enkelt virksomhet bidra til å redusere samfunnets *sårbarhet*. Kriser oppstår ofte uten varslingstid som gir mulighet til å iverksette ytterligere tiltak. Derfor må virksomhetene prioritere god grunnsikring og evne til å håndtere hendelser.

[1] FFI-rapport 2014/00948 Norges sikkerhetstilstand – en årsaksanalyse av mangelfull forebyggende sikkerhet.

[2] Et styringssystem handler om hvordan virksomheten arbeider i tillegg til å beskrive hvordan virksomheten styrer og utfører tiltakene og aktivitetene sine.

FAKTA

RISIKOTREKANTEN



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

Verdier og interesser

STATEN OG ANNEN offentlig myndighet, norske statlige og private nærings-virksomheter samt enkeltpersoner forvalter en rekke verdier som er attraktive for ulike trusselaktører. Dette omfatter blant annet kritiske samfunnsfunksjoner, det vil si de funksjonene som dekker samfunnets og befolkningens grunnleggende behov.[3] Kritiske samfunnsfunksjoner omfatter å

- ivareta nødvendig matforsyning
- ivareta nødvendig drikkevannsforsyning
- ivareta befolkningens behov for varme
- ivareta nasjonal sikkerhet
- ivareta styring og kriseledelse
- opprettholde demokratisk rettsstat
- opprettholde trygghet for liv og helse
- opprettholde lov og orden
- opprettholde finansiell stabilitet
- opprettholde grunnleggende sikkerhet for lagret informasjon
- sikre kulturelle verdier av nasjonal betydning
- beskytte natur og miljø

Virksomheter med en kritisk samfunns-funksjon er avhengig av innsatsfaktorer for å kunne produsere og levere. Under er noen viktige innsatsfaktorer det er naturlig å ha nasjonale forventinger til:

- ekom[4]-tjenester
- elektrisitetsforsyning
- vannforsyning
- avløpshåndtering
- drivstofforsyning
- vare- og persontransport
- satellittbaserte tjenester
- meteorologiske tjenester

Disse verdiene kan bli utsatt for angrep fra trusselaktører, blant annet via internett.

De siste årene har det blitt oppdaget IKT-angrep mot norsk forsvars-, sikkerhets- og beredskapssektor, politiske prosesser, norsk kritisk infrastruktur og enkeltvirksomheter eksempelvis innen petroleum, kraftproduksjon, romfart, shipping og elektronisk kommunikasjon. Dette viser hva trusselaktørene er ute etter. Trusselaktørene gjør nøye vurderinger av hva som er informasjon av høy verdi.

Den enkelte eier av informasjon eller objekt som er sensitiv eller skjermings-verdig, må selv foreta en verdivurdering for å finne riktig grad av beskyttelsestiltak.

Fagdepartementenes arbeid med å utpeke og klassifisere skjermingsverdige objekter er derfor en nødvendig strategisk nasjonal tverrsektoriell verdivurdering.

[3] Informasjonen om kritiske samfunns-funksjoner og innsatsfaktorer er hentet fra Direkto-ratet for samfunns-sikkerhet og beredskaps rapport «Sikkerhet i kritisk infrastruktur og kritiske samfunns-funksjoner – modell for overordnet risiko-styring», KIKS-prosj-ektet – 1. delrapport 2012.

[4] Elektronisk kom-munikasjon.

Dataangrep mot Norge

Svært mye av virksomheten til Nasjonal sikkerhetsmyndighet handler om å beskytte informasjon. En av de største truslene er dataangrep; målrettede spionasjeoperasjoner for å få tak i informasjon som har stor verdi for aktørene som står bak. Slik foregår det, og slik jobber vi for å stoppe det:

E-POST

En e-post er ofte veien inn i norske data-systemer. I e-posten er det som regel et vedlegg eller en lenke til en nettside. Når mottakeren klikker på vedlegget eller lenken, infiseres data-maskinen av virus, dersom den ikke er godt nok sikret.

INFISERTE NETTSIDER

Infiserte nettsider er en annen vei inn i norske datasystemer. Trusselaktørene infiserer nettsider de vet offeret vil besøke. Nettsiden serverer virus til datamaskinene som går inn på sidene.

E-POSTEN ÅPNES IKKE

NSM har nådd frem med informasjon om sikkerhet, og mottakeren åpner ikke e-posten.

VIRUSET STOPPES

E-posten eller nettsiden åpnes, men alle dataprogrammer er oppdatert, og virksomheten har god sikkerhetsstyring. De har også fulgt NSMs fire grunn-leggende tekniske tiltak for å stoppe dataangrep. Tiltakene stopper 80-90 prosent av alle kjente dataangrep.

HELE DATASYSTEMET BLIR INFISERT

Offeret klikker eller går inn på en infisert nettside. Datamaskinene er ikke godt nok sikret, og viruset kommer inn i data-systemene på jobben.

ANGREPET STOPPES

Sikkerhetsleder og datasikkerhetsleder har vært på kurs hos NSM. De har folk som kan håndtere dataangrep og gode logger, og iverksetter tiltak for å stoppe angrepet. De varsler også NSM, som deler informasjon med andre aktører.

DATAANGREPET OPPDAGES

Mange dataangrep oppdages først når det er gått tid, i enkelte tilfeller måneder og i noen tilfeller år. I slike tilfeller har trussel-aktørene fått tak i store mengder informasjon. Konsekvensene er store. Ofte er det tilfeldigheter som gjør at denne typen angrep oppdages.

VARSLING OG OPPRYDDING

NSM NorCERT kontaktes ofte i slike tilfeller, bistår med teknisk analyse og koordinerer hånd-teringen nasjonalt. Vi samarbeider blant annet tett med Etterretnings-tjenesten og PST i Cyber-koordinerings-gruppen.

ANGREPET STOPPES

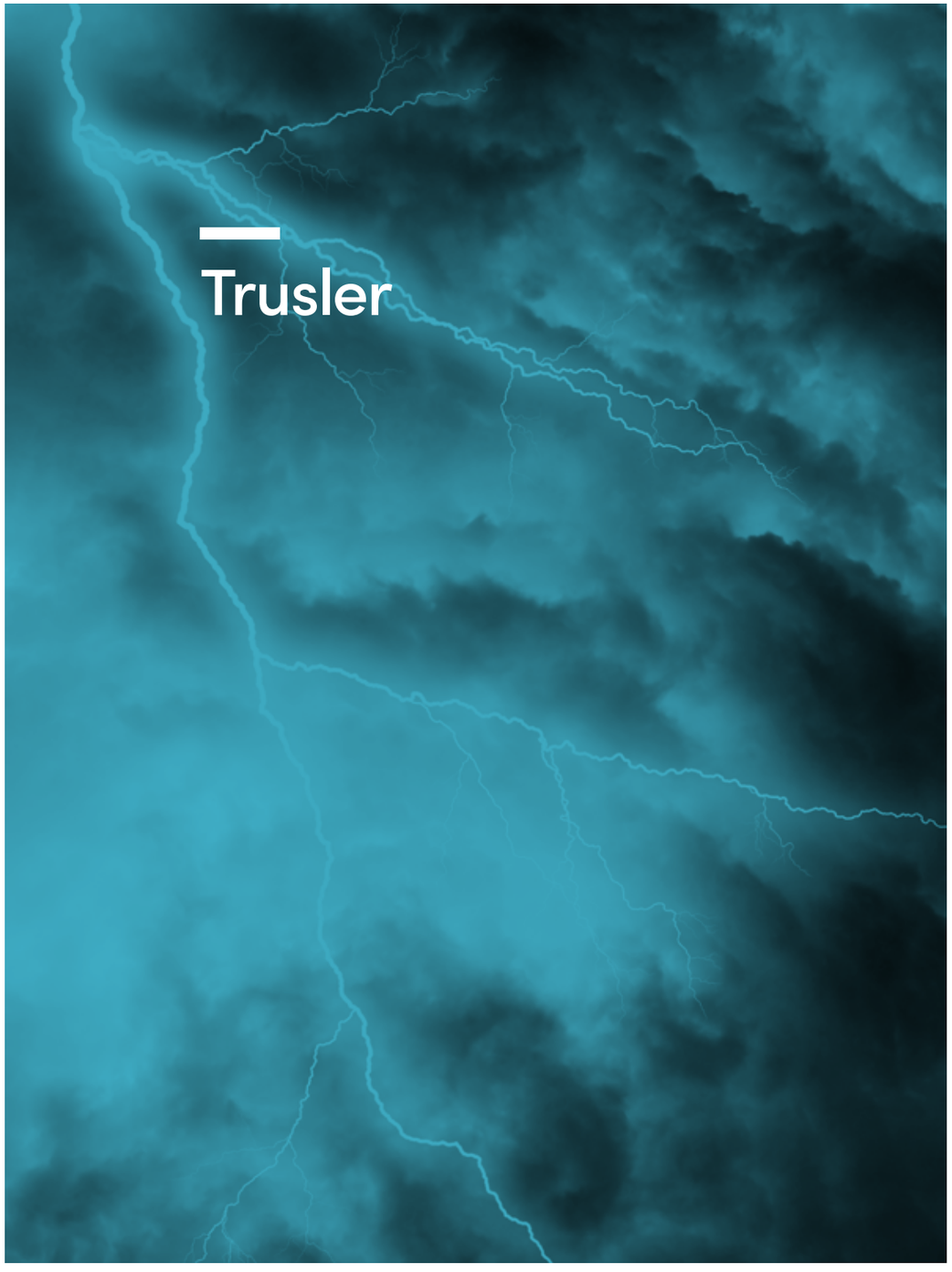
Kappløpet mellom de som ønsker å stjele informasjon og de som ønsker å beskytte informasjonen, blir stadig mer utfordrende. Etter at dataangrepet er oppdaget, avverget eller stoppet, starter opprydningen, både gjennom teknisk opprydning i datasystemene, analyse av hva som har skjedd og informasjonsdeling om hvordan vi kan unngå samme typen angrep fremover.

ALARMEN GÅR I NSM NORCERT, ANGREPET STOPPES

Virksomheten er koblet til Varslingssystem for digital infrastruktur når ondsinnet trafikk oppdages, NSM NorCERT varsler umiddelbart virksomheten, koordinerer nasjonalt og bistår i håndteringen ved behov. NSM bistår blant annet ved å dele informasjon, drive teknisk analyse og levere situasjonsrapporter til departementene. De har folk som kan håndtere dataangrep, gode logger og iverksetter tiltak for å stoppe angrepet.

Hvem har ansvaret?

Norske virksomheter har hovedansvaret for å forebygge mot dataangrep og håndtere dem på en god måte. Myndighets-organene i de ulike sektorene har ansvaret for at sikkerheten i deres egen sektor er god nok. NSM jobber sektorovergripende og bistår og koordinerer håndteringen på nasjonalt nivå når det gjelder alvorlige dataangrep.



Trusler

IFØLGE ETTERRETNINGSTJENESTEN søker fremmede stater, grupper og personer etter kunnskap om forhold i Norge som kan brukes politisk, økonomisk eller militært.[5] Etterretningstrusselen har vært økende i flere år, og fremmede etterretningstjenester benytter ulike metoder for å få tak i ønsket informasjon. Omfattende sikkerhetspolitiske endringer den siste tiden har ført til endringer i trusselbildet.[6] Dette bidrar til en situasjon med potensielt kort varslingstid ved uønskede tilsiktede handlinger. Kortere varslingstid utfordrer samfunnets evne til å reagere på slike handlinger.

Innsidetrusselen er betydelig i flere virksomheter. Eksempelvis forsøker fremmede etterretningstjenester både å rekruttere ansatte i PST og få egnede personer til å søke bestemte stillinger.[7] Hensikten er å avdekke metoder, personell og teknologiske muligheter. Et annet eksempel er den økende bruken av skylagring og skytjenester der kommersielle interesser lagrer store datamengder. Ifølge Etterretningstjenesten vil det være et prioritert mål for trusselaktører å få tilgang til medarbeidere på innsiden av slike datasentre.[8]

De mest kraftfulle vedvarende truslene på nettet dreier seg hovedsakelig om spionasje. Målsettingen kan være å skaffe seg informasjon om slike verdier som er nevnt ovenfor. Det kan også være et mål å skade en motpart ved å påvirke, redusere eller ødelegge funksjonalitet i produksjonssystemer eller å stjele privat informasjon fra enkeltpersoner.[9]

Gjennom IKT-angrep kan trusselaktører ramme mange mål på én gang og innhente store mengder gradert og sensitiv informasjon. IKT-angrep kan i tillegg brukes til å skade eller lamme norsk kritisk infrastruktur. Slike operasjoner kan også legge til rette for sabotasje eller krigshandlinger som kan bli brukt ved eventuelle fremtidige konflikter eller krig. IKT-angrep kan ha alvorlige og omfattende skadevirkninger på hele spekteret av norske interesser.[10] Sabotasje eller terrorisme over internett kan være mulig i fremtiden, spesielt hvis terrorgrupper tilegner seg relevante teknologier. Dette anses som en potensielt alvorlig trussel.

Statlige aktører står bak den mest alvorlige trusselen i det digitale rom. Fremmede stater har i dag evne til å kunne gjennomføre IKT-angrep som eksemplifisert ovenfor. I Fokus 2016 nevner Etterretningstjenesten spesielt Russland og Kina som to av statene som driver etterretningsvirksomhet mot norske verdier. I tillegg til forsøk på å innhente informasjon kan stater også spre propaganda og desinformasjon for å legitimere egen politikk samt påvirke opinion og beslutningsprosesser.[11] Dette kan også påvirke norske interesser.

Uønskede handlinger via IKT og internett fortsetter å øke i antall og kompleksitet. NSM NorCERT[12] registrerte 20 886 saker og håndterte[13] 4327 saker individuelt i 2015, mot henholdsvis totalt 17 662 registrerte og 5066 individuelt håndterte saker i 2014. Dette innebærer en økning på over 3000 registrerte saker i 2015. Samtidig arbeidet NSM med færre alvorlige hendelser i 2015 enn i 2014. I 2015 var det 22 saker som anses som spesielt alvorlige ugraderte hendelser.

[5] Fokus 2016. Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer.

[6] SFR: Risikobildet.

[7] Politiets sikkerhetstjeneste (PST): Åpen trusselvurdering 2015.

[8] Fokus 2016. Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer.

[9] NSM halvårsrapport 2015.

[10] Politiets sikkerhetstjeneste (PST): Åpen trusselvurdering 2015.

[11] Fokus 2016. Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer.

[12] Norwegian Computer Emergency Response Team

[13] Individuell håndtering kan variere fra enkel utsjekk av noe som viser seg å være en bagatell, til full håndtering: deteksjon, varsling, koordinering, nettverksanalyse, skadevareanalyse og forensics.

Hovedårsaken til reduksjonen i antallet slike hendelser er følgende:

- Hendelsene øker i kompleksitet og omfang og krever stadig mer ressurser for å håndteres.
- I 2015 gjorde NSM NorCERT en tydeligere prioritering av sin bistand til håndtering av hendelser, med spesielt fokus på eiere av kritisk infrastruktur eller samfunnskritiske funksjoner.

Angrep som er avdekket i løpet av 2015 er større, mer avanserte og mer komplekse enn før. Derfor kan nedgangen ikke tolkes som at trusselen har blitt mindre. Tvert imot har NSM holdepunkter for å si at det er stor aktivitet fra trusselaktører. Angriperne utvikler sine teknikker raskere enn utviklingen av mottiltak. Dette er i praksis et våpenkappløp, og vi forventer at slike angrep vil øke fremover.

Det er gjennomført flere avanserte målrettede angrep mot norske offentlige virksomheter, ofte gjennom teknikker som «phishing» og «spear phishing» via e-post.

Som et eksempel kjenner NSM til at det har vært gjennomført målrettede e-post-kampanjer med avansert skadevare mot en offentlig virksomhet i Norge. Angrepet har kommet i flere bølger, og skadevaren har vært skreddersydd og endret mellom angrepsbølgene. Dette gjør det krevende å oppdage og håndtere angrepene.

NSM har også erfart denne sårbarheten gjennom inntrengingstester i en annen offentlig virksomhet. Halvparten av de som mottok e-post med vedlegg som inneholdt skadevare, åpnet denne slik at deres egen datamaskin ble infisert av skadevare. Når en trusselaktør først oppnår fotfeste i et system eller nettverk, kan veien inn til verdifull og sensitiv informasjon i mange tilfeller være kort. Avanserte trusselaktører er i stand til å infiltrere systemer og hente ut informasjon uten å bli oppdaget. NSMs inntrengningstester har til hensikt å avdekke sårbarheter i informasjonssystemer, slik at virksomhetene kan forbedre sikkerheten og motvirke IKT-angrep.

> «Angrep som er avdekket i løpet av 2015 er større, mer avanserte og mer komplekse enn før.»

Det forventes en dreining av trusselaktørenes fokus mot sektorer som alternative energikilder, jordbruk og helse. Samtidig er sektorer som forsvar, havforskning og satellittkommunikasjon fortsatt mål for etterretningsvirksomhet.

FAKTA

INNTRENGNINGSTESTER

Virksomheter som er underlagt sikkerhetsloven kan be NSM om å gjennomføre inntrengningstester av egne eller underlagte virksomheters datasystemer. NSM gjennomfører da et kontrollert dataangrep som prøver ut motstandskraften i systemene gjennom målrettede søk og analyser og forsøksvis utnyttelse av sårbarheter, feil og mangler vi finner. I ettertid lages det en rapport som dokumenterer sårbarheter og gir virksomheten råd for hvordan disse kan utbedres. Målet er å hjelpe virksomheten i det langsiktige sikkerhetsarbeidet.

Sårbarheter

Sikkerhetsstyring

NORGE ER ET AV verdens mest digitaliserte land. Samfunnets evne til å utnytte internett vil være en viktig del av den fremtidige verdiskapingen. Fordi samfunnet blir mer digitalisert og bundet sammen av datanettverk, øker avhengigheter på tvers av sektorer. Dette skaper og forsterker sårbarheter.

NSMs tilsyn med virksomheter underlagt sikkerhetsloven er én av flere viktige kilder til denne rapporten. Sikkerhetsstyring er et tema i alle tilsyn med bakgrunn i sikkerhetslovens krav til sikkerhetsadministrasjon. NSMs informasjonsgrunnlag og en studie fra FFI[14] viser at de fleste sikkerhetshendelser skyldes organisatoriske sårbarheter. Svakheter i den overordnede styringen av forebyggende sikkerhet fører til svakheter i virksomheters sikkerhetsstyring. Vi ser ofte at det ikke stilles tilstrekkelige krav og resultatmål til virksomhetene når det gjelder forebyggende sikkerhet. Svakheter i mange enkeltvirksomheter kan få nasjonale konsekvenser.

LEDERFORANKRING OG LEDERENS EVALUERING

Sikkerhetsarbeidet er ikke tilstrekkelig forankret hos ledelsen i flere av virksomhetene som er underlagt sikkerhetsloven. IKT-sikkerhet, fysisk sikring og personellsikkerhet ses ofte ikke i sammenheng av virksomhetene. Forholdet mellom disse aspektene av forebyggende sikkerhet må utgjøre en balansert helhet for at sikkerhetsarbeidet skal være vellykket.

Forebyggende sikkerhet blir ikke prioritert så lenge virksomhetsledere ikke blir målt på det, kjenner til behovet eller forstår konsekvensene av mangelfull sikkerhet. NSM ser stadig flere avvik fra bestemmelsene om at ledere skal evaluere den generelle sikkerhetstilstanden. Mange virksomheter gjør heller ikke nødvendige verdivurderinger, og uten verdivurderinger blir også risikovurderingene mangelfulle. Dette fører til at det blir vanskelig å iverksette riktige beskyttelsestiltak som virker etter hensikten.

Mange virksomheter mangler også tiltak for økt sikkerhetsmessig beredskap og har heller ikke løpende kontrollert at sikkerhetstiltak som er pålagt eller besluttet etablert, faktisk er iverksatt og fungerer etter sin hensikt. Slike mangler svekker den generelle grunnsikringen.

Ofte finner vi at sikkerhetspersonellet gjør en god jobb, men at dette har begrenset effekt på grunn av manglende oppfølging i ledelsen. Gjennom et tilsyn konstaterte NSM at en sikkerhetsleder i en virksomhet jobbet nidkjært med sikkerheten og at det meste av revisjoner, risikovurderinger, evakueringsplaner og instrukser var gjort, men at det ikke var noen andre i virksomheten som visste om denne dokumentasjonen. Sikkerhetsarbeidet hadde ingen forankring hos ledelsen, og dokumentasjonen ble dermed ikke implementert i virksomheten. I en kritisk situasjon ville denne dokumentasjonen ikke kommet til nytte slik den burde.

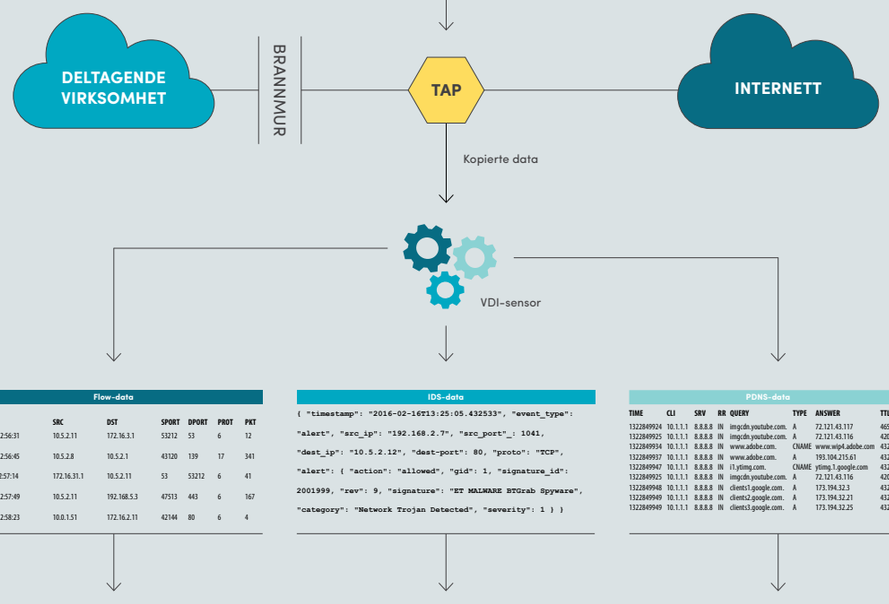
DETEKSJON OG HENDELSESHÅNDTERING

NSM mener at den nasjonale evnen til å oppdage IKT-hendelser ikke er

[14] FFI-rapport 2014/00948 Norges sikkerhetstilstand – en årsaksanalyse av mangelfull forebyggende sikkerhet.

FAKTA

VARSLINGSSYSTEM FOR DIGITAL INFRASTRUKTUR



NETWORK FLOW DATA

En sekvens av IP-pakker fra en kilde til en distinasjon som er del av samme sesjon. Slik sesjonsdata er nyttig da det gir et overordnet blikk på trafikk-flyten for eksempel i forbindelse med en konkret hendelse.

IDS-DATA

En alarm fra et system for deteksjon av inntrengning (IDS). En alarm genereres når et gitt mønster/signatur oppdages. Slike signaturer er ofte konkrete spor på skadevare og kompromitteringer.

PDNS-DATA

Passiv-DNS-data består av spørsmål og svar i DNS-protokollen. Det er verdifullt å ta vare på denne historikken da skadevare ofte og raskt bytter adresser og domener.

tilstrekkelig utviklet. Dagens Varslings-system for digital infrastruktur (VDI) har ikke god nok sensordekning, og vi har dermed ikke en komplett oversikt over digitale angrep mot norske mål. Dette gjør at IKT-angrep ikke blir oppdaget raskt og at effektive mottiltak kommer for sent. VDI-systemet må også videreutvikles og tilpasses den teknologiske utviklingen.

Den nasjonale evnen til håndtering av IKT-hendelser har blitt styrket de senere år, men er fortsatt ikke robust nok til å møte fremtidens utfordringer. De fleste virksomheter er dessuten ikke i stand til å håndtere avanserte vedvarende angrep fra ressurssterke trusselaktører. Dette gjør at den samlede håndteringsevnen er sårbar. Samtidig ser vi at kompleksiteten i skadevaren som brukes av trussel-aktørene har økt betydelig og krever stadig mer ressurser for å håndteres.

KOMPETANSE

Det er tydelig gjennom tilsyn og annen virksomhet at det er betydelige svakheter innen sikkerhetsbevissthet og sikkerhets-kompetanse.

Årlig tas rundt 1500 studenter opp i ulike IKT-utdanninger på universiteter og høgskoler i Norge. På flere universiteter er ikke IKT-sikkerhet et obligatorisk fag som ledd i IKT-utdanningen. Det utdannes for få personer med relevant kompetanse innen forebyggende IKT-sikkerhet. Dette hemmer evnen til å gjennomføre gode IKT-sikkerhetstiltak. Det vil også hemme evnen til å forbedre risikobevissthet hos brukere av IKT-systemer.

Det utdannes heller ikke nok spesialister på skadevareanalyse og angrepsanalyse innen hendelseshåndtering på IKT-området. Som følge av dette er det stor konkurranse om de som er tilgjengelig.

Innenfor objektsikkerhet ser vi at objekteiere ofte mangler kompetent personell til å planlegge fysisk sikring og sikre at sensitiv informasjon om objektet ikke kommer på avveie.

Vi ser også at virksomheter unnlater å rapportere alvorlige sikkerhetshendelser. I tillegg til de direkte sikkerhetsmessige konsekvensene dette har, forhindrer mangelfull registrering og rapportering oss fra å lære av feilene vi gjør.

ANDRE SIKKERHETSMESSIGE UTFORDRINGER

SIKKERHETSKLARERINGER OG INNSIDETRUSLER

Sikkerhetsklarering av personell er en sentral del av det forebyggende sikkerhetsarbeidet, og vi er nødt til å ha trygghet for at de som blir klarert er til å stole på.

Virksomheter og skjermingsverdige objekter er sårbare overfor innsidetrusler. PST vurderer at samarbeid med personer på innsiden er en effektiv etterretnings-metode som kan ha stort skadepotensial for Norge.[15] NSM anser at tilknytning til andre stater kan være en sårbarhet ved personer som sikkerhetsklareres.

Anmodninger om klarering av personer med tilknytning til andre land er økende. Det er en grunnleggende forutsetning for klarering at det er mulig å innhente bakgrunnsinformasjon om både de som skal klareres og deres nærstående. Sikker identifisering av personell er viktig i hele personellsikkerhetskjeden.

[15] Politiets sikkerhets-tjeneste (PST): Åpen trusselvurdering 2016.

E-POST OG PRIVAT IKT-UTSTYR

Den enkleste måten å bryte seg inn i virksomheters informasjonssystemer på er gjennom e-post eller fysisk innbrudd. Felles for avdekkede angrep på IKT-systemer det siste året er at e-post har vært veien inn og at dette er altfor enkelt. «Spear phishing» (målrettet e-post) er brukt i alvorlige angrep.

Det er også økende press fra ansatte om å få lov til å bruke personlig IKT-utstyr som mobiltelefon og nettbrett i virksomhetens datasystemer og på innsiden av virksomhetens brannmurer. I den digitale hverdagen er dette oppfattet som praktisk. Åpner virksomheten opp for dette, åpnes det samtidig opp for svakere sikkerhet og kontroll i virksomhetens IKT-systemer. Dette er ofte ikke brukerne oppmerksomme på. Bruk av virksomhetsintern e-post på enheter utenfor arbeidsgivers kontroll er et eksempel på handlinger som kan utsette virksomhetens informasjon for risiko.

AVLYTTING OG KRYPTERING

Kommunikasjon og data lar seg avlytte eller avlese med relativt enkle midler. Samtaler kan avlyttes, mobiltelefonen kan aktiveres til romavlytting og kamera kan aktiveres. Bilder, avtaler, kontaktlister, meldinger, e-post, websurfing og posisjonsdata kan avleses uten at brukeren vil fatte mistanke. Økt konkurranse har medført at prisene på verktøyene som benyttes til avlytting har falt, samtidig som produktene har blitt mer kommersielt tilgjengelige. Med økt utbredelse øker også sannsynligheten for at verktøyene benyttes i større omfang.

Kryptoløsninger for sensitiv informasjon vil sterkt bidra til å redusere risiko for at informasjon utilsiktet skal komme på avveie. Slike løsninger kan være basert på åpne standarder og sertifiserte, kommersielt tilgjengelige produkter.

SIKKERHET I FORVALTNINGEN AV INFORMASJONSSYSTEMER

Utilstrekkelig styring av tilgang i IKT-systemer er en grunnleggende utfordring. Dette er virksomhetenes ansvar, og det kan ikke forventes at de enkelte brukerne har kompetanse til å ivareta dette. Virksomhetens systemer utsettes da for betydelig risiko som brukerne ikke er oppmerksomme på.

For lite fokus på at det kan finnes feil, svakheter og konstruksjonsavvik i maskinvare leder til mange ulike sårbarheter. For graderte systemer er det etablert en godkjent produktliste (GPL), der leverandører må kvalifisere sine produkter i henhold til gitte krav. For ugraderte systemer er dette ikke etablert på tilsvarende måte. Dette øker risikoen for at det anskaffes produkter med svakere sikkerhet. For å bøte på dette kan åpne standarder og oversikter over sertifiserte, kommersielt tilgjengelige produkter være relevante for dette formålet.

NSM vurderer at det finnes store tekniske sårbarheter knyttet til digitale prosesskontrollsystemer i kritisk infrastruktur. Slike systemer er ofte komplekse og gamle og i mange tilfeller koblet mot internett, noe de i utgangspunktet ikke var konstruert for.

Et nylig eksempel er hendelsen i Ukraina i desember 2015, der et hackerangrep stoppet strømforsyningen til over 200 000 mennesker. Angriperen brukte «spear phishing» for å oppnå tilgang til tre kraftselskapers prosesskontrollsystemer og slo deretter ut et antall transformatorstasjoner, slik at strømmen forsvant. Selv etter at kraftselskapene fikk kontroll over systemene sine igjen, klarte de ikke å fjernstyre transformatorstasjonene, ettersom angriperen hadde isolert dem fra prosesskontrollsystemene. Stasjonene måtte derfor manuelt gjenopprettes før kundene kunne få tilbake strømmen.[16] [17]

INFORMASJONSSYSTEMER I OFFENTLIG SEKTOR – SPESIALBEHOVENE FÅR STYRE

Offentlige virksomheter i Norge har svært ulike IKT-løsninger. Utvikling, forvaltning og drift av IKT-løsninger for det offentlige er spredt på forskjellige aktører. Løsningene er bygd opp ulikt og har ulik grad av sikkerhet. Dette skaper utfordringer og sårbarheter og kan øke sannsynligheten for sikkerhetsbrudd og lite effektiv ressursbruk. Mange kompetansemiljøer er for små og for lite robuste til å kunne håndtere dette.

Informasjonssystemer utvikles ikke alltid etter en helhetlig og langsiktig plan. Til tross for store fellestrekk mellom kravene til IKT innen kontorstøtte og elektronisk kommunikasjon i offentlig sektor er det ofte spesialbehovene til den enkelte virksomheten som blir styrende for hele løsningen når nye systemer anskaffes. Hver enkelt virksomhet lager kravspesifikasjoner relativt uavhengig av hverandre, også for det som burde være

[16] Ifølge amerikanske Department of Homeland Security (https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01)

[17] Fokus 2016. Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer.

standardfunksjoner. Det er opp til den enkelte virksomhet å anskaffe, forvalte og drifte alle elementer i sine egne IKT-løsninger på en sikker måte. Dette har ført til unødvendig oppsplitting av både tekniske løsninger og kompetansemiljøer, noe som øker den samlede risikoen for svikt i IKT-sikkerheten.

OBJEKTSIKKERHET

Under tilsyn finner vi mange svakheter innenfor sikkerhetslovens regime for objektsikkerhet. Et gjennomgående trekk er at skadevurderinger som skal ligge til grunn for utvelgelse og klassifisering av objektene er fraværende. Det er også ofte manglende beskrivelse av hvilken betydning eget objekt kan ha for andre objekter samt avhengighet av blant annet elektrisitet og elektroniske kommunikasjonstjenester. Det mangler også ofte avtaler som beskriver forpliktelser utover normalsituasjonen, for eksempel leveranser av drivstoff, service- og reparasjonspersonell og reservedeler.

Frist for førstegangs innmelding av skjermingsverdige objekter til NSM var 31. desember 2012, og oversikten revideres nå kontinuerlig ettersom det gjøres endringer i infrastruktur. Departementene får ny erfaring med regelverket, og tidligere skadevurderinger revideres og endres. NSM sitter i dag med en god oversikt over spesielt skjermingsverdige objekter innenfor Forsvaret, justissektoren, elektronisk kommunikasjon, samferdsel, departementsfellesskapet og offentlig forvaltning. Innen kraft- og petroleums-sektorene er det ikke klassifisert noen objekter etter sikkerhetsloven.

FYSISK SIKRING

Riksrevisjonen har pekt på at objekt-sikkerhetsforskriftens krav om permanent grunnsikring av departementsbygningene fortsatt ikke var oppfylt i 2014 og anså dette som alvorlig. Andre sikkerhets-oppgraderinger var sterkt forsinket eller satt på vent.[18] [19]

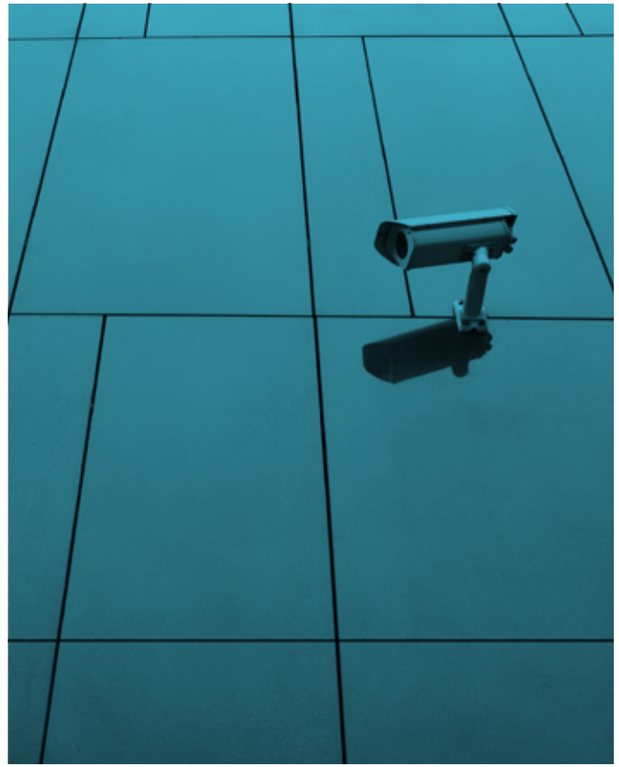
Selv om det er gjennomført mange forebyggende sikkerhetstiltak mot terrorhandlinger ved skjermingsverdige objekter, må det regnes med at et terrorangrep vil medføre store materielle skader og tap av menneskeliv. Selv relativt ressurssvake trusselaktører vil fysisk kunne skade de fleste skjermingsverdige objekter i sivil sektor.

NSM har undersøkt sikkerheten i adgangssystemer og funnet at enkelte typer adgangskort kan kopieres i løpet av svært kort tid og ved hjelp av enkle virkemidler. Kopier av reelle adgangskort kan gi uautorisert tilgang der disse adgangskortene anvendes. Et eksempel på uheldig eksponering er bilder av adgangskort som legges ut på internett. Med enkle midler kan trusselaktører kopiere slike adgangskort.

UTKONTRAKTERING OG EIERSKAP TIL SIKKERHET

Utenlandske investeringer i kritiske samfunnsfunksjoner eller kritisk infrastruktur kan medføre økt usikkerhet og potensiell risiko for spionasje. Internasjonale investorer kjennetegnes ofte av komplekse eierstrukturer som er mindre transparente. Eierskap, drift og leveranser til kritisk infrastruktur blir stadig mer oppstykket. I tillegg vil objekteiers leverandører ofte ha under-leverandører. Dette gir en leveransekjede og verdikjede til kritisk infrastruktur og skjermingsverdige objekter som det er vanskelig å holde oversikt over. I mange tilfeller er fysisk drift og systemdrift av IKT-infrastruktur splittet opp på ulike virksomheter. Uklar ansvarsdeling og svakt eierskap til sikkerhetsarbeidet kan resultere i sårbarheter.

De siste årene har fremmede etterretningstjenester vist interesse for å utnytte konsulentselskaper. I dag kan norske konsulentselskaper holde sine kundelister hemmelige og dermed potensielt skjule andre staters interesser. [20]



[18] Riksrevisjonen.no: En rekke etater har alvorlige svakheter ved sikkerheten i informasjons-systemer. Publisert 21.10.2015.

[19] I et brev av 15.08.2015 fra Kommunal- og moderniserings-departementet til Riksrevisjonen vises det til at samtlige departementer nå har funksjonelle lokaler med et grunnsikrings-nivå i tråd med sikkerhetslovens forskrift om objektsikring. Departementet opplyser at de foreløpige sperre-tiltakene utenfor og rundt lokalene skal erstattes med permanente sperretiltak. Ifølge departementet var dette under oppstart og det tas sikte på at det alt vesentlige av utskiftningen skal være ferdig senest ved utgangen av 2016. Brevet er gjengitt i Riksrevisjonens rapport om den årlige revisjon og kontroll for budsjettåret 2014 (s. 131–132).

[20] PSTs åpne trussel-vurdering 2015.

Risikovurdering

NSMS OVERORDNEDE VURDERING er at samfunnets sikkerhetsmessige sårbarheter fremdeles er betydelige. Svakheter i den overordnede styringen av forebyggende sikkerhet medfører sårbarheter som svak lederforankring og sikkerhetsstyring i virksomhetene. Manglende verdivurderinger, risikovurderinger og risikoforståelse gjør at det ikke tas tilstrekkelig informerte valg om aksept av risiko eller tiltak for å redusere sårbarheter. NSM vurderer at disse svakhetene fremdeles bidrar til å påføre Norge stor risiko for digital og annen spionasje mot verdier av nasjonal betydning i 2016.

Årsaken til at denne trenden er relativt uendret, er at utviklingen av sårbarhetsreduserende tiltak ikke følger trusselutviklingen på en slik måte at gapet reduseres. Så lenge ledere ikke blir målt på forebyggende sikkerhet, ikke kjenner behovet eller ikke forstår konsekvensene av mangelfull sikkerhet, så blir ikke dette arbeidet prioritert. Sikkerhetsstyringen i virksomheter det er ført tilsyn med, har ofte svakheter. Virksomhetene risikerer å utsette samarbeidende virksomheter for risiko gjennom potensiell overføring av digital skadevare.

Det er stor risiko forbundet med at den samlede nasjonale evnen til å oppdage og håndtere IKT-hendelser ikke er tilstrekkelig videreutviklet. Det samme gjelder virksomhetenes egenevne til å håndtere hendelser. Det er nylig etablert flere responsmiljøer i sektorene, men disse må utvikles videre for å få effekt.

Utilstrekkelig fokus på sikkerhet i IKT-utdanningen utgjør en betydelig risiko for samfunnet. NSM vurderer at det utdannes for få personer med spesialistkompetanse på skadevareanalyse og angrepsanalyse innen håndtering av IKT-hendelser. Dette har fått og vil få konsekvenser for IKT-sikkerhetsarbeidet både nasjonalt og i virksomhetene og gjør at norske verdier er unødvendig sårbare for digitale angrep.

Innsidetrusler utgjør en sårbarhet for virksomheter og skjermingsverdige objekter. En innsider betyr at forebyggende sikkerhetsarbeid innenfor organisatoriske og teknologiske rammer vil miste store deler av sin hensikt. Innsidere kan gjennom sin posisjon i det stille undergrave eksternt rettede sikkerhetstiltak og kan dermed forårsake store skader.

Det kan være betydelig risiko knyttet til sikkerhetsklarering av personer med tilknytning til fremmede stater. Sikkerhetsklarerte personer med slik tilknytning kan medføre økt risiko for å bli utsatt for press, fristelse og/eller forledelse fra trusselaktører som kan utnytte sårbarheter ved tilknytningen.

ID basert på usikkert grunnlag kan medføre risiko for infiltrasjon fra personer og organisasjoner som kan utgjøre en sikkerhetstrussel.

«Utviklingen av sårbarhetsreduserende tiltak følger ikke trusselutviklingen på en slik måte at gapet reduseres.»

Avslutning

«Sikkerheten kan aldri bli bedre enn det svakeste ledd.»

VI MÅ FOKUSERE PÅ det vi kan gjøre noe med, og det er å redusere egne sårbarheter. For å klare dette må vi få til bedre overordnet styring av sikkerhetsarbeidet på alle nivåer. Det innebærer å sette mål og følge opp gjennom aktiv styring og rapportering. Sikkerhetsarbeidet må forankres i ledelsen i både privat og offentlig sektor. Først da kan sikkerheten styres.

For å redusere sikkerhetsmessig risiko i samfunnet er det behov for en omfattende nasjonal satsning på forebyggende sikkerhet i årene som kommer. Dette bør gjøres innen områdene informasjons- og IKT-sikkerhet spesielt, men også innenfor personellsikkerhet og fysisk sikring. Utviklingen av sikkerhetsmessig robusthet og motstandskraft bør komme i takt med trusselutviklingen. I Sikkerhetsfaglig råd (SFR) har NSM derfor foreslått en rekke tiltak. Sikkerhetsfaglig råd er for tiden til behandling i Forsvarsdepartementet og Justis- og beredskapsdepartementet som et ledd i arbeidet med den neste langtidsplanen for forsvarssektoren og den nye samfunnssikkerhetsmeldingen i justissektoren.

Det er virksomhetene selv som har ansvaret for egen sikkerhet. Sikkerheten kan aldri bli bedre enn det svakeste ledd. Det betyr at sikkerhet angår oss alle.

NASJONAL SIKKERHETSMYNDIGHET

Postboks 814, 1306 Sandvika

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