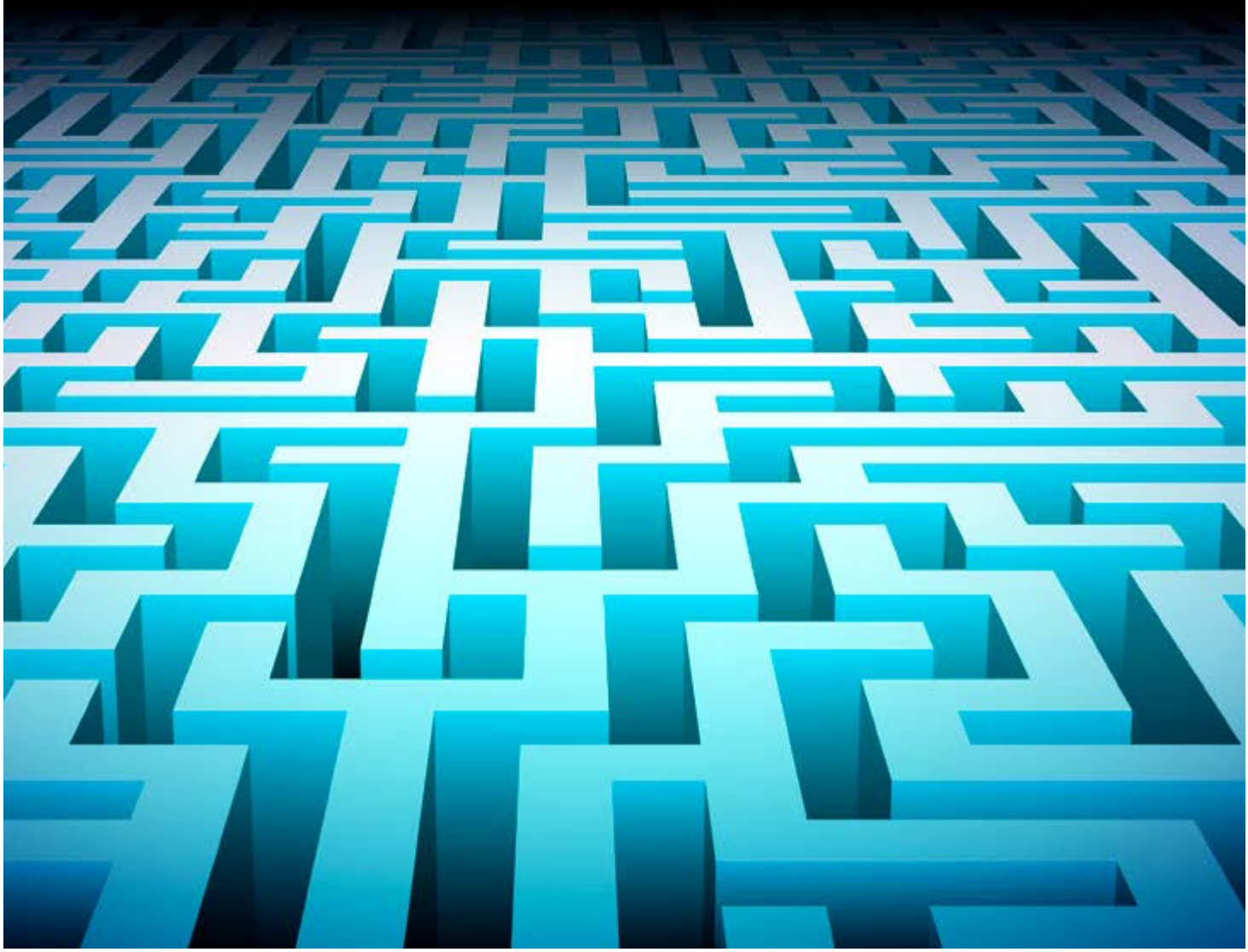
NSM

Helhetlig IKT-risikobilde 2016



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

1.

Sammendrag

Helhetlig IKT-risikobilde er en årlig rapport som har til hensikt å øke bevisstheten om IKT-sikkerhet. Den offentliggjøres i forbindelse med den årlige sikkerhetsmåneden i oktober. Rapporten er vinklet mot virksomheter, men er også relevant for samfunnet som helhet.

Rapportens første del beskriver utfordringer for IKT-sikkerhet. Norge er et av verdens mest digitaliserte land, og vi er også et av de landene som er flinkest til å sikre IKT-systemer.

Både virksomhetene og samfunnet eier og forvalter store verdier i form av informasjon på IKT-systemer. Verdivurdering vil gi den enkelte virksomhet oversikt over hvilke verdier som er viktigst å sikre. Lange digitale verdikjeder gjør at virksomhetens verdier også kan ha betydning for andre virksomheter eller individer, eller for samfunns- og statssikkerheten.

IKT-risikobildet er ulikt for forskjellige samfunnsaktører og ut fra forskjellig ståsted. For statens sikkerhet utgjør etterretningsvirksomhet fra fremmede stater den høyeste IKT-risikoen. Nettverksoperasjoner og digital spionasje fra fremmede stater utgjør også den høyeste IKT-risikoen for virksomheter som forvalter kritisk infrastruktur, kritiske samfunnsfunksjoner eller høyteknologi. De mest attraktive målene blir overvåket døgnet rundt gjennom avanserte vedvarende trusler, slik at den minste sårbarhet kan utnyttes i det den oppstår.

For enkeltvirksomheter utgjør digital kriminalitet den største IKT-risikoen. Mange virksomheter er utsatt for løsepengevirus, direktørsvindel og lignende fenomener. Det er vanlig at det digitale angrepet foretas gjennom målrettede e-poster med infiserte vedlegg.

Rapporten beskriver også farer og utilsiktede hendelser som kan ramme norske virksomheters verdier. Denne delen er et innspill fra Direktoratet for samfunnssikkerhet og beredskap (DSB).

I rapportens andre del gir NSM to overordnede anbefalinger for IKT-sikkerhetsarbeidet i virksomhetene. Den første anbefalingen er at sikkerhet bør være en del av virksomhetens langsiktige strategi. Mangel på styring gjør ofte sikkerhetsarbeidet fragmentert og ufullstendig, noe som kan føre til at sikringstiltakene ikke settes inn der risikoen er størst.

Den andre anbefalingen er at virksomheter bør innføre IKT-grunnsikring for å redusere et bredt spekter av sårbarheter. En slik IKT-grunnsikring bør baseres på en helhetlig og langsiktig forvaltning av IKT-systemer. For å oppnå sikre systemer må selve IKT-plattformen være robust. Det må være gode rutiner for vedlikehold og drift, og det må være gode rutiner for å håndtere uønskede hendelser og gjenopprette funksjoner.

Helhetlig IKT-risikobilde er et resultat av NSMs egen informasjon og innspill fra andre offentlige og private virksomheter og samarbeidspartnere. Vi ønsker spesielt å takke Etterretningstjenesten, Politiets sikkerhetstjeneste (PST), Direktoratet for samfunnssikkerhet og beredskap (DSB), Direktoratet for forvaltning og IKT (Difi), Norges vassdrags- og energidirektorat (NVE), Nasjonal kommunikasjonsmyndighet (Nkom), Finanstilsynet, Riksrevisjonen, KraftCERT og Statistisk sentralbyrå (SSB) for innspill og godt samarbeid.

2.

Innledning

2.1 HENSIKTEN MED RAPPORTEN

Helhetlig IKT-risikobilde 2016 er laget av NSM etter oppdrag fra Justis- og beredskapsdepartementet (JD) og Forsvarsdepartementet (FD). Formålet med rapporten er å øke bevisstheten om IKT-sikkerhet i offentlige og private virksomheter for å kunne redusere samfunnets digitale sårbarhet.

Første del av rapporten beskriver *hva* virksomhetene bør beskytte sine verdier mot – det vil si hvilke trusler vi ser og hvilke sårbarheter som utnyttes. En enkelt virksomhets sikkerhet kan ha stor betydning for samfunnet og for den enkelte, men også for statens sikkerhet.

Andre del av rapporten beskriver *hvordan* virksomhetene bør beskytte sine verdier. For å møte et komplekst og omfattende trussel- og sårbarhetsbilde kreves en helhetlig og systematisk tilnærming til sikkerhetsarbeidet.

I arbeidet med rapporten har NSM samarbeidet med en rekke offentlige og private virksomheter. Resultatet er et oppdatert bilde over sårbarheter, trusler og tiltak tilknyttet den teknologiske utviklingen. Fjorårets rapport ga en omfattende oversikt over fenomener og temaer knyttet til IKT-risikobildet og er et referansegrunnlag for denne rapporten. Årets rapport omtaler et utvalg av de mest relevante temaene.

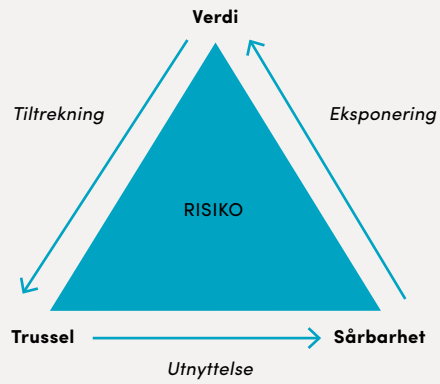
2.2 MÅLGRUPPE

Rapporten er primært vinklet mot ledere i offentlige og private virksomheter i alle sektorer. Begrepet *helhetlig* er i samråd med oppdragsgiver tolket slik at rapporten skal ha relevans i et spenn fra virksomhet til samfunn og omhandle både uhellshendelser og bevisste uønskede handlinger.

2.3 METODEGRUNNLAG

NSMs vurdering av IKT-risiko forholder seg til strukturen i NS 5832:2014[1] og til begrepsbruken i NS 5830:2012.[2] Disse utgjør et overordnet rammeverk og ikke en ferdig utviklet metode. NSM har utgitt en håndbok i risikovurdering for sikring. Denne håndboken er basert på NS 5832 og er laget for å hjelpe virksomhetene til å bruke risikovurdering som en del av sin sikkerhetsstyring.[3] De grunnleggende sammenhengene mellom verdier, trusler og sårbarheter er illustrert i modellen nedenfor. I et IKT-perspektiv skal sikringstiltak beskytte informasjonens konfidensialitet, integritet og tilgjengelighet.[4]

FIGUR 1: RISIKOTREKANTEN



2.4 BAKGRUNN

Norge er samlet sett et av verdens mest digitaliserte land, på fjerde plass av 139 land i 2016, mot en femteplass i 2015.[5] Mer enn 96 prosent av befolkningen er online. Vi er på 18. plass i bruk av IKT i offentlig forvaltning, seks plasser opp siden i fjor. Våre nærmeste naboer Finland og Sverige ligger på andre og tredje plass, og andre

[1] Norsk Standard NS 5832:2014 Samfunnssikkerhet - Beskyttelse mot tilsiktede uønskede handlinger. Krav til sikringsrisikoanalyse. Standardene i denne serien er ikke spesifikt rettet mot IKT-risiko, men mot sikringsrisiko allment.

[2] Norsk Standard NS 5830:2012 Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger. Terminologi.

[3] NSM: *Håndbok i risikovurdering for sikring*, mars 2016.

[4] Konfidensialitet vil si at informasjonen ikke skal være tilgjengelig for uautorisert personell eller lagres i ikke-godkjente systemer. Med integritet menes trygghet for at informasjonen forblir fullstendig, riktig og gyldig både i systemet og under forsendelse. Med tilgjengelighet forstås at informasjonen er tilgjengelig for de som skal bruke den.

[5] World Economic Forum/ Cornell University/INSEAD (eds.): *The Global Information Technology Report 2015*.

World Economic Forum/ Cornell University/INSEAD (eds.): *The Global Information Technology Report 2016*.

land i vår nærhet scorer også høyt.

93 prosent av norske foretak med minst ti ansatte og 99 prosent med minst 100 ansatte hadde internettilknytning[6] i 2015.[7] I 2014 hadde 66 prosent av norske private foretak utført elektronisk handel, opp hele ti prosentpoeng fra året før.[8]

Norge kommer godt ut sammenliknet med andre land når det gjelder å holde internett «rent». Vi kjøper nye datamaskiner med stadig bedre sikkerhetsløsninger og bruker oppdaterte operativsystemer. Rundt elleve prosent av datamaskinene i Norge var infisert av skadevare i fjerde kvartal 2015, sammenlignet med syv prosent året før. Verdensgjennomsnittet var 21 prosent, mot 16 prosent året før.[9] Andelen infiserte datamaskiner har økt betydelig på kort tid, både i Norge og på verdensbasis.

I rapporten kommer vi flere steder tilbake til sikkerhetsmessig risiko og risikohåndtering ved bruk av skytjenester. I 2014 kjøpte 29 prosent av norske private foretak en eller flere skytjenester; dette økte til 38 prosent året etter.[10] 43 prosent av statlige virksomheter brukte i 2014 en eller flere slike tjenester.[11] I 2015 var antallet økt til 53 prosent.

Skytjenester

Skytjenester er skalerbare tjenester som blir levert over nett. Regjeringen har i Nasjonal strategi for bruk av skytjenester valgt å benytte den amerikanske standardiseringsorganisasjonen NIST (National Institute of Standards and Technology) sin definisjon av skytjenester: «Skytjenester (cloud computing) er leveransemodeller som muliggjør nettverksbasert tilgang til et sett konfigurerbare dataressurser (herunder nettverk, servere, lagring, applikasjoner og andre tjenester) som er tilgjengelig over alt, blir levert og prises etter behov (on demand), skalerer dynamisk etter kapasitetsbehov, og som raskt kan avsettes og klargjøres med minimal administrasjon eller involvering fra tilbyderen.»

Spekteret av skybaserte tjenester er under hurtig utvikling. Det er vanlig å skille mellom tre hovedkategorier av tjenestemodeller. Hver kategori henviser til ulike nivå av tjenester virksomheten har bruk for.

- Hvis tjenestenivået er programvare eller applikasjon kalles dette gjerne for **«programvare som en tjeneste»** (Software as a Service – SaaS). Sluttbruker trenger da ikke å beskjeftige seg med å installere, konfigurere, oppdatere og vedlikeholde programvaren lokalt. I stedet kjører sluttbruker programvaren gjennom sin nettleser eller en annen type nettbasert klient. Tekstbehandler, regneark, regnskap og lønn, CRM og ERP er noen eksempler på programvare som kan tilbys som SaaS.
- Det neste tjenestenivået omtales som **«plattform som tjeneste»** (Platform as a Service – PaaS) og gir kunden mulighet til å installere og konfigurere programvare/applikasjon hos skyleverandøren. Sluttbruker gis da en plattform hvor de kan installere, konfigurere og vedlikeholde sine tjenester. Sluttbruker trenger ikke å beskjeftige seg med drift og vedlikehold av servere og nettverk.
- Det tredje tjenestenivået kalles **«infrastruktur som tjeneste»** (Infrastructure as a Service – IaaS) og gir sluttbruker tilgang til grunnleggende ressurser som lagring, nettverk og prosessortid hvor kunden kan installere, konfigurere og ha kontroll på operativsystem, lagring og annen installert programvare. Dette gir kunden tilgang til de dataressurser man normalt vil ha i sitt eget datasenter: nettverk, servere og lagring.

Andre tjenestemodeller eksisterer, men er gjerne en kombinasjon eller variant av de tre nevnt over.

[6] Gjelder alle typer bredbånd.

[7] Statistisk sentralbyrå (SSB), Statistikkbanken: Bruk av IKT i næringslivet, Tabell 10970: Private føretak. Internettilknytning etter beste teknologi, etter mengd sysselsette (prosent).

[8] SSB, Statistikkbanken: Bruk av IKT i næringslivet, Tabell 10974: Private føretak. Elektronisk handel, etter mengd sysselsette (prosent).

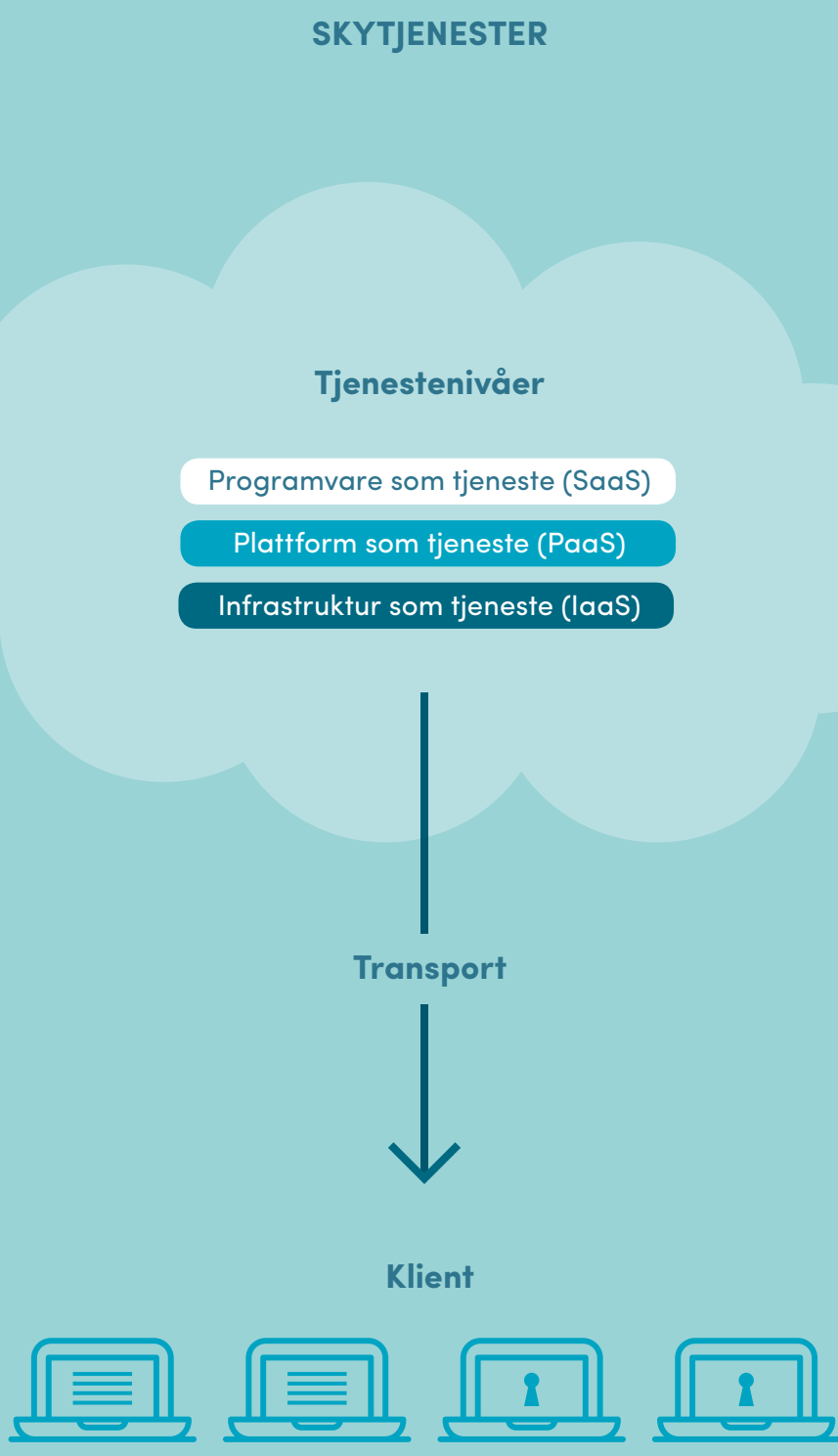
[9] Microsoft Security Intelligence Report Volume 18, *Regional Threat Assessment*, 2014, s. 618, og Volume 20 (*Norway*) 2015

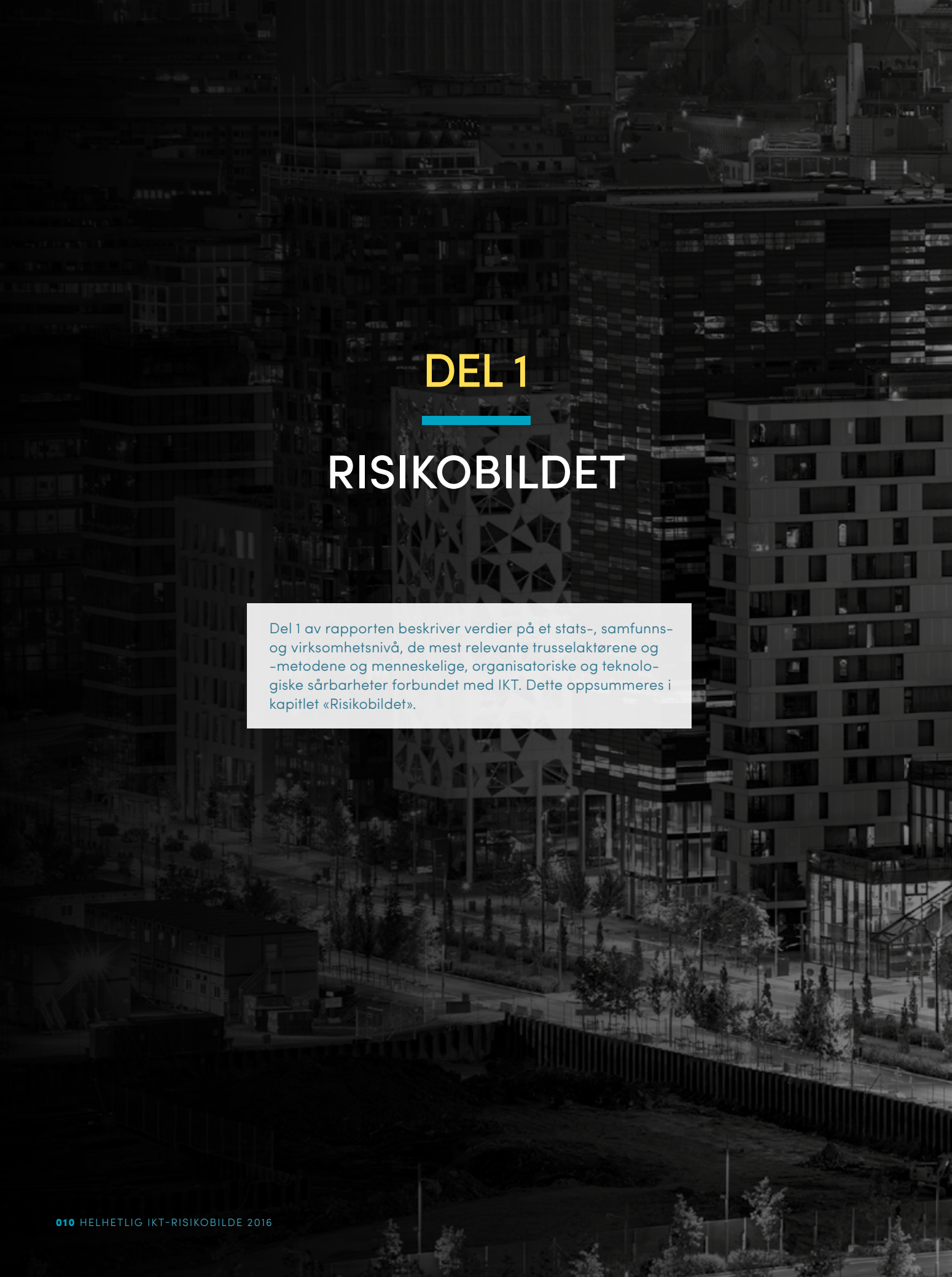
[10] SSB, Statistikkbanken: Bruk av IKT i næringslivet, Tabell 10641: Private føretak. Kjøper nettskytenester, etter teneste og mengd sysselsette (prosent). (oppdatert 2015)

[11] SSB, Statistikkbanken: Bruk av IKT i staten, Tabell 10609: Statlige virksomheter. Bruk av nettskytjenester, etter type og sysselsettingsgruppe (prosent).

[12] https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-bruk-av-skytenester/id2484403/

[13] National Institute of Standards and Technology: «The NIST Definition of Cloud Computing», NIST Special Publication 800-145, 2011.


SKYTJENESTER
Tjenestenivåer
Programvare som tjeneste (SaaS)
Plattform som tjeneste (PaaS)
Infrastruktur som tjeneste (IaaS)
Transport
Klient



DEL 1

RISIKOBILDET

Del 1 av rapporten beskriver verdier på et stats-, samfunns- og virksomhetsnivå, de mest relevante trusselaktørene og -metodene og menneskelige, organisatoriske og teknologiske sårbarheter forbundet med IKT. Dette oppsummeres i kapitlet «Risikobildet».

3

Verdier og interesser

Sikkerhet handler om å beskytte verdier. I risikometodikken som er beskrevet i metodegrunnlaget, er verdivurdering en viktig del. Forebyggende sikkerhetsarbeid begynner med å kartlegge hvilke verdier som er viktigst for det virksomheten leverer og dermed viktigst å beskytte. Verdiene er ressursene virksomheten er avhengig av i sine verdiskapende prosesser.[14]

Dagens digitaliserte samfunn og globaliserte verden er preget av det Lysneutvalget omtaler som «lange og uoversiktlige digitale verdikjeder, som gjerne spenner over mange sektorer og flere land».[15] Uønskede hendelser som rammer en virksomhets verdier kan ha konsekvenser for andre virksomheter eller individer, eller for samfunns- eller statssikkerheten. Slike avhengigheter må kartlegges når en virksomhet vurderer sine verdier.

I denne rapporten ser vi på verdier som har betydning for tre nivåer:

- staten
- samfunnet og dets funksjoner
- den enkelte virksomheten

3.1 VERDIER I STAT OG SAMFUNN

I et stats- og samfunnsperspektiv er det definert et sett med overordnede verdier, kalt kritiske samfunnsfunksjoner og innsatsfaktorer.[16] Kritiske samfunnsfunksjoner omfatter blant annet å:

- ivareta nasjonal sikkerhet
- ivareta styring og kriseledelse
- opprettholde en demokratisk rettsstat
- opprettholde trygghet for liv og helse
- opprettholde lov og orden
- opprettholde finansiell stabilitet
- opprettholde grunnleggende sikkerhet for lagret informasjon

For å opprettholde kritiske samfunnsfunksjoner er man avhengig av såkalte innsatsfaktorer, blant annet:

- ekom-tjenester
- kraftforsyning
- vannforsyning
- vare- og persontransport

Slike innsatsfaktorer er verdier som forvaltes av virksomheter på vegne av samfunnet.

3.2 VERDIER I VIRKSOMHETENE

Under følger noen eksempler på virksomhetens verdier[17] som enten kan være digitale, tilgjengelige gjennom digital plattform eller påvirkes av IKT-hendelser:

- informasjon, eksempelvis virksomhetskritisk informasjon, som patenter, anbud, produksjonsplanlegging, budsjetter og produksjonsbeskrivelser
- digital infrastruktur, som nettverk og servere
- programvare, for eksempel industrielle kontrollsystemer (SCADA-systemer)[18] som styrer produksjon
- økonomiske verdier
- personell og personopplysninger
- organisasjonsstrukturer
- aktiva, som produksjonsutstyr

Gjennom en verdivurdering vil virksomheten selv vurdere hvilke konsekvenser det kan få dersom verdiene skulle rammes av en uønsket hendelse.

[14] Se NSMs *Håndbok i risikovurdering for sikring*, 2016 og *Veiledning i verdivurdering*, 2009.

[15] NOU 2015:13 *Digital sårbarhet – sikkert samfunn*, s.15.

[16] Direktoratet for samfunnssikkerhet og beredskap (DSB): *Sikkerhet i kritisk infrastruktur og kritiske samfunnsfunksjoner – modell for overordnet risikostyring*, KIKS-prosjektet – 1. delrapport 2012.

[17] NSMs *Håndbok i risikovurdering for sikring*, 2016 og *Veiledning i verdivurdering*, 2009.

[18] De IKT-baserte kontrollsystemene som styrer kraftforsyningen og elektronisk kommunikasjon, blant annet telefoni, internett, kringkasting og satellittkommunikasjon, er blant landets viktigste.

Verdivurderinger ved bruk av skytjenester

Skytjenester kan gi bedre sikkerhet fordi sikkerhetsfunksjonene og tiltakene profesjonaliseres i større grad enn hva informasjonseier selv kan være i stand til å levere. For en del virksomheter med svak sikkerhetsstyring og mangelfulle ressurser til sikkerhetsarbeidet kan bruk av skytjenester være med på å heve grunnsikringen. Men bruk av skytjenester fritar ikke en virksomhet fra sikkerhetsarbeidet.

En anskaffelse skal møte virksomhetens behov. Dette krever bestiller- og sikkerhetskompetanse. Utilstrekkelig kompetanse kan medføre at enkelte virksomheter anskaffer skytjenester uten tilstrekkelig kartlegging av behov og uten å ha gjennomført de viktige vurderinger som skal gjøres i forkant av en anskaffelse. Dette er en risikofaktor i et helhetlig IKT-risikobilde.[19]

Ved anskaffelse av skytjenester bør virksomheten vurdere følgende momenter:

- Skal all informasjon i virksomheten lagres i nettskyen, eller finnes det informasjon som er av en slik betydning eller verdi at den trenger høyere beskyttelse enn hva en skyleverandør har mulighet til å levere?
- Hvor og hvordan lagres informasjonen hos skyleverandøren? En skyleverandør har som regel flere datasentre. Hvor er disse lokalisert? Hva er den fysiske sikringen til disse? Hvem har fysisk og logisk tilgang?
- Hvordan blir informasjonen sikret under transportetappen mellom skyleverandøren og kunden?
- Kan skyleverandøren levere etter bransjespesifikke krav? Dette gjelder spesielt data som det stilles spesielle krav til, som persondata, gradert informasjon m.m.
- Kan ulike skyleverandørers tekniske løsninger snakke med hverandre, eller er man bundet til å ha én leverandør? Går det an å avslutte et kundeforhold og skifte leverandør?
- Er skyleverandøren finansielt stabil og en langsiktig aktør?

Sikkerhetspolitiske utfordringer ved bruk av skytjenester

Ved bruk av skytjenester som er utenfor nasjonal kontroll må sikkerhetspolitiske forhold vurderes. Dette gjelder særlig dersom man vurderer å plassere skjermingsverdig eller sensitiv informasjon i skyen.

Følgende forhold må vurderes:

- Samfunnsforholdene og stabiliteten i vertslandet.
- Handelsavtaler med tanke på rettsikkerheten for norske virksomheter i vertslandet.
- Lover og regler i vertslandet som gjelder sikkerhet og personvern.
- Hvilken tilgang har utenlandske myndigheter, eller andre aktører, til informasjon i skyen? Dette inkluderer også de landene dataene passerer ved lagring, transport og behandling, selv ved bruk av kryptografiske sikkerhetsmekanismer. Store mengder data lagret på ett sted kan være interessant for en avansert trusselaktør. En utro tjener på innsiden av en skylagringstjeneste vil kunne gi bredere aksess enn en innsider i en virksomhet.[20]

Dette er forhold som kan være utfordrende å regulere gjennom kontrakter, og ved å benytte skytjenester utenfor nasjonal kontroll har man mindre av grad kontroll over verdikjeder og underleveranser.

[19] Innspill fra Direktoratet for forvaltning og IKT til *Helhetlig IKT-risikobilde 2016*.

[20] Innspill fra Etterretningstjenesten til *Helhetlig IKT-risikobilde 2016*.

4.

Trusler og farer

Vi skiller mellom begrepene trussel og fare. Trussel innebærer risiko for handlinger hvor noen bevisst forsøker å påføre andre skade eller tap. Fare bruker vi i forbindelse med risiko for hendelige uhell og andre hendelser som ikke er bevisst forsøkt påført av andre.

NSM har gjennom flere år sett en tydelig og jevn økning av antall målrettede IKT-angrep mot norske interesser, både offentlige og private. I tillegg er det et stadig økende omfang av ulike politisk og kriminelt motiverte handlinger i det norske digitale rommet.

4.1 TRUSSELAKTØRER

Trusselaktører kan grovt sett deles inn i om de velger målene sine vilkårlig eller om de søker helt spesifikke mål. Målrettede aktører, for eksempel en etterretningstjeneste, søker etter utvalgte verdier og vil kartlegge og utnytte sårbarhetene som gir tilgang til disse verdiene. Aktører som for eksempel er interessert i økonomisk vinning vil ramme bredere og mer vilkårlig og utnytte de samme sårbarhetene i forskjellige virksomheter, så lenge metoden gir gevinst.[21]

Nedenfor beskriver vi de trusselaktørene som er mest relevante for norske virksomheter.

4.1.1 STATLIGE AKTØRER

Statlige aktører[22] står bak de mest alvorlige, vedvarende truslene.[23] Vi ser at disse aktørene har ressurser til metodisk aktivitet over lengre tid. NSM koordinerte håndteringen av flere tilfeller av digital spionasje mot statlige virksomheter i 2015.[24] Digital spionasje er nettverksbaserte etterretningsoperasjoner der målet er å få tak i gradert eller annen sensitiv informasjon eller å skaffe seg tilgang til ettertraktet teknologi.

NSM registrerer at statlige aktører forsøker å etablere seg i norske offentlige virksomheters digitale infrastruktur. Det er også tilfeller der statlige trusselaktører har kompromittert datasystemene til bedrifter som leverer varer eller tjenester av stor etterretningsverdi.[25] Det observeres en økende interesse for å fremskaffe personopplysninger via nett, deriblant passfoto og biometriske data.[26]

Nettverksbaserte etterretningsoperasjoner retter seg ikke bare mot statshemmeligheter, men også mot høyteknologiske virksomheter, spesielt innen romfart, forsvars- og olje- og energisektoren. Ettersom teknologibedrifter ofte har lange leverandørkjeder for å utvikle og produsere avanserte produkter, kan den letteste veien til målet gå gjennom andre virksomheter. EOS-tjenestene har registrert at underleverandører er utnyttet som mål i spionasjesaker, ettersom trusselaktøren i prinsippet kun trenger ett svakt punkt for å komme seg på innsiden.[27]

NSM har koordinert håndteringen av flere tilfeller av digital spionasje hvor norske virksomheter ikke var et direkte mål, men hvor antatt statlige aktører hadde kompromittert små og mellomstore bedrifter for å benytte deres webservere som infrastruktur i videre angrep. I flere av tilfellene har virksomheten hatt svært begrenset kunnskap og mulighet til å forebygge, oppdage og håndtere denne type angrep.

Digitale sabotasjehandlinger vil si å utnytte IKT-systemer til å skade eller ødelegge sivile eller militære verdier, som for eksempel infrastruktur. I *Fokus 2016*[28] skriver Etterretningstjenesten at det er usikkert hvilket skadepotensial slike sabotasjehandlinger har. Derfor antas det at statlige aktører i en langsiktig strategi vil kartlegge sårbarhetene i den digitale infrastrukturen som eventuelt kan utnyttes til slike formål. Av scenarioene Nasjonal kommunikasjonsmyndighet (Nkom) vurderer i EkomROS, knyttes det høyest risiko til at utenlandsk etterretning kartlegger[29] kritisk ekom-infrastruktur og kritisk personell knyttet til denne.[30]

4.1.2 KRIMINELLE AKTØRER

Kriminelle aktører er typisk involvert i svindel innen elektroniske betalingstjenester, e-handel og elektroniske finansielle transaksjoner.[31] Tyveri av pengeverdier gjennom digital plattform er en økende trussel. Dette kan ramme banker, i form av større digitale bankran, men også brukerne av betalingstjenester på internett ved at innloggingsdetaljer blir stjålet.[32] I tillegg kan de kriminelle tilegne seg pengeverdiene

[21] Se også NSMs håndbok *Risikovurdering for sikring* (mars 2016), kap. 4.5 Trusselvurdering – matriser for virksomhetens vurdering av trussel.

[22] Statlige aktører omfatter særlig fremmede staters etterretnings- og sikkerhetstjenester, men kan også omfatte private aktører som arbeider på vegne av fremmede stater.

[23] Innspill fra Etterretningstjenesten til *Helhetlig IKT-risikobilde 2016*.

[24] For ytterlige informasjon om digital spionasje, se også NSMs temahefte «Håndtering av digital spionasje», 2015.

[25] Innspill fra Politiets sikkerhetstjeneste til *Helhetlig IKT-risikobilde 2016*.

[26] Innspill fra Etterretningstjenesten til *Helhetlig IKT-risikobilde 2016*.

[27] Etterretning, Overvåkning, Sikkerhet. Samlebetegnelse her for Etterretningstjenesten, Politiets sikkerhetstjeneste og NSM.

[28] Etterretningstjenesten: *FOKUS 2016: Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer.*

[29] Slik kartlegging kan foregå på flere måter, deriblant ved hjelp av IKT og internett.

[30] Nasjonal kommunikasjonsmyndighet (Nkom): *EkomROS 2016*. Risikovurdering av ekomsektoren.

[31] European Union Agency for Network and Information Security (ENISA): *Threat Landscape 2014*, s. 44.

[32] McAfee Labs: *2016 Threat Predictions*.

gjennom bedrageri og utpressing, som ved bruk av løsepengevirus og direktørsvindel.

Metoder kriminelle benytter seg av for å gjøre dette er blant annet spam på e-post, nettfiske, skadevare, identitetstyveri og manipulasjon av nettbanker.[33] Det mørke nettet (dark net) er en arena for utveksling av tjenester og gjennomføring av kriminelle handlinger.[34] Dette illegale markedet har utviklet seg fordi internett gjør det mulig å svindle eller stjele store beløp ved relativt lave investeringer.[35]

4.1.3 HACKTIVISTER

Hacktivister er aktivister som benytter illegale virkemidler på internett til å fremme et standpunkt eller en politisk agenda. Angrepsmetodene og konsekvensene knyttet til denne typen aktører varierer kraftig. Tjenestenektangrep (DDoS; Distributed Denial of Service) er mye brukt, fordi konsekvensen ofte er synlig og lett får medieomtale. DDoS er også lett og billig å gjennomføre i korte perioder. En annen angrepsmetode er å endre innholdet på nettsiden til offeret (også kalt «defacing»). Det er også blitt mer vanlig å publisere sensitivt materiale på nett, som igjen kan skade virksomhetens omdømme.

NSM har så langt ikke observert noen angrep utført av hacktivister som har fått store samfunnsmessige konsekvenser, men lengre nedetid på tjenester og nettsider har forekommet. NSM ser en økende tendens til at hacktivisme blir utført mot norske interesser.

4.2 TRUSSELMETODER

Utviklingen innen trusselmetoder og mottiltak er ved flere anledninger beskrevet som et kappløp.[36] Trusselmetodene er i rask utvikling, og angrepene som NSM koordinerer håndteringen av er mer avanserte og mer komplekse enn før. Nedenfor beskrives noen av de vanligste trusselmetodene som rammer norske virksomheter.

4.2.1 AVANSERTE VEDVARENDE TRUSLER

En avansert vedvarende trussel (APT[38]) er en samlebetegnelse for avanserte og målrettede angrep som har som formål å etablere bakdører, plante og spre skadevare og hente ut skjermingsverdig informasjon. Angrepene kjennetegnes av langsiktighet og av at trusselaktøren er ressurssterk.

NSM registrerer stadig angrep mot samfunnskritisk infrastruktur eller samfunnsviktige funksjoner. Vi ser at en andel av angrepene har blitt mer avanserte. Det som imidlertid i størst grad kjennetegner APT-angrepene er at de er vedvarende, noe som viser at trusselaktørene har ressurser til metodisk aktivitet over lengre tid. Angrep som benytter eldre tekniske sårbarheter lykkes fortsatt. Det er kun unntaksvis at ikke-kjente sårbarheter, såkalte 0-dags-sårbarheter,[38] blir utnyttet. Det siste året har NSM vært involvert i flere saker der utdaterte webserverinstallasjoner hos mindre bedrifter med begrensede IT-ressurser har blitt kompromittert. De kompromitterte serverne blir så brukt som mellomledd i nye angrep mot andre mål, både nasjonalt og internasjonalt.

Statlige trusselaktører og APT

Statlige trusselaktører står ofte bak APT. Metodene som benyttes kan være avanserte, men trenger ikke å være det. De kjennetegnes først og fremst av at de er utholdende. Rob Joyce, sjef for National Security Agencys Tailored Access Operations, advarer derfor mot å tro at et sikkerhetshull er for lite til å bli utnyttet.[39] Statlige trusselaktører har kapasitet og ressurser til å vente på åpninger i en virksomhets datasystemer. De skanner angrepsmålet og aktiviteten der og blir så godt kjent med nettverket at de kjenner det bedre enn de som satte det opp. De kjenner teknologien i nettverket ned til minste detalj, alle dets sikkerhetsfunksjoner og svakheter. Aktørene har et sett av ulike måter å trenge inn i et datanettverk på og benytter seg av enkleste og minst risikofylte måte. Når de først er inne, klorer de seg fast og blir der i måneder og år. Inne i nettverket ser de etter det som er tilgjengelig.

[33] Bundesamt für Sicherheit in der Informationstechnik (BSI): *Die Lage der IT-Sicherheit in Deutschland 2015*.

[34] KRIPOS: *Trendrapport 2016*.

[35] RAND Corporation: *Markets for Cybercrime Tools and Stolen Data*, 2014, s.3.

[36] Se bl.a. NSMs *Risiko 2016* og Etterretningstjenestens *Fokus 2016*.

[37] APT står for Advanced Persistent Threat.

[38] Fra engelsk zero-day vulnerability.

[39] Rob Joyce, sjef for NSAs Tailored Access Operations på konferansen USENIX Enigma 2016. Foredraget «Disrupting Nation State Hackers» er tilgjengelig på YouTube https://www.youtube.com/watch?v=bDJb8WOJYdA

4.2.2 INNSIDERE

EOS-tjenestene advarer mot innsidere i virksomhetene.[40] Det å ha noen på innsiden er en effektiv etterretningsmetode med stort skadepotensiale.[41] En innsider er en person som har tilgang til en virksomhets interne systemer, informasjon eller prosesser og som kan kjenne svakhetene ved interne sikkerhetstiltak.[42]

Innsideren som aktør kan deles i tre hovedkategorier; infiltratøren, den ondsinnede innsideren som er vervet eller handler på eget initiativ og den ubevisste innsideren. Sistnevnte ønsker ikke bevisst å kompromittere informasjon eller virksomheten, men vedkommendes vurderinger og handlinger gjør at personen uforvarende blir en innsider eller medvirker til innsidevirksomhet.

Det hevdes at den alvorligste sikkerhetstrusselen mot amerikanske selskaper ikke er hackere som sitter langt unna, men innsidere som allerede har full tilgang til alt av informasjon.[43] En rapport fra IBM viser at i 2015 ble 60 prosent av registrerte angrep uført av ondsinnede innsidere (44,5 prosent) eller var resultat av «ikke-intenderte» handlinger (15,5 prosent).[44] Kriminalitets- og sikkerhetsundersøkelsen til Næringslivets sikkerhetsråd viser at nesten tre av ti norske virksomheter har avdekket utro tjenere og at fire prosent har ansatte som har opplevd trusler med krav om å utføre uønskede handlinger.[45]

Innsideren kan være en trussel i alle virksomheter som har verdier som kan utnyttes av en ekstern aktør. Eksempelvis kan innsidere utgjøre en særlig trussel i store datasentre som betjener leverandører av skytjenester, fordi de potensielt får tilgang til og kan stjele eller ødelegge mye data.

4.2.3 LØSEPENGEVIRUS

Bruk av krypterende løsepengevirus til utpressing har i 2016 vært økende på verdensbasis.[46] Også norske foretak er utsatt for dette. NSM og samarbeidende sektorvise responsmiljøer har ved flere anledninger advart mot angrepsbølger. Finanstilsynet trekker også frem løsepengevirus og direktørsvindel i sin risiko- og sårbarhetsanalyse for 2015.[47] NSMs advarsler har understreket viktigheten av å ha gode sikkerhetskopier, fordi det i mange tilfeller har vært svært vanskelig å hente tilbake krypterte filer.

Nye krypteringsvirus dukker stadig vekk opp på markedet. Så lenge ofrene velger å betale, kan man anta at denne type aktivitet vil fortsette å øke.

NSM får daglig rapporter fra samarbeidspartnere om kompromitterte norske nettsider som re-dirigerer til nettsider som er infisert av skadevare, såkalte exploit kits. Dette har vært en vanlig angrepsmåte for distribusjon av krypteringsvirus, men andre typer skadevare har også vært distribuert. Det er trolig store mørketall når det gjelder løsepengevirus.

> Datasystemer ved sykehus er sårbare og sykehuspersonell er avhengig av tilgang til systemer og elektroniske pasientjournaler for å redde liv.[48] I løpet av første halvår har flere sykehus og helseforetak i USA blitt rammet av løsepengevirus som krypterer filer i datasystemene slik at disse blir låst. Mange har betalt for å få tilbake tilgang til lagrede filer, men det er ikke alltid dette løser problemet. I Kansas fikk et sykehus tilleggskrav etter å ha betalt det trusselaktøren krevde.[49]

4.2.4 E-POSTANGREP

NSM registrerer fortsatt at den vanligste angrepsmetoden i vellykkede, målrettede angrep er e-post til brukere i virksomheten som rammes. E-post kan brukes til å smugle inn skadevare for å stjele informasjon eller for å plante programvare som senere kan utnyttes til sabotasje. E-posten kan også mer direkte brukes til å lure mottakeren til å utføre handlinger som er uheldige for virksomheten.

Målrettet nettfisking

Nettfisking (phishing), og særlig målrettet nettfisking (spear phishing), retter seg mot utvalgte IKT-brukere som er nøye studert på forhånd, slik at angriperen kan skreddersy angrepet. E-posten inneholder et ondsinnet vedlegg eller en lenke til en side som serverer ondsinnet kode, som kan etablere bakdører for videre angrep. Det er i

[40] Innspill fra Etterretningstjenesten og Politiets sikkerhetstjeneste til *Helhetlig IKT-risikobilde 2016*.

[41] Politiets sikkerhetstjeneste (PST): *Trusselvurdering 2016*

[42] En innsider kan være en ansatt eller en tredjepart – en forretningspartner, klient, konsulent eller samarbeidende kontraktør – et individ du stoler nok på til å gi vedkommende tilgang til systemene dine.

[43] Robert N. Rose i et gjesteinnlegg på Forbes.com. www.forbes.com/sites/realspin/2016/08/30/the-future-of-insider-threats/#5425f7416726 - Publisert 2016-08-30, lastet 2016-08-31.

[44] IBM Security: *IBM 2015 Cyber Security Intelligence Index*

[45] Næringslivets sikkerhetsråd: *KRISINO 2015. Kriminalitets- og sikkerhetsundersøkelsen i Norge.*

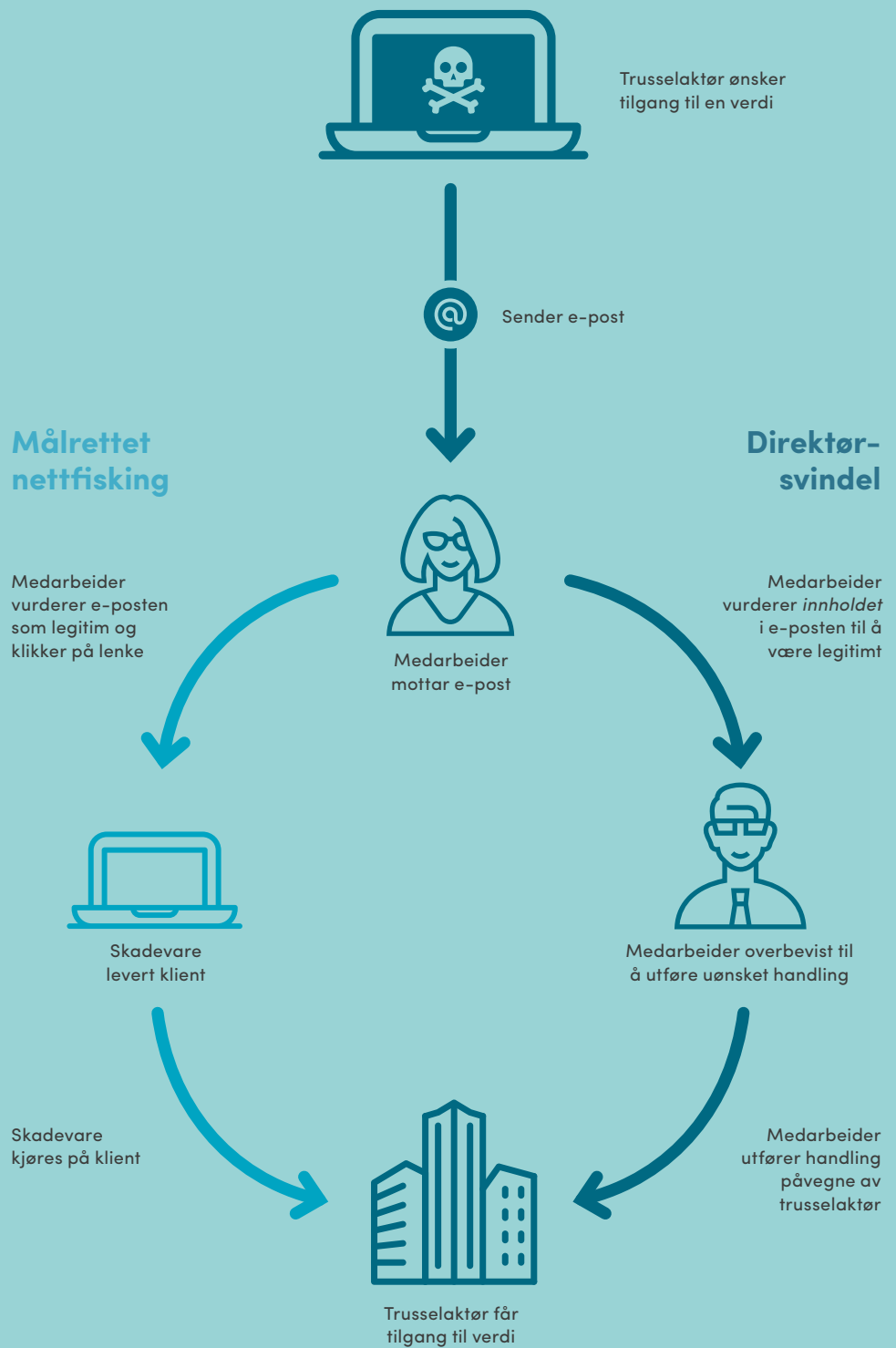
[46] Verizon: *2016 Data Breach Investigations Report* (s. 46)

[47] Finanstilsynet: *Risiko- og sårbarhetsanalyse (ROS) 2015.*

[48] Sykehus er lette bytter for slik kriminalitet fordi de er avhengig av oppdatert pasientinformasjon, og fordi ansatte der ikke har fokus på cybersikkerhet. www.wired.com/2016/03/ransomeware-why-hospitals-are-the-perfect-targets/ - Publisert 2016-03-30, lastet 2016-08-19.

[49] www.digitaltrends.com/computing/ransomeware-hospital-hackers-demand-more-money - Publisert 2016, lastet 2016-08-19.

ANGREPSMETODER E-POST



hovedsak kjente sårbarheter som utnyttes.

NSM observerer at i mange tilfeller er e-posten utformet med informasjon som er relevant for mottakeren og at den kun sendes til et fåtall utvalgte brukere. Informasjonen om e-postmottakeren blir hentet ut gjennom analyser av informasjon som angriper har tilgang til, enten via åpne kilder eller tidligere kompromittert informasjon. Informasjon hentet fra én virksomhet kan brukes i angrep mot andre.

Når en trusselaktør har etablert fotfeste gjennom utnyttelse av sårbarheter i kombinasjon med e-postmottakerens legitime rettigheter, blir aktøren ofte vanskelig å oppdage. Da kan datauthenting skje gjennom legitime trafikkprotokoller, i små mengder og i kryptert tilstand. Det vil kreve stadig høyere kompetanse å oppdage trusselaktører som har fått fotfeste på innsiden.

Direktørsvindel

En ny, kraftig nettfisking-trend i 2016 er direktørsvindel.[50] Økokrim og NorSIS har tidligere i år advart mot denne formen for svindel,[51] [52] og amerikanske FBI[53] rapporterte i vår at direktørsvindel og liknende metoder var i kraftig økning og kostet amerikanske virksomheter store summer.[54] Essensen i slike angrep er at trusselaktørene på forhånd gjør undersøkelser av virksomheten de ønsker å angripe ved å kartlegge økonomisjefer eller ansatte med ansvar for transaksjoner. Angrepet starter ofte med en e-post med forfalsket avsender. E-postene er gjerne skrevet på godt norsk, og man blir bedt om å gjennomføre en hastebetaling som må holdes hemmelig.

Denne sosiale manipulasjonen har vist seg å være svært effektiv, og NSM har informasjon om at flere norske virksomheter har betalt store summer til utlandet. I perioden juni til august 2016 ble NSM direkte varslet av 45 virksomheter som hadde blitt utsatt for direktørsvindelforsøk.

4.2.5 VANNHULLSANGREP

I et vannhullsangrep kompromitterer en trusselaktør en internettside som hyppig besøkes av personer i en aktuell målgruppe slik at besøkende på nettsiden serveres skadevare. Sofistikerte aktører «hvitelister» vannhullene sine, noe som innebærer at kun besøkende i målgruppen vil bli servert skadevare.[55] [56] Målet er å skaffe trusselaktøren tilgang til offerets nettverk. Vannhullsangrep har vært i sterk vekst de siste årene, og NSM får daglig rapporter fra samarbeidspartnere om dette fenomenet.

[50] Også kalt bl.a. CEO-svindel, toppsjefsvindel og «whaling». CEO er forkortelse for Chief Executive Officer, tilsvarende administrerende direktør eller toppsjef på norsk.

[51] www.okokrim.no/artikler/social-engineering-fraud-ceo – Publisert (oppdatert) 2016-03-07, lastet 2016-09-01.

[52] norsis.no/oppblomstring-av-direktor-svindel-pa-nettet/ - Publisert 2016-06-23, lastet 2016-08-19.

[53] Federal Bureau of Investigation.

[54] www.fbi.gov/contact-us/field-offices/phoenix/news/press-releases/fbi-warns-of-dramatic-increase-in-business-e-mail-scams - Publisert 2016-04-04, lastet 2016-08-19.

[55] Innspill fra Politiets sikkerhetstjeneste til *Helhetlig IKT-risikobilde 2016*.

[56] Innspill fra Etterretningstjenesten til *Helhetlig IKT-risikobilde 2016*.

Farer – utilsiktede hendelser

Målrettede, villede angrep mot IKT-systemer får med rette mye oppmerksomhet. Allikevel er det slik at mange alvorlige sikkerhetsbrister skyldes utilsiktede hendelser. Rapportene *Annual Incident Report* 2014[57] (AIR) og *2015 Information Security Breaches Survey*[58] (ISBS) viser dette med all tydelighet.

AIR er en sammenstilling av sikkerhetsbrudd for alle EU- og EØS-land i ekom-nett. Den største feil-kilden er systemfeil, med menneskelige faktorer som en god nummer to. Rapporten viser også at menneskelige faktorer er kategorien hvor feil på-virker flest brukere.

ISBS er en spørreundersøkelse den britiske regjeringen har gjort hvor offentlige og private virksomheter i ulike sektorer har rapportert på hvilke typer informasjonssikkerhetsbrister de har opplevd siste år. Virksomhetene har også gitt opplysninger om hvilke tiltak de gjør og om ressursbruken på området. Hele 50 prosent av virksomhetene meldte at den verste informasjonssikkerhetsbristen de hadde, skyldtes utilsiktede menneskelige feil.

Selv om denne studien er britisk, er det lite som tyder på at situasjonen er vesentlig annerledes i Norge. Det betyr at dette er et område med stort forbedringspotensial, og at virksomheters informasjon ikke nødvendigvis er sikret selv om den tekniske sikringen er god.

Å redusere utilsiktede menneskelige feil er en krevende oppgave. Først og fremst er det en virksomhetsintern oppgave i form av kompetanseheving, gode rutiner og bevisstgjøring. I bunn må ledelsesforankring og involvering ligge. ISBS viser at virksomheter hvor informasjonssikkerhetsarbeidet er dårlig ledelsesforankret er mer utsatt for utilsiktede menneskelige feil enn virksomheter hvor toppledelsen har fokus på dette.

Samtidig har digitaliseringen av samfunnet medført at de digitale verdikjedene, ref. Lysneutvalget, beveger seg langt utenfor virksomhetenes grenser. Når dette kombineres med utstrakt bruk av utkontraktering av tjenester hvor relasjoner styres av kontrakter, er det nødvendig å se utfordringen med utilsiktede menneskelige feil i en større sammenheng.

I et samfunnssikkerhetsperspektiv gjelder dette spesielt for virksomheter med ansvar for kritiske samfunnsfunksjoner, samt virksomheter med ansvar for kritisk infrastruktur. Eksempelvis skyldtes brudd i fiberforbindelsen til Svalbard 2. juni 2014 en feil som oppsto ved en planlagt oppgradering.

Den teknologiske utviklingen innebærer at IKT-systemene blir stadig mer komplekse, som igjen gir muligheter for flere utilsiktede menneskelige feil. Dette er en problemstilling som må tas på alvor – særlig for virksomheter med ansvar for kritiske samfunnsfunksjoner og/eller kritisk infrastruktur. Lysneutvalget gir flere gode anbefalinger som kan gjøre norske virksomheter bedre rustet til dette. En anbefaling er å utvikle et rammeverk for analyse av digitale verdikjeder. Et slikt rammeverk vil kunne sette myndigheter og andre virksomheter bedre i stand til å forstå kompleksiteten i IKT-systemene sine. En annen anbefaling er at virksomheter må inkludere IKT-sikkerhet i virksomhetsstyringssystemene sine og på den måten synliggjøre risiko.

Kilde: Direktoratet for samfunnssikkerhet og beredskap.

[57] European Union Agency for Network and Information Security (ENISA) (2015), *Annual incident Report 2014*.

[58] HM Government (2015), *2015 Information Security Breaches Survey*.

5.

Sårbarheter

Digitaliseringen av samfunnet skaper hele tiden nye verdier og utviklingsmuligheter, men kan også utvide sårbarhetsflaten til verdier og interesser vi ønsker å beskytte.

Det finnes sikkerhetsmessige sårbarheter på alle nivåer og langs flere dimensjoner i enhver virksomhet. Mange sårbarheter er knyttet til bruk av IKT. For å tegne et helhetlig IKT-risikobilde må man se teknologiske, menneskelige og organisatoriske sårbarheter i sammenheng. Den enkelte virksomhet må identifisere egne sårbarheter og tenke helhetlig for å være sikker på å få med alle aspekter.

NSM gjennomfører rundt 50 tilsyn hvert år. Funnene peker i retning av mangelfull sikkerhetsstyring. Vi ser at det er til dels store forskjeller i modenhetsnivået på styringssystemet for sikkerhet i de forskjellige virksomhetene, og vi erfarer også at mangelfull sikkerhetsstyring fører til ulik intern forståelse av sikkerhetstilstanden i virksomheten. Vi har blant annet sett eksempler på virksomheter som fokuserer på avanserte sikringsmetoder, uten at de har nødvendig grunnsikring på plass. Dette kan resultere i fragmenterte tiltak som ikke sees i sammenheng. NSMs tilsyn viser videre at tre av fire virksomhetsledere ikke har gjennomført evaluering av sikkerhetsarbeidet, slik at man ikke avdekker virksomhetens reelle sikkerhetstilstand. Virksomheten kan dermed risikere at tiltak ikke blir iverksatt der hvor sårbarhetene er størst.

Mange av sårbarhetene NSM avdekker, kunne virksomhetene avdekket selv med enkle virkemidler, for eksempel ved å gjennomføre interne sikkerhetsrevisjoner. Blant virksomhetene NSM førte tilsyn med i 2015, hadde seks av ti avvik som gikk på manglende gjennomføring av sikkerhetsrevisjoner.

5.1 MENNESKELIGE SÅRBARHETER

Virksomheter gjennomfører ulike tiltak for å ivareta konfidensialiteten, integriteten og tilgjengeligheten til informasjon, systemer, objekter og prosedyrer. Menneskene som er gitt legitim tilgang kan imidlertid svekke effekten av disse tiltakene eller omgå tiltakene fullstendig og utgjør derfor en sårbarhet. Mennesket står således i sentrum ved at det både utgjør en sårbarhet i seg selv og påvirker hvilke organisatoriske grep som tas og hvordan teknologien brukes. Menneskelige sårbarheter kan utnyttes på mange måter, blant annet ved sosial manipulasjon. Vi lar oss lure til å gi fra oss informasjon, både ved direktekontakt, på nettet og via telefon. Informasjonen kan være tilgangsrettigheter som kan utnyttes både fysisk og digitalt, eller det kan være personopplysninger, informasjon om patenter, gradert informasjon eller annen sensitiv informasjon.

Informasjon om enkeltmennesker eksponeres på mange arenaer og kan utnyttes av trusselaktør. Informasjon om en e-postmottaker kan hentes gjennom tilgjengelige kilder, eksempelvis en virksomhets internettside eller fra tidligere kompromittert informasjon.

E-post med ondsinnet innhold er en av hovedveiene inn i datasystemer. En internasjonal undersøkelse viser at i 30 prosent av nettfiskingsforsøkene ble e-postene åpnet, og 12 prosent klikket i tillegg på det ondsinnede vedlegget eller lenken, slik at angrepet kunne lykkes.[59] NSM kan vise til tilsvarende erfaring. Den internasjonale undersøkelsen viste at gjennomsnittlig tid for å åpne en ondsinnet e-post var ett minutt og 40 sekunder. Gjennomsnittstiden for å klikke på vedlegget var tre minutter og 45 sekunder.

En annen type menneskelig sårbarhet er unøyaktighet, slurv og forglemmelse. Alle mennesker gjør feil fra tid til annen, og noen ganger kan dette ha uheldige konsekvenser. Ubetenksomme handlinger kan kompromittere informasjon, eksempelvis ved at e-post eller dokumenter blir sendt til feil mottaker eller offentliggjort på nett. Feilkonfigurering av brannmurer kan gi tilgang til sensitive data for flere enn de som skulle ha slik tilgang.[60]

Ubetenksomhet og manglende sikkerhetsbevissthet medfører at informasjon ikke skjermes tilstrekkelig eller deles med tilfeldig forbipasserende fordi vi ikke tar hensyn til omgivelsene og kanskje er uforsiktige med hva vi sier i en mobiltelefonsamtale.

[59] Verizon: *2016 Data Breach Investigations Report*

[60] Verizon: *2016 Data Breach Investigations Report*

En ubevisst innsider er en person som forårsaker en svakhet i virksomhetens sikkerhetstiltak ved ubetenksomhet eller ved å ha blitt forledet eller manipulert av en trusselaktør. Den ubevisste innsideren har ikke nødvendigvis kunnskap eller intensjon om at en trusselaktør utnytter slike sikkerhetssvakheter og oppfatter kanskje ikke konsekvensen av egne handlinger eller unnlatelser. Et fellestrekk for handlingene til den uforvarende innsideren er at det er personens manglende evne til å forstå eller rette seg etter sikkerhetstiltak som gjør at vedkommende uforvarende kompromitterer informasjon, system eller objekt.

Mennesker vil alltid ha ulik grad av sårbarheter som en trusselaktør kan utnytte. Slike sårbarheter kan være misnøye med arbeidsforholdet, personlige problemer, økonomiske vansker eller delte lojaliteter.[61] Vi har også ulik grad av sikkerhetsbevissthet og motivasjon for å følge regelverk og retningslinjer. Dersom en rutine oppleves tungvinn, kan det være fristende å finne en snarvei utenom for å effektivisere eget arbeid.

5.2 ORGANISATORISKE SÅRBARHETER

Organisatoriske sårbarheter kan sees på som systemsvikt, mangelfulle barrierer eller mangelfull sikkerhetsstyring. Når sikkerhet ikke følges opp systematisk, er det en organisatorisk sårbarhet, selv om sårbarheten gjelder manglende systematisk oppdatering av programvare, oppfølging av logger eller oversikt over sikkerhetskompetansebehov i virksomheten.

NSM har også tidligere påpekt at organisatoriske sårbarheter dominerer sårbarhetsbildet og at *mangelfull sikkerhetsstyring* er en hovedutfordring. Andre eksempler på organisatoriske sårbarheter er[62]:

- manglende risikovurdering og risikobevissthet
- manglende situasjonsforståelse
- manglende systemer for oppdatering av dataprogrammer og logging av datatrafikk
- manglende dokumentasjon av sikkerhetsarbeidets målsettinger, krav, instrukser og resultater
- mangler i passordadministrasjon og annen tilgangskontroll, samt manglende oversikt over disse
- utilstrekkelig kompetanse til å bestille tekniske sikkerhetsløsninger

En annen sårbarhet vi vil trekke frem er manglende tilgangsstyring og soneinndeling, både i datasystemer og når det gjelder fysisk sikring av virksomhetens lokaler. Dette kan sees på som teknologiske sårbarheter, men de har også en organisatorisk side. Hvem som skal ha tilgang hvor er en organisatorisk beslutning som må tas, basert på hvilke verdier som må skjermes og hva den enkelte arbeidstaker har behov for tilgang til. Manglende soneinndeling gjør at mulige innsidere lett kan nå frem til ønsket informasjon. Mangelfulle rutiner eller svak oppfølging av disse kan også medføre at tidligere ansatte fortsatt har adgangskort eller mulighet for ekstern pålogging til virksomhetens datasystemer.[63]

5.3 TEKNOLOGISKE SÅRBARHETER

Teknologiske sårbarheter kan finnes i alle typer teknisk utstyr og programvare. Sårbarheter i maskinvare kan finnes på ulike nivåer, som modifikasjoner ved at det er satt på ekstra

[61] NSM: *Sikkerhetsfaglig råd 2015* s. 17.

[62] For flere eksempler se NSMs håndbok *Risikovurdering for sikring.*

[63] Verizon omtaler dette som TGYFBFTDHRA – «that guy you fired but forgot to disable his remote access» Verizon: *2016 Data Breach Investigations Report*, s. 35.

Tilsyn og revisjoner utført av NSM og Riksrevisjonen[64] viser at virksomheter i varierende grad har etablert tilfredsstillende styringssystem for sikkerhet og implementering av sikringstiltak. Riksrevisjonens funn viser svakheter ved ledelsesforankring, risikostyring og identifisering og klassifisering av aktiva. For flere virksomheter er det manglende sammenheng mellom klassifisering, risikovurdering og tiltak. Både NSM og Riksrevisjonen erfarer at det er mangler ved rapportering og læring av avvik og at mange virksomheter ikke vurderer om styringssystemet fungerer etter sin hensikt.

En konsekvens av mangelfull sikkerhetsstyring er også at arbeidet med tiltak ikke er tilfredsstillende. Manglende oppfølging fra ledelsen gjør at NSMs tilsyn ofte avdekker mange følgefeil som virksomhetene selv burde ha avdekket og kontrollert. Typiske eksempler på slike feil er manglende sikkerhetsoppdateringer, at maskinvare generelt ikke er oppdatert og at tilgangs-/rettighetskontroll i systemene ikke er à jour. Summen av slike følgefeil er at sikkerhetsnivået svekkes betydelig.

Riksrevisjonens revisjoner av informasjonssikkerhet fra 2015 vurderte blant annet kvaliteten på sikkerhetstiltak relatert til tilgangsstyring, sikkerhetsoppdateringer, autoriserte/uautoriserte enheter i nettverket og autorisert/uautorisert programvare. Revisjonene viser at det er store mangler i implementasjonen av tiltak:

- Det er mangler i tilgangsstyringen til systemene.
- Virksomhetene har manglende oversikt over administratorbrukere og manglende logging og oppfølgning av disse.
- Få virksomheter har kontroll på autorisert programvare i nettverket og mindretallet har kontroll på autoriserte enheter i nettverket.
- Flere har åpnet for lokale administratorer på klienter.

Positivt var at flertallet har tilfredsstillende rutiner for patching/sikkerhetsoppdatering, da spesielt når det gjelder oppdatering av Windows operativsystem. Konklusjonen er likevel at mange virksomheter har et stort forbedringspotensial, både når det gjelder styringssystemer og hvordan tiltak implementeres.

moduler, endring av brytere, manipulering av mikrobrikker eller programvaremodifikasjon på firmware-nivå.[65] Eksempelvis kan tastatur og USB-enheter få tilleggsfunksjoner som innebærer at data blir sendt ved hjelp av radiosignaler.[66] Mobile enheter som smarttelefoner, nettbrett og klokker kan inneholde sårbarheter som kan utnyttes. Sårbarheter i firmware kan ha store konsekvenser og er vanskelige å oppdage.[67]

Nye sårbarheter i programvare oppdages daglig. En internasjonal undersøkelse viser at halvparten av registrerte dataangrep hvor sårbarheter utnyttes, skjer i perioden fra ti til 100 dager etter at informasjon om sårbarheten er publisert.[68] Tidsrommet fra en sårbarhet er kjent til den blir lukket gjennom en sikkerhetsoppdatering (patching) er en gylden mulighet for trusselaktør til å trenge inn i et datanettverk. NSM ser gjentatte ganger at denne muligheten utnyttes. Samtidig ser vi at gamle sårbarheter fortsatt utnyttes av trusselaktørene.

Et fellestrekk i vellykkede dataangrep i Norge er at trusselaktør benytter kjente sårbarheter for å få tilgang til ønsket informasjon. Generelt kan vi si at trusselaktørene synes å gå «minste motstands vei» ved at de utnytter sårbarheter og metoder som er kjent av mange. Dette er sårbarheter som i mange tilfeller kunne vært lukket dersom programvaren hadde vært oppdatert. Noen ganger benyttes også ukjente

[64] Innspill fra Riksrevisjonen til *Helhetlig IKT-risikobilde 2016* basert på revisjoner i 2015.

[65] Firmware er grunnleggende intern programvare eller kontrollsystem som styrer elektriske enheter, et slags operativsystem for ulike former for elektronikk. Firmware finnes i alt fra i datamaskiner, fjernkontroller, digitale klokker, mobiltelefoner, digitale kamera, til mikrobølgeovner, vaskemaskiner og trafikklys. (Kilde: Wikipedia)

[66] Bundesamt für Sicherheit in der Informationstechnik (BSI): *Die Lage der IT-Sicherheit in Deutschland* 2015

[67] National Cyber Security Centre: *Cyber Security Assessment Netherlands CSAN 2015.*

[68] Verizon: *2016 Data Breach Investigations Report*

sårbarheter, såkalte 0-dags-sårbarheter.

NSM NorCERT har i 2016 sett mange eksempler på kompromittering av internettservere i små virksomheter med begrensede IT-ressurser. I mange av disse tilfellene er det utdaterte webserverinstallasjoner som har blitt kompromittert. Målet med slike angrep kan være å hente informasjon fra virksomheten som angripes eller å benytte serveren som angrepsverktøy mot et annet mål. Dette betyr at din server kan bli brukt som en del av en infrastruktur i angrep mot en annen virksomhet, nasjonalt eller internasjonalt.

Teknologi benyttes også i forbindelse med fysisk sikring av IKT-infrastruktur, eksempelvis i adgangskontrollsystemer. Manglende sikring kan gi uautorisert tilgang til servere og annet IKT-utstyr koblet til datanettverket. NSM har sett eksempler på virksomheter som har slik sikring, men som samtidig har nettverkspunkter plassert i fellesareal. Nettverkspunktene er dermed tilgjengelige for uvedkommende som kan få tilgang til virksomhetens datanettverk.

Manglende fysisk sikring av IKT-infrastruktur der utstyret er plassert, enten i virksomhet eller i eksterne datahaller dersom virksomheten bruker skytjenester, utgjør en sårbarhet som kan utnyttes. Dersom hvem som helst kan ta seg inn i serverrommet, vil det være umulig å sikre seg mot fysisk ødeleggelse av IKT-utstyret der. Det vil ta vesentlig lenger tid å gjenopprette IKT-systemer som er ødelagt av brann eller fysiske angrep enn det tar å gjenopprette etter digitale angrep. Ved planlegging av IKT-systemer tas det ofte ikke høyde for at gjenoppretting etter fysisk ødeleggelse kan ta måneder eller år, mens det gjerne er snakk om timer før normaltilstand er gjenopprettet etter digitale angrep.

IKT-systemer kan avleses på flere måter. Det hjelper ikke å ha adgangskontrollen i orden inne i en bygning dersom noen kan stå utenfor bygningen og lese direkte fra dataskjermen til ansatte gjennom et uskjermet vindu. Likeledes kan personlige koder lett avleses direkte dersom tastaturet på kortleseren er uheldig plassert, eller det kan benyttes hjelpemidler til å avlese hvilke tall koden består av, for så å knekke koden i etterkant.

Adgangskort på avveie eller eksponert på internett er en annen sårbarhet. Noen typer adgangskort inneholder teknologi som lett kan kopieres og brukes til å produsere falske adgangskort.[69] Dette åpner for at uautoriserte personer kan få tilgang til (antatt) sikrede områder.

Uvedkommende kan også ta seg inn på adgangskontrollerte områder ved at de går inn samtidig med personell som har adgang, også kalt «tailgating».

Industrielle styringssystemer (SCADA/ICS) koblet til internett har sårbarheter som gjør at de er utsatt for angrep. Det har vært flere eksempler på dette det siste året (se tekstboks).
For en liste over andre teknologiske sårbarheter, se NSMs risikovurderingshåndbok.[70]

Cyberangrepet som slo ut deler av strømnettet i Ivano-Frankivsk-regionen vest i Ukraina i desember 2015 berørte omtrent 225.000 mennesker.[71] Ukrainske myndigheter rapporterte i januar at lignende skadevare som ble benyttet i angrepet mot strømnettet også var funnet i systemer på Kievs hovedflyplass Boryspil.[72] Et sikkerhetsselskap kunne rapportere at de hadde sett spor av forsøk på lignende angrep mot ukrainske gruve- og jernbaneselskaper.[73]

I august 2015 ble det danske energiselskapet NRGI rammet av et omfattende hackerangrep.[74] En rekke servere ble da utsatt for angrep som rammet selskapets hjemmeside, app og telefonsystemer.

Det amerikanske responsteamet for cyberhendelser i industrikontrollsystem, ICS-CERT, fikk i 2015 innrapportert 295 hendelser, en økning på 20 prosent fra 2014.[75] [76] Tallene forteller om mange angrep mot tilvirkning av kritiske produkter, energi, vann og demninger og transport. Det er grunn til å anta at det reelle antallet hendelser er enda høyere, både på grunn av underrapportering av hendelser og fordi slike angrep kan være vanskelige å oppdage og identifisere som målrettede.

[69] NSM: *Risiko 2016*

[70] NSMs håndbok *Risikovurdering for sikring*

[71] BBC News http://www.bbc.com/news/technology-35204921 - Publisert 2016-03-16, lastet 2016-06-06.

[72] www.reuters.com/article/us-ukraine-cybersecurity-malware-idUSKCNOUW0RO Publisert 2016-01-18, lastet 2016-08-18 www.independent.co.uk/news/world/europe/ukraine-cyberattakck-boryspil-airport-kiev-russia-hack-a6818991.html Publisert 2016-01-18, lastet 2016-08-22

[73] blog.trendmicro.com/trendlabs-security-intelligence/killdisk-and-blackenergy-are-not-just-energy-sector-threats/ - Publisert 2016-02-11, lastet 2016-08-18

[74] Berlingske: www.b.dk/nationalt/jysk-energigigant-ramt-af-hackerangrep - Publisert 2015-09-01, lastet 2016-09-01.

[75] https://securityintelligence.com/news/ics-cert-reports-increase-in-fy2015-infrastructure-attacks/ - lastet 2016-08-19

[76] Booz Allen Hamilton: *Industrial Cybersecurity Threat Briefing.*

6.

Risikobildet

Samfunnets samlede digitale plattform er stor. Økende digitalisering introduserer stadig flere sårbarheter, samtidig som gamle sårbarheter ikke er lukket. Den digitale plattformen vokser hele tiden og blir større for hvert år, noe som gjør risikobildet mot norske virksomheter stadig mer omfattende og komplekst.

IKT-risikobildet på et stats- og samfunnsnivå preges av nettverksoperasjoner fra fremmede stater. Interessen for skjermingsverdig og sensitiv informasjon om norsk forvaltning er vedvarende høy.

På samfunnsnivå er det viktig at kritiske funksjoner er tilgjengelige og fungerer som de skal, også i situasjoner hvor de kan settes under press eller angripes. Mange viktige deler av verdikjeden bak disse leveres av få leverandører, av og til med tilnærmet monopol, slik som kraft og elektronisk kommunikasjon. Angrep mot samfunnsfunksjoner synes å være knyttet til potensielle konfliktsituasjoner med fremmede stater.

Virksomheter som utvikler høyteknologi, særlig innen romfart, forsvarssektoren og olje- og energisektoren, er også mål for statlige aktører.

Statlige aktører står ofte bak avanserte vedvarende trusler, som kjennetegnes av høy kompetanse og stor tålmodighet. En typisk metode er målrettet nettfisking (spear phishing). NSM registrerer at angrep fra statlige aktører blir mer avanserte og vanskeligere å oppdage.

For offentlig forvaltning vurderer NSM at det er høyest IKT-risiko knyttet til nettverksangrep og digital spionasje fra statlige aktører som er ute etter skjermingsverdig eller sensitiv informasjon. Også for virksomheter som forvalter kritisk infrastruktur, kritiske samfunnsfunksjoner eller som utvikler høyteknologi, vurderer NSM at det er høyest IKT-risiko knyttet til nettverksangrep, digital spionasje og kartlegging av infrastruktur fra statlige aktører.

IKT-risikobildet for den enkelte virksomheten avhenger av verdiene som befinner seg i virksomheten og hva virksomheten produserer eller leverer. Dersom virksomheten har verdier som kan stjeles og omsettes eller forårsake ødeleggelser, spesielt via internett, har den risiko. Store verdier trekker til seg flere og mer ressurssterke trusselaktører. Verdiene kan være teknologi, patenter, forretningshemmeligheter eller liknende som gjør at virksomheten stikker seg ut i mengden. Trusselaktører rammer i noen tilfeller små og mellomstore virksomheter for å bruke virksomhetenes systemer som infrastruktur i videre angrep eller fordi virksomheten er underleverandør eller tilknyttet interessante mål i et samfunns- eller statsperspektiv.

Volumet av forsøk på digitale tyverier mot virksomheter, eksempelvis i finanssektoren, er betydelig. NSM registrerer at mange kjente metoder brukes for å stjele verdier og utnytte sårbarheter.

E-post er den enkleste veien inn til virksomheten, og manipulerende svindelforsøk, som direktørsvindel, er vanlig. Utnyttelse av slike menneskelige sårbarheter utgjør en viktig del av risikobildet for virksomhetene.

For enkeltvirksomheter vurderer NSM at det er høyest IKT-risiko knyttet til digital kriminalitet, særlig fra aktører som er ute etter økonomiske verdier.

Det er sårbarhetene som i størst grad påvirker IKT-risikobildet. Verdiene i samfunnet er verdier fordi de utgjør en nødvendig funksjon. Sårbarhetene er avhengige av utvikling i både verdi og trussel. Nye sårbarheter oppstår og lukkes hele tiden. Trusselaktørene utvikler seg og utnytter stadig nye sårbarheter. Bildet er derfor i konstant utvikling.

DEL 2

TILTAK FOR HELHETLIG IKT-SIKKERHET

Norske virksomheter rammes daglig av uønskede sikkerhetshendelser, og kjente sårbarheter utnyttes stadig. NSM erfarer at mangelfull sikkerhetsstyring er en overordnet sårbarhet. Resultatet av dette er at det iverksettes sikringstiltak som ikke sees i sammenheng, noe som fører til utilstrekkelig grunnsikring.

Risikostyring og sikkerhet handler om en helhetlig tilnærming, der sikkerhetsarbeidet gjennomsyrer virksomheten fra ledelsen til IT-personell og ansatte generelt.

Hensikten med del 2 av rapporten er å gi virksomheter anbefalinger om hvordan de best kan redusere og håndtere egen IKT-risiko. NSM ønsker derfor å gi to tydelige budskap:

- Sikkerhet bør både være en del av virksomhetens strategi og løpende styring.
- Virksomheter bør implementere IKT-grunnsikring for å redusere et bredt spekter av sårbarheter.

Pilaren i en slik IKT-grunnsikring er helhetlig og langsiktig forvaltning av IKT-systemer. Utgangspunktet for en slik forvaltning er å etablere en sikker plattform. Denne må driftes og vedlikeholdes over tid og man bør ha evne til å håndtere hendelser, fra hendelsen oppstår til man er i stand til å gjenopprette en sikker tilstand.


9
11
13
15
17
19
18
20

7.

Sikkerhetsstyring

NSM har over flere år gjentatt at mangelfull sikkerhetsstyring hindrer tilfredsstillende sikring av norske virksomheter. Manglende ledelsesforankring og svak sikkerhetsstyring fører til at sikringen av informasjonssystemer ikke er tilstrekkelig. NSMs tilsyn viser at årlig sikkerhetsrevisjon av informasjonssystemer ofte er mangelfull, og i noen virksomheter er det heller ikke etablert rutiner eller praksis for dette. Det er grunn til å tro at dette også gjelder virksomheter utenfor sikkerhetsloven. En konsekvens er at mangler og sårbarheter som oppstår i informasjonssystemer, gis mulighet til å utvikle seg i stedet for at korrigerende sårbarhetsreduserende tiltak blir besluttet og iverksatt.

NSM har erfart at IT-avdelingen i virksomhetene ofte har implementert gode og fornuftige sikringstiltak, men at tiltakene ikke er forankret i virksomhetsledelsen. Ledelsen får dermed ikke anledning til å prioritere sikkerhetsarbeidet på en hensiktsmessig måte som en del av den løpende styringen av sin virksomhet. Samtidig erfarer NSM altfor ofte at tiltakene ikke er fokusert rundt verdiene i en virksomhet og at viktige elementer er utelatt fordi det ikke er lagt til grunn en helhetstankegang ved valg av tiltak. I verste fall kan tiltakene virke mot sin hensikt. Da sitter man igjen med spørsmålet: *«Tiltakene er riktig implementert, men er det de riktige tiltakene som er implementert?»*

NSM har fokusert på og kommunisert viktigheten av å implementere, som et minimum, fire effektive sikringstiltak mot dataangrep. Vi mener dette er hensiktsmessige tiltak, fordi de blokkerer inntil 90 prosent av kjente dataangrep og

NSMs fire effektive tiltak:

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

blant annet reduserer sårbarheter som er enkle for en trusselaktør å utnytte. Tiltakene er ikke nødvendigvis teknisk kompliserte eller vanskelig å forstå, men vår erfaring viser at de tidvis oppleves som vanskelige å etterleve i praksis.

Organiseringen av sikkerhetsarbeidet kan beskrives som et hierarki av forutsetninger som bør være på plass for å kunne implementere relevante sikringstiltak:

Forankring i ledelsen er en forutsetning for alt sikkerhetsarbeid. Det er avgjørende at lederen er inkludert i sikkerhetsarbeidet i alt fra prioriteringer og risikoforståelse til kontinuerlig forbedring. Forankringen må skje både oppover og nedover; oppover ved at virksomhetens medarbeidere fremmer forslag til anbefaling og nedover ved at ledelsen formidler beslutninger om for eksempel ambisjonsnivå.

Deretter følger kompetanse og ressurser, som er materialiseringen av ledelsesforankringen, og en sikkerhetspolicy som definerer sikkerhetsarbeidet i virksomheten. Forankring, forpliktelse og forståelse er tre sentrale begreper som danner grunnlag for å utarbeide og vedlikeholde en god sikkerhetspolicy.[77]

[77] NSM: *Veileder i sikkerhetsstyring.*

1) **Forankring:** Ledelsen må sette mål for sikkerhet, tildele nødvendige ressurser og evaluere sikkerhetstilstanden i virksomheten årlig. Basert på evalueringen kan ledelsen sette nye mål og ambisjoner for sikkerhetsarbeidet.
2) **Forpliktelse:** Virksomheten må forplikte seg ved å utvikle relevant sikkerhetsdokumentasjon med klare føringer for sikkerhetsarbeidet. Det må etableres en tydelig ansvarsfordeling og klare rapporteringslinjer for å sikre at alle oppgaver gjennomføres.
3) **Forståelse:** Det må arbeides kontinuerlig med å bevisstgjøre, motivere, øke forståelsen og heve kompetansen innen sikkerhet på alle nivåer i virksomheten.

Det er helt avgjørende at det settes av tilstrekkelige ressurser med hensiktsmessig kompetanse til å utforme og utøve sikkerheten i en virksomhet. Hva som er tilstrekkelig med ressurser og hvilke prioriteringer som er nødvendige, er en konkret vurdering i hver enkelt virksomhet. Sikkerhetsarbeidet bør inkludere hele organisasjonen fra prosesseiere, IT og strategi til de som har sikkerhet som hovedfokus.

Sikkerhetspolicyen er et strategisk dokument som må operasjonaliseres og omsettes til målbare krav. Policyen skal være avstemt mot øvrig virksomhetsstyring og strategisk plan og skal tydelig understøtte prioriterte oppdrag. Av en policy vil det fremgå at sikkerhetsarbeidets formål er å understøtte virksomhetens oppdrag, samtidig som eksterne krav og føringer ivaretas. Dette medfører behov for hensiktsmessige tiltak i normalsituasjonen, fleksibilitet til å håndtere ekstraordinære hendelser samt langsiktige vurderinger som tar høyde for endringer i risikobildet. Virksomheten må omsette sikkerhetskrav til konkrete rutiner tilpasset sitt oppdrag og gjennomføre kontinuerlig risikostyring, for å identifisere endrede eller nye sikkerhetsbehov. Med dette menes det å identifisere hvilke risikoer som kan aksepteres, deles, overføres eller reduseres. Der man må redusere en risiko, må tiltak identifiseres, besluttes, utformes, implementeres og evalueres.

For å forvalte denne helheten over tid må sikkerhetsarbeidet styres. Prosesser må etableres, roller og ansvar fordeles og arbeidet må kontinuerlig evalueres og forbedres. Sikkerhetsstyringen må integreres i virksomhetsstyringen på lik linje med andre områder virksomhetsledelsen følger opp. Når virksomheten gjennomfører risikovurderinger, må sikkerhetsdimensjonen være en del av dette. Sikkerhetsarbeidet har både en kontrollerende og en utøvende dimensjon. Den kontrollerende dimensjonen kan med fordel sees i sammenheng med andre interne kontrollfunksjoner/-oppgaver som utøves i virksomheten, slik at det å kontrollere sikkerheten ikke behandles annerledes enn andre virksomhetsområder.

NSM erfarer at flere og flere ledere setter sikkerhet på agendaen, og vi ser et økt fokus på sikkerhet i virksomhetene. Oppdraget gis til strategiske organisasjonsenheter, og en strategi etableres. Imidlertid erfarer vi altfor ofte at forankringen er på plass og at de strategiske prosessene eksisterer på papir, men ledelsen har ikke forstått at denne forankringen i praksis innebærer endring i prioriteter, endret funksjonalitet, endringer i organisasjon eller økte kostnader. Man utelukker flere steg i pyramiden og går altfor ofte rett på tiltak. Det medfører at tiltakene ikke er de riktige, og man kan ikke begrunne hvorfor de er der.

8.

Helhetlig sikkerhetstankegang og forvaltning

NSM anbefaler en helhetlig tilnærming til hvordan tiltak velges ut og implementeres for å beskytte risikoutsatte verdier. En slik helhetlig tilnærming bør omfatte tiltak som tar høyde for både tilsiktede og utilsiktede hendelser. Ofte forvaltes en virksomhets verdier i informasjonssystemer som er utsatt for kjente sårbarheter. Etter en risikovurdering kan virksomheten velge å akseptere situasjonen, men ofte vil det være behov for å iverksette tiltak for å redusere disse sårbarhetene. Det kan bety iverksettelse av nye tiltak eller forbedring av eksisterende tiltak.

Som nevnt i forrige kapittel må imidlertid utvelgelsen av tiltakene styres ved at de prioriteres, implementeres, evalueres og forankres. Alle trinnene i pyramiden må være på plass for at de riktige tiltakene implementeres, og det er sikkerhetsstyringen i virksomheten som ivaretar helheten i sikringsarbeidet. For enkelte virksomheter er sikkerhetsstyringen lovpålagt.

Virksomheter underlagt sikkerhetsloven må ha et styringssystem og internkontroll.[78] Alle offentlige virksomheter er også pålagt å ha internkontroll på informasjonssikkerhetsområdet.[79] Men virksomheter som ikke har et direkte lovkrav om å etablere et styringssystem for sikkerhet, bør likevel implementere det for å kunne beskytte de verdiene virksomheten forvalter.

Om man forvalter verdier som ved tap kan få konsekvens for staten (sikkerhetsgradert informasjon), et individ (eksempelvis personopplysninger) eller en virksomhet (konkurransedrivende informasjon) har man uansett en risiko som må håndteres.

For å sikre at de riktige tiltakene implementeres, anbefaler NSM å basere sikkerhetsarbeidet på anerkjente standarder. Som vist i pyramiden over er sikkerhetsstyringen grunnlaget for et godt tiltaksarbeid. Både NSMs og Difis veiledningsmateriale i sikkerhetsstyring og internkontroll er basert på ISO/IEC 27001:2013. En slik tilnærming vil stille krav til etablering, vedlikehold, implementering og kontinuerlig forbedring av et ledelsessystem for informasjonssikkerhet.[80]

Når det gjelder utforming av sikringstiltak, er ISO/IEC 27002:2013 en anerkjent og velprøvd industristandard innen informasjonssikkerhet basert på mønsterpraksis. Standarden er en del av ISO 27000-serien og knytter tiltakene opp mot virksomhetens risikostyring. I tillegg bør andre relevante standarder vurderes, spesielt der det finnes bransjespesifikke rammeverk. Et eksempel er NIST Cyber Security Framework som er rettet mot sikring av kritisk infrastruktur.

Hvilket modenhetsnivå virksomheten befinner seg på innen sikkerhetsstyring, påvirker hvordan det jobbes med tiltak. NSMs veileder i sikkerhetsstyring presenterer en modell for modenhetsnivå innenfor sikkerhetsstyring.[81] Modellen viser at modenheten øker i takt med lederforankring, ansvar og roller, dokumentasjon og systematisering som vist i tabellen under.

[78] Forskrift om sikkerhetsadministrasjon § 1-2

[79] http://internkontroll.infosikkerhet.difi.no/, lastet 2016-08-29

[80] ISO/IEC 27001:2013

[81] Se *Veileder i sikkerhetsstyring*, s. 26 («Capability Maturity Model Integration (CMMI)»).

Modenhet	**1. Brannslukking – Tilfeldig**	**2. Stykkevis og delt – Fragmentert**	**3. Ledelsesforankring – Formalisert**	**4. Risikostyring – Systematisert**	**5. Kontinuerlig forbedring og utvikling – Optimalisert**
Sikkerhetsstyring	• I etterkant • Ingen dokumentasjon	• Uklart skille mellom utøvende og kontrollerende oppgaver • Lite dokumentasjon	• Engasjert toppledelse • Sikkerhetsdokumentasjon er på plass og ansvar og roller er tydelige • Sikkerhetsstaben er etablert	• Kompetanse i virksomheten • I forkant (risikobasert) • Fanger opp endringer i risikobildet	• Bruker hele styringshjulet • Sikkerhet er integrert i virksomheten • Adferden gjenspeiler forståelse for at «Sikkerhet er alles ansvar»
	Tilfeldig	Fragmentert	Formalisert	Systematisert	Optimalisert

Virksomhetenes modenhet innen sikkerhetsstyring kan grovt deles i to kategorier:

- Virksomheter som har en ubevisst styring av det forebyggende sikkerhetsarbeidet befinner seg i intervallet 1-2. Disse virksomhetene har ofte gått rett på tiltakene, men mangler resten av hierarkiet i sikkerhetspyramiden.
- Virksomheter der ledelsen aktivt støtter opp om sikkerhetsarbeidet vil befinne seg på nivå 3 til 5.

Erfaringene fra NSMs tilsyn og Riksrevisjonens revisjoner viser at mange virksomheter befinner seg på modenhetsnivået «ledelsesforankring» eller lavere. Hvis man da ser tilbake på sikkerhetspyramiden, har virksomhetene forankringen på plass, men tiltakene hviler på ufullstendige eller fraværende forutsetninger.

Dette medfører at mange virksomheter ikke har en velfungerende risikobasert tilnærming til utvelgelse, implementering og vurdering av tiltak. Det gjør at modenheten til tiltak i virksomheten grovt kan deles inn i to kategorier som vil kreve ulik tilnærming til hvordan virksomheten jobber med sikringstiltak:

- Virksomheter som ikke har kompetanse om verdier, trusler og sårbarheter i egen virksomhet befinner seg i intervall 1 til 3.
- Virksomheter med kompetanse om verdier, trusler og sårbarheter i egen virksomhet kan gjennomføre risikovurdering og innføre hensiktsmessige sikringstiltak og befinner seg på intervall 4-5.

Hvordan en virksomhet bør arbeide med tiltak basert på modenhet kan eksemplifiseres med NSMs «Fire effektive tiltak mot dataangrep» og «Ti viktige tiltak mot dataangrep».[82] Alle ti tiltakene kan i hovedsak fordeles over de tre laveste modenhetsnivåene. Det betyr at det er helt grunnleggende tiltak som må på plass for å etablere seg på et modent sikkerhetsnivå. Samtidig vil man da, når man har implementert disse tiltakene og klatret opp til modenhetsnivået «risikostyring», kunne risikostyre seg vekk fra enkelte av disse tiltakene.

At etablerte mekanismer kan fjernes og virksomheten likevel kan bli værende på modenhetsnivået, virker selvmotsigende. Dette er mulig i og med at modenhetsnivået består både av menneskelige, organisatoriske og tekniske tiltak. Når organisasjonen har etablert tilfredsstillende risikostyring, kan man med kunnskap om verdi, sårbarheter og trusler ivareta dette på en adekvat måte og finne kompenserende og risikoreduserende tiltak. Det betyr at organisasjonens kunnskap og erfaring fra alle organisasjonens systemer gjør at man i enkelte systemer eller delsystemer kan vurdere å fravike ti viktige tiltak mot dataangrep.

NSMs rådgivningsmiljø anbefaler stadig virksomheter å innføre fire effektive og ti viktige tiltak mot dataangrep, men opplever ofte at tiltakene ikke er tilstrekkelig implementert. Dette understøttes av Riksrevisjonens funn. Virksomheter som ikke har innført tiltakene og begrunner det med at det er dyrt og vanskelig, vil fortsatt rådes om å prioritere disse tiltakene. Samtidig vil vi anbefale virksomheten å forbedre styringssystemet for sikkerhet. Dersom bedriften har gjennomført en vurdering av verdiene i organisasjonen, sikkerhetsmekanismene som

[82] NSM: S-02 *Ti viktige tiltak mot dataangrep.*

beskytter dem og kan begrunne fraværet av de grunnleggende tiltakene, kan NSM gå videre med rådgivning for mer avanserte sikkerhetsmekanismer, som kan implementeres i stedet for eller i tillegg til de ti rådene. I enkelte tilfeller kan det være mer skadelig for en virksomhet å følge rådene, eksempelvis ved å installere programvareoppdateringer på et utdatert system. Da er det viktig at virksomheten har et godt styringssystem for sikkerhet, slik at de gjør gode vurderinger. Eksempelvis kan virksomheten vurdere å implementere kompenserende tiltak eller investere i en helt ny infrastruktur.

NSM arbeider med et sett med tiltak basert på ISO/IEC 27002 som anbefales som minimum grunnsikring av et informasjonssystem. Eksempelvis vil NSMs ti effektive tiltak være inkludert i grunnsikringen. For virksomheter på modenhetsnivå 1 til 3 innen sikkerhetsstyring vil disse tiltakene kunne gi en tilfredsstillende grunnsikring mot et bredt spekter av sårbarheter. Neste kapittel omtaler de viktigste momentene i denne grunnsikringen.

For virksomheter med et høyere modenhetsnivå i sikkerhetsstyring og der forutsetningene for selv å arbeide med tiltak er tilstede, er anbefalingen å basere utvelgelsen av tiltak på sikkerhetsstandardene nevnt over. Selv med god risikostyring må de tiltakene som iverksettes sees i en sammenheng. Tiltak skal komplettere hverandre. Sikkerhet i dybden er en forutsetning for god sikring av informasjonssystemer der tiltakene er en kombinert løsning med deteksjonsmuligheter og barrierer i flere ledd, i tillegg til et reaksjonsapparat for å opprette normaltilstand når en hendelse inntreffer.

9.

Sikre informasjonssystemer

Sikring av et informasjonssystem er en aktivitet som bør pågå i hele systemets levetid. Etablering av gode prosesser for å ivareta sikkerheten over tid er en viktig del av sikkerhetsstyringen.

Etter NSMs vurdering er det like viktig at en løsning kan forvaltes på en hensiktsmessig måte som at den møter funksjonelle krav. Helhetlig forvaltning av IKT og IKT-sikkerhet innebærer blant annet bruk av løsninger hvor man gjenbruker sikkerhetsmekanismer på tvers av ulike plattformer, tjenester og applikasjoner. Det kan ofte være et problem at budsjetter ikke tar høyde for at enheter må skiftes ut, at det trengs personell for å drifte et stadig mer automatisert og komplekst system og at man må følge med på hvilke sårbarheter som må oppdateres.[83]

Følgende grunnprinsipper kan legges til grunn for en god forvaltning av et informasjonssystem:

- variantbegrensning – færrest mulig varianter av utstyr, leverandører, tjenester eller applikasjoner vil forenkle antallet som må oppdateres, vedlikeholdes eller oppgraderes.
- gjenbruk av både komponenter og sikkerhetsmekanismer
- felles systemer på tvers av plattformer, tjenester eller applikasjoner – eksempelvis felles brukerkonto og krypteringsfunksjonalitet
- konfigurasjonsstyring – forvalte utstyret over tid
- automatisering – konsolidere prosesser, redusere ressursbruk og sjansen for feil

Gjenbruk av mekanismer er viktig for å forenkle forvaltning, som utrulling, oppdatering, sikkerhetsoppdatering og informasjonsutveksling. NSM anbefaler at anerkjente standarder benyttes der disse eksisterer.

For å ivareta en god forvaltning er det en forutsetning å forstå hva informasjonssystemet faktisk består av. Det innebærer å ha oversikt over brukere, utstyr, tjenester og linjer. For å kunne oppdatere et informasjonssystem må virksomheten vite hva som er utdatert og må oppdateres. Det er viktig å være klar over at forvaltningen omfatter hele informasjonssystemet. Av utstyr skilles det ikke på om den fysiske enheten er en server, en klient (mobile og stasjonære) eller nettverkskomponent, men det kan være ulikt behov for hvordan enheten forvaltes. Tingenes internett, som i større grad bringes inn i virksomheters prosesser og infrastruktur, er ikke noe annet enn en type kategori av utstyr som må forvaltes.

Løsninger som kan oppgraderes og oppdateres må benyttes og rutiner og prosedyrer for oppdatering, endring og utvikling må etableres. Ved å gjenbruke mekanismer vil dette forenkles ved at færre ulike systemer for drift og vedlikehold må anskaffes. Applikasjoner og tjenester som benytter statiske komponenter, det vil si komponenter som ikke kan oppdateres, endres og utvikles, bør unngås.

I tillegg til tiltak som sikrer en god forvaltning, anbefaler NSM at tiltakene som utformes bør dekke tre hovedmål for informasjonssikkerhet[84]:

1) Etablering av en sikker plattform, en helhetlig og enhetlig IKT-infrastruktur, med en sikringstilstand med et akseptabelt risikonivå.
2) Sikker drift og vedlikehold av systemet innenfor den sikre tilstanden.
3) Sikker hendelseshåndtering og gjenoppretting ved sikkerhetstruende hendelser.

Neste kapittel vil diskutere utvalgte tiltaksområder NSM mener er viktige innen de ulike hovedmålene.

9.1 SIKKER PLATTFORM

Med sikker plattform menes det å etablere en helhetlig og enhetlig IKT-infrastruktur med nødvendige sikkerhetsfunksjoner, strukturer og tillitsnivå.[85] I tillegg til de teknologiske sikringstiltakene må det etableres rutiner og arbeidsprosesser for å forvalte løsningen over tid. Det innebærer å dokumentere en sikker tilstand, det vil si at sårbarheter for den sikre infrastrukturen reduseres til et akseptabelt nivå.

NSMs fire effektive tiltak mot dataangrep bør inngå i etablering av en sikker plattform. Disse tiltakene er ment å beskytte informasjonssystemer mot internettrelaterte angrep. I hovedsak er tiltakene rettet mot å sikre endepunktene i en

[83] Innspill fra NVE til *Helhetlig IKT-risikobilde 2016*.

[84] Forskrift om informasjonssikkerhet.

[85] Forskrift om informasjonssikkerhet.

kommunikasjon, det vil si klientmaskiner og servere. Dette er viktige tiltak, da flesteparten av angrepene rettes mot disse enhetene, og de er eksponert for et stort antall sårbarheter.

En forutsetning for systemteknisk sikkerhet er bruk av kryptografiske mekanismer. Mens man har dører, murer og segl for å sikre fysisk informasjon og objekter, benyttes autentisering, konfidensialitetsbeskyttelse og integritetsbeskyttelse for å sikre elektronisk informasjon.

Det er viktig at man har mekanismer som beskytter informasjonssystemet og informasjonen i dette fra vugge til grav. Kryptografiske mekanismer benyttes for begge, både for å sikre og verifisere at informasjonssystemet er i sikker tilstand og at informasjonen er autentisk og ikke lar seg kompromittere. Kryptering av lagrede og overførte data er nødvendig for dette, noe som innebærer blant annet krypterte harddisker, sikkerhetskopier og minnepinner i tillegg til sikker fjerntilgang og sikre nettsteder.[86]

Tekniske løsninger for beskyttelse er tilgjengelige på alle modenhetsnivåer, men forvaltningen og ressursbruken er svært forskjellig fra enkeltstående og brukerstyrte løsninger (nivå «tilfeldig» og «fragmentert» i modenhetsmodellen) til forvaltede og sentraliserte løsninger som gjenbruker den sikre plattformens tjenester (nivå «formalisert» og høyere). NSM anbefaler digitale sertifikater og policybasert offentlig nøkkelinfrastruktur for forvaltning av kryptonøkler (nivå «systematisert»). NSM har også anbefalinger for algoritmer og nøkkellengder som bør benyttes og tillitsnivået de kryptografiske løsningene bør inneha.[87]

NSMs fire effektive tiltak og bruk av kryptografiske mekanismer er bare to sentrale grupper med sikringstiltak som bør implementeres for å etablere en sikker plattform. NSM anbefaler at anerkjente standarder, eksempelvis ISO/IEC 27002:2013, legges til grunn når virksomheten vurderer hvilke sikringstiltak som er nødvendige. Vi anbefaler også at det benyttes evaluerte og sertifiserte teknologiske løsninger, eksempelvis gjennom Common Criteria.[88]

9.2 SIKKER DRIFT OG VEDLIKEHOLD

Målet for sikker drift og vedlikehold skal være å opprettholde og eventuelt forbedre sikkerhetsnivået definert i sikker plattform. For å oppnå dette anbefaler NSM virksomheten å etterleve anbefalingene som gis i ISO/IEC 27002:2013 samt tilpasse seg til ITIL-rammeverket der det er relevant.

Hvis disse anbefalingene følges, vil virksomheten kunne planlegge for og etablere nødvendig kompetanse, rutiner, policyer, prosesser og driftsarkitektur. Dersom dette skulle vise seg å være mangelfullt utført når produksjonen starter, vil det bli utfordrende å oppnå sikker drift og vedlikehold av informasjonssystemet. Erfaringsmessig har det å korrigere for disse manglene i etterkant ofte vist seg å være kostnadskrevende og forstyrrende for virksomhetens hovedaktiviteter.

For noen virksomheter (særlig de mindre) kan anbefalingen virke omfattende, men den kan tilpasses på mange måter. Det viktige er at tilpasningen skjer basert på virksomhetens behov og økonomiske muligheter. Ved å gjennomføre en risiko- og sårbarhetsanalyse for området sikker drift og vedlikehold vil virksomheten være i bedre stand til å avgjøre hvilke anbefalinger man bør prioritere. Samtidig er det viktig å påpeke at sikker drift og vedlikehold også vil gi betydelige gevinster for virksomheten gjennom høyere tilgjengelighet, større fleksibilitet og reduserte kostnader.

Dersom en virksomhet ser at grunnsikring ikke oppnås i den daglige driften, bør man vurdere å sette ut oppgaven til en profesjonell aktør underlagt de samme kravene som virksomheten selv. Med profesjonell menes at sikker drift og vedlikehold er operatørens primæroppgaver. Moderne drifts- og vedlikeholdsmodeller baserer

[86] NSM: *Prosjektrapport – HTTPS for offentlige nettsteder* https://www.nsm.stat.no/globalassets/rapporter/https.pdf

[87] Kortliste krav til krypto, https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/kortliste-kravkrypto1_0.pdf

[88] Se www.commoncriteriaportal.org

seg på at virksomhetene får sine behov levert fra eksterne driftsoperatører tilpasset virksomhetens sikkerhetsnivå. Dette fritar ikke virksomheten for ansvaret knyttet til sikker drift og vedlikehold, men innsatsen kan tilpasses avtalen som inngås.

Det antas at digitaliseringen i offentlig sektor[89] vil medføre en ytterligere konsolidering av dagens driftsmiljøer/-operatører samt at bruken av skytjenester vil øke. Sett fra virksomheten vil alle disse leveransene skje via driftsoperatøren som vil besørge at kravene til sikker drift og vedlikehold ivaretas sammen med helheten i brukeropplevelsen.

Driftsoperatøren har i teorien mange muligheter for å realisere sine leveranser både av infrastruktur, plattformer og programvare. Leveransene kan realiseres via egne datasentre, fra skyleverandører eller som hybridmodeller av disse. Ansvaret for at dette skjer i henhold til virksomhetens krav ligger hos virksomheten selv og må være avtaleregulert. Virksomheten må derfor inneha god nok kompetanse (eventuelt støttet av tredjeparter) til å kunne gjennomføre tilsyn, teknisk kontroll og revisjon av driftsoperatøren.

9.3 HENDELSESHÅNDTERING OG GJENOPPRETTING

Sikker hendelseshåndtering og gjenoppretting er en viktig del av informasjonssikkerhet. Dette innebærer at en hendelses karakter og omfang skal identifiseres, mottiltak iverksettes og informasjonssystemets sikre tilstand gjenopprettes. Det er vanlig å skille mellom tilsiktede og utilsiktede hendelser. Felles for begge kategorier av hendelser er at de vanligvis beskrives som en ikke-planlagt forstyrrelse eller forringelse av tjenestenivået til et IKT-system.

Industriell mønsterpraksis som ITIL og ISO/IEC 27001:2013 standardiserer hendelseshåndtering og gjenoppretting av normaltilstand som viktige prosesser med tilhørende sikringstiltak som må være på plass. NSM mener imidlertid at det er viktig å presisere at en hendelse ikke trenger å defineres kun ut fra om den er forstyrrende eller tjenestereduserende. NSM har erfart at tilsiktede sikkerhetshendelser (dataangrep) ikke trenger å medføre en forstyrrelse eller være tjenestereduserende på IKT-systemene. Konsekvensene kan likevel være svært alvorlige for virksomheten og kunder fordi kritisk informasjon kan komme på avveie.

Hendelseshåndtering og gjenoppretting kan inndeles i faser. Hver av fasene kan favne menneskelige, organisatoriske og tekniske tiltak.[90]

1) **Forberedelse og planlegging:** Få på plass intern prosedyre for håndtering av hendelser, inkludert rapportering, ansvarslinjer og eskaleringsrutiner. Etabler og sett av dedikerte ressurser til et hendelseshåndteringsteam og implementer tekniske støtteverktøy for både å oppdage og håndtere hendelser.
2) **Deteksjon og rapportering:** Tekniske sikkerhetsmekanismer benyttes i henhold til rutiner for deteksjon. Mulige hendelser («treff») rapporteres i henhold til etablerte rutiner. Eskalerings- og rapporteringsrutiner må følges.
3) **Evaluering:** Vurdere om det faktisk er snakk om en hendelse.
4) **Respons:** Hendelsen må analyseres og kontrolleres, skadeomfanget begrenses, årsaken til hendelsen elimineres og sikker drift reetableres.
5) **Lær av hendelsen:** Utover identifisering av selve hendelsen, bør det også være prosesser for å trekke lærdom som kan brukes for å forbedre egenkompetanse, bedre rutiner og intern organisering samt styrke tekniske sikringstiltak i virksomheten.

[89] KMD: *Digitaliseringsrundskrivet H-17/15*, datert 20.11.2015

[90] Hentet fra ISO/IEC 27035-1 som er under utvikling.

Vedlegg 1
Ordliste

Adgangskort
Plastkort som via magnetstripe, radiofrekvensgjenkjenning og/eller pinkode gir adgang til et fysisk område eller til bruk av utstyr.

Administrator (IKT)
Den eller de som drifter IKT-systemer for en virksomhet, som regel intern IKT-enhet.

Autentisering
Verifisere identiteten og andre egenskaper til en bruker. Sterk autentisering / to-faktor-autentisering = autentisering ved bruk av flere metoder, f.eks. minst to av pinkode, passord, fingeravtrykk.

Avanserte vedvarende trusler (Advanced Persistent Threats, APT)
Vedvarende og målrettet angrep på systemer med formål å etablere bakdører, plante og spre skadevare og hente ut fortrolig informasjon. Angriperen er gjerne ressurssterk, bruker avansert skadevare og opererer langsiktig. Også betegnelse på aktøren bak et slikt angrep.

Avvik
Brudd på bestemmelse i regelverk eller standard.

Bakdør
Skadevare som gir angriper uautorisert adgang til og mulighet til å kontrollere systemer.

Computer Emergency Response Team (CERT)
Koordinerende enhet for informasjonssikkerhet; ekspertgruppe som håndterer uønskede hendelser på internett.

Deteksjon
Tekniske indikasjoner på angrep på IKT-system.

Difi
Direktoratet for forvaltning og IKT

Digital spionasje
Spionasje ved hjelp av IKT-utstyr, særlig via internett.

DSB
Direktorat for samfunnssikkerhet og beredskap

ENISA
European Union Agency for Network and Information Security. Den europeiske etaten for nettverks- og informasjonssikkerhet.

EOS
Etterretning, Overvåking, Sikkerhet

FD
Forsvarsdepartementet

FinansCERT
CERT for finanssektoren.

Fjerntilgang
Tilgang til et ikke-offentlig IKT-system for autorisert bruker via internett.

Forebyggende sikkerhet
Policyområde for tiltak for å forhindre sikkerhetstruende hendelser.

Grunnsikring
Sikkerhetstiltak som er iverksatt i normalsituasjonen, med grunnlag i verdivurdering.

Hacker
Person som på ulovlig vis forsøker å kompromittere et datasystems sikkerhet.

Hacktivisme
Politisk motivert hacking.

Helhetlig IKT-risikobilde 2015
Ugradert rapport, årlig rutine (første utgave).

Hendelseshåndtering
Policyområde for tiltak for å håndtere oppståtte sikkerhetstruende hendelser, særlig på IKT-området.

Identitetstyveri
Når noen anskaffer, overfører, besitter eller fremstår som rette innehaver av personlige opplysninger tilhørende en privatperson eller virksomhet på en uautorisert måte, med den hensikt å begå bedrageri eller annen kriminalitet.

IKT
Informasjons- og kommunikasjonsteknologi. Teknologi for innsamling, lagring, behandling, overføring og presentasjon av informasjon over elektronisk medium.

IKT-sikkerhet
Tiltak for å sikre blant annet konfidensialitet, tilgjengelighet og integritet med hensyn til informasjon som behandles eller lagres på IKT-systemer.

Informasjonssikkerhet
Policyområde for å sikre blant annet konfidensialitet, tilgjengelighet og integritet med hensyn til informasjon, blant annet i henhold til sikkerhetsloven. Det finnes flere regimer på dette.

Innsider, innsideaktør
Individ eller gruppe innen en virksomhet som forårsaker (IKT-)sikkerhetshendelser innenfra.

Inntrengingstest (penetrasjonstest, PENTEST)
Kontrollert forsøk på å trenge inn i et datasystem eller nettverk for å identifisere svake punkter i sikkerheten, med teknikker som i et reelt angrep. Gjennomføres av NSM med begrensninger som anført i sikkerhetslovens § 15.

Integritet
Pålitelighet. Korrekt, komplett, betimelig, autorisert. At informasjonen ikke blir endret i forhold til hva den skal være.

JD
Justis- og beredskapsdepartementet

KMD
Kommunal- og moderniseringsdepartementet

Kompetanse
Her: kompetanse som muliggjør forebyggende sikkerhet og hendelseshåndtering.

Konfidensialitet
At kun de som skal ha tilgang, får tilgang.

Konsekvens
NS 5814:2008, Mulig følge av en uønsket hendelse.

KraftCERT
CERT for kraftsektoren.

KRIPOS
Kriminalpolitisentralen (nasjonal etterforskningsressurs).

Kritisk infrastruktur
System og struktur for fysisk leveranse av grunnleggende tjenester som kraft, kommunikasjon eller vann.

Kritisk samfunnsfunksjon
Tjenester som befolkningen er avhengig av for liv og velferd, som lov og orden, vareforsyning eller samfunnsledelse.

Kryptering
Koding av informasjon slik at den blir uleselig for uvedkommende.

Lederforankring
Det at virksomhetsleder har eierskap til sikkerhetsarbeidet, setter målsetninger og etterspør resultater.

Løsepengevirus (ransomware)
Løsepengevirus låser alle eller noen filer på ofrenes PC med sterk kryptering. Ofrene får krav om å betale løsepenger for å låse opp innholdet.

Maskinvare (hardware)
Fysiske komponenter i datamaskiner.

Mykvare (software)
Program, programvare i datamaskiner.

Nettverksoperasjoner
Dataangrep, datainnbrudd via internett.

NorCERT
Funksjon i NSM; nasjonal CERT.

Norsk Standard 5830:2012
Norsk standard som gir terminologi beregnet på risikovurdering av uønskede handlinger.

NSM
Nasjonal sikkerhetsmyndighet (cybersikkerhet, objektsikkerhet, personellsikkerhet).

Objektsikkerhet
Policyområde for å sikre fysiske objekter i henhold til sikkerhetsloven. Det finnes også andre regimer for dette.

Oppdatering
Regelmessig fornyelse av IKT-programvare, særlig for å tette sikkerhetsmessige tekniske sårbarheter.

Passordadministrasjon
Rutine for å sikre at passord til blant annet IKT-systemer byttes med jevne mellomrom og er av tilstrekkelig kvalitet.

Patche
«Lappe», oppdatere/reparere programvare, ofte regelmessig rutine ved hjelp av oppdateringer fra systemleverandør.

Personellsikkerhet
Policyområde innen forebyggende sikkerhet som skal sikre at uegnede personer ikke får tilgang til sikkerhetsgradert informasjon.

Phishing
Det å gi seg ut for å være en annen og i denne forkledning be en person om opplysninger for å kunne plante skadevare. Personens tillit til den originale avsenderen blir forsøkt utnyttet. Se spear phishing.

PST
Politiets sikkerhetstjeneste (innenlands-etterretning).

Risiko
NS 5830:2012 Uttrykk for forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifiserte trusselen.

Risikoaksept
Aksept av restrisiko etter at risikoreduserende tiltak er gjennomført.

Risikobilde
NS 5830:2012 En tidsavgrenset beskrivelse av en entitets risiko. Innen forebyggende sikkerhet utgjør risikobildet en samlet vurdering av samfunnets verdier, truslene mot disse og sårbarheter som eksisterer i forhold til truslene.

Sannsynlighet
De vanligste definisjonene av sannsynlighet er frekvensbaserte, det vil si at antallet hendelser over en viss tid fremskrives som en sannsynlig fremtidig trend. Når det gjelder trusler, det vil si uønskede, tilsiktede handlinger, kan det være vanskelig å etablere trender. En alternativ definisjon er sannsynlighet basert på kvalitativ kunnskap. Synonymer til sannsynlig blir da mulig eller trolig. Jf Etterretningsdoktrinens bruk av dette begrepet.

SCADA
Supervisory Control And Data Acquisition. System eller nettverk som brukes til å kontrollere (industrielle) prosesser eller infrastrukturer.

Sikkerhetsbrudd
Avvik fra sikkerhetslovens regelverk.

Sikkerhetsdokumentasjon
Virksomhetens dokumentasjon av egne sikkerhetstiltak.

Sikkerhetsrevisjon
Virksomhetens interne revisjon av (styringen av) eget sikkerhetsarbeid.

Sikkerhetsstyring
Virksomhetens styring av eget sikkerhetsarbeid.

Sikkerhetstruende hendelse
Hendelse som truer en verdi, uansett om årsaken er handling fra trusselaktør eller et sikkerhetsbrudd i virksomheten.

Skadevare (Malware)
Skadelig programvare, f.eks. virus eller trojaner.

Skadevareanalyse
Analyse av det tekniske innholdet i skadevare.

Skytjeneste, nettskytjeneste (Cloud computing)
Distribuert databehandling via et nettverk. Mulighet for å kjøre program på mange sammenknyttede servere. Skytjenester kan være både private og offentlige, eller en blanding av disse. Brukes ulikt av ulike leverandører, leveres via internett.

Sluttbruker (IKT)
Den vanlige brukeren av IKT-utstyr i en virksomhet.

Sosial manipulering (social engineering)
Angrepsteknikk som unytter menneskelige sårbarheter som nysgjerrighet, tillit eller grådighet for å få tak i sensitiv informasjon eller påvirke offerets handlinger.

Spam
Uoppfordret / uønsket e-post med reklame.

Spear phishing
Se phishing; målrettet mot spesielle personer, ofte med unik skadevare.

SSB
Statistisk sentralbyrå

Sårbarhet
NS 5830:2012 Manglende evne til å motstå en uønsket hendelse eller opprette ny stabil tilstand dersom en verdi er utsatt for uønsket påvirkning.

Tilgjengelighet
At informasjon er tilgjengelig for rettmessig bruker når det er behov for det.

Tilsyn, NSM
Tilsyn med sikkerhetslovens regelverk.

Tingenes internett (Internet of things, IoT)
Om det fenomen at gjenstander inneholder datamaskiner, eventuelt sensorer, og kan kommunisere over internett.

Tjenestenekt-angrep (DoS, DDoS)
Et internettangrep som overbelaster en server ved at stor trafikk rettes mot serveren, gjerne ved bruk av et botnet. Hensikten er å hindre normal tilgang fra ordinære brukere.

Trussel
NS 5830:2012 Mulig uønsket handling som kan gi en negativ konsekvens for en entitets sikkerhet.

Trusselaktør
NS 5830:2012 En kjent eller ukjent entitet som forbindes med en trussel.

Verdi
NS 5830:2012 Ressurs som hvis den blir utsatt for en uønsket påvirkning vil utgjøre en negativ konsekvens for den som forvalter eller drar fordel av ressursen.

Verdivurdering
Virksomhets vurdering av hvilke verdier den har som har sikkerhetsmessig betydning.

Virus
Skadevare (program) som infiserer andre programmer og reproduserer seg selv.


Spor
Track 15-19
Buss for tog
Bus for train
Toaletter
Toilets
Operaen
Opera House
Spor
Track 13-14
Utgang syd
Exit south
TAXI
Flytogterminalen
Airport Express Train
Bagasjeoppbevaring
Luggage lockers

Vedlegg 2
Litteraturliste

Booz Allen Hamilton, *Industrial Cybersecurity Threat Briefing*. http://www.boozallen.com/content/dam/boozallen/documents/Viewpoints/2016/06/industrial-cybersecurity-threat-briefing.pdf?elqTrackId=2da38e620e83443ebe4051c95018ecbf&elq=be589e226e9f4028850dafcd1b50862e&elqat=1&elqCampaignId=

Bundesamt für Sicherheit in der Informationstechnik (BSI). (2015). *Die Lage der IT-Sicherheit in Deutschland 2015*.

Direktoratet for samfunnssikkerhet og beredskap (DSB). (2012). *«Sikkerhet i kritisk infrastruktur og kritiske samfunnsfunksjoner – modell for overordnet risikostyring»*, KIKS-prosjektet – 1. delrapport 2012.

Direktoratet for forvaltning og IKT ((Difi): http://internkontroll.infosikkerhet.difi.no/, lastet 2016-08-29

Direktoratet for økonomistyring (DFØ). (2013). *Veileder i internkontroll*.

Etterretningstjenesten. (2016). *FOKUS 2016: Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer*.

European Network and Information Security Agency (ENISA). (2015). *Annual Incidents Reports 2014*.

European Network and Information Security Agency (ENISA). (2014). *Threat Landscape 2014, Overview of current and emerging cyber-threats*.

FBI, www.fbi.gov/contact-us/field-offices/phoenix/news/press-releases/fbi-warns-of-dramatic-increase-in-business-e-mail-scams - Publisert 2016-04-04.

Finanstilsynet. (2016). *Finansforetakenes bruk av informasjons- og kommunikasjonsteknologi (IKT), Risiko- og sårbarhetsanalyse 2015*.

Forskrift om informasjonssikkerhet
Forskrift om sikkerhetsadministrasjon
HM Government. (2015). *2015 Information Security Breaches Survey*.

IBM Security. (2015). *IBM 2015 Cyber Security Intelligence Index*

ISO/IEC 27001:2013 Information Technology – Security Techniques – Information Security Management Systems – Requirements

ISO/IEC 27002:2013 Information Technology – Security Techniques – Code of Practice for Information Security Management.

ISO/IEC 27035-1 ... (er under utvikling)

Kommunal- og moderniseringsdepartementet (KMD). (2015). *Digitaliseringsrundskrivet nr. H-17/15*, datert 20.11.2015

Kommunal- og moderniseringsdepartementet (KMD). (2016). *Nasjonal strategi for bruk av skytjenester*.

Kripos. (2016). *Trendrapport 2016, Organisert og annen alvorlig kriminalitet i Norge*.

KS, FoU-prosjekt 144008 (2015), Utredning av juridiske forhold ved bruk av nettsky i kommunal sektor – en mulighetsstudie. Føyen Thorkildsen Advokatfirma.

McAfee Labs. (2016). *2016 Threat Predictions*.

Microsoft Security Intelligence Report, Volume 18 | July through December 2014 *Regional threat assessment*.

Microsoft Security Intelligence Report, Volume 20 | July through December 2015 *Norway*.

The NIST Definition of Cloud Computing, National Institute of Standards and Technology, Special Publication 800-145.

National Cyber Security Centre. (2015). *Cyber Security Assessment Netherlands*, 2015, CSAN-5.

Nasjonal kommunikasjonsmyndighet (Nkom). (2016). *EkomROS 2016. Risikovurdering av ekomsektoren.*

norsis.no/oppblomstring-av-direktor-svindel-panettet/ - Publisert 2016-06-23, lastet 2016-08-20.

Norsk Standard NS 5830:2012 Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger. Terminologi.

Norsk Standard NS 5832:2014 Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger. Krav til sikringsrisikoanalyse.

NOU 2015:13 (2015). *Digital sårbarhet – sikkert samfunn. Beskytte enkeltmennesker og samfunn i en digitalisert verden.*

NSM. (2016). *Håndbok: Risikovurdering for sikring.*

NSM. (2016) *Kortliste krav til krypto*, https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/kortliste-kravkrypto1_0.pdf

NSM (2016). *Prosjektrapport – HTTPS for offentlige nettsteder* https://www.nsm.stat.no/globalassets/rapporter/https.pdf

NSM (2015). *Sikkerhetsfaglig råd.*

NSM (2015). *Veileder i sikkerhetsstyring.*

NSM (2016). Sjekkliste nr. 2, *Ti viktige tiltak mot dataangrep.*

NSM (2009). *Veiledning i verdivurdering.*

Næringslivets sikkerhetsråd. (2015). KRISINO 2015. *Kriminalitets- og sikkerhetsundersøkelsen i Norge.*

Politiets sikkerhetstjeneste (PST). (2016). *Trusselvurdering 2016.*

RAND Corporation, National Security Research Division (2014). *Markets for Cybercrime Tools and Stolen Data. Hackers' Bazaar.*

Statistisk sentralbyrå (SSB), Statistikkbanken, Bruk av IKT i næringslivet, diverse tabeller.

Statistisk sentralbyrå (SSB), Statistikkbanken, Bruk av IKT i næringslivet, Tabell 10641: Private føretak. Kjøper nettskytenester, etter teneste og mengd sysselsette (prosent). (oppdatert 2015)

Statistisk sentralbyrå (SSB), Statistikkbanken, Bruk av IKT i næringslivet, Tabell 10970: Private føretak. Internettilknytning etter beste teknologi, etter mengd sysselsette (prosent).

Statistisk sentralbyrå (SSB), Statistikkbanken, Bruk av IKT i næringslivet, Tabell 10974: Private føretak. Elektronisk handel, etter mengd sysselsette (prosent).

Statistisk sentralbyrå (SSB), Statistikkbanken, Bruk av IKT i staten, diverse tabeller.

Statistisk sentralbyrå (SSB), Statistikkbanken: Bruk av IKT i staten, Tabell 10609: Statlige virksomheter. Bruk av nettskytjenester, etter type og sysselsettingsgruppe (prosent).

Verizon (2016). *2016 Data Breach Investigations Report.*

World Economic Forum/Cornell University/INSEAD (eds.). (2015). *The Global Information Technology Report 2015.*

World Economic Forum/Cornell University/INSEAD (eds.). (2016). *The Global Information Technology Report 2016.*

Økokrim, www.okokrim.no/artikler/social-engineering-fraud-ceo – Publisert (oppdatert) 2016-03-07, lastet 2016-09-01.

NASJONAL SIKKERHETSMYNDIGHET

Postboks 814, 1306 Sandvika

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