NSM

Risiko 2022

Økt risiko krever
økt årvåkenhet

Marius Kaniewski /
Forsvaret

NSMs rapport «Risiko» er én av tre offentlige trussel- og risikovurderinger som utgis i første kvartal hvert år. De øvrige gis ut av Etterretningstjenesten og Politiets sikkerhetstjeneste.

Nasjonal sikkerhetsmyndighet

NSM er Norges direktorat for forebyggende nasjonal sikkerhet. Direktoratet gir råd om og gjennomfører tilsyn og andre kontrollaktiviteter på sivil og militær side knyttet til sikring av informasjon, systemer, objekter og infrastruktur av nasjonal betydning. NSM har også et nasjonalt ansvar for å avdekke, varsle og koordinere håndtering av alvorlige IKT-angrep. «Risiko»-rapporten er NSMs årlige vurdering av risikobildet for nasjonal sikkerhet. I rapporten vurderer NSM hvordan sårbarheter i norske virksomheter og samfunnsfunksjoner påvirker risikobildet, i lys av trusselbildet som er trukket frem av Etterretningstjenesten og PST. Rapporten anbefaler også tiltak for å redusere risiko forbundet med sikkerhetstruende virksomhet.

Etterretningstjenesten

E-tjenesten er Norges nasjonale utenlandsetterretningstjeneste. Tjenesten er underlagt forsvarssjefen, men arbeidet omfatter både sivile og militære problemstillinger. E-tjenestens hovedoppgaver er å varsle om ytre trusler mot Norge og prioriterte norske interesser, støtte Forsvaret og forsvarsallianser Norge deltar i, og understøtte politiske beslutningsprosesser med informasjon av spesiell interesse for norsk utenriks-, sikkerhets- og forsvarspolitikk. I den årlige trusselvurderingen «FOKUS» gir E-tjenesten sin analyse av status og forventet utvikling innenfor tematiske og geografiske områder som tjenesten vurderer som særlig relevant for norsk sikkerhet og nasjonale interesser.

Politiets sikkerhetstjeneste

PST er Norges nasjonale innenlands etterretnings- og sikkerhetstjeneste, underlagt justis- og beredskapsministeren. PST har som oppgave å forebygge og etterforske alvorlig kriminalitet mot nasjonens sikkerhet. Som ledd i dette skal tjenesten identifisere og vurdere trusler knyttet til etterretning, sabotasje, spredning av masseødeleggelsesvåpen, terror og ekstremisme. Vurderingene skal bidra i utformingen av politikk og støtte politiske beslutningsprosesser. PSTs årlige trusselvurdering er en del av tjenestens åpne samfunnskommunikasjon der det redegjøres for forventet utvikling i trusselbildet.

Om rapporten

Risiko 2022 beskriver sårbarheter i virksomheter og samfunnet, hvordan trusselaktørene kan utnytte dem og hvilken risiko dette medfører. Rapporten omtaler også hvordan virksomhetene og myndighetene bør redusere sårbarheter for å gjøre trusselaktørenes jobb vanskeligere.

Risiko 2022 henvender seg til ledere og personell med sikkerhetsoppgaver i alle sektorer. Målet med rapporten er å gi virksomhetene bedre forutsetninger for å sette sikkerhetsarbeidet i en bredere kontekst. Dette er spesielt viktig for virksomheter underlagt sikkerhetsloven, men også for andre virksomheter.

Rapporten kan lastes ned på nsm.no/Risiko2022

Mer krevende å beskytte Norge 6
Oppsummering 8
Vi må beskytte nasjonens viktigste verdier 10
Våre viktigste nasjonale verdier må kartlegges 11
Risikobildet 16
Viktige samfunnsfunksjoner kan rammes 17
Trusselaktører utnytter sårbare verdikjeder 20
Lav sikkerhetsbevissthet svekker nasjonal sikkerhet 23
Et taktskifte i cyberdomenet 26
Tiltak for å styrke sikkerheten 28
Sikkerhetsbevisstheten hos ledere og ansatte må heves 29
Ta ansvar for sikkerhetsarbeidet 33
Sikkerheten i IKT-systemene må styrkes 36
Hjelp oss med å bygge et nasjonalt situasjonsbilde 38
Hvordan varsler du NSM? 38

Mer krevende å beskytte Norge

I løpet av 2021 har det blitt enda mer komplekst og krevende å beskytte Norge mot alvorlige trusler. Stortinget ble rammet av et alvorlig cyberangrep i mars. Angrepet traff hjertet i vårt demokrati. Likevel gjennomførte vi et sikkert stortings- og sametingsvalg.

Ikke siden andre verdenskrig har så mange mennesker vært på flukt i verden. Sårbare flyktninger blir brukt som brikker i et strategisk maktspill mellom nasjoner. Også konflikten mellom Russland og Ukraina er en viktig påminnelse om hvor skjør freden er.

Strategiske investeringer som gir fremmede stater tilgang til viktige verdier og beslutningsprosesser, er en metode vi må ta på høyeste alvor. Fremmede staters metoder kombinerer legitime og ulovlige virkemidler. Det setter oss i en rekke dilemmaer, noe vi så da salget av motorfabrikken Bergen Engines ble stanset.

Også metoder som rammer våre digitale og teknologiske systemer må vi være oppmerksomme på. Selv om vårt høyteknologiske samfunn er sårbart, vet vi mye om hvordan vi kan øke sikkerheten. Det gir oss et godt utgangspunkt for arbeidet som må gjøres. Fremtiden vil utfordre oss enda mer enn i dag, så det gjelder å møte den klare til innsats.

Koronapandemien har allerede utfordret oss – mer enn vi kunne forestilt oss. Men den har også lært oss mye. En av lærdommene er at til tross for den økte digitale risikoen vi advarte om da hele Norge ble sendt på hjemmekontor, så ser det ut til å ha gått bra. Teleoperatørene har levert stabile tjenester når Norge trengte det mest. Det er imponerende.

En annen erfaring er at globale forsyningslinjer er sårbare. Produksjon av blant annet mikrochiper har blitt betydelig redusert på grunn av pandemien. Dette lammer produksjonskjeder i alt fra bilindustri til forsvarsindustri verden over, og forsinker viktig sikkerhetsarbeid.

Globalisering og internasjonal handel vil fremover bli utfordret av klimatiltak og komplekse verdikjeder. USA har allerede besluttet å gjøre seg mindre avhengig av andre lands produksjon. I fremtiden kan også vi måtte innstille oss på mer lokal produksjon av varer og tjenester, for eksempel matvareproduksjon. Det vil øke den relative viktigheten av verdier som i dag ikke anses som avgjørende for nasjonal sikkerhet.

Hybride trusler vil prege vår fremtid. Nasjonal sikkerhet må bli alles ansvar. Media har gjennom det siste året satt søkelys på viktige saker som gjelder vår felles sikkerhet. Dette gjør oss mer vaktsomme og øker vår motstandskraft.

NSMs viktigste budskap inn i 2022 er at toppledere må prioritere å beskytte seg og samfunnet enda bedre i tiden fremover. Risiko 2022 skal bidra til å øke vår felles årvåkenhet og beslutsomhet. Sikkerhetsklimaet har blitt kaldere.

Sofie Nystrøm
Direktør

Oppsummering

Den spente sikkerhetssituasjonen i Europa aktualiserer bruken av hybride trusler, såkalte sammensatte virkemidler. Russland og Kinas omfattende verktøykasser truer viktige nasjonale verdier og interesser. Risikoen for at vi ikke er i stand til å ivareta viktige sikkerhetsinteresser øker. En forverring av sikkerhetssituasjonen vil forsterke risikoen ytterligere. Den mest alvorlige utviklingen i det nasjonale risikobildet kan oppsummeres i tre hovedpunkter.

For det første øker gapet mellom trusselen og sikkerhetsnivået i norske virksomheter og samfunnsfunksjoner. Det skyldes blant annet at bevisstheten og kompetansen om trussel- og risikobildet og hva som utgjør god nok sikkerhet, er for svak. Sikkerhetstiltakene er ikke dimensjonert for det reelle trusselbildet eller innføres ikke raskt nok når nye sårbarheter oppstår. Forståelsen for trussel- og risikobildet må økes og tiltak må iverksettes nå. Dette er et ledelsesansvar.

For det andre ser vi at sårbarheter i verdikjeder utnyttes mer målrettet. Gjennom stadig nye metoder og virkemidler, som cyberoperasjoner, investeringer og oppkjøp, utnytter trusselaktørene at virksomhetene er knyttet sammen i lange og komplekse verdikjeder. De leter etter sårbarheter hos leverandører og tilknyttede virksomheter. Ett av virkemidlene de bruker er å investere – direkte eller indirekte – i verdikjeder som er viktige for nasjonal sikkerhet. Dette gjør de gjennom kommersielle selskaper, og i de fleste tilfeller er aktiviteten helt lovlig.

Uoversiktlige verdikjeder gjør det vanskeligere å beskytte viktige nasjonale verdier. Verdikjedene må kartlegges, og sikkerhetsstyringen av

leverandører og underleverandører må prioriteres høyere. For enkelte virksomheter kan det innebære at de må forenkle verdikjedene for å oppnå forsvarlig sikkerhet.

Datasentre og teleinfrastruktur, som igjen er avhengige av kraft, utgjør fundamentet i vår nasjonale digitale infrastruktur. Svikt i verdikjeder, også digitale, kan få konsekvenser både for samfunnssikkerheten og statssikkerheten, eksempelvis dersom sivile virksomheters tjenester eller leveranser til Forsvaret skulle falle bort. Viktige funksjoner må være tilgjengelige i fred, krise og krig.

For det tredje ser vi at taktskiftet i cyberaktivitet mot Norge skjerper den digitale risikoen. Fra 2019 til 2021 har NSM sett en tredobling i antall alvorlige hendelser og cyberoperasjoner. Fremmede etterretningstjenester står bak flere alvorlige hendelser i denne perioden. Risiko for alvorlige cyberoperasjoner er høy og øker for virksomheter som arbeider med utenriks-, forsvars- og sikkerhetspolitikk. Det samme gjelder virksomheter som driver forskning og utvikling innenfor forsvar, helse, maritim teknologi, petroleum og romvirksomhet.

I tillegg ser vi en kraftig økning i digital utpressing og sabotasje, såkalte løsepengevirus eller ransomware. Både her hjemme og i andre land har slike hendelser fått omfattende konsekvenser ved at systemer lammes og viktige tjenester stopper. Bare i desember 2021 ble matvareprodusenten Nortura, mediekonsernet Amedia og Nordland fylkeskommune rammet av slike cyberhendelser.

Selv om flere tar innover seg alvoret i det digitale trussel- og risikobildet, går den teknologiske utviklingen og endringene i sårbarhetsbildet så raskt at den digitale risikoen fortsetter å øke. Sikkerheten i IKT-systemene i norske virksomheter må derfor styrkes. NSMs grunnprinsipper for IKT-sikkerhet er et godt utgangspunkt for IKT-sikkerhetsarbeidet.

Nasjonal sikkerhet utfordres av teknologiutviklingen fordi vi gjør oss avhengige av nye tjenester, og fordi nye sårbarheter oppstår. Utviklingen innen satellitt- og romteknologi, droner, telekommunikasjon og kvanteteknologi er eksempler på fremskritt som også skaper sårbarheter trusselaktører kan utnytte. Vi må kontinuerlig utvikle sikkerheten i takt med den teknologiske utviklingen.

Det er et bredt spekter av både offentlige og private virksomheter som utgjør første skanse i beskyttelsen av Norge i dag. Det må settes av tilstrekkelige ressurser for å få på plass operasjonell risikostyring. Tiltak må iverksettes fortløpende basert på oppdaterte risikovurderinger.

For å styrke nasjonal sikkerhet trenger vi et betydelig løft i bevissthet og kompetanse om trusselbildet og sikkerhetsarbeidet, fra virksomhetens øverste ledelse til den enkelte ansatte. I denne rapporten gir vi en rekke anbefalinger for å bedre sikkerheten i norske virksomheter og øke den nasjonale motstandskraften mot hybride trusler.

Økt risiko krever økt årvåkenhet. Hjelp oss med å bygge et nasjonalt situasjonsbilde gjennom å rapportere sikkerhetstruende aktivitet og hendelser. Slik kan vi sammen iverksette de riktige og viktige tiltakene.

Vi må beskytte nasjonens viktigste verdier

Våre viktigste nasjonale verdier må kartlegges

Målet med å få en oversikt over de viktigste nasjonale verdiene er at vi skal bli i stand til å prioritere og disponere ressurser slik at vi ivaretar våre nasjonale sikkerhetsinteresser.

Vi skal beskytte Norges suverenitet, territorielle integritet og demokrati. Vi skal sikre vår handlefrihet, vår økonomiske stabilitet, vårt forhold til andre stater og befolkningens grunnleggende sikkerhet. Disse overordnede interessene ligger fast, men konkretiseres gjennom grunnleggende nasjonale funksjoner.

Departementene har gjort et stort arbeid med å identifisere grunnleggende nasjonale funksjoner og virksomheter som understøtter disse. Tempoet i arbeidet som gjenstår må økes. Dette er en forutsetning for at private bedrifter og offentlig sektor kan starte arbeidet med å omsette intensjoner til praktisk handling. Målet er å sikre de konkrete verdiene som våre nasjonale sikkerhetsinteresser er avhengige av.

Disse verdiene kan være samfunnsfunksjoner, store kommunikasjonsinfrastrukturer, datasentre og informasjonssystemer, bygninger, transportknutepunkt, anlegg, serverrom, databaser og antenner. Det kan være kunnskap, teknologi og tjenesteleveranser i tillegg til fysiske varer.

Arbeidet med nasjonal sikkerhet favner videre enn virksomheter som i dag er omfattet av sikkerhetsloven. Leveranser og avhengigheter gjennom verdikjeder gjør at noen virksomheter kan være så viktige at de bør omfattes av loven. Dette må vi vurdere fortløpende. Virksomheter kan også bli viktigere å beskytte dersom trusselen mot dem øker.

Arbeidet med nasjonal sikkerhet favner videre enn virksomheter som i dag er omfattet av sikkerhetsloven

Under en øvelse i november 2021 skjøt Russland ned en av sine egne satellitter i verdensrommet. Deler av romsøppelet flyter fortsatt i verdensrommet og utgjør en risiko for aktive satellitter, også norske. NATO omtalte hendelsen som uansvarlig. Rivalisering i verdensrommet vil utgjøre en betydelig risiko for verdier og funksjonalitet som er viktige for Norges sikkerhet. Flere av disse er i dag ikke omfattet av sikkerhetsloven.

Oljefondsjef Nicolai Tangen forvalter Norges sparebøsse, en av Norges viktigste verdier. Oljefondet hadde en avkastning på 1580 milliarder kroner i 2021. Foto: Ole Berg-Rusten / NTB

Norge ligger langt fremme i teknologiutvikling, innovasjon og forskning på mange områder – også innen forsvarsindustrien. Russland og Kina søker å styrke sin kompetanse og produksjon av teknologi som kan bidra til å styrke deres militære kapasitet og økonomiske posisjon. Norske bedrifter og offentlige virksomheter som produserer slike varer og tjenester, eller har verdifull kompetanse, vil kunne bli mål for fremmede stater. De kan bli utsatt for forsøk på investeringer eller oppkjøp fra disse landene, direkte eller indirekte. Når slike bedrifter og virksomheter anskaffer varer eller tjenester, vil de også kunne oppleve at aktører med sekundære målsettinger er villige til å presse prisen ned for å vinne anbudet.

> Norske bedrifter og offentlige virksomheter kan være mål for fremmede stater

Dette gjelder særlig private bedrifter og forsknings-institusjoner som utvikler og produserer teknologi som er attraktiv for trusselaktørene og der norsk utvikling og produksjon holder høy internasjonal standard. Eksempler på dette er teknologi knyttet til maritim sektor (herunder undervanns-teknologi), olje- og gass-utvinning, satellitt-teknologi, droner og kryptoutvikling.

Mange bedrifter med interesser i disse markeds-segmentene er ikke om-fattet av sikkerhetsloven. Da har de heller ikke juridiske verktøy eller tilgang til informasjon som gjør at de kan iverksette nødvendige tiltak for å sikre verdiene.

Evnen til å forsvare Norges territorium er identifisert som en grunnleggende nasjonal funksjon av Forsvarsdepartementet. Denne evnen utøves blant annet av gardistene utenfor Slottet. Foto: Theodor Haugen / Forsvaret

Hva er grunnleggende nasjonale funksjoner?

Grunnleggende nasjonale funksjoner er funksjoner som har betydning for statens evne til å ivareta landets suverenitet, territorielle integritet, demokratiske styreform og overordnede sikkerhetspolitiske interesser. Grunnleggende nasjonale funksjoner identifiseres av departementene innenfor deres respektive ansvarsområder.

For mer informasjon om grunnleggende nasjonale funksjoner, se NSMs temaside på **nsm.no**[1]

1 https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnleggende-nasjonale-funksjoner-gnf/

Foto:
Marius Vågenes
Villanger /
Forsvaret

I produksjonshallen til Bergen Engines produseres blant annet materiell til det norske og amerikanske forsvaret. Foto: Bergen Engines

Russisk oppkjøp av motorfabrikken Bergen Engines stanset av regjeringen

I februar 2021 ble det offentlig kjent at Rolls Royce hadde besluttet å selge motorfabrikken Bergen Engines til det russiske selskapet Transmashholding (TMH). Bergen Engines produserer motorer blant annet til norske og amerikanske militærfartøy.

Saken førte til en offentlig debatt om konsekvensene av et potensielt salg for nasjonale sikkerhetsinteresser. Regjeringen besluttet å stanse salget med hjemmel i sikkerhetsloven. Beslutningen kom blant annet som følge av at teknologien ved Bergen Engines ville styrket Russlands militære kapasitet og gitt Russland tilgang til viktig militærstrategisk kunnskap og teknologi.

Bergen Engines-saken viser hvor krevende det er å få oversikt over risiko i en kompleks verdikjede med anskaffende virksomheter, leverandører og underleverandører på tvers av sektorer og landegrenser. Trusselaktører bruker bevisst ulike økonomiske virkemidler for å få innpass i slike verdikjeder.

Risikobildet

Viktige samfunnsfunksjoner kan rammes

Risikoen for at vi ikke er i stand til å ivareta viktige sikkerhetsinteresser øker.

Politiets sikkerhetstjeneste (PST) og Etterretningstjenesten har i sine trusselvurderinger de senere år fremhevet kinesiske og russiske statlige eller statstilknyttede aktører som den mest alvorlige trusselen mot norske sikkerhetsinteresser. De ønsker å påvirke norske beslutningsprosesser og Norges handlingsrom, styrke sin militære evne og svekke våre nasjonale sikkerhetsinteresser. Den spente sikkerhetssituasjonen mellom Russland og Vesten aktualiserer bruken av hybride trusler mot både Norge og våre allierte.

Statlige trusselaktører viser en økende vilje til å utnytte våre sårbarheter gjennom en helhetlig og langsiktig tilnærming. De utnytter kombinasjoner av virkemidler som cyberoperasjoner, påvirkningsoperasjoner, posisjonering i forskningssamarbeid og oppkjøp og investeringer. De rekrutterer og utnytter enkeltpersoner for å få tilgang til informasjon.

Statlige trusselaktører viser en økende vilje til å utnytte våre sårbarheter

I cyberdomenet ser vi en økende trusselaktivitet i Norge, både fra statlige aktører og kriminelle. Internasjonalt samarbeid og etterforskning har fått økt betydning for å møte trusselen som cyberkriminelle utgjør, og dette gir gode resultater. Hydro ble i 2019 utsatt for digital utpressing som kostet selskapet minst 800 millioner kroner. I 2021 deltok Kripos i en internasjonal politiaksjon mot organiserte cyberkriminelle i Ukraina. Hackerne ble siktet for å stå bak angrepet mot Hydro i tillegg til en rekke lignende angrep i andre land. Andre saker forblir uløste.

Det er vesentlige forskjeller mellom kriminelle og statlige eller statstilknyttede aktørers intensjon og kapasitet. Selv om målet for en kriminell aktør kan være økonomisk vinning, kan det ramme viktige samfunnsfunksjoner. Kraftforsyning, tele-infrastruktur, helsetjenester og matforsyning – digital utpressing og sabotasje kan

Like før jul ble matprodusenten Nortura utsatt for et digitalt angrep. Det førte til forsinkelser i leveringer over hele Norge. Foto: Coop

treffe hvem som helst. Det er kun et spørsmål om tid før slike hendelser får alvorlige konsekvenser for samfunnsfunksjoner og nasjonal sikkerhet.

Hendelsene vi oppdager, enten de gjelder cyber, oppkjøp, påvirkning eller skip som kartlegger vår undersjøiske infrastruktur, er sannsynligvis bare toppen av isfjellet. For å oppdage avvikene fra normalen kreves det årvåkenhet og en forståelse av normalbildet. Slike avvik kan være lovlige eller kriminelle handlinger og kan skje i alle sektorer. Samfunnet vårt er ikke godt nok rustet for å oppdage avvik fra normalen og å se sammenhenger mellom disse avvikene. Vår oversikt over verdier, verdikjeder og avhengigheter er heller ikke god nok til at vi klarer å iverksette riktige tiltak på rett sted og til rett tid.

For å oppdage avvikene fra normalen kreves det årvåkenhet og en forståelse av normalbildet

Nasjonal sikkerhet utfordres av teknologiutviklingen fordi vi gjør oss avhengig av nye tjenester, og fordi nye sårbarheter oppstår. Satellitt- og romteknologi bidrar til økt effektivitet, konkurransedyktighet og innovasjon, men gjør oss sårbare for manipulering av teknologien. Moderne droneteknologi utfordrer vår evne til å beskytte oss mot etterretning og sabotasje fra luften. Den teknologiske utviklingen vil akselerere med innføringen av 5G og kvanteteteknologi. Sikker innføring og effektiv utnyttelse av ny teknologi avhenger av at vi klarer å beskytte oss mot at trusselaktører utnytter den samme teknologien for å ramme oss. Det krever god kunnskap om teknologi og sikkerhet.

Trusselaktører utnytter sårbare verdikjeder

I 2021 har vi sett flere tilfeller der trusselaktører har utnyttet sårbarheter i verdikjeder.

Det er i mange tilfeller enklere å få tilgang til en virksomhets teknologi, bedriftshemmeligheter eller annen sensitiv informasjon gjennom å utnytte en leverandør eller underleverandør enn ved å ramme en virksomhet direkte.

Verdikjedene utnyttes på mange måter. Cyberoperasjoner rammer virksomheter som leverer tjenester til en lang rekke andre virksomheter med viktige samfunnsfunksjoner. SolarWinds-saken viste hvor omfattende konsekvenser et leverandørkjedeangrep kan få. I slike operasjoner utnyttes programvare eller andre digitale leveranser eller tjenester som benyttes av mange virksomheter. Investeringer i og oppkjøp av virksomheter og eiendom er en annen effektiv metode for å få tilgang til informasjon eller beslutninger gjennom verdikjeder. Verdikjedene er helt sentrale i effektiv verdiskapning, samtidig som den totale angrepsflaten øker. Dette gjør oss sårbare.

Aktiviteten rammer bredere enn åpenbare etterretningsmål. Den rammede virksomheten er ikke nødvendigvis et mål i seg selv, men kan være et middel for å nå det endelige målet. Uoversiktlige verdikjeder og avhengigheter på tvers av samfunnsfunksjoner gjør at hendelser kan innvirke både på samfunnssikkerheten og statssikkerheten etter hvert som skillet blir mindre tydelig. Forsvarssektorens økende avhengigheter til sivil sektor, og særlig til private bedrifter, illustrerer hvor aktuell denne problemstillingen er.

Sårbarheter eller hendelser i ett ledd av verdikjeden vil raskt få ringvirkninger til andre virksomheter eller funksjoner. Hendelser hos store leverandører av IT-tjenester eller programvare vil kunne få konsekvenser for svært mange virksomheter. Økende avhengigheter mellom virksomheter sammen med trusselaktørenes evne til å finne og å utnytte sårbare ledd i kjeden gjør at risikoen har økt.

Hendelser i verdikjeden vil raskt få ringvirkninger til andre virksomheter eller funksjoner

Under den pågående pandemien har verden opplevd forsyningsproblemer i flere ledd og innen mange sektorer. I en slik situasjon kan en virksomhet eller dens leverandør måtte inngå samarbeid med nye underleverandører. NSM har sett eksempler på at slike endringer i leverandørkjeden har blitt gjennomført uten nødvendige sikkerhetsmessige vurderinger.

Leverandørkjedeangrep mot amerikanske SolarWinds

Sent i desember 2020 ble det kjent at det amerikanske IT-selskapet SolarWinds hadde blitt utsatt for et leverandørkjede-angrep. Dette var en sofistikert og omfattende cyberoperasjon hvor trusselaktørene klarte å etablere en bakdør i et av programmene til SolarWinds. Bakdøren ble så med i en oppdatering av programmet som Solarwinds selv distribuerte til sine kunder, over 18 000 virksomheter verden over. Kundene installerte da en offisiell og tilsynelatende sikker oppdatering fra selskapet, men med en bakdør som bare trusselaktøren visste om og kunne utnytte for videre kompromitteringer hos kundene. Programmet som ble rammet er designet for å utføre nettverksovervåking, og vil derfor som regel ha vide tilganger i virksomheters infrastruktur.

Dette gjorde at aktøren fikk et svært gunstig utgangspunkt for å komme videre inn i nettverket og omgå sikkerhetsmekanismer. Da angrepet ble kjent, ble omfattende informasjonskampanjer iverksatt verden over for å sikre at berørte virksomheter gjorde nødvendige risikoreduserende tiltak. Amerikanske myndigheter gikk senere ut og pekte på at aktøren bak angrepet sannsynligvis hadde russisk opphav. Flere av Solar Winds' kunder i Norge hadde installert en kompromittert versjon av programmet.
De store konsekvensene uteble fordi bakdøren ikke ble utnyttet hos disse kundene. Denne typen leverandørkjedeangrep er noe vi kan forvente mer av i tiden fremover, muligens også med betydelige konsekvenser for norske virksomheter.

Har du kontroll på alle delene av ditt adgangskontrollsystem?

Selv sikringstiltak har kompliserte verdikjeder. Sikkerhet kan i verste fall snus til risiko. Et komplett elektronisk adgangskontrollsystem inneholder mange komponenter: Det inneholder en kortleser med programvare som må oppdateres jevnlig, ofte med sentralstyrt oppdatering fra leverandøren. Videre inneholder det et adgangskort, ofte med en mikrochip som inneholder informasjon om tilganger. Adgangskontroll er ofte koblet til overvåkningssystemene. Registreringer fra kortleser og overvåkningskameraer logges som regel i en programvare på datamaskiner, som ofte ender opp i en ekstern alarm- eller vektersentral. Alle delkomponentene leveres av ulike leverandører, som igjen har sine underleverandører.

For å ha kontroll på verdikjeden må du vite hvem som leverer kortleserne, adgangskortene, sensorene, programvare og maskinvare. Du må stole på at leverandørene og alarmsentralen forvalter tilliten de har blitt vist gjennom å levere varen eller tjenesten på en sikker måte. Hva skjer dersom din leverandør bytter underleverandør av for eksempel adgangskort? Er dine fysiske sperrer eller bevegelsessensorer levert av en produsent fra et land som på et tidspunkt kan ha interesse av å sette dem ut av spill? Lagres informasjonen fra systemet ditt i en sky? Hvem leverer den skyen, hvor befinner den seg fysisk og hvilke personer har adgang til serverne hvor den er lagret?

Lav sikkerhetsbevissthet svekker nasjonal sikkerhet

Sikkerhetsbevisstheten påvirker vår evne til å avdekke sårbarheter og iverksette tiltak – både i den enkelte virksomhet og nasjonalt.

Sikkerhetsspørsmål settes stadig på den nasjonale agendaen. Dette er positivt. At de hemmelige tjenestene deltar i den offentlige debatten, er viktig. Det samme er medienes rolle. På dette området har det skjedd en markant endring gjennom 2020 og 2021. Stadig oftere ser vi at mediene setter kritisk søkelys på nasjonale sårbarheter som utnyttes, både lovlig og kriminelt. Dette bidrar til å fjerne barrierer i samfunnet og hjelper oss med å utføre samfunnsoppdraget vårt.

Likevel ser vi at bevisstheten om nasjonal sikkerhet ikke er god nok. Statsministeren påpekte i sin halvårlige pressekonferanse i desember 2021 at den sikkerhetspolitiske situasjonen i Europa ikke har vært mer alvorlig siden 1989. Han formidlet også at regjeringen gjennom sin politikk vil holde Norge trygt i møte med utfordringer i sikkerhetspolitikken. Erkjennelsen av at den sikkerhetspolitiske situasjonen angår oss alle, har ikke fullt ut sunket inn. Det er en trygghet i at vi har på plass en ny sikkerhetslov som tvinger oss til å øke bevisstheten om nasjonal sikkerhet, blant annet gjennom prosessen med å identifisere grunnleggende nasjonale funksjoner og verdier som understøtter disse. Dette arbeidet må fortsette med uforminsket styrke.

> Det er store mørketall om alvorlige sikkerhetstruende hendelser i Norge

Lav bevissthet om hva som står på spill og hvilke sårbarheter som kan utnyttes, påvirker vurderinger av risiko i den enkelte virksomhet, privat som offentlig. Dette kan føre til at sårbarheter ikke blir avdekket og at nødvendige sikkerhetstiltak ikke blir iverksatt. På denne måten utsetter virksomheten både seg selv og andre for risiko som kan få konsekvenser for våre nasjonale sikkerhetsinteresser.

Det er store mørketall om alvorlige sikkerhetstruende hendelser i Norge. Dette påvirker evnen til å ivareta nasjonal situasjonsforståelse, som er avgjørende for å kunne prioritere ressurser til de riktige tiltakene. Det gjør også at evnen til å ta lærdom av tidligere hendelser svekkes, og at sårbarheter får bestå.

Alle kan delegere oppgaver i arbeidet med å oppnå forsvarlig sikkerhet, men ikke ansvaret for det. Samarbeid mellom virksomheter er viktig for å utnytte kompetanse og ressurser i et land som Norge, men det innebærer også en risiko for at helhetlig sikring ikke blir godt nok ivaretatt. Fravær av risikostyring og gode nok avtaler mellom virksomheter gir grensesnittutfordringer som kan ha konsekvenser både for de involverte virksomhetene og nasjonal sikkerhet.

Sikkerhetsbevisst bruk av kinesisk teknologi

Kinesisk dominans på verdensmarkedet innenfor enkelte teknologiområder utgjør en økende utfordring for å kunne ivareta forsvarlig sikkerhet. Kina produserer rimelig teknologi av høy kvalitet, noe som gjør kinesiske produkter til et naturlig valg.

Samfunnet vårt er avhengig av stadig ny teknologi for å levere varer og tjenester vi tar for gitt. Disse funksjonene skal drives på en kostnadseffektiv måte, og det er et mål at vi kan benytte oss av god teknologi til en god pris. Kinesisk teknologi har blitt og vil bli anskaffet også av norske virksomheter. Slike anskaffelser er ofte ikke hyllevare, men produkter skreddersydd og produsert for den enkelte virksomhet etter gitte spesifikasjoner.
Et forsvarlig sikkerhetsnivå må nås gjennom høy bevissthet om risikoen knyttet til anskaffelsen og bruken av teknologien.

Kinesiske myndigheter har ifølge deres etterretningslov utstrakt anledning til å pålegge kinesiske virksomheter og enkeltpersoner å samarbeide med og utlevere informasjon til kinesisk etterretning. NSM legger til grunn at en stor del av kinesiskprodusert teknologi vil kunne benyttes som en plattform for innhenting av ulovlig etterretning til fordel for Kina.

Risiko kan reduseres ved å unngå en unødvendig høy konsentrasjon av leveranser fra samme produsent og samme land. Videre kan bruken av teknologien begrenses til områder der den ikke kan samle inn informasjon om viktige nasjonale verdier.

Et taktskifte i cyberdomenet

Flere alvorlige cyberhendelser i 2020 og 2021 understreker det omfattende og komplekse trusselbildet vi står overfor.

Trusselaktørene viser stor kapasitet til å gjennomføre cyberangrep. Siden 2019 har NSM sett en tredobling i antall cyberhendelser som får alvorlige konsekvenser for virksomheter i Norge.

Det siste året har kartleggingsaktivitet, phishing[2], digital utpressing og sabotasje[3], og utnyttelse av digitale sårbarheter hos et stort antall virksomheter preget cyberbildet. Kartleggingsaktivitet kan innebære kartlegging av tekniske sårbarheter, hvilken informasjon som ligger på åpne nettsider og kartlegging av personer eller organisasjoner. Vi må være oppmerksomme på at dette kan være forberedelser til neste fase i et cyberangrep.

Cyberoperasjoner rammer i økende grad flere mål samtidig, på tvers av sektorer og med aktivitet som vedvarer over tid. Avanserte aktører har det siste året utført aktivitet mot virksomheter i blant annet sentralforvaltningen, forsknings- og utdanningssektoren, forsvarssektoren og andre virksomheter innen høyteknologi.

Enkelte avanserte trusselaktører forsøker å etablere et fotfeste i norske virksomheter. Cyberoperasjoner mot viktige institusjoner og samfunnsfunksjoner kan ha direkte og umiddelbare konsekvenser. Trusselaktøren kan få tilgang til systemer og sensitiv informasjon, og de kan endre innhold eller gjøre tjenester utilgjengelige. Samtidig kan cyberoperasjoner også få alvorlige langsiktige konsekvenser ved at det legges til rette for fremtidig påvirkning eller sabotasje.

Cyberoperasjoner rammer i økende grad flere mål samtidig, på tvers av sektorer

Det siste året har det vært en markant økning i mengden hendelser med digital utpressing og sabotasje. Dette rammer bredt – på tvers av alle sektorer og både privat næringsliv og offentlige myndigheter. Risikoen for digital utpressing og sabotasje er høy.

I romjulen 2021 ble mediekonsernet Amedia rammet av et cyberangrep. Det førte til at papiravisene til mer enn 80 lokalaviser ikke kunne publiseres den påfølgende dagen. Angrepet mot Amedia var ett av flere cyberangrep som rammet norske virksomheter julen 2021. Forekomsten av cyberoperasjoner øker ofte i forbindelse med høytider.

Slike angrep kan ha store økonomiske konsekvenser for virksomhetene som blir rammet,

2 Målrettede e-poster for å manipulere noen til å trykke på vedlegg eller lenker med ondsinnet innhold

3 Løsepengevirus eller «ransomware»

USAs president Joe Biden i et digitalt møte med Russlands president Vladimir Putin. 2021 var et år hvor stemningen ble dårligere mellom landene. Foto: Reuters

og personlige konsekvenser for ansatte og kunder hvis personopplysninger havner på avveie. Samtidig kan det også ha store konsekvenser for samfunnet som helhet når varer, funksjoner og tjenester blir utilgjengelige.

Det er krevende å holde tritt med et sårbarhetsbilde som er i utvikling fra dag til dag. Pandemien har akselerert innføringen av nye digitale løsninger hos mange. Med nye løsninger følger nye sårbarheter og behov for nye risikoreduserende tiltak. Både i offentlig og privat sektor har vi sett evne til mobilisering i ekstraordinære situasjoner for å sette fokus på digital sikkerhet. Samtidig ser vi at økt bevissthet om digital risiko for sjelden blir omsatt til handling.

Det er fortsatt slik at det generelle sikkerhetsnivået i IKT-systemer hos norske virksomheter er for lavt. I de fleste tilfeller er det tekniske sårbarheter som utnyttes for å kompromittere systemene. De aller fleste cyberhendelser som rammer norske virksomheter og myndighetsorganer, kunne vært unngått eller fått langt mindre alvorlige konsekvenser dersom NSMs grunnprinsipper for IKT-sikkerhet ble fulgt. Svak sikkerhet gir høy risiko for at virksomheter rammes av cyberhendelser.

Ved angrepet på Stortinget i mars 2021 utnyttet trusselaktøren en nulldagssårbarhet[4] i Stortingets systemer. Nulldagssårbarheter er en kamp mot klokka. Det er avgjørende å oppdatere programvaren før trusselaktører utnytter sårbarheten. Dette så vi i forbindelse med de brede informasjonskampanjene som ble iverksatt da den store sårbarheten i Microsoft Exchange ble offentliggjort i mars, og da den enda mer alvorlige sårbarheten i Log4J ble offentliggjort i desember 2021. Foreløpig ser det ut til at norske virksomheter har klart seg bra gjennom dette og at sikkerhetsoppdateringer ble utført raskt hos de aller fleste. Likevel vet vi ikke med sikkerhet om sårbarhetene kan ha blitt utnyttet av trusselaktører som har lagt inn usynlige bakdører i virksomheters systemer for å utnytte disse på et senere tidspunkt, hvis og når de ønsker det.

> I de fleste tilfeller er det tekniske sårbarheter som utnyttes for å kompromittere systemene

4 En nulldagssårbarhet er en sårbarhet programvareutvikleren ikke ennå har oppdaget eller laget sikkerhetsoppdatering for.

Tiltak for å styrke sikkerheten

Sikkerhetsbevisstheten hos ledere og ansatte må heves

Private bedrifter og offentlige virksomheter må være bevisste endringer i trussel- og risikobildet.

Som øverste ansvarlig for sikkerheten bør ledelsen i utsatte bedrifter og virksomheter be om en årlig gjennomgang av de nasjonale trussel- og risikovurderingene. Det er også mye å lære av sektorer som har lang erfaring med sikkerhet og risikostyring slik som luftfarten, finanssektoren og forsvarssektoren. I disse sektorene er risikostyring innarbeidet i alle faser av operasjonene og i alle ledd av organisasjonen.

Mange virksomheter sikrer seg mot driftsforstyrrende hendelser som innbrudd eller nedetid på systemene. Men disse sikringstiltakene beskytter ikke nødvendigvis mot målrettede trusselaktører. Et tilstrekkelig sikkerhetsnivå avhenger av at virksomheter oppdaterer sin kunnskap, blir mer sikkerhetsbevisste og tilpasser sikringstiltak etter endringer i trusselbildet. Sikkerhetsbevissthet er avgjørende for å forhindre og avdekke innsiderisiko, risiko for avlytting og sikkerhetstruende økonomisk virksomhet. Disse metodene er vanskelig å avdekke. Er vi ikke årvåkne, avdekker vi ikke slik aktivitet – aktivitet vi vet at forekommer.

> Sikkerhetsbevissthet er avgjørende for å forhindre og avdekke sikkerhetstruende virksomhet

Risikoreduserende tiltak mot innsidervirksomhet[5]

1. **Skap et helhetlig system for å styrke personellsikkerheten.** Dette innebærer å vurdere den menneskelige faktoren i alle deler av sikkerhetsarbeidet og innarbeide mulige konsekvenser av innsidevirksomhet i virksomhetens risikovurdering.

2. **Ivareta personellsikkerheten før, under og etter ansettelse.** Dette innebærer å sikre at risikoreduserende tiltak iverksettes i alle ledd av ansettelsesforholdet, herunder bruk av bakgrunnssjekk.

3. **Sørg for at virksomheten har tilstrekkelig sikkerhetskompetanse og -ressurser.** Dette er nødvendig for å kunne beskytte virksomhetens verdier mot innsidevirksomhet, men også for at virksomheten skal settes i stand til å følge opp sårbarheter som oppstår hos ansatte.

4. **Legg til rette for god sikkerhetskultur.** Dette innebærer å gjøre personellsikkerhet til en naturlig del av virksomheten, øke forståelse av sikkerhetsregler og rutiner samt tilrettelegge for oppfølging av ansatte for å avdekke misnøye eller andre forhold.

5. **Håndter hendelser, evaluer tiltak og lær av erfaringene.** Ved sikkerhetsbrudd bør virksomheten identifisere hvilken rolle personen på innsiden har hatt, og virksomheten bør arbeide systematisk for å lære av erfaringer og bruke lærdommen til å styrke arbeidet med å forebygge, avdekke og motvirke innsidevirksomhet.

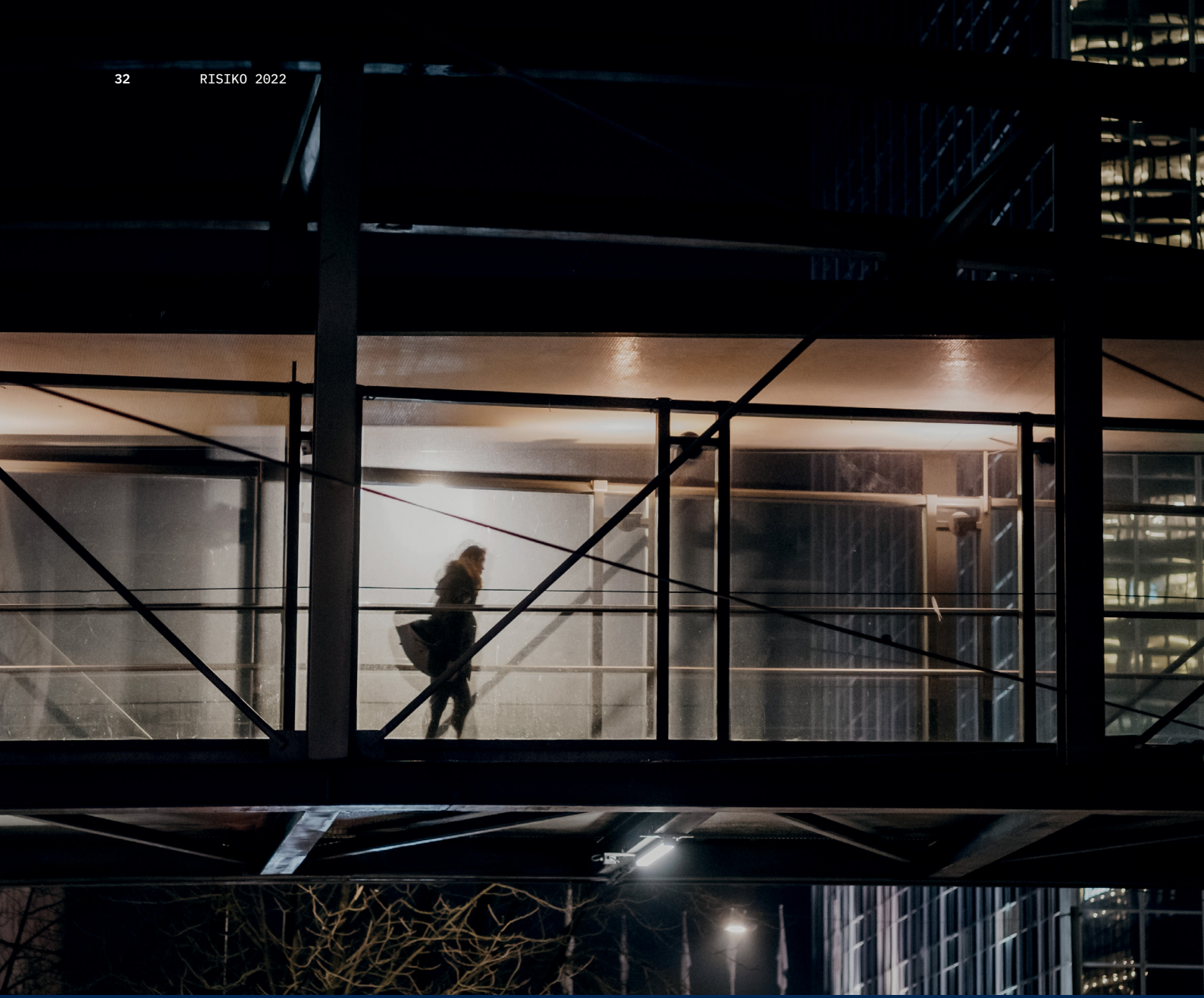
5 NSM (2019), Temarapport. Innsiderisiko.

Konsulent dømt til tre års fengsel for spionasje i Sverige

Göteborgs tingsrätt dømte 15. september 2021 en 47-årig svensk sivilingeniør til tre års fengsel for spionasje til fordel for Russland. Mannen arbeidet som konsulent for personbilprodusenten Volvo i 2016–2017 og for lastebilprodusenten Scania fra 2018 til han ble pågrepet i 2019. Han er dømt for å ha anskaffet og gitt fra seg forretningshemmeligheter fra Scania til en russisk diplomat, som han hadde hatt jevnlig kontakt med siden 2016. Mannen var også tiltalt for å ha gitt tilsvarende hemmelige opplysninger fra Volvo, men ble frikjent for dette. Da saken kom opp, var det første gang på 18 år at en person var tiltalt for spionasje i Sverige.[6, 7]

6 https://www.svt.se/nyheter/lokalt/vast/nu-inleds-rattegangen-mot-misstankt-spion

7 https://www.domstol.se/nyheter/2021/09/konsult-doms-till-tre-ars-fangelse-for-spioneri/



Kinesisk kvinne identifisert av britiske MI5 som påvirkningsagent

I januar 2022 kom nyheten i britiske medier om at landets sikkerhetstjeneste MI5 har varslet britiske parlamentsmedlemmer om en navngitt kinesisk kvinne bosatt i Storbritannia.[8] MI5 mener kvinnen er en påvirkningsagent for det kinesiske kommunistpartiet.

Ifølge BBC har kvinnen gitt store donasjoner til en rekke parlamentsmedlemmer. Finansieringen til disse donasjonene skal i mange tilfeller ha kommet fra Kina. Et parlamentsmedlem er oppgitt å ha mottatt til sammen over 420 000 britiske pund over en femårsperiode. Kvinnens sønn skal også ha jobbet for det samme parlamentsmedlemmet.

Ifølge BBC skal MI5 ha informert parlamentsmedlemmene om at kvinnen har hatt en fordekt koordinering av sine aktiviteter med en del av det kinesiske kommunistpartiet som har som oppgave å fremdyrke relasjoner med innflytelsesrike personer som kan påvirke andre lands politiske klima til fordel for det kinesiske kommunistpartiet.

8 https://www.bbc.com/news/uk-politics-59984380

Ta ansvar for sikkerhetsarbeidet

Sikkerhetsarbeid kan tjenesteutsettes, men ikke ansvaret for sikkerheten.

Dette innebærer at krav til sikkerhet må inngå i kontrakter mellom virksomheter. Slike krav må forhandles, styres og følges opp. Krav til rapportering av endringer og hendelser som påvirker sikkerhet må inngå i dette. Det samme må sikkerhetskrav til bruk av underleverandører.

Sårbarheter kan oppstå når flere virksomheter deler ansvar for sikkerheten, der man legger andres risikovurderinger til grunn eller der man antar at sikkerheten blir ivaretatt av andre.

Det er ikke prinsipielt galt å samarbeide eller tjenesteutsette, såfremt vi ikke mister oversikten over helhetsbildet. Gjør andre arbeidet, må det være klare og kontraktsfestede ansvars- og rolleavklaringer.

Sårbarheter kan oppstå når flere virksomheter deler ansvar for sikkerheten

Leverandørkjedeangrep mot tjenesteleverandøren Kaseya

I juli 2021 ble den amerikanske programvareleverandøren Kaseya utsatt for et cyberangrep. Trusselaktøren utnyttet en sårbarhet i Kaseyas systemer til å spre skadelig programvare til IT-systemene til Kaseyas kunder og krevde at virksomhetene utbetalte løsepenger for å få gjenopprettet systemene sine.

Ifølge Kaseya ble systemene til rundt 60 kunder rammet direkte av angrepet, blant annet kassasystemene til svenske Coop-butikker.

Hendelsen viser at cyberangrep mot store tjeneste-leverandører kan føre til omfattende konsekvenser for svært mange virksomheter. Jo flere ledd det er i en verdikjede, jo flere muligheter er det for trusselaktører å finne en inngangsport. Dersom mange virksomheter og samfunns-funksjoner er avhengige av én og samme leverandør, kan en enkelthendelse føre til utbredte og alvorlige konsekvenser.

Angrepet på teknologi-leverandøren Kaseya førte til at betalingsløsninger på alle Coop-butikker i Sverige ble tatt ned en periode. Foto: AP / Ali Lorestani

Helhetlig risikostyringsprosess må etableres

Både private bedrifter og offentlige virksomheter som understøtter viktige verdier, må ha oppdaterte vurderinger av risiko og en gjennomgående risikostyringsprosess.

Arbeidet kan gjerne inngå som en del av den overordnede virksomhetsstyringen, men den må være kunnskaps- og risikobasert. Det innebærer at styring og oppfølging må ledes av ansatte som kjenner virksomheten godt og som også har god og oppdatert forståelse for trussel- og risikobildet. De må også ha den øverste ledelsen i ryggen.

1. **Begynn kartleggingen i det små.**
2. **Prioriter ressurser internt til jevnlig arbeid i stedet for store prosjekter med ekstern ekspertbistand.**

Sikkerheten i IKT-systemene må styrkes

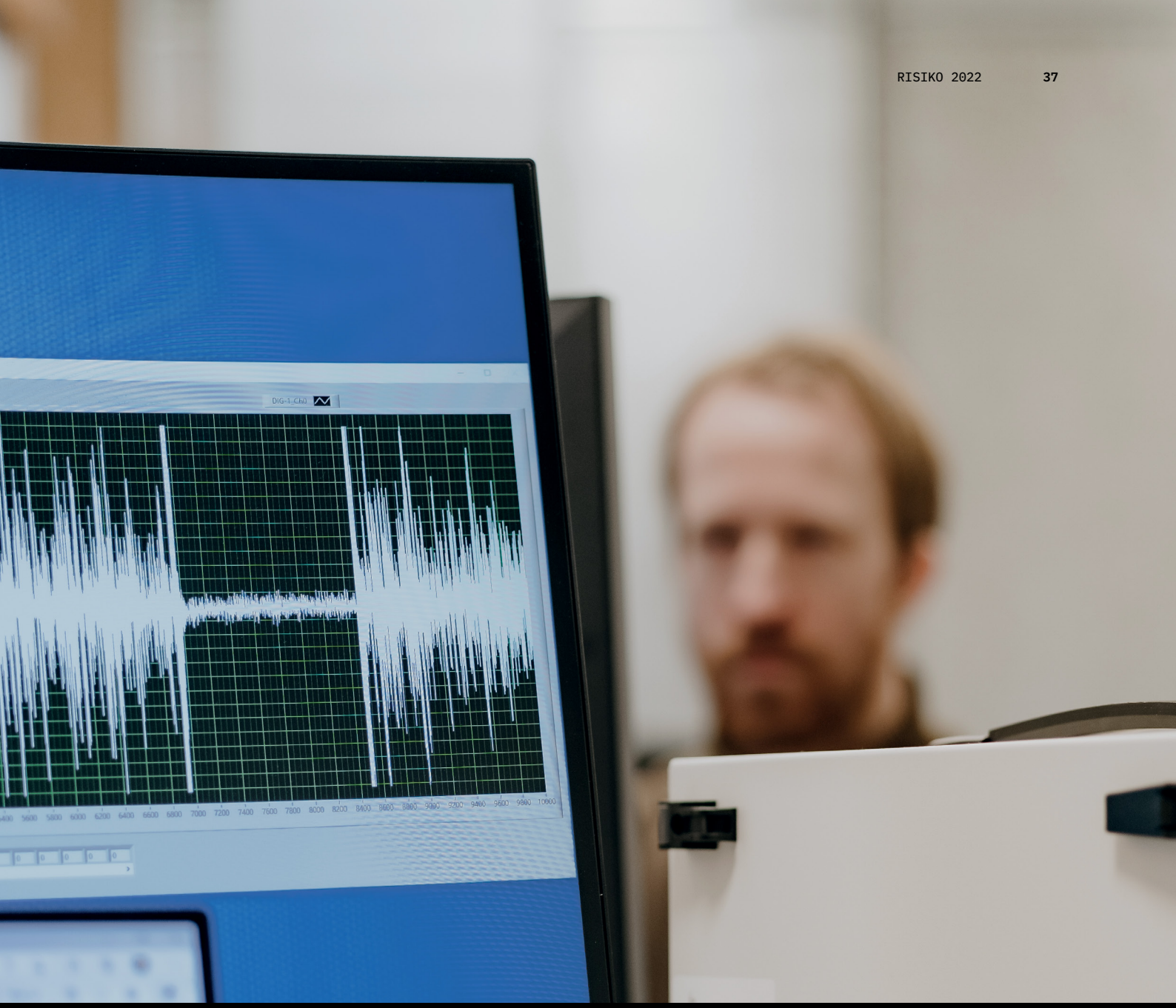
Alle virksomheter må korrigere tekniske sårbarheter.

Dette innebærer kontinuerlig å oppdatere IKT-systemer, lukke sårbarheter i nettverks-, klient- og serverkonfigurasjon og kontrollere rettighetsstyringen internt. Flerfaktor-autentisering øker sikkerheten, og logging i systemene muliggjør kontroll og raskere gjenoppretting hvis en hendelse inntreffer. Informasjon om ansatte på internett bør reduseres. NSMs grunnprinsipper for IKT-sikkerhet og den årlige rapporten *Nasjonalt digitalt risikobilde* er gode kilder for IKT-sikkerhetsarbeidet.

Cybersikkerhet er et tema som får stor oppmerksomhet. Rammede virksomheter deler stadig oftere sine erfaringer i offentligheten for å hjelpe andre til å unngå det. Mange sektorer peker på NSMs grunnprinsipper for IKT-sikkerhet som et viktig verktøy for å oppnå godt sikkerhet. Ved Nasjonalt cybersikkerhetssenter sitter det partnere fra mange sektorer sammen med NSM, Etterretningstjenesten, PST og Kripos for å bidra til å bygge den nasjonale IKT-sikkerheten.

> Det grunnleggende sikkerhetsnivået i norske virksomheter er for lavt

Likevel er det grunnleggende sikkerhetsnivået i norske virksomheter for lavt. Det er imidlertid en styrke i det digitale sikkerhetsarbeidet at vi i stor grad vet hva som virker og hva vi kan gjøre for å redusere sårbarheter.



NSMs grunnprinsipper for IKT-sikkerhet er et effektivt verktøy

Trusselen øker fra både statlige aktører og kriminelle i det digitale domenet, men det finnes gode verktøy som kan bidra til å redusere sårbarhetene som utnyttes. Økt bevissthet om trusselen er ikke nok. Tiltakene må følge etter.

Over flere år har NSM erfart at det ofte er de samme feilene som gjøres, både i offentlige virksomheter og private bedrifter. Hadde NSMs grunnprinsipper vært fulgt, hadde de fleste cyberhendelser vært avverget eller fått begrenset skadeomfang.

Hjelp oss med å bygge et nasjonalt situasjonsbilde

Avvik fra normalen må varsles til myndighetene. Gjør dere kjent med hva som skal varsles, til politiet, PST, NSM eller andre. Det viktigste er ikke hvem varselet går til eller hvordan det er formulert, men at det skjer. Lag deres egne rutiner for varsling slik at ansatte er trygge på hva de skal gjøre.

Varsler om uønskede hendelser eller mistanke om dette er avgjørende for den nasjonale situasjonsforståelsen. Varslingsplikten til NSM omfatter all aktivitet, eller mistanke om aktivitet, som direkte eller indirekte kan skade nasjonale sikkerhetsinteresser, uavhengig om den er lovlig eller kriminell. Gjennom slik rapportering forstår vi bedre det som skjer rundt oss, slik at vi kan iverksette de riktige tiltakene, små eller store. Ofte er ikke en hendelse isolert fra en annen.

Hvordan varsler du NSM?

Telefon:
02497 (24/7)

E-post
cyberhendelser:
cert@ncsc.no

E-post
sikkerhetstruende
virksomhet og hendelser:
varsel@nsm.no

Sikkerhetsgradert informasjon må ikke inngå i varselet.

NASJONAL
SIKKERHETSMYNDIGHET

Postboks 814,
1306 Sandvika
Tlf. 67 86 40 00

Tlf. 67 86 40 00
nsm.no/risiko2022
www.nsm.no