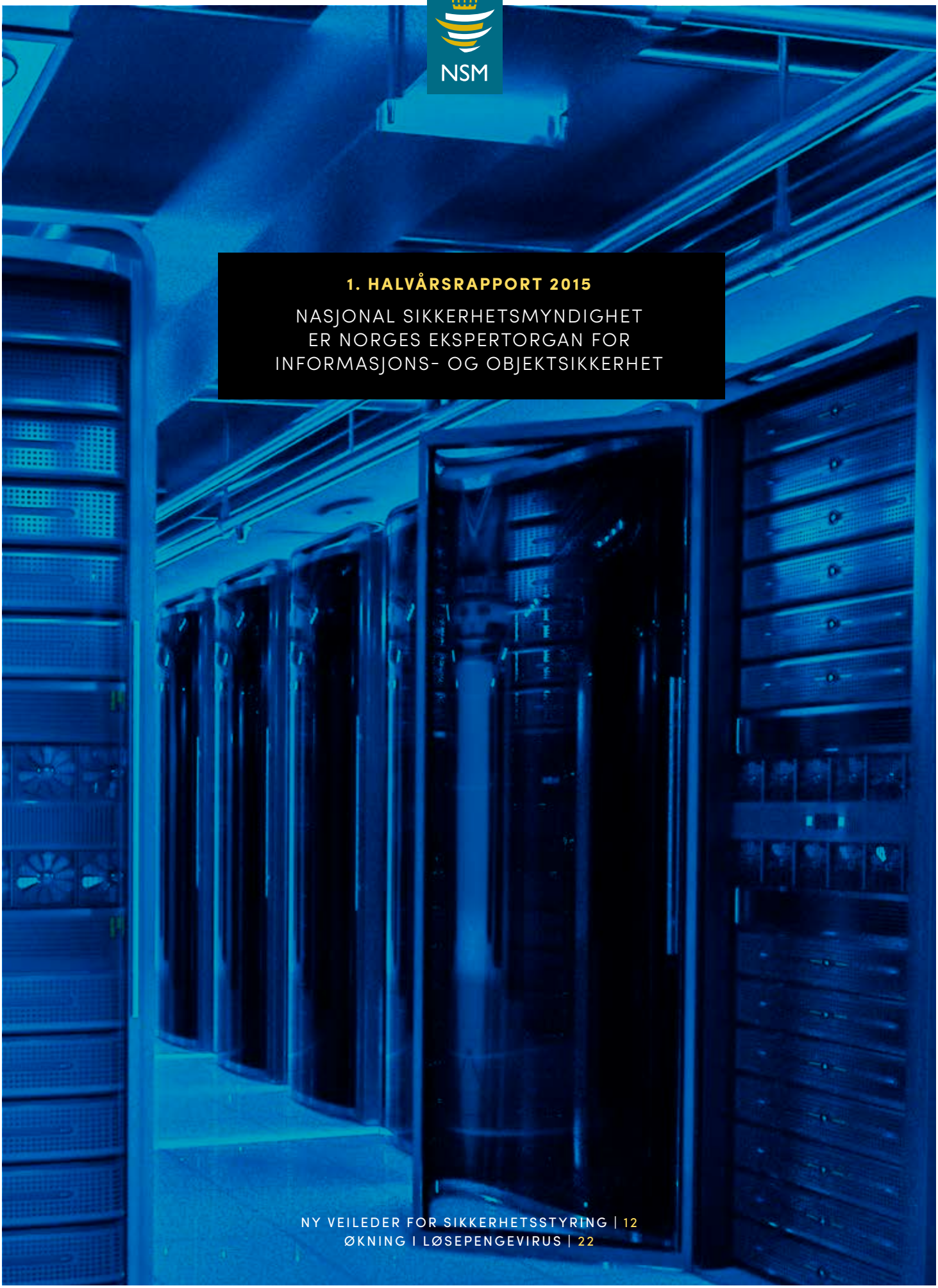


NSM

1. HALVÅRSRAPPORT 2015

NASJONAL SIKKERHETSMYNDIGHET ER NORGES EKSPERTORGAN FOR INFORMASJONS- OG OBJEKTSIKKERHET

NY VEILEDER FOR SIKKERHETSSTYRING | 12
ØKNING I LØSEPENGEVIRUS | 22

EN SIKKERHETSVERDEN I RASK ENDRING

FØRSTE HALVDEL av 2015 har vært både krevende og travelt for oss i Nasjonal sikkerhetsmyndighet. Vi lever og jobber i et samfunn og en bransje som endrer seg raskt, noe som gir oss både utfordringer og muligheter. Denne utviklingen er både spennende og krevende for våre ansatte.

I denne rapporten kan du lese om Sikkerhetsfaglig råd, som vi fikk i oppdrag å utarbeide ved årsskiftet. Dette leverte vi til Forsvarsdepartementet og Justis- og beredskapsdepartementet i begynnelsen av september, og det er et arbeid som har involvert de aller fleste i organisasjonen på en eller annen måte. Sikkerhetsfaglig råd er NSMs vurdering av hvordan Norge bør innrette arbeidet med sikkerhet mot 2020 og videre fremover, og hvordan Norge bør møte de økte sikkerhetsutfordringene. De til sammen 72 rådene er åpenbart noe som også vil påvirke hvordan vi i NSM vil jobbe i fremtiden.

I tillegg til Sikkerhetsfaglig råd, leverer vi rapporten «Helhetlig IKT-risikobilde» 1. oktober. Rapporten omfatter utviklingstrekk, utfordringer og mulige tiltak av betydning for statssikkerhet, samfunnssikkerhet og individsikkerhet, og har et vidt nedslagsfelt ved å omhandle utfordringer både for tilsiktede og utilsiktede uønskede hendelser knyttet til IKT-utstyr og internett. Det er første gang også denne rapporten blir skrevet, og formålet er å tilføre mer kunnskap som øker bevisstheten rundt behovet for IKT-sikkerhet og behovet for å vurdere informasjonens verdi.

Du kan også lese at det blir stadig vanskeligere å oppdage cyberangrep, og for første gang på flere år blir det nå registrert færre angrep av denne typen. Det skyldes neppe at det er mindre som skjer, men at angriperne mer og mer tilpasser seg vår evne til å oppdage angrepene. Dette er et kappløp, og vi jobber kontinuerlig med å utvikle oss for å holde følge.

Kunnskap og deling av informasjon er viktig for å styrke sikkerheten. I mars arrangerte vi som vår tradisjonelle sikkerhetskonferanse, med rekordmange påmeldte og et svært spennende program. I tillegg til 800 deltakere, inviterte vi i år for andre gang 100 utvalgte toppledere innenfor privat og offentlig sektor, for å minne dem på at sikkerhet er et lederansvar, og at samarbeid på tvers er nødvendig. Tilbakemeldingene fra Sikkerhetskonferansen 2015 har vært overveldende, og vi er allerede i gang med å planlegge neste års konferanse, som går av stabelen 16. og 17. mars i Oslo.

Med vennlig hilsen

Kjetil Nilsen
Direktør
Nasjonal sikkerhetsmyndighet

1. HALVÅR 2015

SEKSJONER

004
RAPPORTERING

010
TILSYN

012
SIKKERHETSSTYRING

014
AKTUELT

024
RAPPORTER

022
OPPLÆRING

Design:
REDINK

Trykk og distribusjon:
RK GRAFISK

RISIKOBILDET: – BETYDELIG RISIKO FOR SPIONASJE, SABOTASJE OG TERROR

Det er store sårbarheter i norske IKT-systemer, og konsekvensen av mangelfull IKT-sikkerhet er at store verdier kan gå tapt. Derfor er det behov for en omfattende satsing på IKT-sikkerhet.

OVERORDNET VURDERING

NSMs overordnede vurdering er at det generelt er betydelig risiko for spionasje, sabotasje og terror, og det er stor risiko forbundet med bruk av IKT. Trusselen er høy og økende, og det er betydelige sårbarheter i norske IKT-systemer. Konsekvensen av mangelfull IKT-sikkerhet er at store verdier kan gå tapt, i et spenn fra individets gode navn og rykte, til nasjonal selvstendighet. Helt grunnleggende sikkerhetstiltak er ofte ikke gjennomført eller mangelfullt implementert. For å redusere risikoen er det behov for en omfattende nasjonal satsning på IKT-sikkerhet i årene som kommer.

SITUASJONSBILDE

NSM har i senere tid sett flere eksempler på vellykkede datainnbrudd der angriperne har fått tilgang til virksomhetskritisk informasjon, og at forretningshemmeligheter, kursdrivende eller annen sensitiv informasjon har kommet på avveie. Det er store mangler i det forebyggende IKT-sikkerhetsarbeidet, og høy risiko forbundet med at store og små virksomheter ikke tar i bruk grunnleggende tiltak for å sikre sine IKT-systemer. De samme sårbarhetene observeres gjentatte ganger og avslører at IKT-sikkerhetsarbeidet er mangelfullt styrt. Den teknologiske utviklingen skjer hurtig, noe som medfører at det stadig oppstår nye sårbarheter som må tettes. Økt kompleksitet har ført til mer avanserte dataangrep. Det er behov for mer kunnskap og bedre ivaretagelse av grunnleggende sikkerhet.

Vi ser at uønskede handlinger via IKT og internett forsetter å øke i antall og kompleksitet. Imidlertid er det registrert færre alvorlige hendelser enn før. Vi har indikasjoner som tyder på at dette skyldes at dataangrepene har blitt mer avanserte, og at det er betydelig læringsevne hos trusselaktørene.

TRUSLER

Trusselen mot norske verdier er høy og økende. Målsettingen kan være å skaffe

seg informasjon om stats- og forretningshemmeligheter, informasjon om forskningsresultater og teknologiske nyvinninger, og informasjon om strategier og planer. Det kan også være et mål å skade en motpart ved å påvirke, redusere eller ødelegge funksjonalitet i produksjonssystemer, eller å stjele privat informasjon fra enkeltpersoner. Nettverksoperasjoner blir stadig mer målrettede og teknisk avanserte. Det er statlige aktører som står bak den mest alvorlige trusselen. Listen over aktører som kan tenkes å ha målsettinger som nevnt over er imidlertid lang, og spenner seg fra overbeviste aktivister og terrorister til organiserte kriminelle, konkurrenter og stater.

Innsidetrusselen i norske virksomheter, både i inn- og utland, er fortsatt reell. Lokalt ansatte ved norske virksomheter ute kan bli utsatt for ulike typer press og fristelser som motiverer dem til å handle i strid med norske interesser. Det samme gjelder utlendinger som jobber i Norge. Dersom de har tilgang på informasjon som har fått ny verdi for en trusselaktør, kan mennesker som tidligere ikke har vært gjenstand for innhenting bli kontaktet nå.

Innsidetrusselen gjelder så vel for nordmenn som utlendinger, og den det gjelder kan handle i tråd med en annen lojalitet enn den til Norge, la seg motivere av gjenytelser, eller bli utsatt for press mot seg eller sine nære.

SÅRBARHETER

Det er store mangler i det forebyggende sikkerhetsarbeidet. Grunnleggende mangler gjør det lett for trusselaktørene å komme seg inn i norske IKT-systemer, inkludert styrings- og prosesskontrollsystemer. Sikkerhetsmessige sårbarheter kan ha tekniske, menneskelige og organisatoriske årsaker. Sårbarheter er den dimensjonen i risikobildet vi alle kan gjøre noe med.

Ved å utnytte menneskelige, organisatoriske og tekniske sårbarheter kan trusselaktør lett hente ut ønsket informasjon. Kritisk mangel på kompetanse innen IKT-sikkerhet og manglende oppdatering av dataprogrammer, kombinert med blant annet mangler i sikkerhetsrutiner, organisering, rolleforståelse og sikkerhetskultur kan få store konsekvenser.

Mangel på IKT-sikkerhetskompetanse er på kort sikt kritisk. Det er stor mangel på kvalifiserte kandidater med både sikkerhetsfaglig og høyere teknisk utdanning. Mangel på kompetanse påvirker både evnen til å løse nasjonale sikkerhetsoppgaver, og sikring av norske virksomheter. Dette hemmer evnen til å gjennomføre gode IKT-sikkerhetstiltak. Helt konkret påvirkes også kapasiteten til å håndtere dataangrep. I tillegg er det en utfordring å følge med på konsekvensene av den teknologiske utviklingen for IKT-sikkerhetsområdet. Mangelfull rapportering av alvorlige IKT-hendelser vil svekke evnen til forbedring og læring innen forebyggende IKT-sikkerhet. Det er behov for å få etablerte strukturer til å virke bedre gjennom å videreutvikle samarbeidsarenaer og gode samarbeidsmekanismer, slik at prosesser rundt politikkutforming, forebyggende sikkerhet og hendelseshåndtering forbedres. Samarbeid mellom ulike offentlige og private aktører kan med fordel utvikles videre. Utvikling, forvaltning og drift av offentlige IKT-løsninger kan samordnes bedre. Kryptering, inntrengningstesting, sertifisering og akkreditering blir alle brukt i for liten grad. Hverken deteksjon eller hendelseshåndtering er tilstrekkelig utviklet.

VERDIER

Norske statlige og private virksomheter har betydelige verdier som er ettertraktet for trusselaktørene. Trusselaktørene gjør gode vurderinger av hva som er informasjon av høy verdi. Konsekvensen av mangelfull IKT-sikkerhet er at store verdier kan gå tapt.

Det er svært mange opplysninger som kan være av interesse for en trusselaktør, og verdien av informasjonen er ikke nødvendigvis åpenbar for den som besitter den. Små bestanddeler av et for oss ukjent helhetsbilde kan hjelpe en trusselaktør til for eksempel å skaffe seg fysisk adgang til fasiliteter, logisk adgang til IT-systemer, eller en forståelse av hva norske beslutningstakere tenker.

TILTAK

Det er sjelden at en gjennomgang av sikkerhetssystemer, -rutiner og planverk ikke fører til at en finner svakheter. Det forteller oss at slike gjennomganger er helt nødvendige.

I vår kontakt med virksomheter den siste tiden er det noen råd som ofte har gått igjen. Når det gjelder IT-systemer, er eksponering av kritisk infrastruktur et tilbakevendende poeng. Egne sikkerhetssoner i systemene og strenge regelsett i brannmurer kan redusere eksponeringen. Det kan også være nyttig å spørre seg om det i det hele tatt er nødvendig at de mest sensitive delene til enhver tid skal være koblet opp mot resten av infrastrukturen.

I perioder hvor man ser behov for ekstra årvåkenhet, er det viktig å følge opp med systematisk logging, og ikke minst varsling av NSM når man avdekker mistenkelig aktivitet.

Både pånsm.stat.no og difi.no finnes veiledere og reglementer som gjør det lettere å sørge for en god sikkerhetsstandard i virksomhetene.

I perioden har NSM levert sikkerhetsfaglig råd til justisministeren og forsvarsministeren, samt utgitt en rapport om det helhetlige IKT-risikobildet. I disse er det en rekke tiltak. Det viktigste tiltaket er imidlertid at alle gjennomfører grunnleggende sikringstiltak for IKT, som vil kunne avverge inntil 90 % av alle digitale angrep. <

NØKKELTALL FRA NSM NorCERT: VANSKELIGERE Å OPPDAGE ANGREP

Antallet avanserte cyberangrep mot Norge går tilsynelatende ned i første halvår 2015, til tross for at antall saker som håndteres fortsatt er økende. Dette er et trendbrudd, da antallet cyberangrep økte kraftig de foregående årene.

FOR FØRSTE GANG på flere år har NSM håndtert færre alvorlige cyberangrep enn i samme periode i fjor. Det gjenspeiler ikke en realitet, men snarere at evnen til å oppdage angrep er under press, noe som understreker kompleksiteten i disse angrepene. NSM har holdepunkter for at det er stor aktivitet fra ondsinnede aktører.

Samtidig har vi registrert 13.773 saker og håndtert 2.943 saker pr. 31. august 2015, mot henholdsvis totalt 17.662 registrerte og 5.066 håndterte saker i hele 2014. Det antas at angriperne i økende grad tilpasser seg den nasjonale evnen til å oppdage angrepene og klarer å gå under radaren. Det oppdages nå lite i bransjer som tidligere var under jevnlig angrep over internett. Det bedømmes at angriperne med stor sikkerhet er der, men at de ikke oppdages. Angriperne utvikler sine teknikker raskere enn utviklingen av mottiltak. Dette er i praksis et slags våpenkappløp. De angrepene som oppdages, er økt i omfang, slik at flere virksomheter inkluderes i samme angrep. Angrepene blir mer avanserte og det gjøres forsøk på å få fotfeste innenfor IKT-strukturen i virksomheten som angripes. Innføring av forbedret deteksjonsteknologi i NSM NorCERT har i løpet av året ført til at deteksjonsraten har tatt seg opp igjen.

Det blir vanskeligere å detektere angrep gjennom tradisjonell bruk av signaturer. Trusselaktørene bruker mer dynamiske vektorer og gjenkjennelige mønstre blir færre. Dette vil gjøre at behovet for kompetanse for å avdekke angrep vil bli sterkt økende, og det vil være en stor risiko for at mange av de mindre aktørene i stadig mindre grad vil evne å avdekke angrep.

De siste 12 månedene er det en økning i antallet kommando- og kontroll servere (CC-servere)[1] som står i norsk infrastruktur. Norske forsknings- og utdanningsinstitusjoner blir kompromittert og benyttet i angrep mot norske bedrifter og institusjoner. Angriperen bytter i større grad mellom mange servere i løpet av et angrep for å redusere sjansen for å bli oppdaget. Utfordringen er at en server som gjennom tradisjonell risikometodikk vil komme ut med lav risiko fordi innholdet på serveren ikke har et stort beskyttelsesbehov, benyttes som en vei inn til infrastruktur hvor verdiene er betydelig høyere.

For nasjonen og staten Norge er fremmede staters etterretning den største trusselen. En rekke land har i løpet av de siste ti årene utviklet en svært omfattende etterretningskapasitet i det digitale rom med vide juridiske og politiske fullmakter til å utnytte disse kapasitetene. Mange stater bruker store ressurser på

« For nasjonen og staten Norge er fremmede staters etterretning den største trusselen.

FAKTA

OPERASJONS-SENTER

NSMs Operasjonssenter sender ut varsler om blant annet sårbarheter, mulige tiltak, rutinemessig patching og andre oppdateringer. Varslene bidrar til at IT-sikkerhetsansvarlig kan treffe beslutninger i forhold til virksomhetens sikkerhetsnivå.

Kontakt oss på *post@cert.no* dersom du ønsker at din virksomhet skal motta varsler fra NorCERT.

etterretningstjenestene og tillegger informasjonen som disse produserer vesentlig rolle i beslutningskjeden.

Et eksempel på dette i 2015 er en nettverkskampanje som har gått målrettet mot offentlig sektor i Norge. Kampanjen bærer preg av nøye planlegging og kompetent fremgangsmåte, og den retter seg mot personer eller systemer som kan gi tilgang til sensitiv informasjon. Aktøren bak er kjent fra før, blant annet fra hendelser i 2014, og går mot mange mål med store ressurser. NSM vurderer dette som en avansert vedvarende trussel. EOS-tjenestene vurderer at trusselaktøren er en fremmed sikkerhets- eller etterretningstjeneste.

De siste 12 månedene har det vært økt aktivitet fra de store statlige aktørene. En av hovedutfordringene er at skadevaren brukes en gang og deretter sendes ut på det kriminelle markedet. Den økte statlige aktiviteten gir andre kriminelle aktører en stor tilgang på skadevare.

Tap av sikkerhetsgradert eller annen taushetsbelagt informasjon av operativ karakter kan både direkte og indirekte medføre tap av menneskeliv. Konsekvensen ved økt digital spionasje av militær karakter må sees i et langsiktig perspektiv. Skadevirkningene blir ikke nødvendigvis synlige før en militær konflikt begynner.

I løpet av 2015 er tidsvinduet mellom publisering av skadevare til en angrepsversjon er tilgjengelig, blitt mindre. Man har ofte ikke mer enn 7 dager fra en patch blir sendt ut fra programvareleverandør til det er skadevare på plass som utnytter sårbarheten. Utfordringen vil øke betydelig i tiden fremover når det gjelder omfang og tidsvinduet man har til å holde egen infrastruktur og klienter oppdatert.

Dette er tall fra siste år vedrørende statlige virksomheter[2]:

- 11,8 % hadde hatt sammenbrudd i forbindelsen til internett eller andre eksterne nettverk,
- 8,3 % hadde hatt virusangrep, ormer eller lignende som resulterte i tap av data eller arbeidstid
- 15,4 % hadde hatt tjenestenektangrep
- 16,7 % hadde hatt uautorisert tilgang til systemer eller data
- 31,1 % hadde opplevd forsøk på identitetstyveri (phishing)
- 44,3 % hadde opplevd at virksomhetens IKT-utstyr hadde kommet på avveier

Det er svært sannsynlig at det i Norge har funnet sted flere alvorlige nettbaserte spionasjehendelser enn det som norske myndigheter har oversikt over. Det er svært sannsynlig at det vil bli flere slike angrep fremover.

Norge har så langt ikke vært utsatt for alvorlige forsøk på å slå ut kritiske infrastrukturer eller kritiske samfunnsfunksjoner. Erfaringer fra de siste årene, i forbindelse med kriser og hendelser i både det fysiske og det digitale rom, er at man ikke lenger kan forvente varslingstid som gir mulighet til å iverksette tiltak. <

FOTNOTE

(1)
Server som er infiltrert av angriper og brukes til å styre angrep

(2)
SSB, Statistikkbanken, Bruk av IKT i staten, Tabell 10859: Statlige virksomheter. IKT-sikkerhetsproblemer i løpet av det siste året (present). Tilsvarende tallmateriale var ikke tilgjengelig for private foretak. De nyeste SSB-tallene for IKT-sikkerhetsproblem i næringslivet var fra 2004, og derfor ikke sammenlignbare.

NØKKELTALL FOR 1. HALVÅR 2015 LIGGER ETTER I VÅPENKAPPLØPET

Antallet cyberangrep håndtert av NSM går ned betydelig ned i første halvår 2015. – Vi er nå bekymret for at det tappes data og at bedrifter mister informasjon uten at vi kjenner til det, sier avdelingsdirektør Hans Christian Pretorius i Nasjonal sikkerhetsmyndighet.

TEKST: KJETIL BERG VEIRE

ANTALLET CYBERANGREP mot Norge har økt kraftig de siste årene. Flesteparten av angrepene hadde som formål å stjele informasjon fra datasystemene til store eller viktige norske bedrifter. For første gang på flere år blir det nå registrert færre cyberangrep. Det skyldes neppe at det er mindre som skjer, tror avdelingsdirektør Hans Christian Pretorius.

Hull i kartet. – Vi ser nå hvordan angriperne mer og mer tilpasser seg vår evne til å oppdage angrepene, for å forsøke å gå under radaren, sier han.

– Dette ser vi blant annet på typen varsler vi får. Når det tidligere gikk flere ulike varsellamper på et angrep, ser vi nå plutselig at flere av varsellampene er forsvunnet. Når vi gjør analyser, ser vi at angriperne har skrevet om kodene sine slik at de går under radaren. Der vi for eksempel før fant mønster i tekstblokker, er mønstrene helt borte eller tilfeldige. Når vi ser på det samlede bildet over bransjer som tidligere har blitt angrepet, ser vi nå at vi har hull i kartet vårt. På bransjer som tidligere jevnlig ble angrepet over internett, ser vi nå lite. Vi er rimelig sikre på at dette ikke betyr at angriperne ikke er der, det er heller det at vi ikke ser dem.

Taper våpenkappløpet. – *Betyr det at dere gjør en dårlig jobb?*

– Nei. Men det betyr at vi må jobbe enda bedre og raskere, og evne å rulle ut ny funksjonalitet i sensornettverkene våre raskere. Vi må hele tiden skrive om, tilpasse, og skrive inn nye ting i funksjonaliteten til sensorene. Speed is everything.

– *Hvorfor har dere ikke gjort dette allerede?*

– Dette har vi gjort hele tiden. Men det vi er bekymret for akkurat nå er at dette er en

> «
> Vi ser nå hvordan angriperne mer og mer tilpasser seg vår evne til å oppdage angrepene, for å forsøke å gå under radaren.

Hans Christian Pretorius avdelingsdirektør i Nasjonal sikkerhetsmyndighet.

type våpenkappløp, hvor den ene parten ligger foran, og den andre ligger bak. Akkurat nå tror vi at vi ligger bak i dette våpenkappløpet, og at tallene fra første halvår i 2015 er en indikasjon på det.

Cyberangrepene blir større. Nasjonal sikkerhetsmyndighet ser også at størrelsen på cyberangrepene går opp, sier Pretorius.

– Vi ser at trusselaktørene angriper flere bedrifter i samme bølge. Selv om det totale antallet har gått ned, vil man nok se at den samlede delen av angrepene er nesten like høy.

– *Hva bør norske bedrifter gjøre, når ikke en gang NSM NorCERT klarer å se angrepene?*

– Det er dessverre slik at trusselaktørene har et lavt gjerde å hoppe over. Det er de enkle tiltakene som vil stoppe dette. Det er så banalt som å oppdatere programvare, skifte ut gammel maskinvare med nyere maskinvare, hviteliste programmer, og de andre rådene vi anbefaler norske bedrifter å gjennomføre.

Store krav til bedriftene. – *Hvorfor gjør ikke flere dette?*

– Det har vi lurt på i lang tid. Til en viss grad skal man være ydmyk for at slike tiltak er komplisert i store driftsorganisasjoner med mange systemer og applikasjoner. Men det er helt prekært å gjennomføre nettopp disse rådene. Vi ser at tiden fra sårbarheter i IKT-systemer blir introdusert til det eksisterer verktøy på internett som kan utnytte sårbarhetene går dramatisk ned. Før gikk det ofte to til tre uker før verktøy for å utnytte nye sårbarheter lå tilgjengelig for hvem som helst på internett, nå er det snakk om en uke. Det setter enda større krav til bedriftene.

– *Hva er konsekvensene for norske bedrifter?*

– Vi er bekymret for at det tappes data fra norske bedrifter. Problemet nå er at vi ikke vet omfanget godt nok. Når det gjelder bedrifter som er tilknyttet sensornettverket vårt, ville vi oppdaget om at det gikk store mengder data ut av bedriften. Men det at vi tror aktørene nå gjør grep for å få fotfeste i IKT-strukturen, er noe vi er bekymret for.

– *Hva bør gjøres?*

– Vi setter nå inn mer ressurser på å raskere utvikle funksjonaliteten i sensorene våre, slik at vi får tilbake evnen vi bør ha. Vi ser allerede nå at vi begynner å detektere ting vi ikke så tidligere i vår. Men dette er et kappløp hele samfunnet må være med på, og ikke bare enkeltbedrifter eller NSM alene, sier Hans Christian Pretorius. <

FAKTA

HVORDAN STOPPE ANGREPENE?

Lurer du på hvordan du skal stoppe mesteparten av dataangrepene mot bedriften din? Les og innfør disse rådene (og tro oss, dette er tiltak som stopper 80-90 prosent av de vanligste angrepene, men som alt for få virksomheter har innført):

1. Oppgrader program- og maskinvare. Nyere produktversjoner har tettet flere sikkerhetshull enn gamle, og er bedre på sikkerhet.

2. Vær rask med å installere sikkerhetsoppdateringer. Kunnskap om nye sårbarheter sprer seg raskt. Derfor bør systemeiere være tilsvarende raske med å oppdatere, før noen bruker sårbarhetene til å bryte seg inn.

3. Ikke tildel sluttbrukere administrator-rettigheter. De fleste vanlige brukere har ikke behov for å installere programvare på maskinen. Overlat administrasjon og distribusjon av programvare til de som kan det.

4. Blokker kjøring av ikke-autoriserte programmer. Bare la brukerne kjøre godkjente programmer ved å bruke verktøy som Windows AppLocker.

Les mer på nsm.stat.no.

– HJELP, VI SKAL FÅ TILSYN!

Å få beskjed om man får tilsyn fra Nasjonal sikkerhetsmyndighet (NSM) er noe som virker skummelt for mange. Allikevel blir de fleste positivt overrasket over besøket, og resultatene viser seg gjennom synlig bedre sikkerhet for de fleste.

TEKST: FREDRIK RUUD JOHNSEN

SOM NORGES EKSPERTORGAN for informasjons- og objektsikkerhet, og det nasjonale fagmiljøet for IKT-sikkerhet, er NSMs oppgaver blant annet å stille krav, føre tilsyn og kontroll, og bygge kompetanse hos landets over 600 virksomheter som er omfattet av sikkerhetsloven.

– Det er viktig å få frem at tilsyn fra NSM er hjelp til selvhjelp, og ikke eksamen, slik mange tror. Det er ingen grunn til å frykte oss når vi kommer på besøk. Vårt mål er å hjelpe virksomhetene til å redusere de sårbarhetene som eventuelt finnes og hjelpe til med en mer systematisk tilnærming til sikkerhetsarbeidet, sier avdelingsdirektør for kontroll Vigdis Grønhaug.

I 2014 gjennomførte NSM 27 tilsyn. I år kommer tallet til å bli dobbelt så høyt, altså 54. Målet med tilsyn er å sette norske virksomheter i stand til å håndtere skjermingsverdig informasjon, og NSM tilbyr også råd og veiledning innenfor forebyggende sikkerhet til virksomheter som har behov for dette. Dette er med andre ord et kontinuerlig arbeid.

Mye har skjedd med tilsynsmetodikken vår de siste årene, og NSMs tilsyn er på ingen måte en bedømmelse av enkeltpersoner, seksjoner eller avdelinger. Tilsynene gjennomføres og ledes av en sertifisert revisjonsleder, med støtte fra fagrevisorer og fageksperter. Standarden NS-EN ISO 19011 – Retningslinjer for revisjon av styringssystemer ligger til grunn ved gjennomføring.

– Vi har gjennom flere år sett at virksomhetene ofte har de samme avvikene og sårbarhetene fra gang til gang. Fra og med 2014 så vi derimot at dette har endret seg vesentlig, og til det bedre. Vi mener årsaken hovedsakelig er at vi følger opp virksomhetene i mye større grad enn tidligere, blant annet må de rapportere at avvikene lukkes innen en gitt tidsfrist etter tilsyn, sier Grønhaug, som også nevner at fjernrevisjoner, eller brevtilsyn, ser ut til å

> «
> Det er viktig å få frem at tilsyn fra NSM er hjelp til selvhjelp, og ikke eksamen, slik mange tror.

Vigdis Grønhaug avdelingsdirektør for kontroll Nasjonal sikkerhetsmyndighet.

SLIK FOREGÅR NSMS TILSYN

Det er et mål for NSM at tilsyn skal være en strømlinjeformet prosess for virksomhetene som får besøk.

Varsel om tilsyn
Et tilsyn starter formelt ved at virksomheten får beskjed om hvilken del og hvilke fagområder det skal føres tilsyn med. Dette varselet inneholder vanligvis også krav om oversendelse av dokumentasjon som underlag for tilsynet. Unntaksvis kan tilsyn gjennomføres uten forutgående varsel, men dette skjer svært sjeldent.

Feltarbeid
Virksomheten får tilsendt en plan for gjennomføring av tilsynet før feltarbeidet starter. Feltarbeidet er normalt mellom to og fire dager med undersøkelser og intervjuer, og er stikkprøvebasert. Dermed blir ikke tilsynet en fullstendig gjennomgang av alt forebyggende sikkerhetsarbeid. Feltarbeidet avsluttes med et sluttmøte, der funn og dokumentasjonen blir presentert og diskutert.

Rapport
I etterkant av feltarbeidet mottar virksomheten en rapport fra NSM, sammen med eventuelle pålegg om forbedringer. Det er spesielt tre uttrykk som er verdt å nevne:

- **Avvik** er manglende samsvar med bestemmelsene og skal korrigeres.
- **Observasjon** er forbedringer NSM mener virksomheten bør vurdere, selv om de ikke er i strid med bestemmelsene.
- **Revisjonsbevis** er faktiske forhold eller annen informasjon, innsamlet under feltarbeidet, som kan verifiseres.

Virksomheten får mulighet til å uttale seg om rapportens innhold, før disse oversendes i endelig rapport. Påleggene i den endelige rapporten, kan påklages.

Avslutning
Tilsyn avsluttes formelt når virksomheten har korrigert eventuelle pålegg om forbedringer, og NSM har mottatt tilbakemelding om dette.

bidra til god forbedring av virksomhetenes sikkerhetsarbeid.

Hvem får tilsyn? Med over 600 virksomheter underlagt sikkerhetsloven, og i overkant av 50 tilsyn i løpet av et år, sier det seg selv at utvelgelsen av tilsynsobjekter må være systematisk.

– Vi kan komme på tilsyn til offentlige og private virksomheter som eier, bruker eller kontrollerer et skjermingsverdig objekt eller som i en eller annen form behandler skjermingsverdig informasjon. Vi prøver gjerne å følge temaer og virksomheter over tid, og gjennomfører såkalt risikobasert tilsyn, som betyr at virksomhetene er valgt ut med bakgrunn i risiko for sikkerhetstruende hendelser og sikkerhetsbrudd og risiko for mangler ved den forebyggende sikkerhetstjenesten. Dette ligger med andre ord mye bak planleggingen av tilsynsprogrammet fra år til år, sier Grønhaug.

I løpet av et tilsyn undersøker NSM om virksomheten beskytter skjermingsverdig informasjon og skjermingsverdige objekter i samsvar med gjeldende bestemmelser. Dette omfatter flere fagområder, og innebærer gjennomgang av dokumenter, intervjuer av ledelse og medarbeidere og stikkprøvekontroller.

Om det avdekkes avvik på tilsyn, er den vanligste reaksjonen at virksomheten får pålegg om å rette opp avvikene innenfor en gitt tidsfrist.

– I mer alvorlige tilfeller kan vi gi direkte pålegg, altså krav om umiddelbar utbedring, og i de alvorligste tilfellene kan virksomheten, i tillegg til pålegg og direkte pålegg, risikere inndragelse av godkjenninger, leverandørklarering og utstyr, samt anmeldelse. Det er viktig å understreke at dette skjer svært sjelden, sier Grønhaug.

Tilsyn er et sikkerhetsløft. NSMs overordnede mål for tilsyn er å bidra til å redusere sårbarheter og dermed begrense risikoen for at sikkerhetstruende hendelser skjer. Tilsyn skal være et sikkerhetsløft, og en gjennomgang av sikkerheten gir økt kunnskap og trygghet for at det virksomheten gjør er i samsvar med gjeldende regelverk.

Rapporter fra tilsyn gir også et bilde av hvordan regelverket fungerer, og gir et grunnlag for forbedring og videreutvikling av disse lovene og reglene. Målet for både oss i NSM og virksomhetene er jo at sikkerheten bedres, gjennom god beskyttelse av skjermingsverdig informasjon og objekter, og dermed også målet om bedre sikkerhetstilstand, avslutter Grønhaug. <

FAKTA

600
virksomheter er underlagt sikkerhetsloven

50
av dem får tilsyn i løpet av et år

BEDRE SIKKERHETSSTYRING SKAL GI BEDRE SIKKERHET

Under Sikkerhetskonferansen i mars lanserte Nasjonal sikkerhetsmyndighet en ny veileder for sikkerhetsstyring. Den trykte utgaven ble revet bort i løpet av konferansens første dag, og foredraget til NSMs Anne Gullhagen Larsen var fylt til siste stol. Men hva er nytt i den nye veilederen?

TEKST: FREDRIK RUUD JOHNSEN

HOVEDFOKUS I VEILEDEREN er på tilsiktede uønskede hendelser, som også er NSMs kjerneområde. På området for utilsiktede uønskede hendelser vises det til at andre fagmyndigheter har oppgaver innen råd og veiledning, og veilederen kan sees på som et supplement til blant annet Direktoratet for økonomistyring (DFØ) sin veileder og relaterte verktøy for internkontroll, og Direktoratet for forvaltning og IKT (DIFI) sin veileder for informasjonssikkerhet.

– Det er liten tvil om at sikkerhetsstyring er et tema som mange interesserer seg for, og vi har fått mange tilbakemeldinger etter at veilederen ble lansert i mars. Veilederen gir råd til virksomheter om hvordan et styringssystem for sikkerhet kan etableres og videreutvikles, og beskriver hvordan virksomheter kan sikre god lederforankring og oppfylle kravene om sikkerhetsdokumentasjon. I tillegg presenteres en strukturert metode for å arbeide med sikkerhetsstyring, sier Gullhagen Larsen, som har vært prosjektleder for veilederen.

Veilederen er generell og aktuell for alle som jobber helhetlig med sikkerhet. Den gir råd i tråd med praksis på området for sikkerhetsstyring og etablering av et styringssystem for sikkerhet.

Forankring, forpliktelse og forståelse. Gullhagen Larsen trekker frem tre momenter som er avgjørende for å bygge opp og videreutvikle et styringssystem for sikkerhet: forankring, forpliktelse og forståelse.

– Et styringssystem for sikkerhet må forankres hos virksomhetens ledelse. 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. Samtidig må virksomheten 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 i realiteten gjen-

« Det må etableres en tydelig ansvarsfordeling og klare rapporteringslinjer for å sikre at alle oppgaver i realiteten gjennomføres.

STYRINGSHJUL FOR SIKKERHET

nomføres. Sist, men ikke minst må det jobbes kontinuerlig med å bevisstgjøre, motivere, øke forståelsen og heve kompetansen innen sikkerhet på alle nivåer i virksomheten. En virksomhet er avhengig av at støttefunksjoner, som eksempelvis IT-drift og HR fungerer, og det må settes mål og krav til disse som er i samsvar med hovedmålene også innen sikkerhet, sier Gullhagen Larsen.

Veilederen består av fem hovedkapitler. Kapittel 1 beskriver veilederens formål, bakgrunn og målgruppe, samt oppbygging av veilederen. Kapittel 2 beskriver virksomhetsleders rolle og viktigheten av å forankre sikkerhetsarbeidet hos virksomhetsledelsen. Kapittel 3 beskriver en strukturert metode for å arbeide med sikkerhetsstyring. Kapittel 4 beskriver de viktigste rollene i virksomhetens sikkerhetsorganisasjon, og viktigheten av at ansvarsfordeling og rapporteringslinjer avklares. Kapittel 5 beskriver forskjellen på styrende, gjennomførende og kontrollerende dokumentasjon innen sikkerhetsarbeidet i en virksomhet.

– Et styringssystem for sikkerhet trenger ikke være komplisert, men det er viktig at den inneholder en prosess som skal bidra til å sikre at virksomhetens verdier er tilfredsstillende beskyttet mot hendelser. Vi har derfor utviklet et styringshjul som består av fem faser: planlegging, sikringsrisikovurdering, tiltak, oppfølging og kontroll, og rapportering. Det viktige er ikke utforming av modellen, men at den tar høyde for de ulike elementene man bør ha for å få en riktig prosess for den enkelte virksomhet, sier Gullhagen Larsen.

Sikkerhet er et lederansvar. For å få et styringssystem som fungerer er det avgjørende at man har forankring hos virksomhetens ledelse. Ledelsen må følge opp og etterspørre resultater. Det er ledelsen som må gå foran for å skape et miljø som gjør at medarbeidere tør å rapportere avvik og sårbarheter.

– Virksomhetens leder har ansvaret for den forebyggende sikkerheten i virksomheten, men også i underliggende virksomheter og hos leverandører. Det er virksomhetens leder som formelt bestemmer og fastsetter hvordan sikkerhetsarbeidet skal gjennomføres og organiseres. I hvor stor grad lederen selv er direkte involvert avhenger av hvordan virksomheten beslutter å organisere sikkerhetsarbeidet. Selv der lederen ikke er direkte involvert i det daglige sikkerhetsarbeidet, er det fremdeles lederen som er ansvarlig. Myndighet og oppgaver kan delegeres, mens ansvar ikke kan delegeres eller tjenesteutsettes, sier Gullhagen Larsen.

NSMs veileder for sikkerhetsstyring er tilgjengelig på nsm.stat.no. <

TRAPPER OPP JAKTEN PÅ ULOVLIG UTSTYR

Nasjonal kommunikasjonsmyndighet (Nkom) vil bruke to millioner kroner ekstra på å styrke evnen til å oppdage ulovlig bruk av teleutstyr, som falske basestasjoner. Samtidig er norske ekomnett blant de sikreste i verden, sier avdelingsdirektør Einar Lunde i Nkom.

TEKST: KJETIL BERG VEIRE

NKOM FIKK i revidert nasjonalbudsjett i vår 5,6 millioner kroner ekstra for å etablere et krise- og beredskapsrom, og styrke kapasiteten for å oppdage ulovlig frekvensbruk, som for eksempel fra falske basestasjoner. Det var Aftenposten som i desember i fjor rettet oppmerksomheten mot mulige falske basestasjoner i telenettene i Oslo sentrum. Flere falske basestasjoner var i bruk, hevdet Aftenposten. Basestasjonene kunne overvåke all mobiltrafikk i området, følge bevegelsene til enkeltpersoner, og avlytte mobiltrafikken. Funnene ble senere i sin helhet avvist av Politiets sikkerhetstjeneste, som etter omfattende etterforskning henla saken. Det fantes ikke bevis for falske basestasjoner.

Vil avdekke ulovlig utstyr. Nkom styrker nå uansett kapasiteten til å avdekke ulovlig bruk av utstyr som falske basestasjoner.

– Det vi ser på nå, er hva konkret vi trenger å styrke oss på, både når det gjelder utstyr og kompetanse, sier avdelingsdirektør Einar Lunde. De vil bygge på kompetansen som allerede finnes i Seksjon for frekvenskontroll, hvor Nkom har noen av de fremste i landet når det gjelder å monitorere frekvenser, sier han.

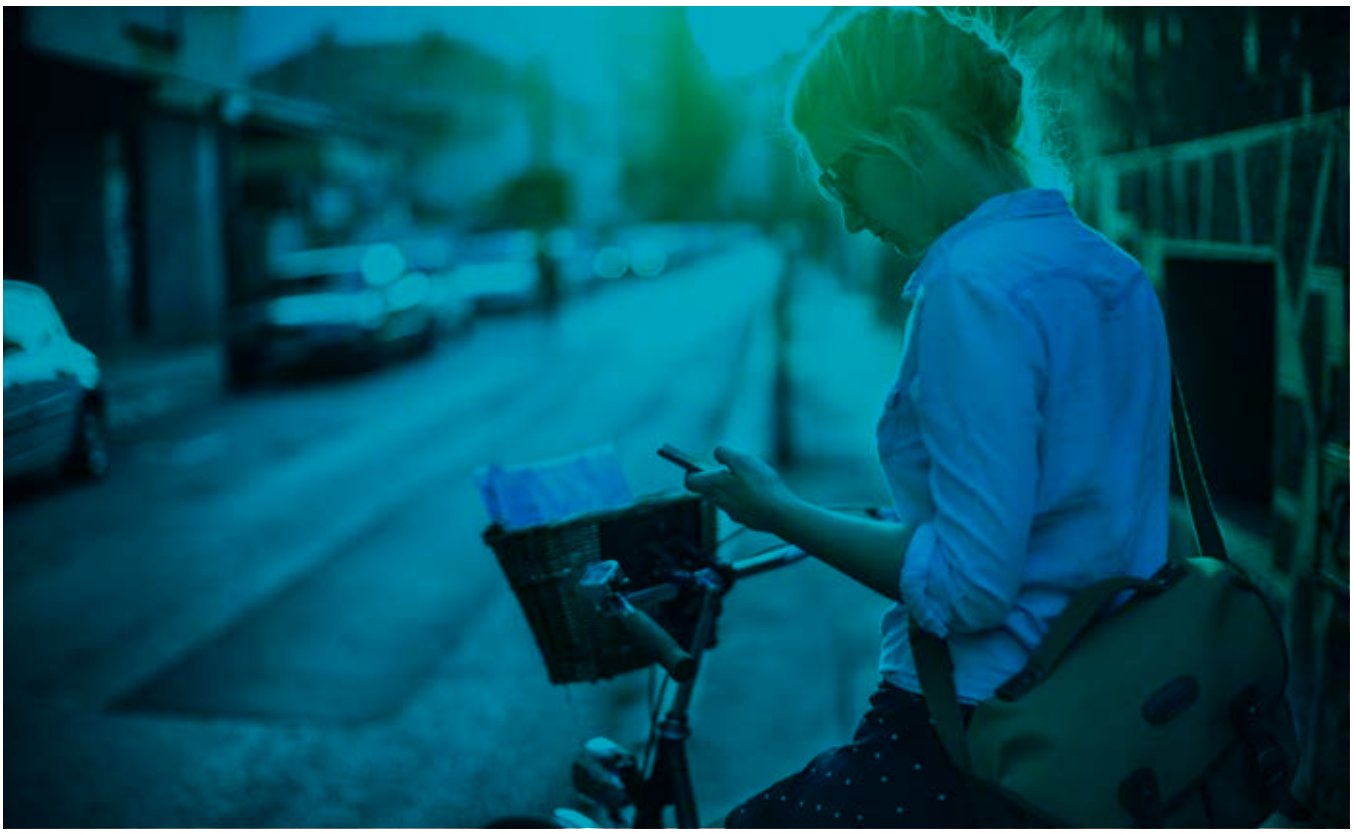
– Vi snakker om å bygge på det vi har, og så komplementere oss på utstyrssiden.

En potensiell trussel. – *Hvorfor er dette nødvendig?*

– Det er nødvendig av flere årsaker. Det er viktig for myndighetene å kunne påvise ulovlig bruk av utstyr og frekvenser. Og vi har oppgaven med å kontrollere ivaretakelse av konfidensialitet og integritet i ekomnettene. Bruk av falske basestasjoner presser begge disse aspektene.

– *Hvor stor er egentlig risikoen for falske basestasjoner i ekomnettene, nå etter at Politiets sikkerhetstjeneste har henlagt saken?*

Einar Lunde avdelingsdirektør i Nasjonal kommunikasjonsmyndighet.



– Først og fremst så vet vi at trusselen er der, selv om dette kanskje ikke er teknologien statlige aktører er mest interessert i for tiden. Vi vet det er et marked for denne typen utstyr. Hvis det er et marked, kan vi forvente at det er kjøpere som vil bruke det. Vi ser fra statistikk fra andre land at dette er utstyr som blir brukt. Hvis det er en potensiell trussel, må man forvente at myndighetene har utstyr for å oppdage det, og vi må ta konsekvensene av at vi ikke er i stand til å gjøre dette godt nok i dag, sier Lunde. Derfor er vi veldig glade for at ansvarlig myndighet har tatt det alvorlig, og bevilget penger for å lukke gapet.

> «
> Som myndighet mener vi at vi har nett som er i øverste klasse hvis vi ser på det globalt. Da støtter vi oss på vurderinger fra tredjepart som mener de norske ekomnettene er de beste i verden.

Best i verden. – *Hvor sikre er egentlig de norske ekomnettene?*

– Som myndighet mener vi at vi har nett som er i øverste klasse hvis vi ser på det globalt. Så kan man jo stille spørsmål ved om vi er uhildet til å mene noe om det. Da støtter vi oss på vurderinger fra tredjepart, som Karsten Nohl og Security Research Lab, som mener de norske ekomnettene er de beste i verden. Likevel er det klart vi har sårbarheter i nettene, og der har vi gjort mye sammen med netteierne for å lukke disse.

Mer rådgivning. Og det er ikke alltid markedet styrer til det beste når det gjelder sikkerhet, sier Einar Lunde. Det gjelder blant annet 2G-teknologien. Teknologien blir brukt i stort omfang over hele landet, og finnes i stort sett alle maskin-til-maskin-løsninger, som alarmløsninger for hus og hytte, overvåkning av maskiner og strømmålere. Samtidig har teknologien store sikkerhetsmessige sårbarheter sammenlignet med 3G og 4G.

– Vi jobber for å fase ut gammel teknologi, og der tror jeg vi ikke har vært aggressive nok. Vi har overlatt utfasing av gammel teknologi til markedet, i god tradisjon med våre europeiske kollegaer. Det er ikke alltid markedet styrer til det beste, sier Einar Lunde. Det vil Nkom rette på gjennom en mer aggressiv informasjon og påvirkning i tiden fremover, avslutter han. ‹

SAMARBEIDET MED SINTEF

For å stå best mulig rustet i kampen mot dataangrep styrker NSM samarbeidet med SINTEF. Samarbeidet, som ble innledet i 2013 med en rammeavtale og et pilotprosjekt, blir stadig utvidet til en rekke områder innen IKT-sikkerhet.

TEKST: JAN ANDRE ENDRESEN

NSM HAR GJENNOM sin satsing på forskning og utviklingsarbeid (FOU) blitt en attraktiv aktør å samarbeide med for utenlandske samarbeidspartnere. Særlig innenfor emisjonssikkerhet har NSM levert nyskapende og gode leveranser innen måleteknologi for IKT-systemer som benytter trådløse nettverksløsninger. Mange av NSMs utenlandske samarbeidspartnere har innledet tette samarbeid med sine respektive nasjonale fagmiljø. For NSM har det vært et mål om å bygge opp nasjonal kompetanse ved å samarbeide med norske kompetanseinstitusjoner. SINTEF er en naturlig samarbeidspartner for NSM fordi de er Skandinavias største uavhengige forskningsinstitusjon med lang erfaring i oljeindustrien, IKT-sikkerhet og mobiltelefoni. De utfører oppdragsforskning som FoU – partner for næringsliv og forvaltning, og har 2000 medarbeidere som i fjor utførte 5300 oppdrag for 3600 kunder til en verdi av 3 milliarder kroner.

– SINTEF har kompetanse på kommunikasjonsteknologi som NSM kan dra nytte av. Blant annet har SINTEF tidligere gjennomført forskning på kommunikasjon under vann på oppdrag for oljeindustrien, som har vist seg å ha verdi også for oss, sier seksjonssjef Hans-Petter Gundersen i NSM.

En del av NSMs arbeid er gradert, og som en konsekvens av dette har 20 ansatte i SINTEF blitt sikkerhetsklarert. Samtidig ble det fort klart at det var behov for å opprette et møtelokale hvor gradert tale og data kunne håndteres på en sikker måte. SINTEF etablerte på kort tid et eget møterom i egne lokaler som senere er blitt godkjent for HEMMELIG av NSM. Det jobbes også for å etablere et videokonferansesystem for og få lettere tilgjengelighet mellom fagpersonellet i SINTEF og NSM.

Prosjekter. Hensikten med FoU prosjektene er å gjenbruke kompetanse hos SINTEF som kan være relevant for NSM. Målet er hele tiden å bygge opp kompetanse hos SINTEF og NSM. NSM skal til en hver tid kunne tolke resultater og forstå disse slik at dette kan gjenbrukes i forskjellige sårbarhetsvurderinger av IKT- systemer. Dette forutsetter en tett oppfølging av aktiviteter fra begge parter.

En av NSMs oppgaver er å godkjenne telefoner beregnet for gradert tale. SINTEF har hjulpet NSM med å konstruere en lukket

> «
> Kompetanse NSM tidligere måtte utenfor landets grenser for å innhente, viste seg å være tilgjengelig ved SINTEF.

FAKTA
SINTEF

2000
medarbeidere

5300
oppdrag

3600
kunder

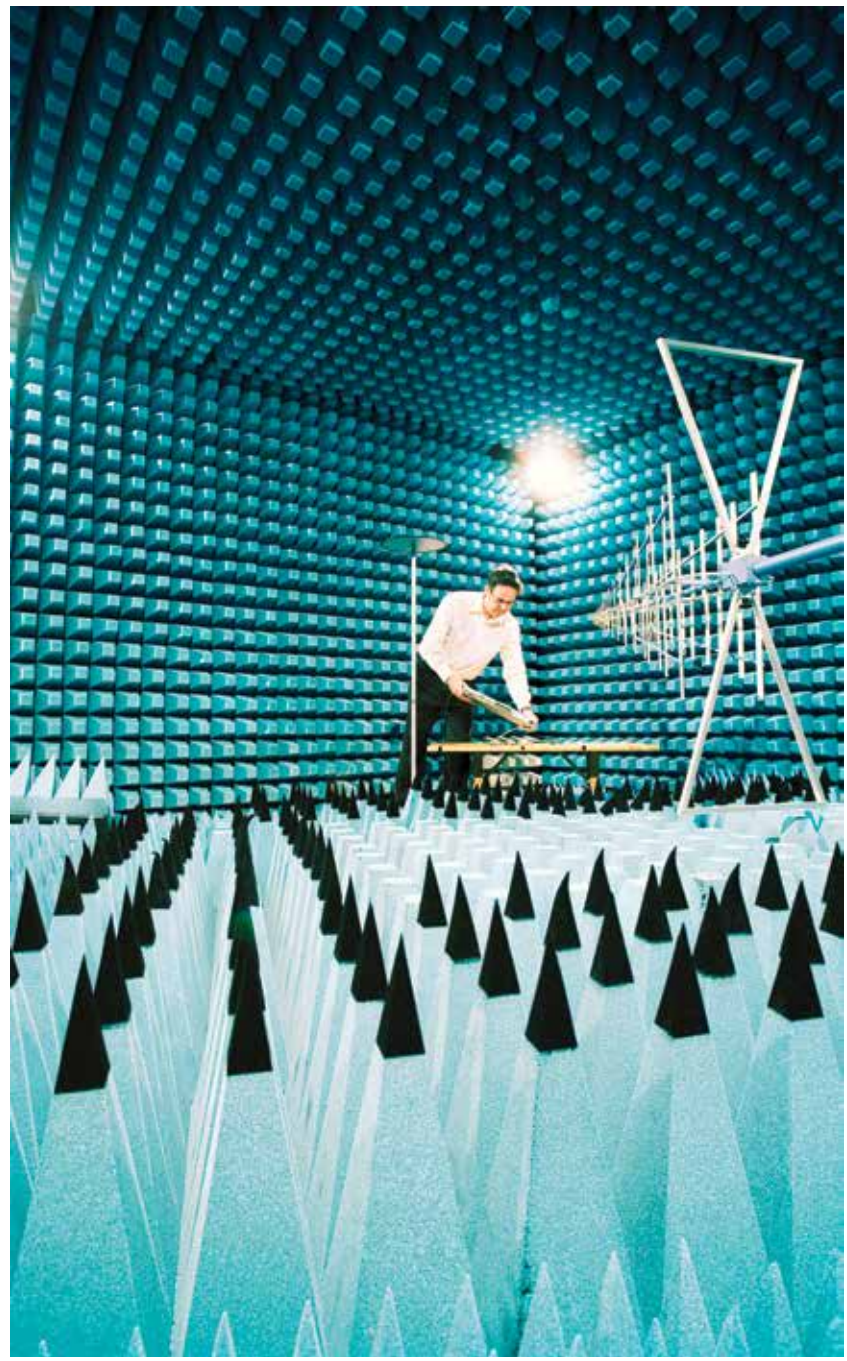
basestasjon, en såkalt PICO-celle, slik at tester av telefoner blir mest mulig realistiske uten at man trenger å koble seg til eksisterende GSM-nett. NSM og SINTEF samarbeider også for å avdekke sårbarheter i pc-skjermer beregnet for gradert informasjon.

Etter at rammeavtalen med SINTEF ble signert høsten 2013 har det blitt gitt flere avrop opp mot rammeavtalen innen forskjellige temaer ut fra NSM sine behov i FoU-prosjekter. Per dags dato er syv ulike samarbeidsprosjekter mellom NSM og SINTEF i gang eller i oppstartsfasen.

– Samarbeidet startet med et enkelt prosjekt, men har i ettertid vokst. Kompetanse NSM tidligere måtte utenfor landets grenser for å innhente, viste seg å være tilgjengelig ved SINTEF i Trondheim, sier seksjonssjef Hans-Petter Gundersen i NSM.

Samarbeidet med SINTEF har så langt vist seg å være et riktig og viktig valg for NSM. Samarbeidet har gitt NSM tilgang til norsk kompetanse innen svært spesielle områder hvor det trengs lang erfaring og spisskompetanse for å kunne dypdykke i teknologien. Samarbeidet har også vært givende for SINTEF.

– NSM har unik kompetanse og erfaring som er av stor verdi for våre forskere. Vi er i fellesskap godt i gang med en rekke prosjekter og forstudier som skal bidra til å redusere risiko for private og offentlige virksomheter, sier konserndirektør i SINTEF IKT Aage Thunem. <



HVORFOR BØR NSM FORSKE?

Forskning gir kunnskap. Forskning gir bedre sikkerhet. NSM har en stor forskningsportefølje innen flere ulike retninger som skal bidra til økt kunnskap som gir bedre løsninger.

TEKST: MONA STRØM ARNØY

OPPDRAGET TIL NSM er å bidra til og styrke sikkerheten i samfunnet. For både å skaffe NSM bedre oversikt over sikkerhetstilstanden, og å videreutvikle sikkerhetstiltak er forskningsprosjekter helt avgjørende.

Bredt ansvarsområde. NSM har et ansvarsområde som går fra forebyggende arbeid, hendelseshåndtering og til kontrolldimensjonen. Forskningsprosjektene understøtter våre ansvarsområder og er integrert med virksomheten og de planer NSM har.

Security by design. NSMs forskning er innrettet i ulike områder: kompetansebygging, forebyggende IKT-sikkerhetstiltak, hendelseshåndtering og beredskap, støtte til norsk kryptoindustri og, ikke minst, personellsikkerhet.

– Vi har også forskningsprosjekter innenfor fysisk sikkerhet. Et samarbeidsprosjekt med Bergen Arkitektskole og PST går på å utvikle sikkerhet integrert fra byggestart – secure by design. Resultatet av dette prosjektet vil komme i bokform senere, sier Christian Reusch i NSM.

Understøtter Forsvaret. NSMs forskningsportefølje understøtter Forsvaret. Forsvarssektoren har en om-fattende forskningsstrategi og et av de kritiske FOU områdene er hensynet til sikkerhet.

– Våre prosjekter understøtter dette. Vi har mange prosjekter rettet mot Forsvaret innenfor mange ulike områder, sier Reusch, og legger til at det er et kappløp å utvikle forebyggende tiltak i takt med et økende trusselbilde.

Større vilje enn budsjettet tillater. – Vi har kommet veldig godt i gang med mange prosjekter. Det er et ønske om at vi kunne gjort enda mer. Vi har flere forskningsideer og prosjektplaner enn vi har midler til å realisere. Det er knallhard prioritering på hva som skal satses på først, sier en oppriktig forskningsansvarlig.

NSMs forslag fremmes til et prosjektråd som tar stilling til om vi skal innvilges oppdraget. I noen prosjekter er NSM partnere med andre institusjoner eller etater.

– Det er viktig å sørge for at våre prosjekter, og resultatene fra dem, medfører gevinstrealisering for sektoren, poengterer Christian Reusch. <

Christian Reusch
Nasjonal sikkerhetsmyndighet.

FORSKET PÅ SIKRINGSRISIKO

Hvilke verdier har jeg? Hvilken risiko sitter jeg på? Det er ikke alltid lett å finne svar. For å hjelpe virksomheter til å identifisere sin risiko i forhold til de verdier de besitter, satte NSM i gang et stort forskningsprosjekt for flere år siden – kalt SÅKOV. Hensikten med dette prosjektet var å analysere årsaker til mangler i sikkerhetstilstanden, og utarbeide konkrete verktøy for å forbedre denne. De første delene er sluttført for en stund siden og nylig er også den siste delen sluttført. Arbeidet er ledet av flere fagpersoner i NSM, med støtte fra forskere i Forsvarets forskningsinstitutt FFI. Det er FFI som har gjennomført dette forskningsarbeidet for NSM.

Den siste og avsluttende delen av SÅKOV har resultert i en enkel håndbok som viser hvordan virksomheter kan gjennomføre sikringsrisikovurderinger. Håndboken vil bli klar for distribusjon i løpet av oktober. Da vil den legges ut på nsm.stat.no

– Håndboken inneholder beskrivelser for hvordan virksomheter kan planlegge, tilrettelegge og organisere arbeidet i forkant av sikringsrisikovurderinger. Håndboken inneholder metode og verktøy for hvordan vurderingene kan gjennomføres i praksis, forteller seksjonssjef Jan Fosse i seksjon for Virksomhetssikkerhet i NSM.

Målgruppen for håndboken er virksomheter som har verdier som trenger beskyttelse. Verdiene som bør beskyttes har imidlertid ulik karakter og alle trenger ikke sikres like godt.

– Hensikten med håndboken er å forenkle, effektivisere og dokumentere arbeidet med sikringsrisiko i virksomhetene. Håndboken legges opp slik at den kan brukes av virksomheter med ulik kompetanse, forskjellige typer verdier og ulikt trusselbilde, forteller Fosse. Han legger til at håndboken bør være spesielt nyttig for ansatte i sikkerhetsorganisasjoner som skal kartlegge risikoer knyttet til tilsiktede uønskede handlinger og utilsiktede uønskede hendelser.

« Håndboken inneholder beskrivelser for hvordan virksomheter kan planlegge, tilrettelegge og organisere arbeidet i forkant av sikrings-risikovurderinger.

HVORDAN SKAL MAN SIKRE SEG MOT ET VÆPNET ANGREP?

De siste årene har flere offentlige og private virksomheter blitt angrepet av personer med våpen. Finnes det forebyggende sikkerhet mot en angriper av denne typen? Hva skal en virksomhet gjøre for å beskytte seg mot denne trusselen?

TEKST: FREDRIK RUUD JOHNSEN

VÆPNEDE TERRORANGREP mot satiremagasinet Charlie Hebdo i Paris og i København har de siste månedene økt oppmerksomheten rundt angrep med skytevåpen. Dette er ikke en ny type trussel, men en variasjon over en økende trend. Skoler, sykehus, arbeidsplasser og offentlige forsamlinger kan alle bli utsatt for et væpnet angrep, også med skytevåpen. Et skytterangrep er ikke en gisselsituasjon, men en eller flere personer med skytevåpen som ønsker å påføre mest mulig skade og død. Noen av disse er mentalt forstyrrede personer, andre har politiske motiver. Det er uansett samme utfall – uskyldige liv blir rammet.

Amerikanske Federal Bureau of Investigation (FBI) har studert denne typen angrep, såkalte «active shooters», i perioden 2000-2013, og trenden er økende. Til grusom effekt har vi også nasjonalt hatt våre erfaringer på Utøya 22. juli 2011. Skytterangrep er plutselige og uforutsigbare. I FBIs studie fremkommer det at denne type angrep er enten over på mindre enn 15 minutter, eller inntil det kommer en væpnet respons for å stoppe hendelsen.

Forebyggende tiltak. Det kan virke som en håpløs oppgave å beskytte seg mot denne typen angrep, men det finnes grep en virksomhet kan ta for å både forhindre at et angrep skjer, og for å minimere skaden hvis angrepet er et faktum.

– En del forebyggende tiltak mot denne typen trussel er organisatoriske, andre fysiske. Begynn med å gjøre en sikkerhetsvurdering mot denne typen trussel. Adgangskontroll og resepsjonsutforming kan forebygge din virksomhet fra å bli et mål i et terrorangrep. Fellesområder kan utformes slik at disse ikke ligger i umiddelbar nærhet til inngangen. Man skal vurdere barrierer og rømningsveier ved forebygging mot en slik type angrep. Første steg er å ha barrierer som begrenser adgang, dernest sinker en gjerningsperson. Dette kan gjøres gjennom soneinndeling ved virksomheten. Samtidig bør personellet kjenne til minst to rømningsveier, slik at man kan få til en effektiv evakuering. Inntil politiet rykker ut med væpnet respons, er du alene med å håndtere angrepet, sier seniorrådgiver Håvard Walla i NSM.

Walla nevner for eksempel tiltak som å innføre panikk-kode på adgangskortet. Her taster man en kode lik sin normale, men med en liten

> «
> Det aller viktigste tiltaket mot skytterangrep er å ha en plan, og å øve på planen.

Håvard Walla seniorrådgiver i Nasjonal sikkerhetsmyndighet.

endring dersom man er tatt som gissel og tvinges til å åpne for en angripende skytter. Dette knyttes opp til en stille alarm som advarer de øvrige på arbeidsplassen, eksempelvis gjennom SMS. For noen virksomheter kan det være også være aktuelt med panikkrom, hvor man kan stenge seg inne med forsterkede vegger og tak.

Plan og øving. – Det aller viktigste tiltaket mot skytterangrep er allikevel å ha en plan og å øve på planen. Å innføre en panikk-kode på adgangskortet har liten effekt dersom man ikke gjennomfører en øving. Som man sier innen operative yrker; man stiger ikke til nye høyder i krise, man synker til sitt nivå av trening. Gjennomgå mulige scenarier og sørg for at de ansatte er kjent med alle nødutganger og anbefalte handlinger dersom et skytterangrep skulle inntreffe, sier Walla.

Vær oppmerksom på at når politiet kommer til en slik hendelse, er det ikke for først å ta seg av sårede og overlevende.

– Politiet er der for å stoppe gjerningspersonen. Forhold deg rolig, selv om politiet peker på deg med våpen. Hold hendende dine synlig og følg politiets instrukser. Vær forberedt på at politiet kan behandle deg som en mulig gjerningsperson og legge deg i bakken, sier Walla, som understreker at dette er traumatiske situasjoner og at det derfor er viktig for at virksomhetene har handlingsplaner for oppfølging etter en slik hendelse som del av sin kriseberedskap. Dette gjelder pårørendekontakt og krisestøtte.

Tre huskeregler ved væpnede angrep.
Basert på råd fra USA og Storbritannia, er det tre huskeregler man kan ta med seg ved et skytterangrep:

- **Løp:** dersom skuddene ikke er i umiddelbar nærhet, løp for å komme deg i sikkerhet. Ikke ta med deg noe og hold hendene synlig. Advar andre og unngå å samle dere på brannoppsamlingsplasser.
- **Skjul:** er du i nærheten av skuddene, barrikader deg og gjem deg samt lås dører der det er mulighet. Sett telefonen på lydløs. Forhold deg rolig.
- **Handle:** rapporter når du har mulighet ved å ringe 112. Om du ikke kan snakke, la telefonlinjen ligge åpen slik at nødsentralen kan lytte. Dersom du ikke har annet valg, angrip skytteren når vedkommende er kommet til deg – det står om livet.

Britiske og amerikanske råd skiller seg litt ad på det siste punktet. Britenes råd er *«Angrip kun dersom det er siste utvei»*, og amerikanernes råd er å være så hensynsløs som over hodet mulig. Når du først gjør dette, er det ingen vei tilbake. <

ØKNING I LØSEPENGEVIRUS

Løsepengevirus dukker opp med jevne mellomrom. I 2015 har trenden for denne typen trusler mot norske virksomheter igjen vært økende.

TEKST: FREDRIK RUUD JOHNSEN

I 2012 BLE flere nordmenn utsatt for et såkalt «politivirus». Viruset låste PCen til en rekke brukere, og hevdet i en melding på skjermen, tilsynelatende fra politiet, at den ikke ville bli åpnet før brukeren hadde betalt bøter på flere tusen kroner.

I første halvdel av 2015 så NSM igjen flere eksempler på denne typen utpressingssaker. Skadevaren CBT-locker gjør ofrenes filer ubrukelige, og de får krav om å betale løsepenger for å låse opp innholdet. Kravet var i dette tilfellet betaling i bitcoins tilsvarende 1500 dollar.

– Det har vært en oppblomstring av datakidnapping og løsepengevirus i Norge i år , både mot privatpersoner, bedrifter og kommuner. For eksempel ble vi varslet av et konsulentselskap at 70 av kundene deres var rammet samtidig. Denne typen virus har eksistert i mange år i ulike varianter, som stort sett har truffet privatpersoner. CBT-Locker har sterkere kryptering, og de som har blitt truffet har vært nødt til å gjenopprette systemene sine fra backup, sier Hans Christian Pretorius, direktør for operativ avdeling i NSM.

Ifølge Pretorius er det svært vanskelig å oppdage denne typen skadevare, og mange antivirusprogrammer og sikkerhetsløsninger har problemer med å fange opp løsepengevirus.

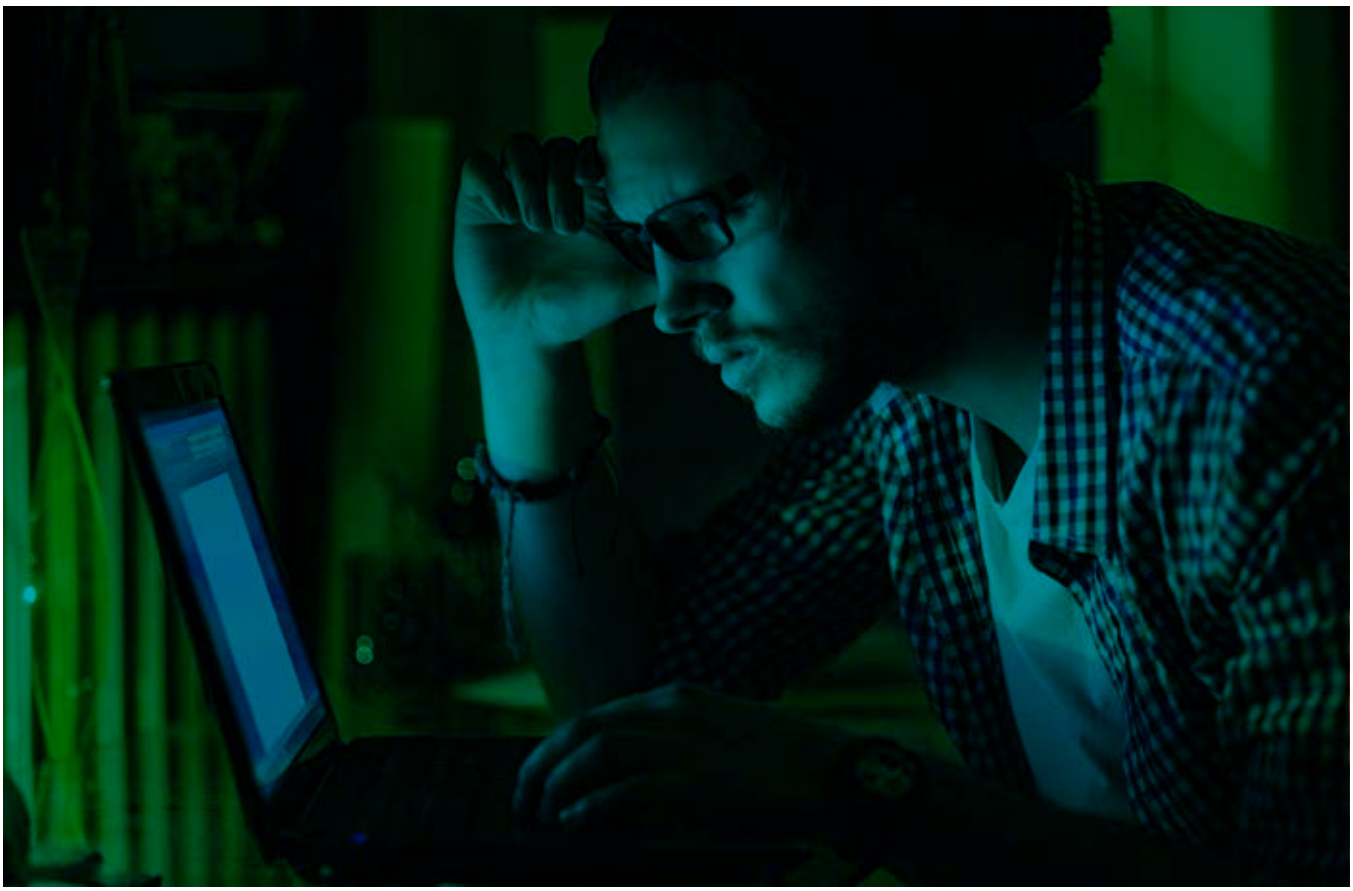
Sikkerhetsselskapet Symantec meldte tidligere i år at antallet forsøk på kidnapping av informasjon økte med 113 prosent fra 2013 til 2014.

– Krypteringen i dagens løsepengevirus er virkelig god, og nærmest umulig å knekke. Det eneste botemiddelet er gjenoppretting av data fra sikkerhetskopi, sier Pretorius, som anbefaler at man ikke betaler utpresserne. Det finnes eksempler på at man får feil nøkkel eller ingen nøkkel i det hele tatt. Dermed er man like langt.

Forventer økning i løsepengevirus. På sensommeren i år skrev flere medier om et løsepengevirus som maskerte seg som en video-

> «
> Krypteringen i dagens løsepengevirus er virkelig god, og nærmest umulig å knekke. Det eneste botemiddelet er gjenoppretting av data fra sikkerhetskopi.

Hans Christian Pretorius avdelingsdirektør i Nasjonal sikkerhetsmyndighet.



spiller for pornografiske filmer på mobiltelefoner. De som lastet ned applikasjonen visste derimot ikke at de ble fotografert av mobiltelefonens kamera mens programmet ble installert. Dette bildet ble så brukt som utpressingsmiddel for å få «offeret» til å betale 500 dollar for å unngå at bildet ble publisert.

Etter hvert som flere og flere enheter blir koblet til internett, fra klokker til biler, forventer eksperter også at omfanget av løsepengevirus vil øke. Det er også bare fantasien som setter grenser. Antallet forskjellige løsepengevirus økte med 127 prosent fra første kvartal 2014 til samme kvartal i år, ifølge tall fra McAfee Labs, og omfanget er forventet å øke ytterligere.

Symantec analyserte tidligere i år 50 internettilkoblede enheter rettet mot husholdninger, og fant ut at sikkerheten i disse enhetene var svært svak. Symantec fant blant annet ut at nesten en femtedel av dingsene ikke brukte en sikker tilkobling mot internett, og svært svake passordregler, noe som gjør det lett for uvedkommende å ta kontroll over enheten.

– Vi er fortsatt tidlig i utviklingen av «internet of things», og vi må forvente at nye sårbarheter dukker opp og blir utnyttet, sier Pretorius. <

IKKE NYTT FENOMEN

Løsepengevirus er ikke noe nytt selv om det ble registrert få tilfeller i Norge før 2012. Det første løsepengeviruset kan dateres helt tilbake til 1989. Dr. Joseph Popp skal da ha sendt ut syv tusen disketter med trojaneren i posten til forskjellige mottakere. Innholdet på disketten så ut til å være informasjon om AIDS, og 3.000 av mottakerne var hentet fra en deltakerliste for WHO-konferansen om AIDS i Stockholm. Et av navnene til skadevaren har derfor blitt «AIDS-trojaneren», et annet navn er «Cyborg trojan» som er basert på firmanavnet. 7.000 disketter ble sendt ut til abonnenter av magasinet PC Business World. Etter 90 oppstarter vil brukerne få en melding fra trojaneren. Etter dette krypterte trojaneren filnavn på maskinen og opprettet en fil som fylte opp harddisken. På denne måten ville ikke maskinen kunne brukes før man betalte lisensavgiften til programvaren.

FAKTA

113%

Antallet forsøk på kidnapping av informasjon økte med 113 prosent fra 2013 til 2014.

ET HELHETLIG IKT-RISIKOBILDE

I begynnelsen av oktober la Nasjonal sikkerhetsmyndighet frem rapporten «Helhetlig IKT-risikobilde 2015». Her følger sammendraget av rapporten, som kan lastes ned i sin helhet på nsm.stat.no.

TEKST: FREDRIK RUUD JOHNSEN

HELHETLIG IKT-RISIKOBILDE 2015 omfatter utviklingstrekk, utfordringer og mulige tiltak av betydning for statssikkerhet, samfunnssikkerhet og individsikkerhet. Rapporten har et bredt nedslagsfelt ved å omhandle utfordringer både for tilsiktede og utilsiktede uønskede hendelser knyttet til IKT-utstyr og internett.

NSM har sett flere eksempler på vellykkede datainnbrudd der angriperne har fått tilgang til virksomhetskritisk informasjon, og at forretningshemmeligheter, kursdrivende eller annen sensitiv informasjon har kommet på avveier. Skadevirkningene kan variere fra sak til sak, men de alvorligste konsekvensene skjer i et langsiktig perspektiv hvor virksomhetene etter tap av immaterielle verdier mister sin konkurranseevne og eksistensgrunnlag.

For offentlige virksomheter kan skadevirkningene være tap av tillit til det offentliges digitale løsninger på en slik måte at det påvirker samfunnets evne til å ta ut ytterligere gevinster ved modernisering og digitalisering.

Potensielt store konsekvenser. Konsekvensene av vellykkede datainnbrudd kan også medføre tap av personopplysninger og annen sensitiv informasjon. Risikoen for mulig tap av virksomhetens omdømme er også til stede. Nedetid på nettsider eller IKT-tjenester er også en konsekvens for mange virksomheter, slik for eksempel flere norske banker opplevde i 2014. Nedetid i kritiske samfunnsfunksjoner som f.eks. helsevesen, energi- og vannforsyning kan ha alvorlige konsekvenser og medføre skade på innbyggernes liv og helse.

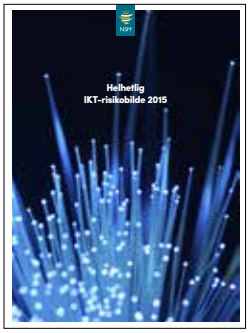
Gitt de verdier som står på spill, en økende og mer sofistikert trussel, og gitt betydelige sårbarheter i det norske samfunnet, konkluderer NSM slik om det helhetlige IKT-risikobildet:

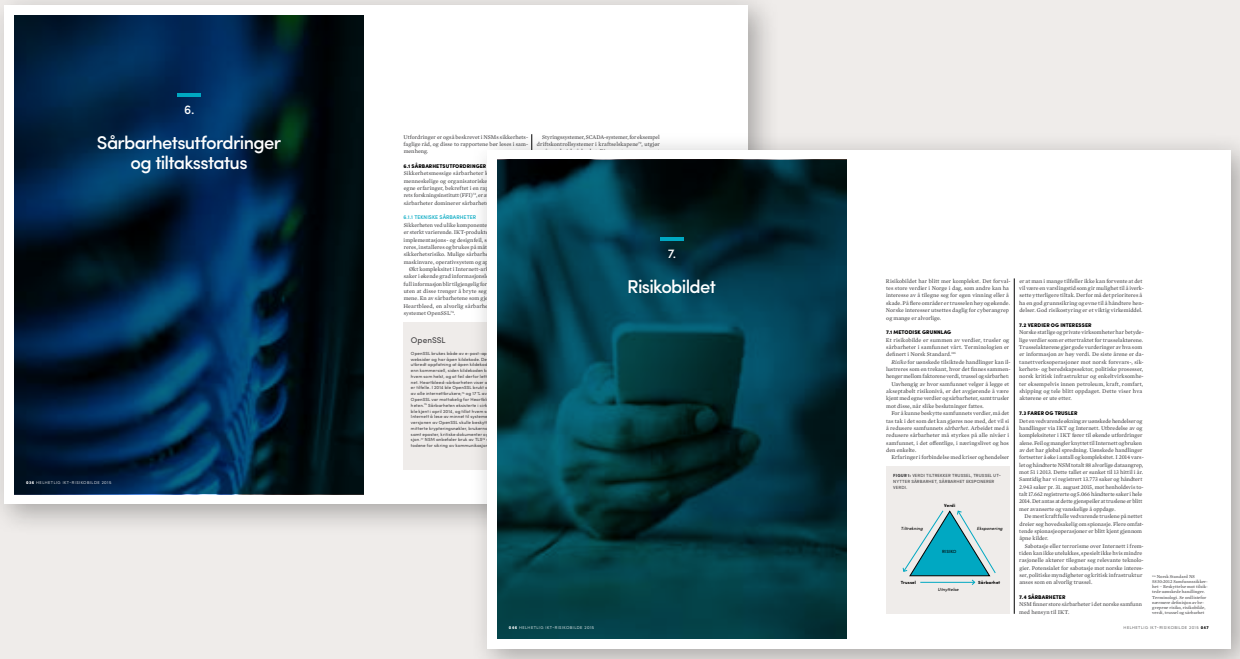
NSMs overordnete vurdering av IKT-risikobildet er at det er høy risiko forbundet med bruk av IKT. Dette gjelder på alle nivåer i samfunnet. Alle er mål for IKT-angrep.

Det er stor risiko forbundet med at store og små virksomheter ikke tar i bruk grunnleggende tiltak for å sikre sine IKT-systemer. Sårbarhetene er den dimensjonen i risikobildet alle kan gjøre noe med. De samme sårbarhetene observeres gjentatte ganger og avslører at IKT-sikkerhetsarbeidet er mangelfullt styrt.

Betydelige verdier. Norske statlige og private virksomheter har betydelige verdier som er ettertraktet for trusselaktørene. Trusselaktørene gjør gode vurderinger av hva som er informasjon av høy verdi. Konsekvensen av mangelfull IKT-sikkerhet er at det kan tapes store verdier.

Uønskede handlinger via IKT og internett fortsetter å øke i antall og kompleksitet. Imidlertid er det registrert færre alvorlige hendelser enn før. Vi har indikasjoner som tyder på at dette skyldes at dataangrepene har blitt mer





avanserte og at det er betydelig læringsevne hos trusselaktørene.

Kunnskapsnivået og tilgang på fagkompetanse er for lavt, i et spenn fra den vanlige IKT-bruker til spesialister i hendelseshåndtering. Dette hemmer evnen til å gjennomføre gode IKT-sikkerhetstiltak. Dette vil sannsynligvis også føre til at det nasjonalt ikke vil finnes tilstrekkelig fagkompetanse til å håndtere større IKT-angrep. I tillegg er det en utfordring å følge med på konsekvensene av den teknologiske utviklingen for IKT-sikkerhetsområdet. Mangelfull rapportering av alvorlige IKT-hendelser vil svekke evne til forbedring og læring innen forebyggende IKT-sikkerhet.

Det er behov for å få etablerte strukturer til å virke bedre gjennom å videreutvikle samarbeidsarenaer og gode samarbeidsmekanismer, slik at prosesser rundt politikkutforming, forebyggende IKT-sikkerhet og hendelseshåndtering forbedres. Samarbeid mellom ulike offentlige og private aktører kan med fordel utvikles videre. Utvikling, forvaltning, og drift av offentlige IKT-løsninger kan samordnes bedre.

Manglende fellesløsninger for IKT-systemer for sensitiv, lavgradert og høygradert informasjon kan føre til dårlig informasjonssikkerhet og kan være kritisk i en krisesituasjon.

Ugradert elektronisk kommunikasjon blir i liten grad blir kryptert. Dette senker terskelen for vellykket avlytting og sensitiv informasjon kan kompromitteres.

Tilbud om gode tjenester, som for eksempel inntrengningstesting av datasystemer, sertifiseringsordninger eller akkrediteringsordninger, blir ikke tilstrekkelig utviklet. Dette kan føre til utilstrekkelig koordinering av politikkutforming, forebyggende tiltak og krisehåndtering.

Sensorkapasiteten i varslingssystemet VDI er ikke tilstrekkelig utviklet. Utviklingen av truslene setter den nasjonale evnen til å håndtere IKT-hendelser under betydelig press og reduserer evnen til både å oppdage og håndtere disse. Det er risiko for at alvorlige IKT-angrep blir oppdaget for sent og ikke blir håndtert på en tilfredsstillende måte.

For å redusere risikoen er det behov for en omfattende nasjonal satsning på IKT-sikkerhet i årene som kommer.

NSM har i sikkerhetsfaglig råd foreslått 72 tiltak for å forbedre sikkerhetsarbeidet. En rekke av disse er relevante for IKT-sikkerhet og er gjentatt i Helhetlig IKT-sikkerhetsbilde. Det foreslås tiltak for å forbedre kunnskapssituasjonen, forbedre nasjonal styring og samarbeid, forbedre forebyggende sikkerhet og forbedre evnen til hendelseshåndtering.

NSM gjentar også sitt råd om å gjennomføre 10 (4+6) grunnleggende sikkerhetstiltak, som vil forhindre 90 % av alle dataangrep. 100 % av de alvorlige dataangrepene NSM har sett de siste 24 månedene hadde blitt stoppet dersom den rammede virksomheten hadde gjennomført 4 av de enkle tiltakene som NSM anbefaler. <

NORGE MÅ SATSE MER PÅ SIKKERHET

– Det er behov for en omfattende satsing på sikkerhet i Norge frem mot 2020. Risiko- og sårbarhetsbildet har blitt mer komplekst og vi må ta tak i det vi kan gjøre noe med for å kunne beskytte verdiene vi har i samfunnet, sier direktør i Nasjonal sikkerhetsmyndighet, Kjetil Nilsen.

TEKST: FREDRIK RUUD JOHNSEN

10. SEPTEMBER overrakte vi i Nasjonal sikkerhetsmyndighet Sikkerhetsfaglig råd til forsvarsminister Ine Eriksen Søreide og statssekretær Gjermund Hagesæter i Justis- og beredskapsdepartementet. Rådet handler om hvordan vi nasjonalt bør møte et endret sikkerhetspolitisk bilde, og nye trusler og sårbarheter. Sikkerhetsfaglig råd skal, på samme måte som Forsvarssjefens fagmilitære råd, fungere som et grunnlag for langtidsplanen for forsvarssektoren, og stortingsmeldingen om samfunnssikkerhet fra Justis- og beredskapsdepartementet. Sikkerhetsfaglig råd er NSMs vurdering av hvordan Norge bør innrette arbeidet med forebyggende sikkerhet frem mot 2020 og i årene etter, og hvordan Norge bør møte de økte sikkerhetsutfordringene. Det er spesielt områdene IKT-sikkerhet, personellsikkerhet og fysisk sikkerhet vi har sett nærmere på.

Et komplekst bilde. – Risiko- og sårbarhetsbildet har blitt mer komplekst. Vi forvalter store verdier i Norge i dag, som andre kan ha interesse av å tilegne seg for egen vinning eller å skade. På flere områder er trusselen økende eller vedvarende høy. Vi vet at etterretningstrusselen fra andre stater er høy, og at de stadig tar i bruk nye metoder, som f.eks. cyberangrep. Vi vet også at risikoen for fysiske angrep er reell og at terrortrusselen er økende, sier Nilsen.

Den sikkerhetspolitiske og samfunnsmessige situasjonen er endret. Forholdet mellom Russland og NATO er forverret, og det pågår flere konflikter som har betydning for sikkerhetssituasjonen i Norge, bl.a i Syria, Irak og Nord-Afrika. Radikalisering og reisevirksomhet påvirker risikobildet. PST melder om et økt antall norske fremmedkrigere, og at dette er en betydelig utfordring.

Gjennom egne undersøkelser og kunnskap om konkrete hendelser har Nasjonal sikkerhetsmyndighet sett eksempler på store sårbarheter som andre kan ha interesse av å utnytte for å nå sine egne mål. Mange av sårbarhetene er til og med av en slik art at nesten hvem som helst kan utnytte dem. Da gjør vi det for lett for alle som har onde hensikter.

– Vi utsettes daglig for cyberangrep. Mange er alvorlige. Vi ser at angriper i hovedsak utnytter kjente sårbarheter. Mange av disse har vi medisin mot, men vi ser at medisinen ikke tas. Derfor står tiltak på området IKT-sikkerhet sentralt i Sikkerhetsfaglig råd, sier Nilsen.

NSM-direktøren legger vekt på at for å kun-

> «
> Arbeidet med å redusere sårbarheter må styrkes på alle nivåer i samfunnet.

Kjetil Nilsen
Direktør i Nasjonal sikkerhetsmyndighet

ne beskytte de verdiene vi har i samfunnet, må vi ta tak i det vi kan gjøre noe med. Det er så enkelt og så vanskelig som å redusere vår egen, og dermed samfunnets sårbarhet. Arbeidet med å redusere sårbarheter må styrkes på alle nivåer i samfunnet – i det offentlige, i næringslivet og hos den enkelte borger. Sikkerheten er ikke bedre enn det svakeste ledd.

En helhetlig omstilling. NSM har identifisert en rekke utfordringer som er beskrevet i Sikkerhetsfaglig råd.

– For å møte disse utfordringene foreslår vi tilsammen 72 ulike tiltak. De er delt inn i områder som organisering, ledelse og koordinering, IKT-sikkerhet, personellsikkerhet, fysisk sikkerhet, samarbeid med næringslivet, kompetanse, og tiltak for å øke Forsvarets operative evne, sier Nilsen.

Sikkerhetsfaglig råd inneholder en rekke større og mindre tiltak. Antallet kan være krevende å forholde seg til. Noen av tiltakene er enkle å gjennomføre. Andre er mer komplekse og sammensatte og vil kanskje kreve større utredninger. Likevel tilsier situasjonen på sikkerhetsområdet, spesielt når det gjelder IKT-sikkerhet, at disse rådene må bli vurdert og utredet nærmere i tiden som kommer.

– Det er behov for en omfattende satsing på sikkerhet frem mot 2020 og i årene deretter. Risikobildet er endret. Truslene og sårbarhetene øker. Vi må bygge motstandsdyktighet og ha evne til å håndtere hendelser. Vi må anerkjenne hverandres roller og ansvar, og legge vekt på evne og vilje til samarbeid for å løse sikkerhetsutfordringene. Men den kanskje aller viktigste jobben må gjøres i virksomhetene selv – de må ta et krafttak for å sikre egne verdier og systemer, avslutter Nilsen. <

OPPLÆRING AV ENKELTMENNESKER STYRKER SAMFUNNET

Opplæring i IKT-sikkerhet på jobben styrker sikkerheten både på jobben og i samfunnet. Det gjør deg også sikrere privat, sier Tone Hoddø Bakås i Norsis.

TEKST: KJETIL BERG VEIRE

DET ER I ÅR femte år Norsis tar initiativ til Nasjonal sikkerhetsmåned, i samarbeid med en rekke ulike aktører over hele landet. Nasjonal sikkerhetsmåned er den årlige kampanjen i Norge hvor målet er å skape bevissthet om informasjonssikkerhet. Måneden blir markert over hele Europa, i fjor var 30 europeiske land med EU-prosjektet European Cyber Security Month. I Norge er sikkerhetsmåneden en stor nasjonal dugnad, hvor alle kan bidra, enten gjennom opplæring i informasjonssikkerhet av egne ansatte, frokostmøter, foredrag og så videre.

Enkeltmennesket viktig. – Det viktigste vi gjør i år handler om opplæring av ansatte. Det øker kompetansen av deg som ansatt, men også som enkeltmenneske, sier prosjektleder Tone Hoddø Bakås i Norsis.

– Veldig mye av det du lærer på jobb tar du med deg hjem, og motsatt. Det å styrke enkeltmennesker, styrker virksomheter, det styrker samfunnet, og vi får et mer motstandsdyktig samfunn, sier hun.

Bedre passord. I år vil Norsis blant annet bruke mye tid på å få folk til å lage bedre passord.

– Alle synes det er vanskelig å huske passord. De fleste har hørt at det er forskjellige regler for passord, med tall, spesialtegn og store og små bokstaver, men reglene er veldig vanskelige. Nå prøver vi å innføre et enkelt forslag på passordregler. Forslaget er at du velger deg en liten sangstrofe, og i tillegg legger på noe som du assosierer med tjenesten du logger deg på. Hvis sangstrofen du velger er Lisa gikk til skolen, kan for eksempel bankpassordet ditt bli «Lisa gikk til banken», sier Bakås. Noen tjenester krever at du har tall eller spesialtegn. Da kan du legge tegnene inn i sangstrofen du velger. Og husk på at Lisa gikk til skolen nå er oppbrukt! sier Tone Hoddø Bakås.

Også totrinnspålogging vil være et av budskapene til folk flest i år, sier hun.

– De fleste kjenner til dette i nettbanker, og i bruken av Altinn. Men muligheten for totrinnspålogging finnes også flere andre steder, som for eksempel på Facebook, sier Bakås.

Mer bevissthet. – Har dere sett noen utvikling rundt bevisstheten om informasjonssikkerhet?

– Vi jobber med et eget pilotprosjekt som skal utvikle målinger av informasjonssikkerhet i Norge. Prosjektet er initiert av Justis- og beredskapsdepartementet, og er forankret i Nasjonal strategi for informasjonssikkerhet. Det vi har sett ellers er at flere og flere gjennomfører opplæring av ansatte. I fjor var det 275 000 ansatte som fikk opplæring. Det er 10,3 prosent av alle arbeidstakere i Norge, sier Tone Hoddø Bakås i Norsis. ‹

Tone Hoddø Bakås
NorSIS

ANSATTE ER VEIEN INN I DATASYSTEMER

– I mange saker ser vi at arbeidstakere blir brukt som en vei for å bryte seg inn i jobbens datasystemer, sier fagdirektør for sikkerhetskultur i Nasjonal sikkerhetsmyndighet, Roar Thon.

TEKST: KJETIL BERG VEIRE

Nasjonal sikkerhetsmyndighet øker aktiviteten med foredrag og informasjon i løpet av Nasjonal sikkerhetsmåned. Fagdirektør Roar Thon forbereder seg foreløpig på rundt 40 foredrag land og strand rundt i oktober. Det viktigste tiltaket er å få ansatte til å forstå at de er viktige i sikkerhetsarbeidet, sier han.

– Fortsatt er det slik at vi må jobbe med å få de ansatte til å forstå at deres atferd er med på å bidra til sikkerhetstilstanden på arbeidsplassen. Din digitale atferd er viktig både for deg selv, og din arbeidsgiver.

– *Hva er problemet slik det er i dag?*

– Det er dessverre slik at arbeidstakeren ofte er veien inn i datasystemene for de som ønsker å bryte seg inn.

– *På hvilken måte?*

– Det går for eksempel via manipulasjon. Å lure folk til ukritisk å åpne en link eller vedlegg i e-post. Det kan være starten på et digitalt angrep på din arbeidsgiver eller deg selv.

– *Hva er det enkleste folk kan gjøre for å beskytte seg?*

– Omgjøre digitale situasjoner til analoge situasjoner ved for eksempel å spørre seg selv om hvordan du hadde handlet om det du blir bedt om gjøre via web/e-post istedenfor hadde skjedd på gaten med et menneske som ber deg om å gjøre det samme. Hadde du da reagert på samme måte, eller ville du ha vært litt mer skeptisk? Ta deg litt bedre tid til å gjøre slike vurderinger sier Roar Thon.

Roar Thon
fagdirektør for sikkerhetskultur i Nasjonal sikkerhetsmyndighet

NSM TRENGER NYE MEDARBEIDERE

NSM ansetter hele tiden nye og dyktige medarbeidere i ulike stillinger. Vi trenger både folk med solid IKT-kompetanse, men også folk med bachelor- eller mastergrad i ulike fagområder,som for eksempel statsvitere, jurister, samfunnsvitere og andre.

Følg med på våre nettsider for utlysning av nye stillinger, eller legg inn en åpen søknad dersom du har lyst til å jobbe i Nasjonal sikkerhetsmyndighet. Vi er et miljø i vekst, og har de siste to årene ansatt rundt 100 nye personer.

http://www.nsm.stat.no/om-nsm/jobb-i-nsm

SIKKERHETS-KONFERANSEN 2016

OSLO KONGRESSENTER
16.–17. MARS

Følg med på nsm.stat.no for oppdaterte nyheter, foredragsholdere og utviklingen av programmet. Har du forslag eller innspill til Sikkerhetskonferansen 2016, ta kontakt på **konferanse@nsm.stat.no**.

NASJONAL SIKKERHETSMYNDIGHET

Postboks 814, 1306 Sandvika

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