NASJONAL
SIKKERHETSMYNDIGHET

Et sikkert digitalt Norge – IKT-risikobilde 2018

NSM har de tre siste årene gitt ut rapporten **Helhetlig IKT-risikobilde**. Denne skal bidra til å øke bevissthet og motivere for bedre IKT-sikkerhet i offentlige og private virksomheter. Rapporten henvender seg til ledere og personell med sikkerhetsoppgaver i alle sektorer. Årets rapport tar for seg et utvalgt tema: Risikobildet med tanke på digitaliseringen som pågår i det norske samfunnet.

Digitalisering og IKT er en suksessfaktor for videreutvikling av det norske samfunnet, samtidig som det gjøres feil som medfører at den digitale risikoen øker. I rapporten belyser NSM utfordringer med digitaliseringen og trekker fram noen tiltak som vil bidra til et sikkert digitalt Norge. Rapporten tar særlig for seg sikkerhet med tanke på uønskede hendelser som skyldes bevisste, ondsinnede handlinger, men omhandler også sikkerhetsrisiko som følge av utilsiktede feil, ulykker og tilfeldige hendelser.

Innhold

004 **Oppsummering**

006 **1 – Digitale muligheter**

008 **2 – Digitale verdier, digitale trusler**
009 2.1 Flere digitale verdier å passe på
009 2.2 Profesjonelle og målrettede trusselaktører
010 2.3 Operasjoner mot norske mål

012 **3 – Slik gjør vi Norge sikrere**
014 3.1 Sikkerhet er et lederansvar
016 3.2 En moderne og ryddig IKT-portefølje
017 3.3 Større profesjonelle IKT-miljø
018 3.4 Sikker tjenesteutsetting
020 3.5 God sikkerhetsarkitektur og økt automatisering
022 3.6 Hjelp sluttbrukeren

Oppsummering

Over hele verden erstattes nå manuelle metoder av digitale prosesser og automatisering. Denne digitaliseringen bidrar til å øke produktiviteten i både privat og offentlig sektor. Norge er et modent digitalt marked, og regjeringen påpeker at vi må utnytte mulighetene IKT og digitaliseringen gir oss for å kunne nå de høye ambisjonene myndighetene har på området. Staten tar blant annet initiativ til å øke digitaliseringen av arbeidsprosesser, gjenbruke data på tvers av virksomheter og samle tjenester i større nasjonale felles IKT-miljøer.

Dagens digitale verden er mer kompleks på mange områder. IKT-miljøene våre består av både nye og gamle systemer basert på ulik teknologi som til enhver tid må fungere sammen. Verdikjeder blir lengre og mer uoversiktlige. Når flere tjenester blir satt ut øker avhengighetene til underleverandørene og mer av virksomhetens systemer eksponeres på nett. Ny teknologi introduseres forløpende og endringer skjer stadig hurtigere.

Denne kompleksiteten kommer ikke uten sikkerhetsutfordringer. Nasjonal sikkerhetsmyndighet (NSM) ser at den digitale risikoen øker. Det er flere verdier som skal passes på, og vi utfordres av profesjonelle og målrettede trusselaktører. Samtidig øker antall sårbarheter i samfunnet og hos norske virksomheter. For virksomheter som arbeider systematisk og godt med sikkerhet, vil digitalisering allikevel kunne gjennomføres med akseptabel risiko.

Sikkerhetsarbeidet krever stadig større innsats i alle deler av virksomheten, men det er mulig å forbedre sikkerheten med noen sentrale grep:

- Kompetanse innen IKT og IKT-sikkerhet må prioriteres i alle virksomheter.
- IKT-sikkerhet må adresseres systematisk på alle nivåer i virksomheten. Ledelsen må prioritere sikkerhet og sørge for at virksomheten gjennomfører risikovurderinger og følger anerkjente rammeverk, som NSMs *Grunnprinsipper for IKT-sikkerhet*.
- Virksomheten må ha en moderne, oppdatert og ryddig IKT-portefølje.
- IKT-miljøet til virksomheten må være tilpasset og profesjonelt for å levere nødvendige tjenester.
- Sikkerhet må være en naturlig del av tjenesteutsetting gjennom hele tjenestens livsløpet.
- Virksomheter må få på plass en god IKT-arkitektur og automatisere sikkerhetsarbeidet.
- Sluttbrukere må tilbys løsninger som fjerner eller reduserer risiko for brukerfeil.

Både som privatpersoner og ansatte i offentlige og private virksomheter er vi avhengige av sikre IKT-systemer. Samtidig er IKT-systemene avhengige av at myndighetene digitaliserer, regulerer, fører tilsyn med og hjelper norske virksomheter med å fokusere på sikkerhet og jobbe systematisk med risiko. Vi har alle et ansvar for å være oppdatert og bruke hodet når vi er på nett. Norge som nasjon har alle forutsetninger for å bli best i klassen på IKT-sikkerhet, og det må være vårt felles mål.

1. Digitale muligheter

I flere tiår har globalisering, automatisering og teknologiutvikling formet det komplekse, digitale samfunnet vi har i dag. Det offentlige Norge går gjennom en stor digitaliseringsprosess. Tjenester blir fortløpende gjort tilgjengelig på nett, blant annet innen helsesektoren og NAV. Digitaliseringen går også raskt i den kritiske infrastrukturen, for eksempel innen samferdsel og kraftsektoren, med mer effektive trafikksentraler og smarte strømmålere.

Norske bedrifter digitaliserer stadig flere arbeidsprosesser, tjenester og funksjoner. De digitale verdikjedene i samfunnet vokser. Kontanter forsvinner fra lommeboken. Isteden betaler vi venner, lokale arrangementer og varer i gårdsbutikken med mobiltelefonen. Dagligvarer selges på nett, forbrukerprodukter blir mer intelligente og industriell produksjon strømlinjeformes. Digitalisering er i mange tilfeller nødvendig for en virksomhets effektivitet og i ytterste konsekvens dens eksistens. Samtidig er det en utfordrende prosess som krever riktig kompetanse og ressurser.

Teknologiutviklingen skaper nye muligheter. Trender som kunstig intelligens og automatisering er ikke bare med på å skape nye tjenester, men også et sikrere samfunn. Ny og oppdatert teknologi legger grunnlaget for nye tjenester og er ofte sikrere enn eldre teknologi.

Bedre funksjonalitet og en moderne IKT-arkitektur kan bidra til kvalitet og effektivitet i sikkerhetsarbeidet. I tillegg gir ny sikkerhetsteknologi bedre beskyttelse og avdekker flere angrep. Digitale kommunikasjonsløsninger kan gi bedre støtte i krise og beredskapsarbeid.

Når virksomheter digitaliserer sentrale arbeidsprosesser går IKT fra å være et støtteverktøy til å bli en fundamental del av virksomhetens operasjon. En vellykket digitalisering kan gi gevinster innen effektivisering og kostnadsbesparelser, men fallhøyden er stor hvis løsningene ikke leverer tilstrekkelig funksjonalitet eller sikkerhet. Med digitaliserte verdikjeder har virksomheten ingen manuelle metoder å gå tilbake til, og avhengigheten til IKT-systemene vil øke.

Et uforutsigbart digitalt rom kan medføre at både forbrukere og virksomheter stiller større krav til sikkerhet. God sikkerhet er en forutsetning for tillit til tjenester og funksjonalitet. Dette skaper nye muligheter for norske virksomheter. Norge er en trygg, pålitelig og stabil nasjon vurdert mot kriterier som statlig styring, IKT-sikkerhet, IKT-infrastruktur, kompetanse og forretningsstabilitet. Vi har gode rammebetingelser for å levere sikre IKT-tjenester, inkludert plassering av internasjonale datasentre med vår billige strøm og vårt milde klima.

«I flere tiår har globalisering, automatisering og teknologiutvikling formet det komplekse, digitale samfunnet vi har i dag.»

2. Digitale verdier, digitale trusler

Det norske samfunnet er avhengig av IKT. Den pågående digitaliseringen skaper stadig flere digitale verdier som eksponeres for trusselaktører som operer i det digitale rom. Digitale tjenester og funksjoner må sikres for å kunne ivareta tilgjengelighet, integritet og konfidensialitet.

2.1 Flere digitale verdier å passe på

Vi legger nå flere av de viktigste verdiene våre i det digitale rom. Den digitale identiteten til norske borgere befinner seg i ulike tjenester bygget på skyteknologi, enkelt tilgjengelig via mobile enheter. Det samme gjelder de digitale verdiene til norske virksomheter. Nesten all kommunikasjon og arkivering gjøres elektronisk, og verdifulle prosesser og forretnings-hemmeligheter eksisterer kun digitalt. Beskyttelse av intellektuelle rettigheter er livsnødvendig for mange høyteknologibedrifter.

«Vi legger nå flere av de viktigste verdiene våre i det digitale rom.»

Det offentlige forvalter nå i stor grad digitale data, inkludert sensitive data som må beskyttes mot uautorisert innsyn. Kritisk infrastruktur baserer seg i økende grad på bruk av digitale data og automatisering og er avhengig av sikre, robuste og alltid tilgjengelige IKT-tjenester.

Digitale løsninger blir mer komplekse når nye og eldre systemer kobles sammen på tvers av virksomheter, leverandører, sektorer og land. Samfunnsfunksjonene våre har blitt avhengige av lange og uoversiktlige, digitale verdikjeder. Dette medfører at dårlig sikrede IKT-systemer, som ikke var viktige i går, blir de svake leddene i en lengre verdikjede.

Med digitaliseringen kommer også nytt lovverk med ny nasjonal sikkerhetslov, ny person-opplysningslov som implementerer en ny europeisk personvernforordning (GDPR), og sektorvise regelverk.

2.2 Profesjonelle og målrettede trusselaktører

Fremmestatlig etterretningsaktivitet mot offentlige og private virksomheter samt datakriminalitet utgjør fortsatt de fremste digitale truslene mot det norske samfunnet i 2018. Digitalisering og globalisering fører til at flere enkeltpersoner, virksomheter og samfunnsfunksjoner er sårbare overfor digitale angrep og hendelser. Alle kan bli offer for økonomisk kriminalitet og destruktiv skadevare eller bli indirekte skadet som følge av målrettede angrep mot enkelte virksomheter og bransjer.

Fremdeles er politiske, militære og økonomiske mål samt virksomheter innen forsvarsindustri, høyteknologi og kritisk infrastruktur særlig utsatt. Vi ser allikevel at både målrettede og ikke-målrettede digitale angrep treffer bredere enn tiltenkt. De som ikke har beskyttet seg må forvente å bli rammet.

Nasjonal sikkerhetsmyndighet og andre parter i FCKS; Politiets sikkerhetstjeneste, Etterretnings-tjenesten og Kripos, ser et jevnt trykk av nettverksbaserte etterretningsoperasjoner fra statlige eller statstilknyttede aktører mot norske myndigheter og virksomheter.

«NSM er kjent med at trusselaktører kompromitterer IKT-systemene til tilfeldige norske virksomheter for å etablere kommando- og kontrollservere i Norge.»

Ettersom penger og andre verdipapirer blir digitale ser politiet at økonomisk kriminalitet oftere blir utført av internasjonale, kriminelle miljøer ved hjelp av digitale verktøy. I mange tilfeller er angrepene heldigitaliserte. Norske virksomheter blir svindlet for millionbeløp på nett, og nettbanksvindel, kredittkortsvindel og identitetstyverier rammer oss som privatpersoner. Alt fra IoT-enheter til kritiske servere blir brukt til uautorisert utvinning av kryptovaluta. Utvalget av sofistikerte digitale angrepsverktøy er viktige drivkrefter bak fjorårets globale løsepengekampanjer og stadig mer omfangsrike tjenestenektangrep. NSM forventer flere og mer avanserte krypterings- og løsepenge-kampanjer i tiden fremover.

Flere virksomheter og enkeltpersoner benytter krypteringsløsninger for å beskytte lagrede data og digital kommunikasjon. NSM forventer at trusselaktører oftere vil angripe de endepunktene som behandler de ukrypterte dataene. Krypterte data skaper også utfordringer ved etterforskning av straffesaker med elektroniske spor.

2.3 Operasjoner mot norske mål

NSM har registrert ulike typer operasjoner mot norske mål og interesser i 2018, inkludert vedvarende, målrettede etterretningsoperasjoner. Disse kan grovt deles inn i: rekognosering og kartlegging, kompromittering av infrastruktur (herunder uautorisert tilgang til data og informasjon) og opprettelse av kommando- og kontrollservere i Norge.

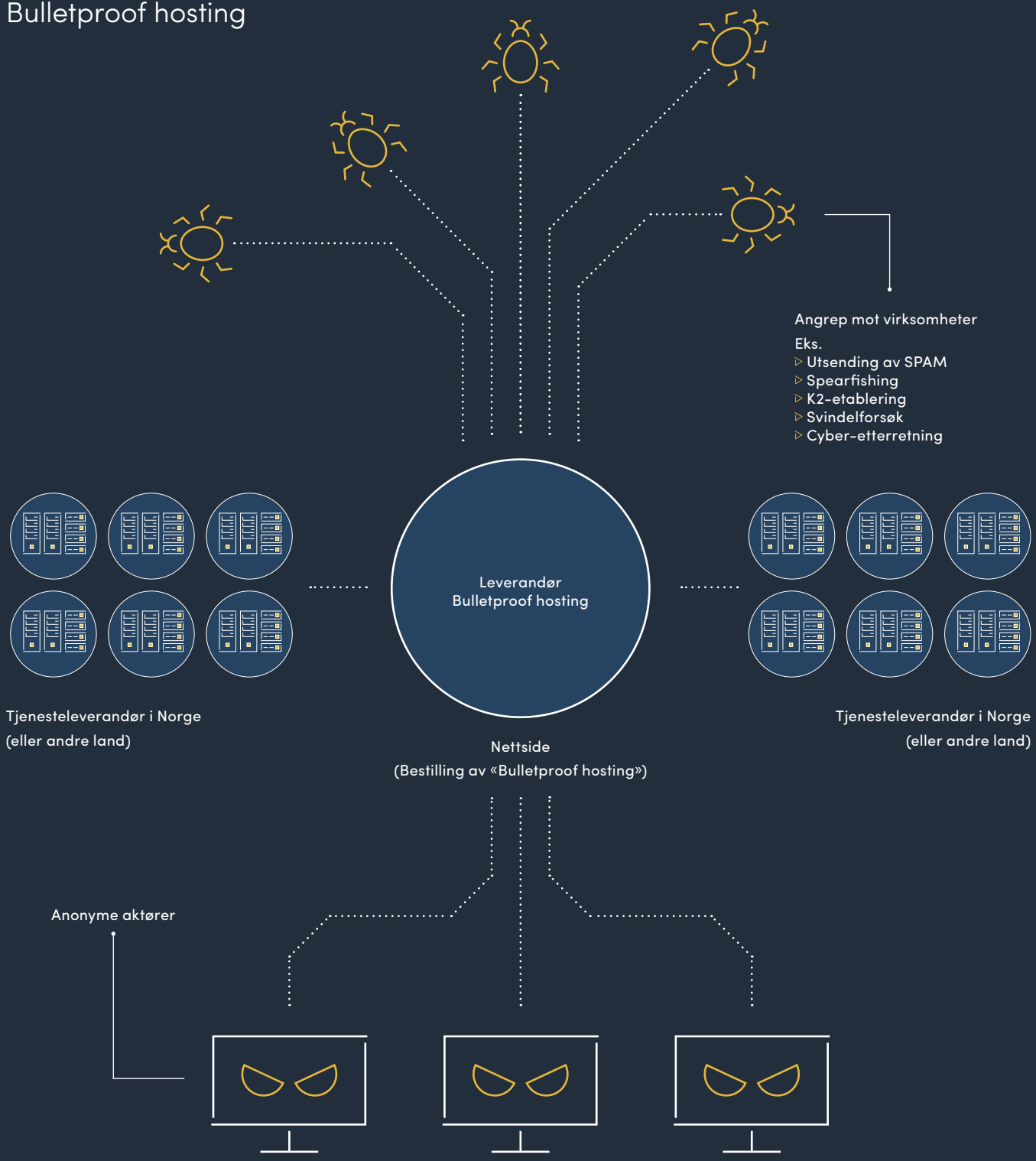
Rekognosering og sårbarhetskartlegging utføres som et forberedende steg til senere operasjoner. Dette innebærer normalt bruk av åpne kilder samt skanning og analyse av eksponerte tjenester.

Virksomhetens infrastruktur kan så bli forsøkt kompromittert for å få tilgang til data og informasjon eller for å få fotfeste i virksomhetens infrastruktur. En angriper vil typisk enten utnytte sårbarheter i eksponerte tjenester eller introdusere skadevare, for eksempel gjennom e-post. I tillegg observerer NSM operasjoner mot tjenesteleverandører i stedet for direkte angrep mot hovedmålet. Disse virksomhetene kan ha svakere sikkerhet og utnyttes bevisst som inngang til hovedmålets systemer og nettverk.

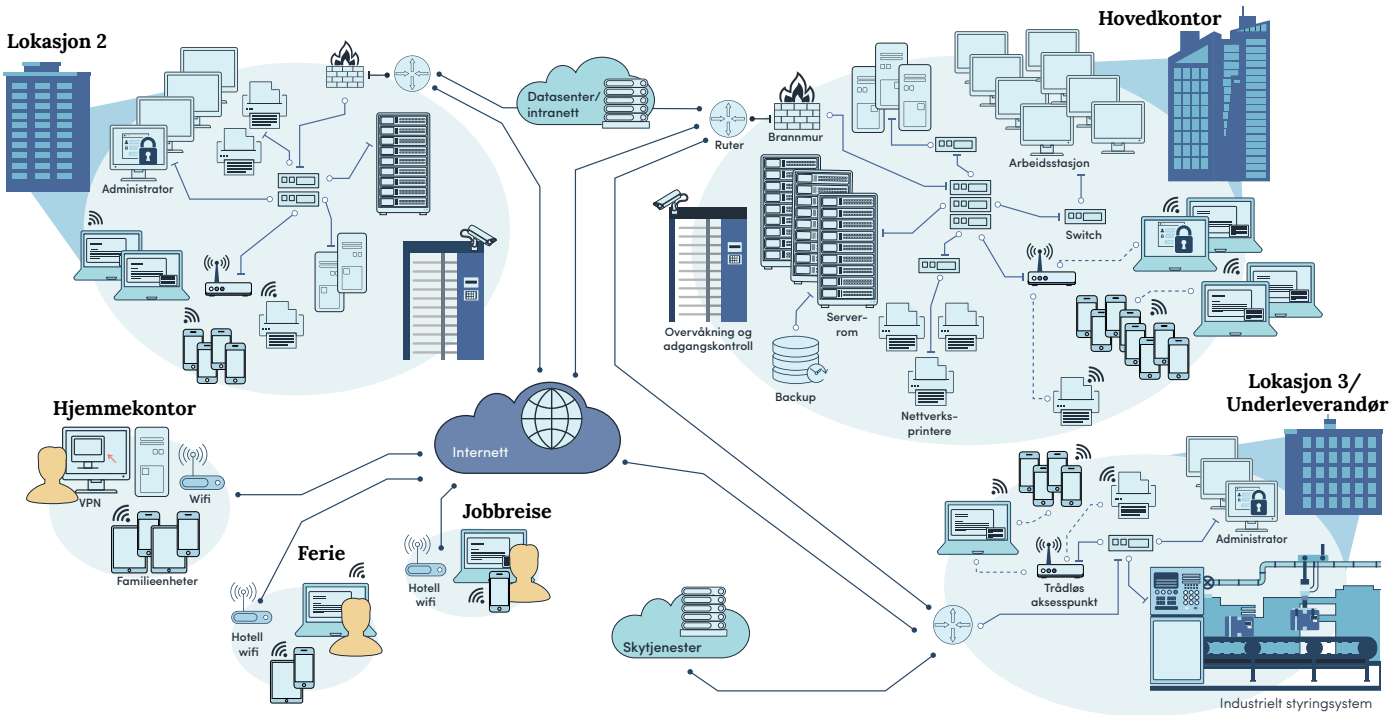
NSM er kjent med at trusselaktører kompromitterer IKT-systemene til tilfeldige norske virksomheter for å etablere kommando- og kontrollservere i Norge. Disse inngår så i trusselaktørens globale infrastruktur. De kompromitterte systemene utgjør ikke mål i seg selv, men fungerer som mellomledd for trafikk mellom målet og trusselaktøren. De blir brohoder i videre operasjoner mot andre mål.

I flere tilfeller er den etablerte infrastrukturen tilknyttet tjenesteleverandører i Norge som tilbyr domener og utleie av nettservere. Leverandørene selger denne kapasiteten til utenlandske virksomheter som tilbyr såkalt «bulletproof hosting». Dette er serverutleie uten krav om informasjon om leietaker. Misbruk av slike hostingtjenester i digitale angrep er en økende utfordring.

Bulletproof hosting



3. Slik gjør vi Norge sikrere



Kompleksitet er den største sårbarheten i det norske digitale samfunnet i dag. De digitale økosystemene består av flere datamaskiner, flere systemer, flere protokoller, flere tjenester og flere og lengre verdikjeder. Alle disse digitale løsningene kobles sammen og skaper uoversiktlige avhengigheter. Angripere utnytter som regel det svakeste leddet i en verdikjede og leter etter den enkleste veien til målet.

Tett sammenkoblede digitale løsninger på tvers av sektorer, har gjort hendelser vanskeligere å håndtere. Dette har konsekvenser for hendelseshåndtering på nasjonalt nivå. Å få oversikt og kontroll på komplekse IKT-systemer har vært en utfordring ved alle alvorlige hendelser NSM NorCERT har håndtert det siste året.

Digitaliseringen er en sentral driver i utviklingen av det norske samfunnet. Virksomheter som digitaliserer med et helthetlig syn på sikkerhets-arbeidet kan identifisere sårbarheter og iverksette risikoreduserende tiltak til en overkommelig kostnad.

«Kompleksitet er den største sårbarheten i det norske digitale samfunnet i dag.»

KOMPLEKSITETSDRIVENDE TEKNOLOGITRENDER

Med endrede behov, større datamengder og mer regnekraft vil nye typer tjenester vokse frem. Dette ser vi allerede innen nettverk, big data/kunstig intelligens, og sluttbrukerapplikasjoner.

Automatisering og kunstig intelligens vil bli viktigere i framtidens digitale tjenester og vil anvendes innen nær sagt alle områder, inkludert sikkerhetsarbeid. Trusselaktører vil også bruke kunstig intelligens til å utvikle mer effektive angrepsmetoder.

Tingenes internett («Internet of things» – IoT) vil fortsette å vokse. IoT-enheter mangler ofte innebygde sikkerhetsmekanismer og oppdateringsmuligheter.

Virksomheter som ønsker å sette ut en tjeneste må ofte få leveransen fra utlandet, fordi flere av de største internasjonale leverandørene ikke har etablert seg på norsk jord.

Helhetlig sikkerhetstenkning

Digitaliseringen gjør IKT til en fundamental del av virksomhetens prosesser. Sikkerhetsarbeidet i en virksomhet må gjøres helhetlig, på tvers av avdelinger og fagområder og må ses i sammenheng med fysiske, organisatoriske og personellmessige tiltak. Helhetlige risikovurderinger må gjennomføres.

Et av de viktigste tiltakene norske virksomheter kan gjennomføre er å ha relevant kompetanse i alle ledd. Virksomhetens ansatte må ha kunnskap om IKT og de mulighetene digitaliseringen gir. De må også ha kjennskap til virksomhetens leveranser, verdier, akseptabelt risikonivå og hvordan de selv kan bidra til bedre sikkerhet.

Implementering av IKT-sikkerhetstiltak

For implementering av tiltak innen IKT-sikkerhet anbefaler NSM å ta i bruk anerkjente rammeverk og høste erfaringer fra myndigheter, bransjeorganisasjoner og sammenliknbare virksomheter.

NSMs *Grunnprinsipper for IKT-sikkerhet* gir en erfaringsbasert oversikt over viktige tiltak en virksomhet bør vurdere for å være motstandsdyktige mot digitale trusler. Både NSM og våre samarbeidspartnere publiserer nyttige veiledere som beskriver enkelttiltak i detalj.

3.1 Sikkerhet er et lederansvar

Digitalisering er en forutsetning for at norske virksomheter skal kunne utvikle og vedlikeholde nødvendig konkurransekraft nasjonalt og internasjonalt og må derfor ha en sentral plass i virksomhetens strategi. Ledelsen må kjenne virksomhetens digitale status når den planlegger vekst, nye markedsmuligheter, oppkjøp, fusjoner og organisatoriske endringer. Den må vite hvilke muligheter og begrensninger som ligger i virksomhetens digitale portefølje og hvilke hensyn som må tas.

Sikkerhet er ikke bare et eget fag. Den har sin naturlige plass i virksomhetens digitaliseringsstrategi på lik linje med modernisering av IKT-arkitekturen, opprettelse av digitale verdikjeder og introduksjon av ny teknologi.

Sikkerhetsansvaret må være tydelig plassert i ledelsen, med oppgaver og myndighet delegert til linjeorganisasjonen. Det må etableres en tydelig modell for hvilke beslutninger linjeledere har myndighet til å ta.

NSM har sett mange eksempler på styrer og ledere som tar store, strategiske avgjørelser uten å kjenne til virksomhetens digitale sikkerhetstilstand. Slike feilgrep fører ofte til store, kostbare opprydningsjobber. Konsekvensen

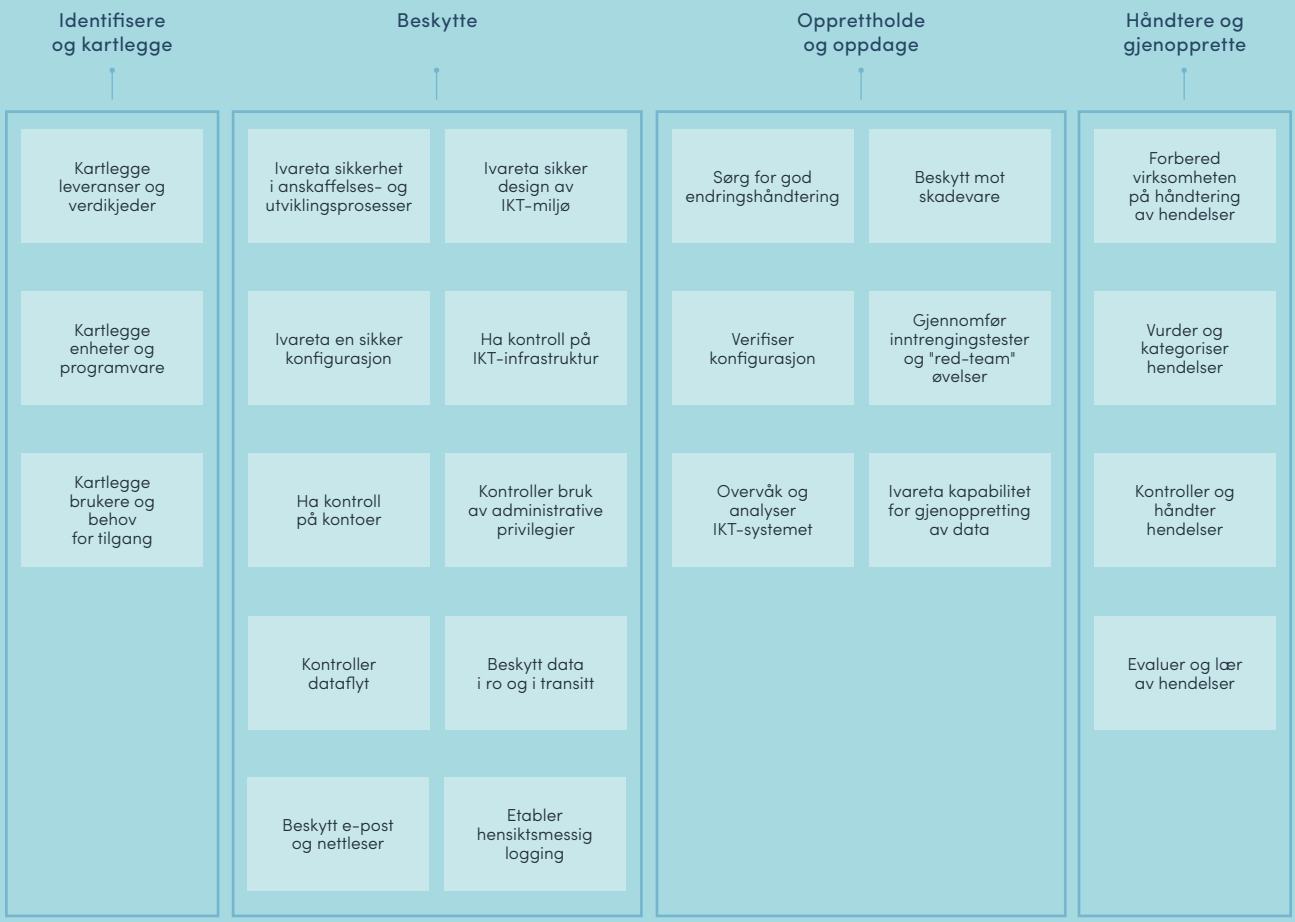
TO SENTRALE MYNDIGHETSTILTAK

- Det nasjonale cybersikkerhetssenteret under NSM skal utvikle tiltak, tilby tekniske tjenester, bistå med hendelseshåndtering, gi råd og samlokalisere kompetanse for å sikre det digitale rom.
- Det nasjonale cyberkrimsenteret under Kripos skal forebygge, avverge og etterforske kriminalitet i det digitale rom.

EKSEMPLER PÅ TEMA SOM BØR ADRESSERES I LEDELSEN

- Virksomhetens verdier og risikovurderinger
- Risikoappetitt og vilje til å investere i beskyttelsestiltak og beredskap
- Etterlevelse av *NSMs Grunnprinsipper for IKT-sikkerhet*
- Kompetansestrategi
- Gjeldende lovverk
- Sikkerhet som konkurransemessig fortrinn.

NSMs Grunnprinsipper for IKT-sikkerhet



NSMs grunnprinsipper for IKT-sikkerhet beskriver 23 prinsipper for god sikring av IKT-systemer. Grunnprinsippene skal hjelpe virksomheter med å velge ut de riktige sikkerhetstiltakene, gi en begrunnelse for hvorfor tiltakene bør implementeres og vise hvilke tiltak NSM mener særlig bør prioriteres.

kan være tapt fortjeneste og rennommé, og virksomheten kan måtte betale erstatninger i forbindelse med avtaler som må endres eller reforhandles. Vi har sett eksempler der styrer har besluttet å tjenesteutsette store deler av virksomhetens portefølje uten å ta hensyn til status og risiko for virksomhetens IKT-systemer. I enkelte tilfeller har dette ført til oppsigelse av avtalen og erstatninger på flere hundre millioner kroner til leverandøren. I tillegg må virksomheten rydde opp i eget hus, noe som ofte koster like mye som erstatningene.

Ledelsen må få på plass effektive styringsprosesser og ha fokus på operasjonell risikostyring. Risikostyring må implementeres i hele organisasjonen og ikke bare være en del av den strategiske styringen av virksomheten. Beslutninger må tas på riktig nivå og strategiske valg for digital sikkerhet må løftes til styrerommet. I en krisesituasjon må viktige, operasjonelle valg være delegert til operasjonelle ressurser. Risikoprosesser må være kjent i hele organisasjonen og harmoniseres på tvers av avdelinger og fagområder. Akseptabelt risikonivå må kommuniseres tydelig og forstås i alle ledd.

Ansatte må ha riktig kompetanse og kjennskap til egen virksomhet for å forstå hvilke digitale verdier som må sikres, hvordan de skal sikres og hvilke sårbarheter og risikoer som finnes i virksomhetens IKT-systemer. Dette gjelder alle, fra øverste ledelse til fagpersonell.

Virksomhetens sikkerhetstiltak må gjennomgås for å sikre at de er kostnadseffektive og fungerer etter hensikt. Dette innebærer sårbarhets-skanninger, gjennomganger, tilsyn og ulike former for testing. Resultatene må rapporteres i henhold til virksomhetens rapporteringsregime slik at ledelse og styret mottar relevant informasjon om status, avvik og risiko forbundet med digital sikkerhet. NSM oppfordrer også til størst mulig åpenhet og informasjonsdeling til myndighetene og andre virksomheter om hendelser.

3.2 En moderne og ryddig IKT-portefølje

Modernisering og digitalisering er ofte to sider av samme sak. En virksomhet lykkes i større grad med digitalisering hvis den benytter oppdaterte og moderne IKT-løsninger.

Det er tids- og kostnadskrevende å implementere ny funksjonalitet. Ofte legges det til nye komponenter uten å rydde opp i gammel teknologi. Virksomheten sitter igjen med løsninger og et sikkerhetsnivå som ikke tilfredsstiller behovet. Det lages også ofte midlertidige løsninger som det ikke ryddes i eller fjernes i ettertid. Dette skaper en teknologisk gjeld som introduserer ytterligere sårbarheter i løsningene. Moderne IKT-infrastruktur med tilhørende tjenester og applikasjoner har helt andre muligheter for å understøtte virksomhetens behov for innovasjon, samhandling, skalerbarhet og sikkerhet.

DIGITALE AVHENGIGHETER

I starten av 2018 ble en sentral, offentlig virksomhet utsatt for et alvorlig digitalt angrep.

Krisestaben vurderte å slå av infiserte IKT-løsninger for å redusere risikoen for spredning av skadevare. Dette var umulig fordi en rekke andre tjenester ville blitt utilgjengelige grunnet tette, digitale koblinger, også til helt andre samfunnssektorer.

«Virksomheter må oppdatere, modernisere og rydde i IKT-porteføljen sin.»

Ny teknologi er ofte sikrere enn gammel teknologi. Nye sikkerhetsmekanismer er gjerne innebygd, det finnes oftere sikkerhetsoppdateringer, og trusselaktøren har hatt mindre tid til å finne sårbarheter. De fleste angrep som lykkes utnytter eldre eller ikke oppdaterte system-komponenter. På grunn av kortsiktige kostnadsvurderinger innføres ny teknologi ofte uten nødvendig modernisering av eksisterende tjenester eller utfasing og sanering av gamle systemer. Dermed vedvarer eller forsterkes sårbarheter og blir trusselaktørens inngangsport til verdikjeden.

Virksomheter må oppdatere, modernisere og rydde i IKT-porteføljen sin. Eldre komponenter må saneres og fases ut. Virksomheter må automatisere arbeidsoppgaver og ta i bruk nye teknologier og applikasjoner som stordata, kunstig intelligens, skytjenester, virtualisering, IoT og mobile løsninger. De nye løsningene vil kunne heve virksomhetens sikkerhetsnivå om de implementeres riktig i en oppdatert sikkerhetsarkitektur. NSM anbefaler virksomheter uten tilstrekkelige ressurser å anskaffe løsningene fra profesjonelle aktører som er i stand til å oppfylle virksomhetens behov.

3.3 Større profesjonelle IKT-miljø

Digitaliseringen krever kostbare oppgraderinger, investeringer og vedlikehold av IKT-porteføljen til en virksomhet. IKT-arkitekturen må oppdateres, sikkerhetsarbeid må automatiseres, og ansatte må vedlikeholde faglig kompetanse. IKT-ressurser må ha tilstrekkelig logisk og fysisk beskyttelse, og viktige funksjoner, som nødstrøm og ekstern lagring av sikkerhetskopi, bør være tilgjengelige. Små IKT-miljøer har færre investeringsmidler og vanskeligere for å tiltrekke seg og bygge opp god IKT-kompetanse, inkludert innen sikkerhet.

Klarer en virksomhet med et lite IKT-miljø å opprettholde IKT-tjenester ved digitale angrep? Hvor sårbar er virksomheten for skadevare som sprer seg hurtig? Har virksomheten oversikt over IKT-ressurser, produksjonssystemer og tjenester den er avhengig av for å opprettholde driften? Kan disse isoleres hurtig fra internett og øvrig infrastruktur dersom man blir truffet av skadevare eller hvis en trusselaktør får tilgang til virksomhetens infrastruktur?

Etter større datainnbrudd møter NSM altfor ofte ledere som hverken kjenner de største risikoene sine eller er klar over tilstanden til IKT-systemene sine. Bare i offentlig sektor er det i dag 600 IKT-miljøer, hvorav de fleste er å betegne som små. Mange virksomheter baserer seg på forskjellige typer nettverk, systemer og tjenester, inkludert dupliserte tjenester. Dette øker kompleksiteten, antall sårbarheter og mulige angrepsflater.

Det er dyrt å ikke ha styring og kontroll når hendelser inntreffer. Når NSM har bidratt med støtte til hendelseshåndtering har vi sett hvor galt det kan gå dersom virksomheter ikke klarer å få oversikt over egne systemer når skadevare eller fremmede aktører kommer innenfor virksomhetens perimetersikring. De som ikke straks identifiserer status og har kontroll på egen infrastruktur, klarer ikke å implementere de riktige tiltakene for å hindre at problemet sprer seg og eskalerer. Det tar da lenger tid å få kontroll over hendelsen. I enkelte tilfeller må man reinstallere alle servere, klienter og tjenester før man igjen kan ha tillitt til egne IKT-systemer. Erfaring fra flere angrep tilsier at tiltak må iverksettes hurtig, ofte innen få timer.

En virksomhet må ha tilstrekkelige ressurser og kompetanse til å vedlikeholde en oppdatert og sikker IKT-portefølje. Hvis ikke bør den enten vurdere å slå sammen flere, mindre IKT-miljøer til større enheter basert på færre plattformer, eller kjøpe tjenesten fra et profesjonalisert IKT-miljø. Et større miljø har vesentlig bedre forutsetninger for å bygge tilstrekkelig kompetanse, skalerbare infrastrukturer og kostnadseffektive sikkerhetsløsninger. Virksomheten får mer stabile og tilgjengelige tjenester i tillegg til lavere og mer forutsigbare kostnader.

Et større IKT-miljø vil kunne tilby en døgnkontinuerlig hendelseshåndteringstjeneste. En slik tjeneste er omfattende, da flere typer fageksperter må samarbeide om å begrense skade og sørge for at viktige tjenester forblir tilgjengelige. En formalisert struktur med krisestab, som inkluderer ledelsen i virksomheten, må være på standby. I ettertid kan det være behov for å gjennomføre en intern utredning av enkelte hendelser. Det er også viktig å ha et godt samarbeid med sektorvise responsmiljøer og NSM NorCERT.

3.4 Sikker tjenesteutsetting

Tjenesteutsetting av IKT-tjenester til profesjonelle aktører kan gi bedre sikkerhet og mer stabile og tilgjengelige tjenester. Man får tilgang til ekspertkompetanse og verktøy man ikke selv besitter mens kostnadene kan bli lavere og mer forutsigbare. Tjenesteutsetting kan bidra til bedre fokus på virksomhetens kjerneaktivitet, men fritar ikke virksomheten og ledelsen fra å ha det hele og fulle ansvaret. En virksomhet må samtidig være bevisst hvilken risiko en tjenesteutsetting medfører. Virksomheten kan få redusert kontroll over stadig mer komplekse verdikjeder, miste intern kompetanse og bli avhengig av eksterne tjenesteleverandører for å kunne levere tjenestene sine.

Vi ser ofte at virksomheter har et ensidig fokus på økonomisk gevinst. Dette kan føre til at det tas snarveier når tjenester skal settes ut og at risikoer ikke blir tilstrekkelig kartlagt og vurdert. Flere virksomheter vi har vært i kontakt med har satt ut viktige tjenester til underleverandører som har dårligere sikkerhet enn virksomheten selv.

En beslutning om tjenesteutsetting bør tas basert på risikovurderinger som inkluderer de faktiske risikoene tjenesteutsettingen medfører og omfatter hele dens livsløp. Vær forberedt på at rett beslutning kan være et «nei» til tjenesteutsetting. NSM gir i sin temarapport *Sikkerhetsfaglige anbefalinger ved tjenesteutsetting* følgende fem råd (se tekstboks):

TRUSSELAKTØREN KAN ANGRIPE LEVERANDØRKJEDEN TIL EN VIRKSOMHET ISTEDENFOR VIRKSOMHETEN SELV.

I NotPetya-kampanjen kompromitterte en ukjent aktør programvaren M.E.Doc som blir brukt i store deler av Ukraina. Alle maskiner som oppdaterte M.E.Doc lastet også ned skadevare. Etterpå spredte skadevaren seg hurtig til andre land i Europa.

Sikkerhetsfaglige anbefalinger ved tjenesteutsetting

1. Sørg for å ha oversikt og kontroll over tjenesteutsettingens livsløp, fra begynnelse til slutt.

Livsløpet deler vi i fire faser (forberedende, anskaffelse, forvaltning og opphør).
I hver fase er det et sett med aktiviteter som virksomheten må ha oversikt og kontroll over.

2. Sørg for god bestillerkompetanse, inkludert virksomhets-, sikkerhets-, integrasjons-, anskaffelse-, og juridisk kompetanse. Hvis ikke, kan det føre til at virksomheten kjøper IKT-tjenester uten tilstrekkelig kartlegging av behov. Dette kan gi utfordringer med å stille gode krav til IKT-sikkerhet eller at feil leverandør velges.

3. Gjør gode risikovurderinger for å kunne ta riktig beslutning. Vår erfaring er at det i alt for stor grad legges vekt på kostnader. Risikovurderinger skal omfatte hele tjenesteutsettingens livsløp, inkludert utfordringer og kostnader i alle faser – ikke bare anskaffelse.

4. Still riktige og gode krav til tjenesteleverandøren og IKT-tjenestene de skal levere. Du må kjenne din egen virksomhet og vite hvilke behov den har. Behovene må uttrykkes som målbare og verifiserbare krav.

5. Treff riktig beslutning på riktig nivå. Bortfall av en IKT-tjeneste vil ofte ha stor påvirkning på virksomheten. Tjenesteutsetting er en viktig, strategisk beslutning og bør ikke tas av virksomhetens IKT-miljø alene, men bør behandles og besluttes av øverste ledelse. For private virksomheter gjelder dette styret, for offentlige virksomheter bør beslutning om tjenesteutsetting forankres hos overordnet fagdepartement.

3.5 God sikkerhetsarkitektur og økt automatisering

Digitalisering innebærer ofte innsamling og foredling av store mengder data, sammenkobling av mange og komplekse systemer og bruk av ny teknologi. På lik linje med automatisering av andre arbeidsprosesser må virksomheter automatisere sikkerhetsarbeidet. Uten en gjennomtenkt IKT-arkitektur er det utfordrende å holde oversikt og kontroll med IKT-systemene, inkludert å avdekke og håndtere hendelser.

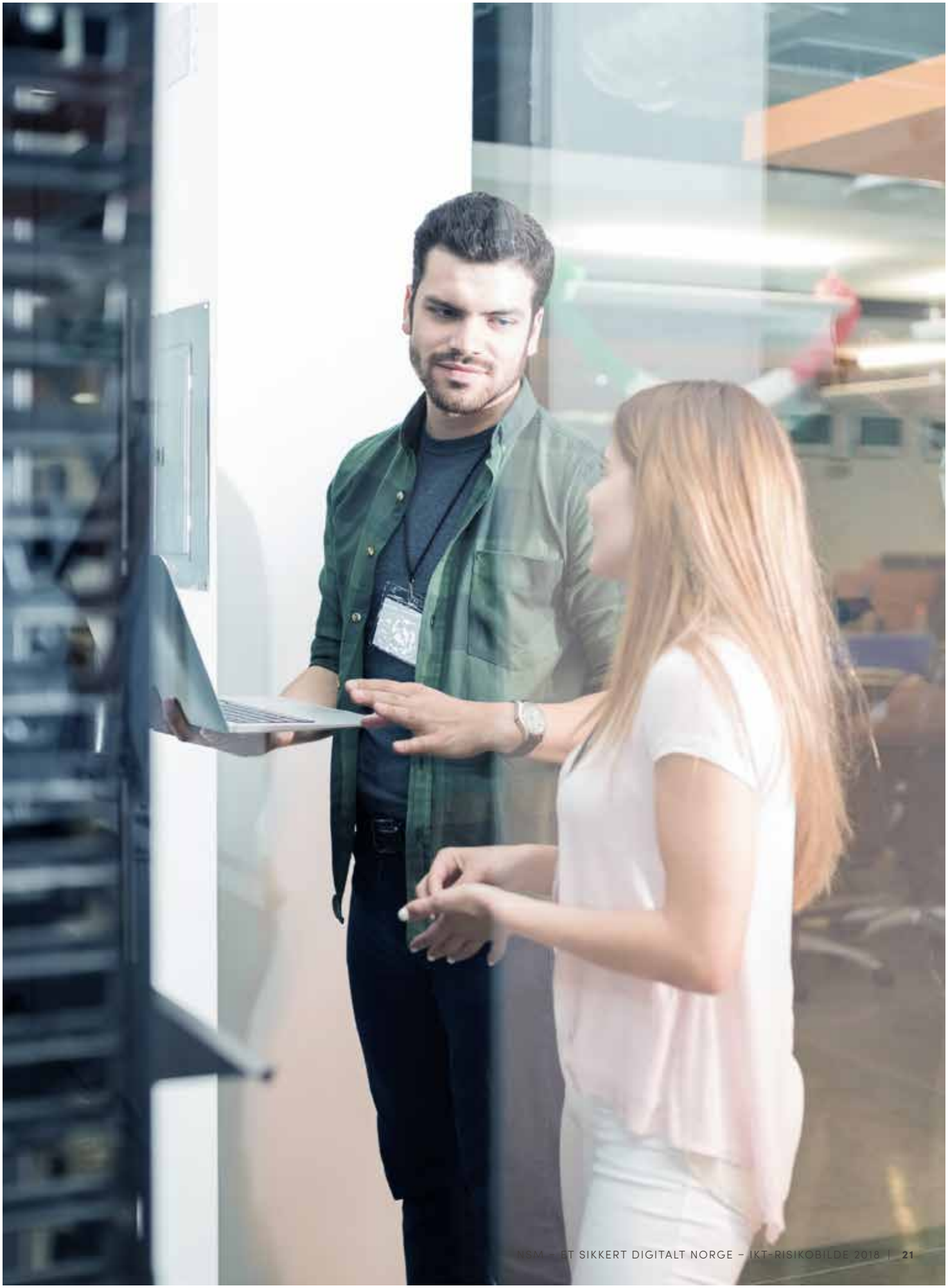
Eksempler på områder som må automatiseres er logganalyse og oversikt over gjennomførte sikkerhetsoppdateringer. NSM erfarer at sikkerhetsarbeidet i mange tilfeller er basert på manuell oppfølging og ikke holder nødvendig kvalitet. Angripere utnytter tjenester som er konfigurert eller designet feil. Sårbare og eksponerte systemer er blant de mest populære angrepsmålene på grunn av mangelfulle rutiner og rutiner som ikke blir fulgt.

NSM ser at virksomheter som mangler automatiserte prosesser for å vedlikeholde IKT-miljøet alltid har sårbarheter som kan utnyttes. NSMs inntrengingstestere utnytter ofte utdaterte eller ikke oppdaterte systemer og systemer satt opp med standard brukernavn og passord. NSM NorCERT har gjentatte ganger sett at virksomheter ikke klarer å finne status på oppdateringsnivå på servere når en hendelse har inntruffet. De vet da ikke hvilke deler av infrastrukturen som er sårbare og må isoleres. De klarer heller ikke å finne ut hvilke deler av infrastrukturen som er rammet av en skadevare eller hvor en trusselaktør har fått fotfeste.

«En virksomhet må digitalisere sikkerhetsarbeidet parallelt med at annen aktivitet digitaliseres.»

En virksomhet må digitalisere sikkerhetsarbeidet parallelt med at annen aktivitet digitaliseres. Automatisering gjør det enkelt å samle inn og analysere sikkerhetsrelatert informasjon. Dermed vil man ikke bare detektere angrep, men også identifisere svakheter i egen infrastruktur. Man vil automatisk kunne oppdage blant annet avvikende brukerpåloggінger, privat utstyr som kobles til nettet, uoverensstemmelser mellom organisasjonsstrukturen og brukergrupper og -rettigheter, svake administratorpassord, samt eldre systemer og systemer som ikke er oppdatert.

En god IKT-arkitektur som har tilrettelagt for og iverksatt automatisering er nødvendig for å forsvare seg mot tilsiktede og utilsiktede hendelser. Soneinndeling må brukes for å skille eksponerte tjenester fra systemer og databaser som er virksomhetskritiske. Et godt loggregime gjør det mulig å spore aktivitet i infrastrukturen. God tilgangsstyring er nødvendig, spesielt når det er mange eksterne med tilgang til virksomhetens systemer.



3.6 Hjelp sluttbrukeren

Mange sikkerhetsråd er rettet mot sluttbrukere: «Bruk lange, vanskelige passord.» «Oppdater operativsystem og programvare.» «Ikke trykk på suspekte lenker i e-post.» Så lenge vi brukere har mulighet til å gjøre feil, vil vi gjøre dem. Angriperne går som regel etter det svakeste ledd, som ofte er den enkelte ansatte. Er det fordi vi ikke kan bruke datamaskiner, eller fordi man ikke tilbyr løsninger som reduserer den risikoen ansatte utgjør?

Gjennom inntregningstester mot norske virksomheter ser NSM mange eksempler på feil sluttbrukere gjør. Ofte er dette feil som kunne vært unngått hvis virksomheten hadde valgt sikre løsninger: Ansatte får tildelt brukerkonti med for mange rettigheter. Det er fritt fram å bruke egne laptoper og mobiltelefoner istedenfor at virksomheten tilbyr flåtestyrte enheter. Brukere blir påtvunget altfor hyppige passordbytter og løser det ved å bruke dårlige passord.

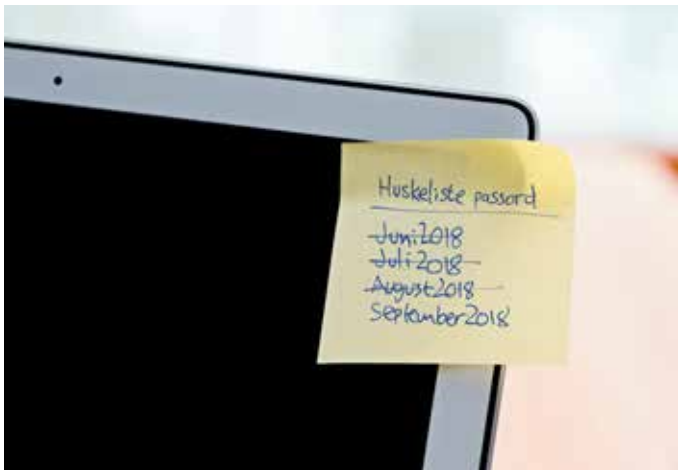
Virksomheter og leverandører av tjenester og produkter må minimere brukernes mulighet til å gjøre feil. Brukervennlige og sikre løsninger bør motivere og veilede brukere til bedre sikkerhet. Moderne IKT-løsninger bør ha så god sikkerhet at sårbarheter som følge av brukerfeil fjernes eller reduseres til et minimum. Løsningene bør begrense konsekvensene dersom de gjenværende sårbarhetene blir utnyttet.

Virksomheten kan innføre mange, gode sikkerhetstiltak rettet mot brukerne. Eksempler er bruk av automatisert oppdatering av enheter, avlesningssikre nøkkelkort, to-faktorautentisering og gode passordregimer. Virksomheten må ha kontroll på administrative privilegier og brukere bør kun ha de rettighetene de til enhver tid trenger. Det bør også legges til rette for at sluttbrukerne kan rapportere sikkerhetshendelser de oppdager.

> «Virksomheter og leverandører av tjenester og produkter må minimere brukernes mulighet til å gjøre feil.»

På tross av en økende bevissthet rundt e-post-angrep er e-post fortsatt en av de største angrepsvektorene. Alle virksomheter bør implementere sikkerhetsmekanismene som er omtalt i NSMs veileder om e-postsikkerhet: *Grunnleggende tiltak for sikring av e-post.*

Til tross for alle tekniske tiltak som innføres, vil det alltid være en viss restrisiko. Det er derfor viktig å fortsette kompetansebygging, opplæring og bevisstgjøring hos sluttbrukere.



Design: Redink
Manus: NSM
Foto: iStock

NASJONAL SIKKERHETSMYNDIGHET

Postboks 814, 1306 Sandvika

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