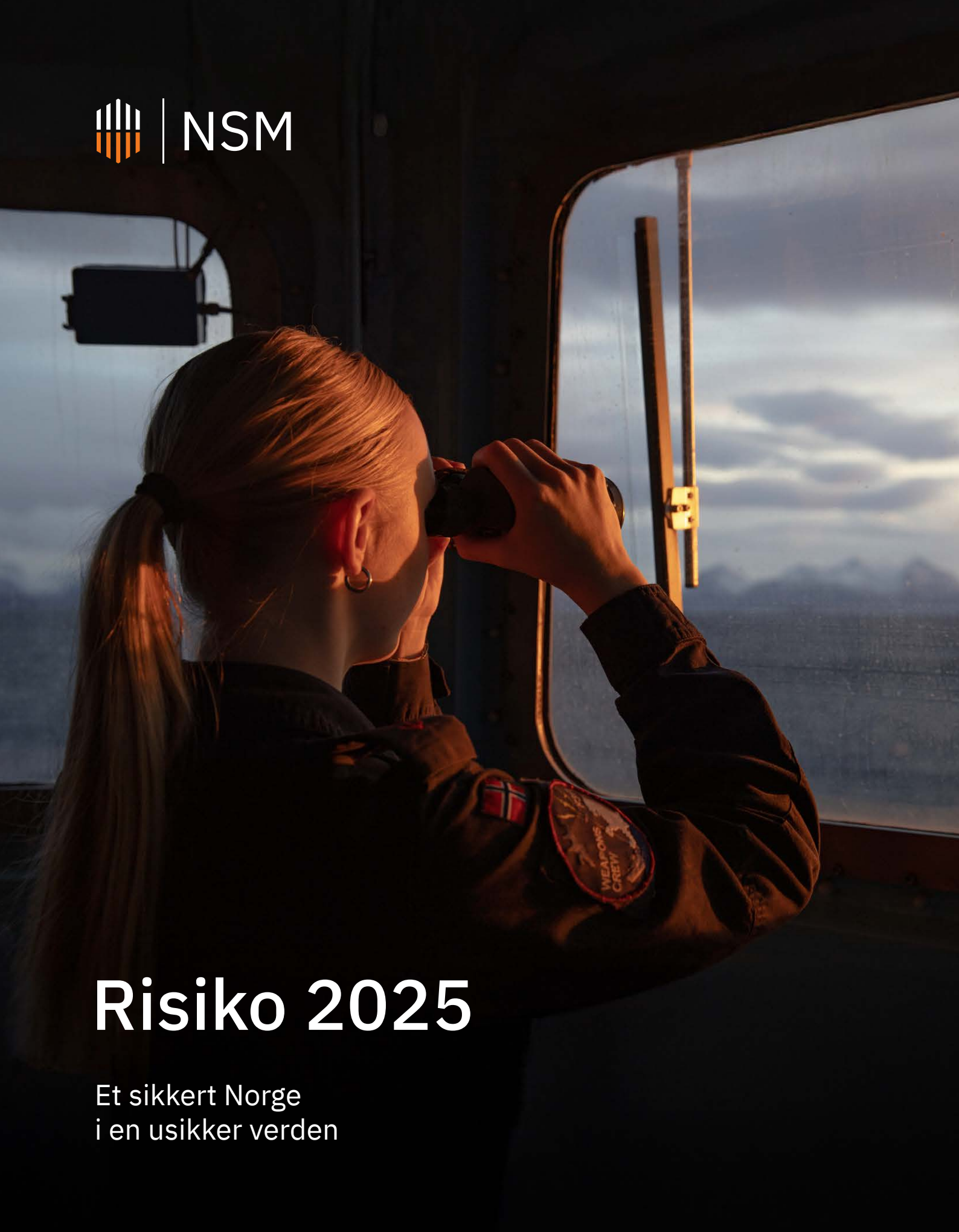


NSM

Risiko 2025

Et sikkert Norge
i en usikker verden

Forsidefoto
Malene Hermansen Flekke/Forsvaret

Risiko fra Nasjonal sikkerhetsmyndighet (NSM) er én av tre offentlige trussel- og risikovurderinger som utgis i første kvartal hvert år. De øvrige gis ut av Etterretningstjenesten og Politiets sikkerhetstjeneste.

NSM

Nasjonal sikkerhetsmyndighet (NSM) er Norges direktorat for forebyggende sikkerhet. Direktoratets hovedoppgave er å bedre Norges evne til å beskytte seg mot spionasje, sabotasje, terror og sammensatte trusler. Gjennom rådgivning, tilsyn, testing, forskning og utvikling bidrar NSM til at virksomheter sikrer sivil og militær informasjon, systemer, objekter og infrastruktur med betydning for nasjonal sikkerhet. NSM er ansvarlig for et nasjonalt varslingssystem (VDI) som skal avdekke og varsle om cyberoperasjoner mot digital infrastruktur. NSM har også et nasjonalt ansvar for å koordinere håndteringen av alvorlige cyberoperasjoner. Risiko, NSMs årlige risikovurdering, skal gi norske virksomheter bedre forutsetninger for å se eget sikkerhetsarbeid i en større sammenheng. Rapporten beskriver sårbarheter trusselaktører forsøker å utnytte og tiltak for å redusere risikoen for at de lykkes.

Etterretningstjenesten (E-tjenesten) er Norges utenlands etterretningstjeneste. 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 vurderingen «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.

PST

Politiets sikkerhetstjeneste (PST) er Norges nasjonale innenlands etterretnings- og sikkerhetstjeneste, underlagt Justis- og beredskapsdepartementet. 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 samt trusler mot myndighetspersoner. Vurderingene skal bidra i utformingen av politikk og støtte politiske beslutningsprosesser. PSTs nasjonale trusselvurdering (NTV) er en del av tjenestens åpne samfunnskommunikasjon der det redegjøres for forventet utvikling i trusselbildet.

Om rapporten

Risiko 2025 beskriver sårbarheter trusselaktører kan utnytte i virksomheter og i samfunnet, og hvilken risiko dette innebærer. I rapporten peker NSM på hvordan myndigheter og virksomheter bør beskytte seg mot truslene som Etterretningstjenesten og PST beskriver i sine årlige trusselvurderinger.

Målet med NSMs risikovurdering er å gi virksomheter bedre forutsetninger for å se sikkerhetsarbeidet i en større sammenheng. Dette gjelder alle virksomheter, men er spesielt relevant for virksomheter underlagt sikkerhetsloven. Rapporten inneholder eksempler og anbefalte tiltak som norske virksomheter må gjøre for best å beskytte seg mot spionasje, sabotasje, terror og sammensatte trusler. Årets rapport er tilgjengelig på nsm.no/risiko2025.

Innhold

Risikobildet krever handling 7

Sammendrag 8

Det overordnede risikobildet 10

En vedvarende krevende sikkerhetspolitisk situasjon 10

Valg og påvirkning 12

Beskyttelse mot alvorlige trusler 14

Sikring mot sabotasje 14

Sikring mot innsidere 16

Sikring mot elektroniske sensorer 18

Et sikkert totalforsvar 20

Avhengigheter til satellittbaserte tjenester 20

Sikkerhet i anskaffelser 22

Lokale forhold påvirker nasjonal sikkerhet 24

Det digitale risikobildet 26

Trender og utvikling i cyberdomenet 26

Tjenesteenheter – en potensiell mobil sårbarhet 34

Digitalsikkerhetsloven 35

Kunstig intelligens utnyttes for å ramme verdier 36

Copernicus Sentinel data (2022), processed by ESA

Risikobildet krever handling

I 2025 markerer vi 80 år siden slutten på andre verdenskrig og 80 år med sammenhengende fred i Norge. Selv om vi ikke er direkte involvert i krig, lever vi ikke lenger i dyp fred. Det er krig i Europa. Russland fører angrepskrig mot Ukraina, og Etterretningstjenesten er tydelige på at uansett utfall av krigen vil Russland utgjøre en trussel mot Norge, Europa og vestlige liberale demokratier i overskuelig framtid.

PST advarer om at sabotasjeforsøk i Norge er sannsynlig. Det er svært alvorlig og noe norske myndigheter og virksomheter må agere på umiddelbart. Vi kan ikke forvente at det kommer flere varsler før en potensiell sabotasjeaksjon.

Vi må i mye større grad være bevisst risiko i samfunnet vårt. Virksomheter i Norge får ikke påvirket trusselbildet, men de kan sikre verdiene og redusere sårbarhetene sine bedre. De kan også redusere konsekvensene av sabotasje eller andre uønskede hendelser.

Nå er det på høy tid å bevege seg fra risikovurderinger til iverksettelse av konkrete tiltak som har en positiv påvirkning på risikoen. Samtidig må vi erkjenne at det ikke vil være mulig å bygge fysiske barrierer rundt alle verdiene våre. Kritisk infrastruktur, som fiberkabler, kraftlinjer og gassrør er eksempler på verdier vi aldri vil klare å sikre fullstendig. Like viktig som sikringstiltak er derfor å sørge for reserveløsninger og god reparasjonsberedskap.

Virksomheter i Norge må ta høyde for ulike scenarioer, også de som for få år siden var utenkelige. Beredskapsplaner må revideres i tråd med scenarioene og planene må øves. Det er avgjørende at alle i organisasjonen forstår egne roller og oppgaver i en beredskaps-situasjon. Målrettet og systematisk arbeid med sikkerhet og beredskap har effekt.

Alle virksomheter er ansvarlige for sikkerheten i egne systemer og tjenesteleveranser. Situasjonen krever at norske virksomheter påvirker egen sikkerhet gjennom forebyggende og risikoreduserende tiltak. Det er et lederansvar. Virksomheter som forvalter grunnleggende nasjonale funksjoner, eller leverer samfunnsviktige tjenester, har et ekstra stort ansvar for vår felles trygghet.


Ole Berg-Rusten/NTB

Arne Christian Haugstøyl
Direktør

En viktig oppgave for NSM er å gi norske myndigheter, virksomheter og enkeltindivider tydelige råd og anbefalinger om tiltak som bør iverksettes for å beskytte seg mot trusselen som Etterretnings-tjenesten og PST beskriver i sine årlige trusselvurderinger. Jeg håper Risiko 2025 motiverer virksomheter til å gå fra *godt sagt* til *godt gjort* i arbeidet med forebyggende sikkerhet.

God lesing!

Sammendrag

Den sikkerhetspolitiske situasjonen gjør at norske virksomheter står overfor alvorlige sikkerhetsutfordringer. For å beskytte seg selv – og felles nasjonale sikkerhetsinteresser – må både offentlige og private virksomheter iverksette nye og skjerpede tiltak.

Tiltakene må ta høyde for scenarioer som for få år siden virket utenkelige. Ødeleggelse av kritisk infrastruktur er ett slikt scenario. Sikring mot sabotasje krever at virksomheter legger mer vekt på reserveløsninger og etablerer god reparasjonsberedskap. Både myndigheter og den enkelte virksomhet må få bedre forståelse av konsekvensene dersom tilgangen på viktige varer eller tjenester faller bort.

Dette krever oversikt over hvilke verdier virksomheten har – og hvilken verdi virksomheten selv utgjør i det store bildet. I noen tilfeller må behovet for lokal utvikling og investeringer vurderes opp mot nasjonale sikkerhetsbehov.

Mennesker er alltid en viktig verdi i enhver virksomhet. Det er de ansatte som daglig har tilgang til informasjon, systemer og anlegg. For å få tilgang forsøker derfor trusselaktører med ondsinnede formål å bygge relasjoner med enkeltpersoner. Daglig sikkerhetsmessig ledelse er et sentralt verktøy for å redusere risikoen for innsidere.

Digitalisering av samfunnet gir store gevinster, men skaper samtidig nye sårbarheter. Uavhengig av om et system slutter å fungere som følge av en tilfeldig, teknisk eller menneskelig feil, eller villede handlinger, er konsekvensene av nedetid store. Utnyttelse av nye sårbarheter i programvarer øker, samtidig som mobiltelefoner, moderne kjøretøy og bruk av kunstig intelligens introduserer nye sårbarhetsflater.

Mange virksomheter baserer egen kjernevirksomhet på teknologi og tjenester fra tredjeparter og underleverandører. Flere er også selv leverandører og blir en del av det nasjonale sikkerhetsarbeidet gjennom ulike leverandørkjeder. Uten god oppfølging av sikkerhetsnivået i hele leverandørkjeden eksponeres virksomheter for unødig risiko.

Virksomheter i Norge forvalter store verdier – både på vegne av seg selv og for andre. Norge er fortsatt en kritisk leverandør av gass og energi til Europa, og blir en stadig viktigere romnasjon. Våre nye allierte i NATO er avhengig av forsyningslinjer som går gjennom Norge. Når den største styrkingen av norsk forsvarsevne på mange år i tillegg står på trappene, er Norge som et lite land avhengig av at alle bidrar.

Den alvorlige sikkerhetspolitiske situasjonen fordrer altså et motstandsdyktig Norge. Det norske totalforsvaret trenger både militær og sivil sektor. Det krever at det sivile samfunnet er forberedt på krise og krig, motstår sammensatte trusler og understøtter militær innsats, som trukket fram i totalberedskapsmeldingen (2024-2025). Risiko 2025 belyser spesielt risikoen for sabotasje og utfordringer knyttet til teknologiutvikling og forsvarsløftet, og deler tiltak for å sikre Norge i en usikker verden.

Theodor Eilertsen/Forsvaret

Det overordnede risikobildet

Verden er ikke blitt tryggere i løpet av det siste året. Det er fortsatt krig og konflikt i Ukraina og Midtøsten. Samarbeidet mellom autoritære stater øker. Virkemiddelbruken eskalerer. Demokratier er under press og samhold utfordres. Dette er forhold som skaper en vedvarende krevende sikkerhetspolitisk situasjon.

En vedvarende krevende sikkerhetspolitisk situasjon

Det er få tegn til at stormaktsrivalisering og globale konfliktlinjer blir dempet i nærmeste framtid. Krig og kriser utspiller seg i flere domener og på tvers av landegrenser. Virkemidler rettes også mot tredjepartsland for å oppnå strategiske mål i konfliktene. Russland benytter ifølge Etterretningstjenesten både fysiske og digitale sabotasjeforsøk for å avskrekke vestlige land fra å støtte Ukraina. Det siste året har det vært en rekke hendelser i europeiske land hvor det er mistanke om sabotasje. PST har tydelig advart om muligheten for sabotasjeforsøk også i Norge. Norske myndigheter og virksomheter må være forberedt på sabotasje, påvirkning og bruk av sammensatte trusler mot norske interesser i tiden framover.

Sommeren 2024 vedtok et enstemmig Storting en ny langtidsplan for forsvarssektoren. I et lite land som Norge har en rekke sivile virksomheter en viktig rolle i å understøtte Forsvaret, enten det er med drivstoff, transporttjenester eller romvirksomhet. Den gjensidige støtten og samarbeidet mellom det sivile samfunnet og Forsvaret, kjent som totalforsvaret, er sentralt for å sikre norsk beredskap i hele krisespekteret.

Et godt totalforsvar fordrer at sikkerheten er på plass hos alle involverte. NSM har tidligere fremhevet hvordan trusselaktører søker enkleste veien inn til et mål. I så måte kan en mindre bedrift som leverer varer eller tjenester enten direkte til Forsvaret eller via andre underleverandører være et startpunkt for et angrepsforsøk. For å forbedre den nasjonale forsvarsevnen må virksomheter på både sivil og militær side jobbe ut ifra de samme scenarioene og med lik forståelse av situasjonen. Norske virksomheter må *bedre* forstå egen rolle i totalforsvaret – og hvilket sikkerhetsnivå som kreves av dem. Det krever oversikt over egne verdier, forståelse av i hvilken grad fremmede stater og trusselaktører er interessert i disse, og en vurdering av hvor sårbare verdiene er. Først da kan virksomhetene iverksette nødvendige og tilstrekkelige risikoreduserende tiltak. Det krever mye av norske virksomheter. Men det lønner seg å jobbe forebyggende framfor skadebegrensende.

Å kartlegge verdiers betydning for nasjonal sikkerhet er et pågående arbeid. Det identifiseres stadig flere områder myndighetene må få bedre oversikt over. I tillegg tar også sektorspesifikt regelverk, som eksempelvis petroleumsloven, i økende grad hensyn til behov for nasjonal sikkerhet og kontroll. Utviklingen gir bedre forutsetninger for det nasjonale forebyggende sikkerhetsarbeidet.

Samtidig er Norge på flere områder avhengig av internasjonalt samarbeid. Sverige og Finlands inntreden i NATO gir Norge en unik mulighet til å bedre den nasjonale sikkerheten. Nordisk samarbeid for å sikre grensekryssende infrastruktur, gjøre internasjonale anskaffelser, og å dele sikkerhetsinformasjon og felles forsvars- og beredskapsplanverk styrker felles evne til beskyttelse. Samarbeidet stiller samtidig nye og endrede krav til Norges evne til å understøtte alliansens nye medlemmer i fred, krise og krig.

Martin Mellquist/Forsvaret

Valg og påvirkning

Tillit er en sentral forutsetning for demokrati. Denne tilliten er under press. Sammensatte trusler, som påvirkningsoperasjoner, kan ha som mål å skade tilliten demokratiet er bygget på. Etterretningstjenesten fremhever hvordan en rekke autoritære stater har som mål å etablere alternativer til vestlig liberalisme og demokrati.

Det var knyttet stor spenning til de mange valgene i 2024 og i hvilken grad trusselaktører ville forsøke å påvirke disse. Desinformasjon og påvirkningsoperasjoner i sosiale medier var framtredende i flere valg. Det er likevel viktig å huske på at påvirkning handler om mer enn desinformasjon og falske nyheter. Det kan skje gjennom hendelser som terror, cyberangrep og sabotasje. I 2024 var det flere mistenkte sabotasjeaksjoner i Europa, og under det amerikanske presidentvalget ble stemmeurner utsatt for sabotasje.

Dagens informasjonssamfunn er helt annerledes enn for kun få år siden. Tilgangen på personlig tilpasset informasjon har økt dramatisk. Hastigheten på informasjonsflommen enkeltpersoner eksponeres for gir ikke rom for dypere refleksjon. Algoritmene i sosiale medieplattformer kan gi et ensidig politisk innhold – og kan inneholde faktafeil og falske nyheter. Argumentene for synspunkter blir ofte forenklet og kan skape et «fiendebilde» av dem som mener noe annet. Utviklingen risikerer å slite på tilliten i samfunnet – både til myndighetene og innad i befolkningen. Det forsterker konfliktlinjer og gjør samfunn mer sårbare for påvirkning fra trusselaktører.

Medietilsynet har sett på nordmenns medievaner. Yngre oppsøker i langt mindre grad nyheter om politikk, samfunn og økonomi enn eldre. Medietilsynet mener at dette kan skape en informasjonskløft mellom de som oppsøker og de som ikke oppsøker redaktørstyrte nyhetsmedier. Unge under 35 år har tydelig lavere tillit til nyheter enn de over 35 år, ifølge Reuters Digital News Report Norway 2024. En informasjonskløft kan utnyttes av trusselaktører for å forsterke splittelse i samfunnet og spre desinformasjon.

Internasjonalt er liberale demokratier på vikende front. Det norske samfunnet er preget av høy tillit, men også i Norge finnes det enkelte tegn som tyder på at dette kan være i endring. Ifølge Direktoratet for forvaltning og økonomistyrings innbyggerundersøkelse 2024 hadde norske innbyggerne lavere tillit til institusjoner og politiske partier i 2023 enn i 2021. Dette er sårbarheter å være bevisst på når Norge avholder stortings- og sametingsvalg i 2025.

En forutsetning for å bygge tillit er at myndighetene trygger grunnleggende demokratiske verdier. Beredskap mot falske nyheter og sosial manipulasjon krever et tett samarbeid mellom myndigheter og sivilsamfunnet.

Regjeringens arbeidsgruppe mot uønsket utenlandsk påvirkning av valg jobber for å trygge valget i 2025. Tiltakene gjelder fysisk sikring av valgsystemene, trygging av kandidatene som stiller til valg, og det digitale sikkerhetsnivået til Valgdirektoratet og kommunene. I tillegg er det

Valgdirektoratet

dialog med de store teknologiplattformene for å redusere trusselen fra falske aktører i sosiale medier. Det er viktig å identifisere trusler, øke bevissthet, styrke koordinering og dele informasjon på tvers av sektorer samt å dele informasjon om valggjennomføringen med befolkningen. Tiltakene blir iverksatt for at befolkningen i Norge fortsatt skal ha tillit til at valg i Norge er demokratiske og frie.

Påvirkningsoperasjoner utnytter kunstig intelligens

Generativ kunstig intelligens (KI) blir i økende omfang brukt til å understøtte påvirkningsoperasjoner. Falsk informasjon, i form av video, bilde, lyd og tekst, blir generert med hensikt å påvirke, forvirre og destabilisere. Innhold i phishingkampanjer kan eksempelvis enkelt genereres med tilgjengelige språkmodeller. Generativ KI kan også brukes til å opprette brukere i sosiale medier i et høyt tempo. Ved hjelp av KI-verktøy kan det enkelt genereres et større antall falske profiler som samhandler seg imellom, noe som øker profilenes legitimitet utad og kan bidra til å spre falsk informasjon.

Presidentvalget i Romania

Det rumenske presidentvalget i november 2024 ble utsatt for en omfattende påvirkningsoperasjon. Rumenske sikkerhetsmyndigheter identifiserte hele 66 000 falske TikTok-kontoer som var brukt til å spre narrativ til fordel for den prorussiske, ytre høyre-kandidaten Calin Georgescu. Ifølge myndighetene stod Russland bak påvirkningskampanjen. Romanias øverste domstol annullerte valgets første runde og kansellerte andre runde på grunn av den omfattende velgermanipulasjonen velgerne allerede var blitt utsatt for.

Valget i Romania viser utfordringene knyttet til falske kontoer og bruken av «boter» i sosiale medier. Påvirkningsoperasjonen kan ha endret rumenske borgeres tillit til selve valgprosessen, tilgjengelig informasjon og landets myndigheter.

Beskyttelse mot alvorlige trusler

Scenarioer som for få år siden virket utenkelige, er i dag realistiske. Sabotasjeaksjoner i Norge er sannsynlig viser trusselvurderingene fra PST. Også innsiderisikoen er reell. Norske virksomheter kan ikke vente på ytterligere advarsler fra sikkerhetstjenestene. Forebyggende tiltak må prioriteres i dag.

Sikring mot sabotasje

PST vurderer det som sannsynlig at Russland kan se seg tjent med å gjennomføre sabotasjeaksjoner mot mål i Norge i 2025. De vurderer også at norskeid energiinfrastruktur og Norges militære bidrag til Ukraina er potensielle mål for slike aksjoner.

En rekke sabotasjeaksjoner i Europa har etter fullskalainvasjonen av Ukraina i februar 2022 blitt attribuert til Russland.

Ifølge PST og Etterretningstjenesten rekrutterer russiske etterretnings- og sikkerhetstjenester proxy-aktører for å utføre sabotasjeaksjoner. Dette er aktører som vanskelig kan spores tilbake til oppdragsgiver. Det er derfor en effektiv måte å skjule forbindelser på. Rekruttering til disse aksjonene foregår som oftest på sosiale medier og er hovedsakelig økonomisk eller politisk motivert.

Den overordnede motivasjonen bak de russiske sabotasjeaksjonene skal være å forbedre Russlands posisjon i krigen i Ukraina, ifølge Etterretningstjenesten og PST. En sabotasjeaksjon mot norske våpenleveranser til Ukraina kan på den ene siden forsøke å svekke ukrainsk forsvarsevne og på den andre siden avskrekke andre land fra å gi ytterligere våpen. Tilstrekkelig sikring av produksjonsfasiliteter og forsyningslinjer fra våpenprodusenter i Norge til brukere i Ukraina er kritisk for å forhindre sabotasje og opprettholde leveringsevnen. Sabotasjeaksjoner er vanskelige både å forutse og å forhindre. Særlig ubemannede og lite skjermede objekter og infrastruktur kan være utsatt for enkle, fysiske sabotasjeforsøk. Dette kan for eksempel være fiberkabler, kraftinfrastruktur som kraftlinjer og koblingsanlegg, transport- og logistikknoder, signalanlegg og undervanns-infrastruktur. Konsekvensene av slike angrep kan være betydelige for nasjonal sikkerhet.

Det er utfordrende å etablere fysiske sikringstiltak som kan forhindre sabotasje mot ubemannet infrastruktur i distriktene. NSM anbefaler å prioritere reserveløsninger og motstandsdyktighet, overvåkings- og deteksjonstiltak samt å øve på beredskapsplaner. Dette for å sikre rask respons og gjenoppretting ved bortfall av kritiske innsatsfaktorer som kraft, transport, internett, vann eller posisjon, navigasjon og tidsbestemmelse (PNT).

Mistenkte sabotasjeaksjoner i Europa i 2024

- Digitale sabotasjeforsøk mot europeiske jernbaner, blant annet i Tsjekkia.
- Frekvensforstyrrelser av GPS-signal i Nord-Norge og Baltikum.
- Fysiske innbrudd i vannverk i Tyskland, Sverige og Finland.
- Angrep mot global flyfrakt, blant annet i Tyskland.
- Omfattende brannstiftelser, for eksempel i Warszawa, Polen.

Proxy-aktører

Proxy-aktører er personer eller organisasjoner uten formell tilknytning til etterretnings- og sikkerhetstjenester eller andre myndighetsorganer, som vitende eller uvitende utfører aktivitet på oppdrag fra, eller til støtte for, myndigheter. Aktiviteten kan være politisk, ideologisk eller økonomisk motivert.

Anbefalinger for å redusere risikoen for sabotasje

- Kartlegg egne verdier og avhengigheter, og vurder hvilke konsekvenser bortfall av disse vil ha. Etabler nødvendige beredskapsordninger for reparasjonskapasitet, reservedeler og personell.
- Søk informasjon hos EOS-tjenestene, sektormyndigheter, sektorvise responsmiljøer og andre relevante myndigheter om hvilke trusler som kan påvirke deres virksomhet samt informasjon om hvilke virkemidler og metoder som benyttes.
- Styrk deteksjonstiltak og øk årvåkenheten. Daglig sikkerhetsmessig ledelse avdekker eventuelle avvik fra normaltilstanden hos de ansatte.
- Sørg for overvåking av digitale systemer for kritisk infrastruktur og reduser digitale sårbarheter der dette er mulig.
- Gjennomgå beredskapsrutiner og øv på bortfall av kritiske innsatsfaktorer.
- Etabler varslingsrutiner med lav terskel for varsling av mistenkelige eller uønskede hendelser, både internt og til politiet og andre myndigheter.

I posisjon for sabotasje mot kritisk infrastruktur

Amerikanske myndigheter delte i 2024 at kinesiske, statssponsede aktører hadde tatt seg inn i datasystemene til kritisk infrastruktur i sektorer som energi, transport og vannforsyning. Myndighetene advarte om at aktørene forsøkte å posisjonere seg i systemene for å kunne angripe på et senere tidspunkt, for eksempel i tilfelle konflikt med USA. Teknikkene er sofistikerte og krever betydelig kompetanse. Samtidig er de vanskelige å oppdage, og trusselaktørene kan derfor oppholde seg i nettverkene over tid.

Aktøren Volt Typhoon skal ha klart å opprettholde tilgang til et nettverk over minst fem år ved å bruke såkalte Living-off-the-Land-teknikker. Teknikkene bruker programvarer og funksjoner allerede tilgjengelig på systemet for å gjennomføre ondsinnede handlinger. Angripere bruker teknikkene til å sanke inn verktøy på målets systemer, slik som komponenter i operativsystem eller installerte programvarer. Det er viktig å overvåke systemene til kritisk infrastruktur for å kunne avdekke uvanlig eller mistenkelig aktivitet.

Sikring mot innsidere

Det siste året har det vært flere saker der personer er mistenkt for å utøve etterretningsvirksomhet, både internasjonalt og i Norge. NSM registrerer at flere underliggende faktorer, knyttet til samfunnsutvikling og endringer i sikkerhetspolitiske forhold, har skjerpet risikoen de seneste årene.

Det er særlig tre faktorer som gir økt risiko for innsidevirksomhet; det geopolitiske spenningsnivået, en større andel av personell med ulike former for tilknytning til andre land, og digitalisering.

Krig, uro og ideologisk konflikt kan bidra til å skape eller forsterke menneskelige sårbarheter. Lojalitetskonflikter er et eksempel på dette. Det skjerpede konfliktnivået i verden øker dessuten mulighetsrommet for å utnytte eller legge press på enkeltpersoner. Dette kan spesielt gjelde personer med tilknytning til krise- og krigsrammede land og områder, eller land som utgjør en høy etterretningstrussel mot Norge.

Trusselaktører tar i bruk både gamle og nye metoder for å rekruttere kilder eller andre som er villige til å samarbeide. Den russiske etterretningskapasiteten ved ambassaden i Oslo er mindre enn tidligere ettersom flere etterretningsoffiserer i 2023 ble erklært uønsket i Norge. Ifølge PST kan Russland derfor søke å kompensere for bortfallet av egne etterretningsoffiserer i Norge med økt bruk av tilreisende agenter og digital rekruttering av personer som allerede er i Norge.

Rekruttering av innsidere og agenter er ikke lenger begrenset til fysiske møter, men skjer stadig oftere via digitale kanaler. Sosiale medier gjør enkeltpersoner mer tilgjengelige – og dermed også mer sårbare – for rekruttering. Trusselaktører bruker profilering og relasjonsbygging i sosiale medier til å finne sårbarheter hos enkeltmennesker, som de utnytter gjennom fristelser, forledelse, manipulasjon eller press.

Menneskelige sårbarheter kan i noen tilfeller være enklere å utnytte enn tekniske eller digitale sårbarheter. Rekrutterte enkeltpersoner og innsidere kan for eksempel bli brukt i påvirkningsoperasjoner, forberedelse og gjennomføring av sabotasje eller andre formål til skade for virksomheter og nasjonale sikkerhetsinteresser.

Virksomheter kan redusere innsiderisikoen med god kompetanse om trussel- og risikobildet, og ikke minst systematisk arbeid for å håndtere risikoen.

Et økende antall virksomheter får betydning for nasjonal sikkerhet. Flere virksomheter som ikke tidligere har hatt skjermingsverdige verdier er nå underlagt sikkerhetsloven og har fått utpekt slike verdier. Disse virksomhetene har behov for å bygge bevissthet om og kompetanse på personellsikkerhet. Det er også viktig å bidra til at de ansatte og andre med tilgang til verdiene forstår egen rolle i sikkerhetsarbeidet.

For virksomheter underlagt sikkerhetsloven gir regelverket et helhetlig system for personellsikkerhet. Dette kan med fordel benyttes som inspirasjon i arbeidet med å forebygge innsidevirksomhet også i virksomheter som ikke er underlagt sikkerhetsloven.

Anbefalinger for å redusere risiko forbundet med innsidere

- Bevisstgjør personell med tilgang til virksomhetens verdier om:
  - innsidetrusselen og metoder som benyttes for å rekruttere innsidere,
  - menneskelige sårbarheter som kan utnyttes og behovet for å håndtere disse i det daglige,
  - hvordan trusselaktører benytter digitale plattformer og sosiale media for å tilegne seg informasjon som kan benyttes til å lure eller lokke enkeltpersoner til samarbeid, og
  - rutiner for å melde fra om oppståtte sårbarheter, sikkerhetshendelser eller kontakt med personer eller organisasjoner som kan representere andre lands etterretnings- eller sikkerhetstjenester.
- Sørg for god kompetanse i virksomheten om innsiderisiko og hvordan man kan forebygge, avdekke og håndtere innsidevirksomhet.
- Etabler eller oppdater retningslinjer og råd for sikker bruk av digitale plattformer og sosiale medier hvor jobb og privatliv møtes (eksempelvis LinkedIn).
- Gjennomgå eget sikkerhetsstyringssystem for å sikre at arbeidet med å forebygge innsidevirsomhet gjøres på en helhetlig og systematisk måte.
- Utøv god sikkerhetsstyring og legg til rette for en god sikkerhetskultur. Følg opp medarbeiderne. Sørg for at personellsikkerheten har oppmerksomhet i hele ansettelsesforholdet.

Innsidevirksomhet

Innsidevirksomhet handler om personer som bruker sine legitime tilganger til virksomhetens verdier for uautoriserte formål, enten bevisst eller ubevisst. En innsider kan være en nåværende eller tidligere ansatt, konsulent eller innleid, som har eller har hatt legitim tilgang til virksomhetens systemer, prosedyrer, objekter og informasjon, og som misbruker denne tilgangen på en måte som påfører virksomheten tap eller skade.

Sosiale medier som rekrutteringsplattform

Rundt 20 000 briter har blitt kontaktet på LinkedIn av kinesiske aktører i forsøk på å stjele industrielle eller teknologiske hemmeligheter. Aktørene nærmer seg enkeltpersoner under dekke av å drive jobbrekruttering. Det fikk sjefen for den britiske sikkerhetstjenesten MI5 til å advare: «Aktiviteten er ikke bare rettet mot statlige eller militære hemmeligheter. Heller ikke bare mot vår kritiske infrastruktur, men i økende grad mot virksomheter i oppstartsfasen, innovative bedrifter som har sitt utspring ved universitetene, i akademisk forskning og hos personer som, forståelig nok, kanskje ikke tror at nasjonal sikkerhet handler om dem». Kilde: The Guardian (17. oktober 2023). NSMs oversettelse.

Sikring mot elektroniske sensorer

I økende grad gjør en rekke elektroniske sensorer hverdagen og arbeidet lettere. Slike sensorer finnes for eksempel i mobiltelefoner, smartklokker, strømmålere, elektroniske dørlåser, droner og moderne kjøretøy. Sensorene kan imidlertid utnyttes til avlytting, overvåking og sporing.

Virksomheter som beskytter sensitive eller skjermingsverdige verdier bør være bevisst sikkerhetsutfordringene elektroniske sensorer kan bringe med seg. Forholdsregler bør tas for å beskytte verdiene de forvalter.

Moderne kjøretøy er et aktuelt eksempel. En moderne bil kan ha over 200 sensorer og funksjoner som samler inn store mengder data. Mange av kamerasensorene bidrar til økt trafikksikkerhet, men de kan også utnyttes til andre formål. Fra et sikkerhetsperspektiv er scenarioene man kan se for seg mange, dersom en trusselaktør får tilgang til bilens sensordata eller kan fjernstyre bilens funksjoner.

Noen biler har ett eller flere kameraer innvendig i kupeen. Hensikten er å hindre at sjåføren sovner, er uoppmerksom eller blir blendet ved kjøring i mørket. Slike kameraer kan være plassert slik at også passasjerene filmes. Mange biler har mikrofoner for håndfri mobiltelefon og talestyring av funksjoner i bilen. Kjøretøyets utvendige sensorer og kameraer kan overvåke personer og annet som befinner seg i kjøretøyets omgivelser. Både lyd og bilde kan utnyttes i etterretningsøyemed, også uten eiers viten.

Moderne kjøretøy har flere nettverk, som nettverkstilkobling via offentlig internett. Disse utgjør en sårbarhetsflate der bilelektronikken kan påvirkes eller styres utenfra. Nettverkstilkoblingen kan også brukes til å sende data fra bilen, utover det som er nødvendig for vedlikehold og oppdatering av bilens programvare. Kjøpskontrakter gir ofte produsenten rettigheter til dataene som bilen samler inn. Dataene kan videreselges, utnyttes som stordata og kombineres med andre data for analyseformål. Det er krevende å vite hva som skjer med informasjonen så snart den har forlatt bilen, noe som kan være problematisk med hensyn til både personvern og sikkerhet.

Det er ikke bare moderne kjøretøy som har slike sensorer. Enorme mengder med innsamlet informasjon fra ulike sensorer og sosiale medier kombinert med verktøy som tale- eller ansiktsgjenkjenning og lokasjonsdata gjør det mulig å spore enkeltpersoner med tilgang til skjermingsverdige eller andre viktige verdier. Det gjør det

Torbjørn Kjosvold/Forsvaret

også mulig å samle inn informasjon om hvor verdiene er lokalisert, hvordan omgivelsene rundt dem er og kartlegge ulike former for sårbarheter. Informasjonsinnsamlingen fra sensorene kan dermed potensielt brukes for å ramme nasjonale verdier.

Anbefalinger for å sikre seg mot elektroniske sensorer

- Samtaler med sensitivt innhold bør ikke skje i nærheten av utstyr med kameraer og sensorer eller i moderne kjøretøy.
- Virksomheter bør vurdere tiltak for å beskytte verdier mot innsyn, avlytting og kartlegging fra moderne kjøretøy og andre produkter med slike sensorer, og tilsvarende tiltak for mobiltelefoner.

Fjernstyring av kjøretøy

I starten av Russlands fullskalakrig mot Ukraina i 2022 stjal russiske tropper moderne landbruksmaskiner av merket John Deere fra en lokal forhandler i Melitopol i Ukraina. Noe av utstyret, deriblant skurtreskere, ble fraktet til Tsjetsjenia, mer enn 112 mil unna. Den amerikanske produsenten brukte fjernstyring til å stenge ned maskinene, slik at de var umulig å starte.

Fjernstyring av de moderne kjøretøyene som kjører på norske veier vil potensielt kunne stenge ned mye av trafikknettet ved å stoppe kjøretøy eller på andre måter kontrollere dem. Dette gir et maktmiddel i konflikter.

Et sikkert totalforsvar

Norge er i gang med den mest omfattende styrkingen av forsvarssektoren på mange år. Skal denne satsingen lykkes, er samarbeid på tvers av militær og sivil sektor avgjørende. Totalforsvaret er den gjensidige støtten og samarbeidet mellom sivil og militær side i fred, krise og krig. Mange norske virksomheter spiller en viktig rolle i dette samarbeidet. God kontroll på verdier og funksjoner med et særskilt beskyttelsesbehov i totalforsvaret er nødvendig.

Avhengigheter til satellittbaserte tjenester

Norge har en avansert romindustri og etablerer nå oppskytingskapasitet på Andøya. Nasjonale satellittkapasiteter og -konstellasjoner, internasjonalt samarbeid og tilretteleggingen for en tilnærmet komplett verdikjede for satellittoppskytning nasjonalt gjør at Norge er i ferd med å bli en viktig aktør også for våre allierte. Dette skjer ikke uten risiko.

Det moderne, digitaliserte samfunnet er avhengig av satellittbaserte tjenester både i sivil og militær sammenheng. De senere årene har den sikkerhetspolitiske dimensjonen av romvirksomhet fått et mer omfattende og betydelig økt fokus, også i Norge. Antisatellittvåpen og ulike måter å forstyrre satellitter og signaler på utvikles raskt, og det er en betydelig vekst i rombasert etterretningskapasitet.

Norsk romsektor er et vedvarende etterretningsmål for trusselaktører, noe PST har påpekt over flere år. NSM har over tid sett en rekke cyberoperasjoner og annen sikkerhetstruende virksomhet mot virksomheter i sektoren. Det er et kontinuerlig press fra trusselaktører som opererer med en lang tidshorisont. Det medfører risiko for at statlige eller ikke-statlige trusselaktører får kontroll over tilbydere av romtjenester gjennom oppkjøp eller cyberoperasjoner. Slike aktører kan også utnytte sårbarheter for å avlytte, sabotere eller manipulere satellittbaserte tjenester.

Samfunnets avhengighet til satellittbaserte tjenester er en strategisk sårbarhet for Norge. Mange virksomheter baserer seg på tredjepartsløsninger som er avhengig av posisjon, navigasjon og tidsbestemmelse (PNT) og kommunikasjon fra satellitt. Eksempler på dette er sammenkoblede digitale systemer, meteorologi, navigasjon, logistikk og finansielle transaksjoner. Disse virksomhetene er i liten grad kjent med egen avhengighet til satellittbaserte tjenester gjennom tredjeparter.

Omfattende bortfall eller manipulering av PNT eller andre sentrale satellittbaserte tjenester vil ha store konsekvenser for samfunnet og totalforsvarets evne til å understøtte Forsvaret. Bortfall av presis tid fører for eksempel til problemer for samhandling mellom digitale systemer. Dette vil få store konsekvenser for samfunnet, virksomheter og individer, avhengig av hvilke systemer som rammes.

Til tross for avhengigheten til PNT er det i Norge i dag for liten tilgang til reserveløsninger. De mest sentrale leverandørene av PNT til Norge er amerikanske GPS og EUs Galileo-system.

Krav til nøyaktighet		Eksempel på bruksområder	Hva kan gå galt om tiden blir feil?
	år	Programvarelisenser	Programmer slutter å virke
		Sikkerhetssertifikater	Pålogging blokkeres
	dag		
	time	Tillitstjenester (pålogging, signaturer)	
	minutt	Å rekke avtaler	
	s	Industrielle kontrollsystemer	Styringskommandoer blir forkastet
		Banktransaksjoner	Transaksjoner går ikke gjennom
		Hendelseslogger	Virkning/årsak byttes om
		Aksjehandel	
300 km	ms	Databaseoppdateringer	Gamle data overskriver nye
		Synkronisering av 5G-basestasjoner	Redusert funksjonalitet eller stopp
300 m	µs	Tidsstempling av målinger i kraftnettet	Feil i systemoversikt > redusert kapasitet
		Luftromsovervåking	Redusert kapasitet
30 cm	ns	Satellittnavigasjon	Redusert nøyaktighet, bortfall av tjeneste

Figur 1: Eksempler på bruksområder/tjenester som er avhengige av en felles tidsangivelse og hva som kan skje om krav til nøyaktighet blir brutt. Satellittnavigasjon stiller størst krav: Klokkefeil på et millisekund (1/1000 s) vil gi 300 km feil i posisjon på bakken. Forventet nøyaktighet på noen få meter krever klokker synkronisert innenfor noen få nanosekunder (milliarddels sekund). Kilde: Justervesenet.

Satellittsignalene fra slike systemer kan forstyrres, blokkeres eller forfalskes. Norge har ingen reserveløsning for å tilgjengeliggjøre presis tid dersom satellittsignalene skulle bli blokkert. Dette kan få betydelige konsekvenser på tvers av sektorer. Etablering av en bakkebasert tidstjeneste er viktig for å gi mer robusthet i samfunnets tilgang til PNT. Det er et viktig steg for å styrke Norges digitale grunnmur.

Anbefalinger for å skape robusthet og redundans i satellittbaserte tjenester

- Virksomheter bør kartlegge egen avhengighet til satellittbaserte tjenester, og særskilt PNT, og vurdere muligheten for å etablere reserveløsninger.
- Myndighetene bør etablere en nasjonal tidstjeneste som ikke er avhengig av globale satellittbaserte navigasjonssystemer (GNSS), og som virksomheter kan koble seg på.
- Nasjonale myndigheter bør aktivt samarbeide med allierte for å skape robusthet og redundans i satellittbaserte tjenester som understøtter viktige samfunnsfunksjoner.

Ole-Sverre Haugli/Forsvaret

Sikkerhet i anskaffelser

Den nye langtidsplanen for forsvarssektoren fordrer en økning i antallet anskaffelser der sikkerhetshensyn må ivaretas. Flere leverandører vil få betydning for nasjonal sikkerhet. Trusselaktørene leter langs hele kjeden av leverandører for å finne og utnytte sårbarheter og skaffe tilganger som kan svekke norsk forsvarsevne. Det gjør det enda viktigere at sikkerhet får nødvendig fokus i anskaffelsesprosesser.

Spesielt i store prosjekter kan det være utfordrende for oppdragsgiver å ha oversikt over og kontroll med alle leverandører og hva de får tilgang til. Det øker sannsynligheten for at trusselaktører kan få adgang til det Norge søker å beskytte. Manglende kontroll med leverandørkjeder kan også øke konsentrasjonsrisikoen. Da kan det oppstå avhengigheter til enkeltleverandører og enkeltland, noe som medfører økt risiko for bortfall og i verste fall kan utnyttes til press og påvirkning.

Mange virksomheter underlagt sikkerhetsloven gjør ikke risikovurderinger før de iverksetter anskaffelser, eller så er vurderingene som gjøres mangelfulle. Gode risikovurderinger er viktig for å avklare beskyttelsesbehov og iverksette nødvendige sikkerhetstiltak i anskaffelsesprosessen. Oppdragsgiver må ta høyde for at verdien eller beskyttelsesbehovet knyttet til anskaffelsen kan endre seg i framtiden. Dersom det ikke tas nødvendige grep fra start, øker risikoen for at trusselaktører sikrer tilgang til verdier som senere får et høyere beskyttelsesbehov.

Oppdragsgivere i sikkerhetsgraderte anskaffelser må ha kontroll med skjermingsverdige verdier som leverandører gis tilgang til. Gode rutiner i anskaffelsesprosesser er viktige for å ha kontroll med skjermingsverdige verdier. For eksempel må virksomheten ha kontroll på hvem som skal ha tilgang til objekt og infrastruktur som understøtter grunnleggende nasjonale funksjoner og sikre at sikkerhetsgradert informasjon ikke kommer på avveie. I tillegg har virksomheter ansvar for å sørge for at leverandører har tilstrekkelig risiko- og sikkerhetsforståelse. Uten nødvendige sikkerhetstiltak evner ikke norske virksomheter å ha god nok kontroll over verdier av betydning for nasjonal sikkerhet. For krav som gjelder i sikkerhetsgraderte anskaffelser, se sikkerhetsloven og virksomhetsikkerhetsforskriften.

Anbefalinger for oppdragsgiver i anskaffelsesprosesser

- Vektlegg sikkerhets- og beredskapshensyn i anskaffelsesprosesser.
- Ha rutiner for å sikre god tverrfaglig kompetanse i anskaffelsesprosessen.
- Kartlegg hvilke verdier anskaffelsen har betydning for.
- Gjennomfør gode og dekkende risiko-vurderinger for å velge riktige sikkerhetstiltak i anskaffelsesprosessen.
- Sikre at relevante krav til sikkerhet framgår av konkurransevilkår og kontrakt.
- Sikre flyt av oppdatert informasjon om endringer eller hendelser som påvirker risiko-vurderinger og valg av sikkerhetstiltak i hele leverandørkjeden.
- Sikre oversikt over underleverandører og leverandørkjeden i sin helhet.
- Etabler gode mekanismer for å følge opp leverandører.
- Sikre at tilgang til skjermingsverdige verdier opphører ved kontraktslutt.
- Prioriter og ressurssett sikkerhet i anskaffelser.
- Virksomheter må overholde krav om årlig å oversende oversikt over alle gjennomførte sikkerhetsgraderte anskaffelser til NSM.

Manglende oppfølging i sikkerhetsgraderte anskaffelser

I 2023 ble NSM varslet om at det ble oppbevart graderte dokumenter i et konkursbo til en privat virksomhet. Dokumentene var fra en rekke offentlige oppdragsgivere, og det var en bekymring for at ingen tok ansvar for disse. NSM hentet dokumentene kun kort tid før huseier overtok lokalene med gjenværende inventar.

Oppdragsgivere har ansvar for sikkerhet i hele anskaffelsen. Dette inkluderer å sørge for at leverandør leverer tilbake gradert informasjon eller bekrefter at den er destruert når oppdraget er avsluttet samt tilbakekall av tilganger til skjermingsverdig objekt og infrastruktur.

Lokale forhold påvirker nasjonal sikkerhet

Utenlandske investeringer kan gi positive ringvirkninger i lokalsamfunn og kommuner i form av verdiskapning og arbeidsplasser. I noen tilfeller kan det samtidig få negative konsekvenser for nasjonale sikkerhetsinteresser.

Dette kan for eksempel være kjøp av eiendom nær verdier Norge ønsker å sikre, eller oppkjøp i virksomheter som utvikler sensitiv teknologi, bygger ut kritisk infrastruktur eller forvalter viktige naturressurser. Lovlig fysisk tilstedeværelse kan legge til rette for sikkerhetstruende aktivitet. Utenlandske investeringer kan også innebære at selskaper med tilknytning til andre stater posisjonerer seg i strategisk viktige markeder. Over tid kan slike investeringer gjøre Norge avhengig av enkeltland, noe som også er nevnt i forbindelse med anskaffelser. Når det først skjer, er det utfordrende å redusere avhengigheten.

Lokale beslutningstakere og virksomheter kan bli stående i et krysspress, med behov for lokal utvikling og vekst på den ene siden og nasjonal kontroll på den andre. Uten et klart bilde av hvilke verdier som må skjermes, blir det utfordrende å vurdere *når* økonomiske transaksjoner kan medføre negative konsekvenser for nasjonale sikkerhetsinteresser. Denne usikkerheten er i seg selv en sårbarhet som trusselaktører kan utnytte. Økt samarbeid mellom lokale myndigheter, lokalt næringsliv og sentrale myndigheter bidrar til bedre situasjonsforståelse. Samarbeid legger også til rette for lettere å identifisere sikkerhetstruende aktivitet og etablere treffende tiltak.

Anbefalinger til virksomheter før oppkjøp og investeringer

- Søk informasjon og bygg kompetanse for å kunne gjøre vurderinger av økonomiske transaksjoner som for eksempel oppkjøp og investeringer opp mot nasjonal sikkerhet. Vurder tidlig i slike prosesser om det er behov for dialog med lokale myndigheter.
- Vurder om konsekvenser for nasjonal sikkerhet må tas hensyn til i egne risikovurderinger.
- Kontakt NSM ved mistanke om økonomiske transaksjoner som kan være sikkerhetstruende.

Kirkenes havn

Sommeren 2024 ble det kjent at Kirkenes havn og det kinesiske shippingselskapet Cosco hadde dialog om et mulig samarbeid. Saken fikk mye oppmerksomhet. Et samarbeid mellom partene kan legge til rette for utvikling og økt aktivitet ved havnen og i lokalsamfunnet, men samtidig medføre en sikkerhetspolitisk utfordring. Havneledelsen og lokale myndigheter ga uttrykk for at det er utfordrende å vurdere handel og nasjonal sikkerhet opp mot hverandre. Nærings- og fiskeridepartementet igangsatte derfor høsten 2024 prosesser for å kartlegge havnens betydning for nasjonale sikkerhetsinteresser.

Ella Hagen/Forsvaret

Det digitale risikobildet

Cyberdomenet er i konstant endring med utvikling av nye metoder og funn av sårbarheter i programvare. Flere cyberangrep utnytter leverandørkjeder for å ramme virksomheter. Potensielt kan angrep som rammer store IKT-leverandører ha lammende effekt på samfunnet. Derfor gjelder det å jobbe forebyggende for å kunne avverge de fleste angrep. I 2025 er det forventet at digitalsikkerhetsloven trer i kraft.

Trender og utvikling i cyberdomenet

Cyberoperasjoner og -kriminalitet forårsaker nedetid, produksjonsstopp og tap av kundedata, patenter og omdømme. I verste fall fører det til store økonomiske tap eller konkurs for rammede virksomheter. Konsekvensene av cyberoperasjoner begrenser seg ikke nødvendigvis til det digitale domenet. De kan også føre til alvorlige fysiske skader på personell og kritisk infrastruktur. Erfaringsmessig kan både tilsiktede og utilsiktede hendelser få store og alvorlige konsekvenser.

Trusselaktivitet i det digitale domenet er noe hele samfunnet må forholde seg til. NSM har registrert cyberhendelser mot så å si alle samfunnssektorer. Enkelte norske verdier er særlig attraktive mål for cyberoperasjoner. Dette er norske virksomheter som arbeider med utenriks-, forsvars- og sikkerhetspolitikk. Det samme gjelder virksomheter og forskningsmiljøer innenfor samfunnsområdene høyteknologi og næring, og finans.

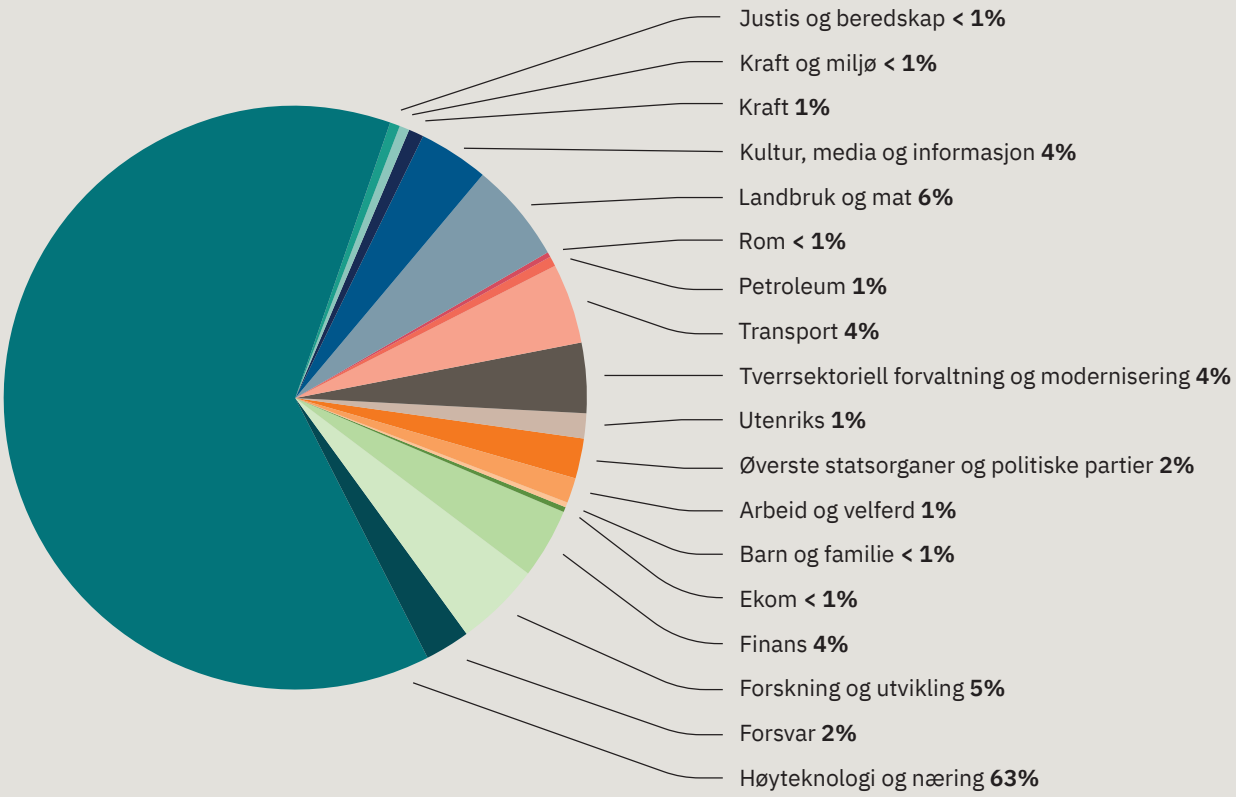
Det siste året har NSM observert en rekke angrep mot virksomheter som enten har informasjon om eller kunne fungert som en vei inn i nettverkene til virksomheter underlagt sikkerhetsloven. Leverandørene er ofte ikke fullt klar over egen betydning. Derfor har de heller ikke sikret egne systemer deretter.

For 2024 registrerte NSM en rekke hendelser i samfunnsområdene for høyteknologi og næring samt landbruk og mat. Antallet hendelser mot disse områdene må ses i lys av at de består av et høyt antall virksomheter. Tallene reflekterer også et pilotprosjekt mellom NSM og Næringslivets sikkerhetsråd, hvor sistnevnte varsler virksomheter som verken etablerte cybersikkerhetsmiljøer eller NSM har et samarbeid med. Bakgrunnen er at NSM og sektorvise responsmiljøer i 2024 observerte en økning av phishingkampanjer, hvor e-postkontoer ble kompromittert og utnyttet til for eksempel fakturasvindel. Såkalte angriper-i-midten-angrep er sammen med nulldagssårbarheter og løsepengeangrep tre metoder som gikk igjen i 2024.

Historiens største IT-kollaps

Utilsiktede hendelser kan gjøre like stor skade som et alvorlig dataangrep. Flyplasser, banker, hoteller, børser, sykehus, apotek, bensinstasjoner og flere ble sommeren 2024 rammet av det som omtales som «historiens største IT-kollaps». En feil i en programvareoppdatering i et antivirusprogram fra datasikkerhetsselskapet Crowdstrike førte til at rundt 8,5 millioner datamaskiner krasjet globalt. Relativt få virksomheter i Norge ble rammet fordi programvaren er mindre utbredt her enn i mange andre land. Statistikk fra EU viser at skade som følge av tilfeldige uønskede hendelser er større enn skade som følger av uønskede hendelser forårsaket av tilsiktede handlinger.

Ilja Hendel/NSM



Figur 2: Prosentandel av cyberhendelser NSM har registrert per samfunnsområde i 2024.

Nulldagssårbarheter er vanskelige å beskytte seg mot. Det ligger i navnet, som spiller på at man har null dager til å kunne forberede seg på utnyttelse av den aktuelle sårbarheten. Trusselaktører jobber kontinuerlig med å avdekke sårbarheter i ulike programvarer. I 2023 økte antallet utnyttede nulldagssårbarheter globalt med 50 prosent fra foregående år, også norske departementer ble rammet.

Nulldagssårbarheter gir størst gevinst for trusselaktører så lenge sårbarheten ikke er kjent. Derfor velger aktører ofte å angripe et fåtall mål i starten, for å unngå at sårbarheten blir oppdaget og lukket.

Når nulldagssårbarheten blir offentlig kjent, kan aktører enkelt endre modus og forsøke å ramme flere for å skape støy og gjøre det vanskeligere å håndtere hendelsen. Også andre trusselaktører kan forsøke å utnytte nulldagssårbarheten til egen vinning. Dette var tilfellet med to nulldagssårbarheter i produktet Ivanti Connect Secure VPN i desember 2023 og januar 2024. Før nulldagssårbarhetene ble kjent, ble kun et mindre antall virksomheter rammet globalt. To dager etter at sårbarhetene ble kjent, ble langt flere virksomheter utsatt for angrep. Også virksomheter i Norge ble rammet. Slik masseutnyttelse kan få omfattende konsekvenser dersom hver enkelt virksomhet som benytter produktet, ikke lukker sårbarheten raskt nok. Det er en risiko for at trusselaktører allerede har oversikt over alle sårbare enheter.

NSM varsler om kritiske sårbarheter til norske virksomheter og anbefaler tiltak. Er mange virksomheter i én sektor sårbare, går varslet gjennom det aktuelle sektorvise responsmiljøet.

Ilja Hendel/NSM

Løsepengeangrep anses som den største utfordringen for norske virksomheter, ifølge en gjennomgang fra de sektorvise responsmiljøene i Norge. Responsmiljøene skal forebygge og håndtere digitale kriser i egen sektor. Løsepengeangrep er en type angrep hvor en aktør bryter seg inn i en virksomhets IKT-systemer for å kryptere og stjele virksomhetens data. Deretter prøver angriperen å presse målet for penger i bytte mot en nøkkel eller et verktøy for å dekryptere dataene samt å ikke lekke eller selge de stjålne dataene. Selv om kriminelle aktører selv får større utbytte fra andre typer svindel, påfører løsepengeangrep større skade for berørte virksomheter på grunn av stopp i drift.

Angrepsmetoden rettes ofte mot små og mellomstore virksomheter. Selv om virksomhetene ikke forvalter samfunnsviktige funksjoner kan angrepene likevel få større konsekvenser hvis selskapene har informasjon om kundeforhold, leveranser eller leverandørkjeder som kan være attraktiv å selge. Informasjon knyttet til nasjonale verdier kan på denne måten bli kjøpt av utenlandske etterretningstjenester.

Angriper-i-midten (eng: adversary-in-the-middle) er en type phishingangrep som det seneste året har rammet et betydelig antall norske virksomheter. Ved å operere mellom offeret og en påloggingsnettside kan angriperen lure til seg passord og komme seg forbi flerfaktorautentisering. E-postkontoer er attraktive mål fordi de gjennom målrettet sosial manipulasjon kan brukes til svindel eller for å komme seg inn i virksomhetens nettverk og systemer. Trusselaktører kan også utnytte tilgangen for å få innsyn i og manipulere kommunikasjon internt i virksomheten eller med eksterne partnere. I tillegg kan angriperen potensielt også få tilgang til skybaserte tjenester, som Microsoft 365 eller Google Workspace. Angriperen får da tilgang og mulighet til å hente ut filer som er lagret i tjenesten.

Figur 3: Hvordan ondsinnede aktører bruker angriper-i-midten-phishing for å lure til seg innloggingsdetaljer og å komme seg forbi flerfaktorautentisering.

Anbefalinger for å redusere risikoen for ulike cyberangrep

- Få oversikt over sårbarhetsflater ved å kartlegge alle IT-systemer og hvilke systemer som er tilgjengelige fra internett.
- Reduser sårbarhetsflater ved kontinuerlig å installere nye sikkerhetsoppdateringer og å innføre andre risikoreduserende tiltak anbefalt av NSM eller leverandører av programvare.
- Kartlegg egne avhengigheter. Skaff oversikt over hvilke leverandørkjeder virksomheten er en del av, enten som kunde eller leverandør.
- Gjennomfør risikoreduserende tiltak for å redusere sikkerhetsrisikoen knyttet til leverandørkjeder.
- Reduser antall systemer tilgjengelige fra internett til et minimum, og beskytt tilgang til disse gjennom tiltak slik som flerfaktor-autentisering.
- Sikre at servere som leverandører og konsulenter har tilgang til, ikke kan benyttes for å få uautorisert tilgang til andre systemer.

Ilja Hendel/NSM

Ilja Hendel/NSM

Varsler fra Nasjonalt cybersikkerhetssenter (NCSC) i NSM

Dette er utdrag fra anbefalinger sendt som varsler fra NSM i 2024. Se nsm.no/varsler for å lese varslene i fulltekst og anbefalte tiltak, både midlertidige og permanente.

Erstatt SSLVPN/WebVPN med sikrere alternativer

Overgang til anbefalt tiltak bør være på plass innen utgangen av 2025. NSM anbefalte virksomheter underlagt sikkerhetsloven å innføre tiltaket før utgangen av 2024.

Bakgrunnen for anbefalingen er at NSM i lengre tid har observert og varslet om kritiske sårbarheter i VPN-løsninger som benytter Secure Socket Layer/Transport Layer Security (SSL/TLS), ofte kjent som SSLVPN, WebVPN eller klientløs VPN. Utnyttelse av sårbarhetene har ført til at flere norske virksomheter har fått enheter kompromittert.

Sårbarhetenes alvorlighetsgrad og aktørers gjentakende utnyttelse av denne typen sårbarheter gjør at NCSC anbefaler å erstatte løsninger for sikker fjernaksess som bruker SSL/TLS med sikrere alternativer. NCSC anbefaler Internet Protocol Security (IPsec) med Internet Key Exchange (IKEv2). Andre lands myndigheter har anbefalt tilsvarende.

Formålet med denne anbefalingen er å redusere sårbarhets- og angrepsflaten for sikker fjernaksess. Det er sannsynlig at det vil avdekkes nye nulldags-sårbarheter i produktkategorien SSLVPN i framtiden. Det må understrekes at løsninger som bruker IPsec med IKEv2 også kan ha sårbarheter, men dette teknologivalget medfører mindre angrepsflate og lavere grad av feiltoleranse i konfigurasjon av løsningen.

For skjermingsverdige og sikkerhetsgraderte informasjonssystemer etter sikkerhetsloven gjelder egne krav som ikke omfattes eller påvirkes av denne anbefalingen. Denne anbefalingen medfører altså ingen endring i gjeldende krav for slike systemer.

Overgang til phishingresistent autentisering

NSM anbefaler virksomheter å gå over til passnøkler (passkeys) eller andre FIDO2-implementasjoner for autentisering. Årsaken er at aktører i økende grad tar seg forbi tradisjonell flerfaktorautentisering. I 2024 har NSM og sektorvise responsmiljøer registrert en rekke phishingkampanjer der målet var økonomisk vinning, ofte via fakturasvindel. Kampanjene lar seg gjennomføre fordi virksomheter ikke påkrever phishingresistent autentisering.

Passnøkler erstatter passord og tradisjonelle flerfaktorløsninger. Passnøkler er teknologien IT-industrien standardiserer seg på, og støttes av populære nettlesere, operativsystemer, mobiltelefoner, identitetsløsninger og skyløsninger.

Passnøkler hindrer angrepsmetoder hvor en angriper har tilgang til eller prøver å få tilgang til brukers passord. Dette inkluderer phishing, varselutmattelse, angriper-i-midten (AitM) og *bruteforce*. Passnøkler fjerner også risikoen med svake og gjenbrukte passord. Passnøkler oppnår dette ved å overta autentiseringsansvaret fra brukeren, slik at trusselaktører verken kan stjele eller lure til seg passnøklene.

NSM anbefaler å prioritere implementering av phishingresistent autentisering på Microsoft 365 og andre skyløsninger samt identitetsløsninger og internetteksponerte tjenester. Prioriter spesielt utsatte brukere som økonomiansvarlige, ledere og systemadministratorer ved gradvis utrulling.

Tjenesteenheter – en potensiell mobil sårbarhet

Tjenesteenheter er en integrert del av organisasjonens digitale infrastruktur med samme behov for sikring som en bærbar datamaskin. Når mer av jobben flytter over på mobilen, må sikkerhetstiltakene følge etter. Mobilen inneholder kontaktlister, meldinger, e-poster og bilder, og den samler inn lokasjonsdata.

Trusselaktører henter ut informasjon fra mobilen gjennom skadevare. Dette kan skje ved nedlasting av applikasjoner som utgir seg for å være legitime, men som inneholder skadevare. Trusselaktører kan også utnytte sårbarheter i utgått programvare til å laste ned skadevare på mobiler. Apple har varslet brukere i over 150 land om at de trolig er blitt utsatt for målrettede angrep fra 2021 til 2024. NSM anser det som sannsynlig at brukere i Norge også er berørt.

NSM ga i 2024 ut en temarapport om mobilapplikasjoner på tjenesteenheter. Her deles anbefalinger inn i tre kategorier; fra generelle retningslinjer for alle ansatte med tjenestetelefon, ansatte som bør ta ekstra forholdsregler, og anbefalinger for særskilte situasjoner hvor det er høy risiko for at tjenesteenheten kan bli utsatt for ondsinnet aktivitet fra trusselaktører. Listen til høyre deler anbefalingene fra rapporten for alle ansatte med tjenestetelefon.

Anbefalinger for sikker bruk av tjenesteenheter for alle ansatte

- Vær kritisk til hvilke applikasjoner som lastes ned og installeres, hvilke tillatelser hver enkelt applikasjon gis og hvilken informasjon applikasjonen får tilgang til.
- Vær særlig oppmerksom på tillatelser til bruk av kamera og mikrofon.
- Bruk stedstjenester kun når det er høyst nødvendig.
- Vær kritisk til bruk av *Near-Field Communication* (NFC), Bluetooth og wifi.
- Vurder å benytte løsninger for kryptert kommunikasjon.

Skadevarer på mobiltelefoner

Det er flere eksempler på skadevare som retter seg mot mobiltelefoner. To skadevarer, kalt WyrmSpy og DragonEgg, skal blant annet ha hatt kapasiteter for å hente ut bilder, lydinnspillinger og kontakter, i tillegg til å kunne både lese og skrive tekstmeldinger. Andre skadevarer kan gjøre mobiler til et mellomstopp i kriminelle aktiviteter. Mobilskadevare kan også være økonomisk motivert. Eksempelvis kan skadevare tappe offeret for kryptovaluta. Dette er tilfellet med skadevaren CherryBlos som leter gjennom bildene på mobiltelefoner etter passord til kryptolommebøker.

Digitalsikkerhetsloven

Lov om digital sikkerhet er forventet å tre i kraft i løpet av 2025. Med ny lov følger flere krav til en rekke norske virksomheter, blant annet formaliserer den krav til digital sikkerhet hos tilbydere av samfunnsviktige tjenester.

NIS1-direktivet fra EU gjennomføres i norsk rett gjennom digitalsikkerhetsloven. På sikt er det forventet at også NIS2-direktivet blir gjennomført.

Sikkerhetsstyringssystemet i virksomheter som er omfattet av digitalsikkerhetsloven og NIS-direktivet, skal omfatte digital sikkerhet. Systemet skal være forankret i virksomhetens ledelse og integrert i den overordnede virksomhetsstyringen, og bør bygge på anerkjente standarder og rammeverk som ISO/IEC 27001 eller NIST Cyber Security Framework.

Når regelverket trer i kraft, må virksomheten sørge for å etablere rutiner for å melde fra om uønskede hendelser.

Allerede nå kan virksomheter begynne å forberede seg

- Fordel roller og oppgaver knyttet til det forebyggende sikkerhetsarbeidet i virksomheten.
- Hold oversikt over viktige informasjonssystemer som kan påvirke virksomhetens tjenesteleveranser.
- Utarbeid gode risikovurderinger og ha en plan for risikohåndtering knyttet til informasjonssystemene i virksomheten.
- Iverksett teknologiske, fysiske, personellmessige og organisatoriske tiltak tilpasset virksomhetens risikobilde.
- Kontroller at tiltakene virker som planlagt og vurder jevnlig behov for justeringer.
- Hold oversikt over avhengigheter i leverandørkjeder og vurder risiko knyttet til leverandører som kan påvirke sikkerheten i virksomhetens informasjonssystemer.

Ilja Hendel/NSM

Kunstig intelligens utnyttes for å ramme verdier

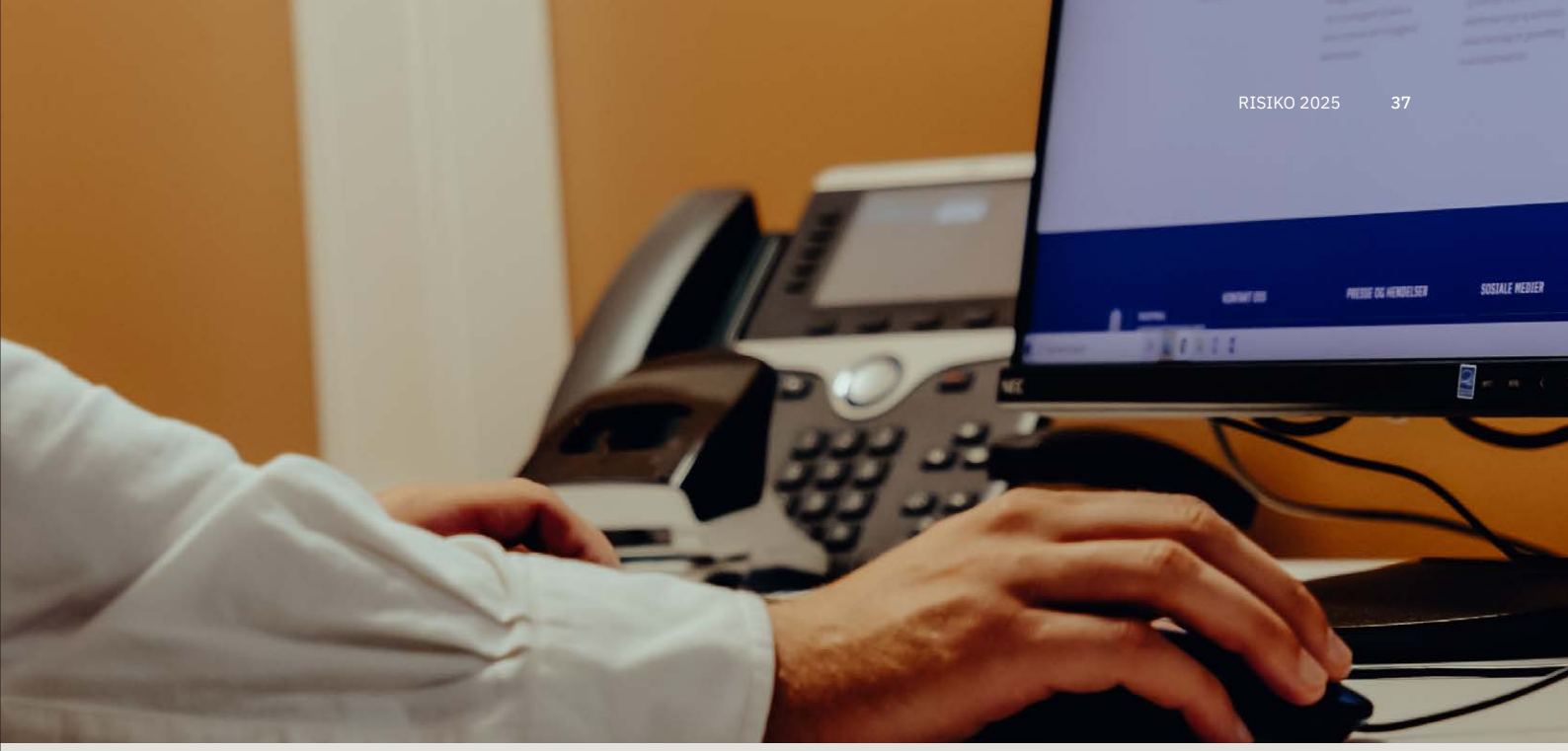
Kunstig intelligens (KI) har i løpet av de siste årene økt i popularitet og tilgjengelighet. Mulighetene som følger av utviklingen i KI er betydelige, samtidig som mulighetene for ondsinnet bruk av teknologien øker tilsvarende.

Verktøy og systemer som benytter kunstig intelligens blir i økende grad brukt både til forsvar og angrep i cyberdomenet. Tilgjengeligheten av KI-modeller har gjort flere aktører i stand til å utføre cyberoperasjoner uten inngående teknisk kompetanse. Det er observert flere tilfeller i løpet av det siste året der aktører har brukt KI for å utføre operasjoner i cyberdomenet.

I februar 2023 benyttet trusselaktøren Indrik Spider seg av OpenAIs ChatGPT-modell til å generere kommandoer for å navigere i skyplattformen Azure og hente ut data fra tjenesten Azure Key Vault som lagrer informasjon sikkert. Trusselaktører kan angripe mer effektivt og raskere enn tidligere ved å bruke kunstig intelligens til å identifisere sårbarheter i programvare eller systemer. Det kan senke terskelen for opportunistiske kampanjer der aktøren ikke behøver inngående kunnskap om metodene du bruker eller systemene de angriper.

KI-modeller kan i seg selv være sårbare for aktører som ønsker å spre skadevare gjennom kompromittert materiale. Hugging Face er en av de største plattformene for deling av trente KI-modeller. Ondsinnede aktører kan utnytte plattformene til å legge inn modeller med bakdører. Derfor har Hugging Face markert rundt 2000 av tilgjengelige modeller som sårbare for muligheten til å kjøre ondsinnet kode når de lastes ned av brukere. En uavhengig skanning av plattformen utført av sikkerhetsselskapet ProtectAI fant ytterligere 1300 usikre modeller. Bruk derfor tilgjengelige ressurser med omhu.

KI-utviklere kan selv bli mål i et globalt KI-kappløp, der det konkurreres om utvikling og tilegning av teknologi som kan gi virksomheter styrket konkurranseevne eller stater økt forsvarsevne. I løpet av det siste året er det også observert cyberoperasjoner rettet direkte mot grupper og enkeltpersoner i KI-miljøer. Cybersikkerhetsselskapet ProofPoint har beskrevet en phishing-kampanje utført av trusselaktøren UNK_SweetSpecter i mai 2024 hvor KI-relaterte temaer ble brukt for å få offeret til å laste ned et e-postvedlegg med skadevare, i den hensikt å infisere og hente ut data fra mottager.



Anbefalinger til virksomheter for sikker utvikling og bruk av KI-verktøy

- Design KI-modellene dine for sikkerhet i like stor grad som for funksjonalitet og ytelse, og sikre leverandørkjeden under utviklingen av KI-verktøy.
- Ha forsvarlig styring på hvilke opplysninger KI-systemet har tilgang til for de enkelte oppgavene som skal løses med kunstig intelligens.
- Gjør ansatte kjent med trusler og risiko for phishingforsøk og andre forsøk på sosial manipulasjon som bruker KI-generert innhold.

Kjøp av datasentertjenester

NSM og Nasjonal kommunikasjonsmyndighet (Nkom) har utarbeidet felles råd for å bistå offentlige og private virksomheter ved kjøp av datasentertjenester. Datasentre er en viktig del av den digitale infrastrukturen i Norge. Det å ha kontroll med datasentrenes lokalisering, drift og sikkerhet er avgjørende for å beskytte samfunnsviktig data og tjenester. Rapporten fra NSM og Nkom gir en innføring i sikkerhet ved fysiske datasenteranskaffelser og dekker temaer som sikkerhetsstyring, risikovurdering og sårbarheter i leveransekjeden. For mer om anskaffelser generelt, se side 22 og 23.

Hjelp oss med å bygge et nasjonalt situasjonsbilde

Avvik fra normalen må varsles til myndighetene. Varsle politiet, PST, NSM eller andre. Det viktigste er ikke hvem varselet går til eller hvordan det er formulert, men at det varsles. Lag egne rutiner for varsling i virksomheten slik at alle ansatte er trygge på hva de skal gjøre.

Alle varsler bidrar til å opprettholde situasjonsbildet for nasjonal sikkerhet. God situasjonsforståelse er nødvendig for at myndigheter og virksomheter skal kunne møte fremtidige sikkerhetsutfordringer med presise sikkerhetstiltak. Norge er avhengig av at virksomheter melder inn sikkerhetstruende aktivitet til NSM. Ditt varsel kan være viktig for landets sikkerhet.

Virksomheter underlagt sikkerhetsloven er lovpålagt å varsle om sikkerhetstruende hendelser, mistanke om dette, og brudd på sikkerhetsloven. Som privatperson kan du varsle om hendelser og observasjoner som du frykter kan skade nasjonale sikkerhetsinteresser eller viktige verdier.

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 ugraderte varsler. NSM har egne kanaler for gradert varsling.

Ilja Hendel/NSM
Design Tank

NASJONAL
SIKKERHETSMYNDIGHET

Postboks 814,
1306 Sandvika
Tlf. 67 86 40 00

25/00063
nsm.no/risiko2025
www.nsm.no