NSM

Risiko 2024

Nasjonal sikkerhet – et felles ansvar

Forsidefoto: Espen Haagensen/NTB

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

Nasjonal sikkerhetsmyndighet (NSM) er Norges direktorat for nasjonal forebyggende sikkerhet. Tjenestens hovedoppgave er å bedre Norges evne til å beskytte seg mot spionasje, sabotasje, terror og sammensatte trusler. Gjennom rådgivning, kontrollaktiviteter, tilsyn, testing og forskning 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.

Etterretningstjenesten

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.

Politiets sikkerhetstjeneste

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 beskriver hvordan trusselaktører kan utnytte sårbarheter hos virksomheter og i samfunnet, og hvilken risiko dette medfører. I rapporten peker NSM på hvordan myndigheter og virksomheter bør redusere sårbarheter for å gjøre trusselaktørenes jobb vanskeligere.

Risiko henvender seg til hele samfunnet, men spesielt til ledere og personell med sikkerhetsoppgaver. Målet med rapporten er å gi virksomheter bedre forutsetninger for å se sikkerhetsarbeidet i en større sammenheng. Dette er spesielt relevant for virksomheter underlagt sikkerhetsloven, men også for andre virksomheter hvor sikkerhet er viktig. Rapporten beskriver eksempler og anbefalte tiltak som norske virksomheter bør gjøre for best å beskytte seg mot spionasje, sabotasje, terror og sammensatte trusler.

Årets rapport kan lastes ned på nsm.no/risiko2024

Innhold

NVE/Arne T. Hamarsland

Demokratier er under press

Land som Kina og Russland ønsker å endre dagens verdensorden. Det er fare for at fremmede staters og trusselaktørers bruk av teknologi kan utvikle seg raskere enn åpne demokratiers evne til å beskytte seg. Autoritære regimer vil kunne utnytte informasjonsteknologi på måter som rammer demokratier med åpne informasjonsmiljøer hardest, som for eksempel Norge.

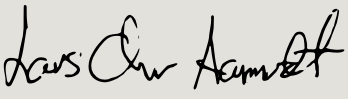
I løpet av valgåret 2024 skal minst 64 land og EU, som til sammen representerer nærmere halvparten av verdens befolkning, avholde valg. Sju av verdens ti største land skal velge nye ledere. Valgresultatene kan få mye å si for den sikkerhetspolitiske utviklingen.

Demokratier er utsatt for sammensatt virkemiddelbruk som ligger under terskelen for væpnet konflikt. Det utgjør en stor utfordring. Spionasje mot statlige og private virksomheter, cyber-operasjoner, sikkerhetstruende oppkjøp, rekruttering av innsidere og påvirkningsoperasjoner mot befolkningen er bare noen av virkemidlene som må forhindres, avdekkes og håndteres hver eneste dag.

Norges sikkerhetsutfordringer treffer hele samfunnet. De påvirker enkeltpersoner, befolkningsgrupper, statlige virksomheter, store og små bedrifter, og demokratiske prosesser og institusjoner. Vi må styrke vår motstandsevne. En trusselbasert «føre var»-tilnærming er avgjørende. Det innebærer å iverksette tiltak som beskytter oss, før skaden inntreffer.

Trusselvurderingene fra Etterretningstjenesten og PST peker på truslene rundt oss. Risiko 2024 bidrar med innsikt som skal gjøre norske virksomheter i bedre stand til å beskytte seg mot spionasje, sabotasje, terror og sammensatte trusler. Det ligger mye kunnskap bak anbefalingene i denne publikasjonen. Jeg oppfordrer derfor alle norske virksomheter til å forberede seg på å kunne møte og takle de utfordringene som usikre tider byr på.


Gorm Kallestad/NTB



Lars Christian Aamodt
Direktør

Når truslene endrer seg, må også vår forståelse av utsatte sårbarheter og verdier endre seg. Utviklingen de siste årene har gjort at både virksomheter og enkeltpersoner som tidligere sjeldent har vært involvert i arbeidet med nasjonal sikkerhet, plutselig er helt sentrale. Privat næringsliv har fått større betydning for landets sikkerhet. Vi som enkeltmennesker og som arbeidstagere har mer å si for vår felles stats- og samfunnssikkerhet enn de fleste kanskje tenker over.

En av NSMs mange oppgaver er inntrengingstesting. Våre inntrengingstestere har som jobb å fysisk og digitalt «bryte seg inn» i landets viktigste virksomheter for å avdekke sårbarheter og teste motstandsevne. Når de likevel oppsummerer noe så ordinært som svake passord som en av de enkleste veiene inn i viktige systemer, har vi alle sammen en jobb å gjøre. Den enkelte kan gjøre en forskjell. Også for nasjonal sikkerhet.

Sammendrag

Privat næringsliv har fått større betydning for nasjonal sikkerhet i lys av sikkerhetspolitiske og teknologiske utviklingstrekk. Derfor belyser Risiko 2024 spesielt situasjonsforståelse, beskyttelse av kritisk infrastruktur og cybersikkerhet som strategiske risikoområder med særlig betydning for nasjonal sikkerhet.

Situasjonsforståelsen må styrkes i hele samfunnet. For virksomheter innebærer det å kartlegge virksomhetens verdier, avhengigheter og relevante trusler. Det sammensatte og dynamiske trusselbildet som Etterretningstjenesten og PST beskriver, gjør helhetlig, forebyggende sikkerhetsarbeid enda viktigere. Det nytter ikke med eksempelvis gode fysiske sikringstiltak dersom virksomhetens verdier enkelt kan rammes digitalt eller gjennom leverandørkjeden. Bortfall av en underleverandør kan få alvorlige konsekvenser, ikke bare for selskaper med avhengighetsforhold, men også for nasjonal sikkerhet.

Kritisk infrastruktur må skjermes mot innsyn og påvirkning. Både utenlandske oppkjøp og investeringer i norske selskaper og anskaffelser må i større grad ses i sammenheng med nasjonal sikkerhet. Importert teknologi kan være utstyrt med skjulte bakdører eller sårbarheter som kan utnyttes. Når sluttbrukeren understøtter grunnleggende nasjonale funksjoner, kan slik utnyttelse få alvorlige konsekvenser for nasjonal sikkerhet. Den samlede, nasjonale avhengigheten til land som utgjør en sikkerhetstrussel mot Norge, er en betydelig sårbarhet for nasjonale sikkerhetsinteresser.

Cybersikkerheten i virksomheter og hos myndigheter utfordres av stadig mer avanserte cyberoperasjoner. Kunstig intelligens må tas i bruk for å styrke analyse og avdekking av cyberoperasjoner. Samtidig må brukere av kunstig intelligens-modeller være bevisst på sårbarheter i teknologien som kan utnyttes av trusselaktører. Kunstig intelligens gjør fabrikkerte nyheter stadig mer troverdige. Kombinert med at desinformasjon kan spres på en helt annen skala enn tidligere, utfordres grunnmuren i demokratiske styresett.

Stian Norum Herlofsen/Forsvaret

Et sikkerhetspolitisk landskap i endring

Russlands angrepskrig mot Ukraina, økende stormaktsrivalisering mellom USA og Kina, og en stadig tiltakende teknologisk utvikling er utviklingstrekk som får konsekvenser for nasjonal sikkerhet.

Norsk næringsliv understøtter også nasjonal sikkerhet

Norge sikrer energi til europeisk industri og oppvarming av millioner av hjem med eksport av gass fra norsk sokkel. Ifølge Etterretningstjenesten har Russland søkt å svekke vestlig samhold og vilje til å støtte Ukraina ved å legge press på Europas energisektor, blant annet ved å strupe den russiske gasseksporten. Det har økt Norges betydning for europeisk energisikkerhet.

Totalt er nesten 9000 kilometer med gassrørledninger tilknyttet norsk gassproduksjon. Det er lengre enn avstanden fra Oslo til Tokyo. En del av dette er kritisk infrastruktur for Norge – og Europa. Sabotasjen mot gassrørledningene Nord Stream 1 og 2 høsten 2022, og skadene på gassrørledningen mellom Finland og Estland høsten 2023, viser at kritisk sivil infrastruktur er sårbar for ytre påvirkning.

Europeiske land kan potensielt bli enda mer avhengige av norsk olje og gass, om konfliktene i Midtøsten skaper forstyrrelser i petroleumsmarkedet. Det øker den sikkerhetspolitiske verdien av norsk petroleumsproduksjon ytterligere, og det øker også risikoen knyttet til norsk petroleumsvirksomhet.

Innsatsen som operatørselskapene gjør på norsk sokkel får dermed stor betydning for nasjonal og internasjonal sikkerhet. Det omfatter også alle de som understøtter innsatsen med tjenester og logistikk. Det samme gjelder andre sektorer og virksomheter nasjonalt. Sikkerhetspolitikk er ikke avskåret fra resten av samfunnet, men både understøttes og påvirkes av en rekke ulike virksomheter.

NVE/Stig Storheil

Nye sårbarheter vokser frem

Ifølge PST utgjør Russland den største etterretningstrusselen mot Norge i 2024, mens trusselen fra Kina vurderes som betydelig og skjerpet. Den kinesiske applikasjonen TikTok fikk mye medieoppmerksomhet i 2023, men NSM vurderer at det er det totale kinesiske fotavtrykket i Norge som utgjør en betydelig risiko for nasjonal sikkerhet.

Eksempelvis vil den grønne omstillingen være avhengig av både mineraler og komponenter som i utstrakt grad kommer fra Kina. Kina står bak om lag 60 prosent av verdens gruveutvinning av sjeldne jordarter og 99,9 prosent av utskillingen av tunge sjeldne jordarter. Disse jordartene er avgjørende for å produsere komponenter som brukes innen blant annet fornybar energi, helseteknologi og forsvarsmateriell.

Norges avhengighetsforhold til Kina er en sårbarhet som kan utnyttes av kinesiske styresmakter. Det er derfor en nasjonal sikkerhetsrisiko at verdier og grunnleggende nasjonale funksjoner i Norge er avhengige av, eller kan påvirkes av, stater som utgjør en betydelig trussel mot Norge. Disse verdiene og funksjonene må fungere i fred, krise og krig. Skulle kritiske leveranser fra Kina opphøre grunnet handels- eller sikkerhetspolitiske forhold, vil det kunne ramme norske virksomheter så vel som nasjonale sikkerhetsinteresser.

Mistet leverandørklarering

Endringer i eierskapsstruktur kan medføre risiko for at sikkerhetsgradert informasjon tilflyter uvedkommende. Derfor er det ingen automatikk i at leverandørklareringer overføres fra et selskap til et annet ved eierskifte.

Oslo Patentkontor AS hadde klarering til å forvalte sikkerhetsgraderte patenter. Patentene kan omhandle våpenteknologi og er høygraderte grunnet betydningen for nasjonale sikkerhetsinteresser. Det er informasjon som er av særlig interesse for blant annet kinesisk etterretning.

Da patentkontoret ble overdratt til et annet selskap med koblinger til et kinesisk partnerselskap i 2022, utløste det tilsyn fra NSM. På bakgrunn av en helhetsvurdering av funn fra tilsynet samt forholdet til det andre selskapet, ble klareringen trukket og NSM fjernet all gradert informasjon fra kontoret.

NSM er ikke kjent med at den graderte informasjon er kompromittert, og har heller ingen grunn til å mistenke det. Uavhengig av intensjonen bak nettopp dette eierskiftet, er overdragelsen et vanlig eksempel på hvordan sikkerhetstruende økonomisk virkemiddelbruk kan se ut. For trusselaktører kan det være enklere å kjøpe seg inn enn å bryte seg inn. Derfor oppfordrer NSM virksomheter til å risikovurdere endringer i eierskapsstruktur, og rådføre seg med NSM i forkant av eierskapsendringer. Virksomheter med leverandørklarering er derimot lovpålagt å informere NSM om endringer i eierskapsstruktur.

Muligheter og sårbarheter i kunstig intelligens

Et tredje utviklingstrekk som bringer både muligheter og utfordringer, er inntoget av kunstig intelligens (KI).

Ved hjelp av kunstig intelligens blir det enklere og rimeligere å produsere innhold som er falskt, enten det er snakk om tekst, bilder eller video. Teknologien utnyttes til å utvikle sofistikerte og automatiserte cyberoperasjoner og til å effektivisere spredningen av desinformasjon og fabrikkerte nyheter på en mer troverdig måte enn tidligere.

Når datamengdene og kompleksiteten øker, er kunstig intelligens og maskinlæring også nødvendig for å skille ondsinnet aktivitet fra legitim aktivitet. Denne teknologien vil også ha en viktig rolle innen analyse og avdekking av cyberoperasjoner mot norske virksomheter. Kunstig intelligens-modeller har imidlertid sårbarheter i seg selv som kan utnyttes av trusselaktører – og som må håndteres forebyggende. Det er viktig at norske myndigheter og industrien henger med i utviklingen av kunstig intelligens for å sikre en trygg, sikker og pålitelig bruk av teknologien i tiden fremover. Sikker anvendelse og god regulering av kunstig intelligens krever menneskelig intelligens.

Kunstig intelligens brukes for å undergrave demokratiske prosesser

I løpet av valgåret 2024 skal minst 64 land og EU, som til sammen representerer nærmere halvparten av verdens befolkning, avholde valg. To eksempler fra 2023 viser hvordan kunstig intelligens kan utnyttes for å påvirke valg og demokratiske prosesser.

I forkant av det slovakiske valget i november 2023 ble et lydklipp der en av kandidatene og en journalist diskuterte hvordan man kunne rigge valget spredt på sosiale medier. Klippet er en såkalt *deepfake*, og både kandidaten og journalisten gikk ut og avkreftet innholdet. *Deepfakes* utnytter kunstig intelligens for å lage videoer og lydinnhold som kan være svært vanskelig å avsløre som falskt.

På samme måte ble en tidligere ordfører i London i november 2023 misbrukt i et lydklipp der han skal ha tatt til orde for å utsette Våpenhviledagen, en viktig minnesmarkering for første verdenskrig. Det klippet var også en *deepfake*.

I disse tilfellene ble lydklippene avslørt som *deepfakes*, men teknologien blir raskt bedre, mer tilgjengelig og vanskeligere å avsløre.

Enkeltvirksomheters og enkeltindividers betydning for nasjonal sikkerhet

De sikkerhetspolitiske og teknologiske utviklingstrekkene reduserer avstanden mellom individer og virksomheter på den ene siden og nasjonal sikkerhet på den andre.

Når en statlig trusselaktør kartlegger verdier og utnytter sårbarheter i Norge, er det ikke nødvendigvis toppolitikere, store industrikonsern eller Forsvaret som er inngangsporten. Det kan være lettere å utnytte en mindre, men like fullt viktig, underleverandør for å få tilgang til et egentlig mål. Det er det flere årsaker til, men særlig fordi det er større sjanse for at underleverandørene ikke har de samme sikkerhetsrutinene på plass. At de ikke er like nøye i bakgrunnssjekken av sine ansatte eller kunder. At den nyeste sikkerhetsoppdateringen av en viktig programvare ikke er lastet ned enda. Eller at det er mindre sjanse for at de rapporterer om mistenkelig aktivitet eller cyberoperasjoner til myndighetene – *for er min virksomhet og min jobb et mål for fremmede etterretningstjenester?*

NSM berømmer at mange virksomheter tar cybersikkerheten på alvor. For trusselaktører øker dette verdien av en velplassert innsider. En innsider kan utføre eller legge til rette for spionasje eller sabotasje fra innsiden av virksomheten.

Stadig mer data behandles gjennom mobiltelefoner. Det gjør telefonen til en potensiell inngangsport til sensitiv og privat informasjon. NSM har sett flere tilfeller av *spearphishing* rettet mot ansatte i virksomheter som forvalter verdier som må beskyttes mot sikkerhetstruende virksomhet, eksempelvis innen forskning og forsvarsindustrien. Det er sjeldent den ansatte i seg selv er av interesse, men heller hvordan enkeltpersoner kan utnyttes som inngangsport til virksomhetens verdier. På denne måten kan en ansatt som i god tro trykker på en lenke eller åpner et vedlegg i e-post som tilsynelatende er sendt fra en kollega, gi en trusselaktør omfattende tilgang til virksomhetens nettverk og interne systemer.

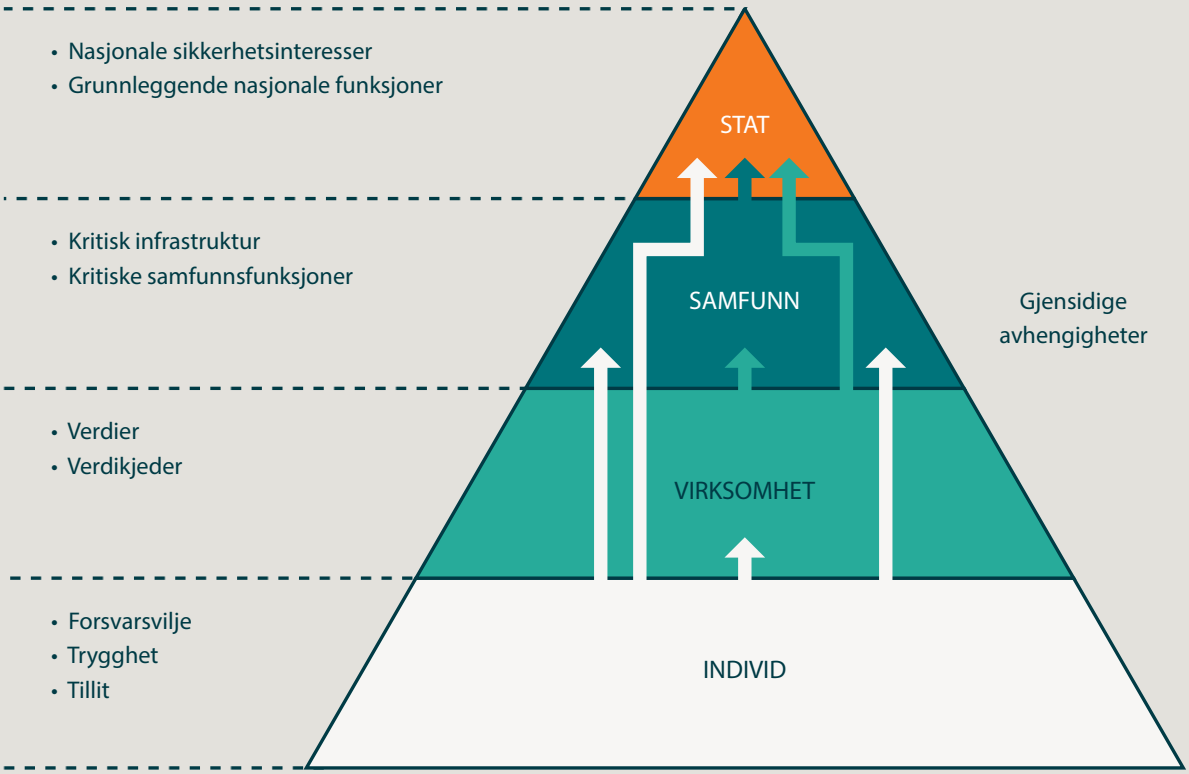
Norges sikkerhetsutfordringer påvirker hele samfunnet. Nasjonal sikkerhet angår de øverste statsorganer, enkeltpersoner og alt i mellom. Spionasje, sabotasje og sammensatte virkemidler kan brukes mot Norge der samfunnet er mest sårbart og hvor det kan medføre skader langt utover de som blir direkte berørt. Nasjonal sikkerhet er et samfunnsansvar.

Spearfishing

Spearphishing retter seg gjerne mot en bestemt person eller virksomhet. Metoden går ut på å bli kjent med denne aktørens handlingsmønster over tid, for så å lure til seg sensitive opplysninger, gjerne via falske e-poster fra en tilsynelatende troverdig person. *Phishing* er derimot mindre sofistikert, mindre ressurskrevende og sendes ofte til et stort antall mer eller mindre tilfeldige mottakere.

NSM/Ilja Hendel

Figur 1:
Gjensidige avhengigheter mellom ulike nivåer av sikkerhet.



Situasjonsforståelse styrker nasjonal sikkerhet i hele krisespekteret

Vet du ikke hva virksomheten din skal beskytte, hvorfor, eller mot hvilke trusler, blir heller ikke tiltakene du iverksetter treffsikre nok. Å kartlegge din virksomhets verdier og å etablere god situasjonsforståelse er avgjørende for å styrke beskyttelsen av din virksomhet og nasjonal sikkerhet gjennom hele krisespekteret – i fred, krise og krig. Departementer og virksomheter underlagt sikkerhetsloven må intensivere arbeidet med å få oversikt over egne skjermingsverdige verdier, sårbarheter og avhengigheter.

Tilsynsfunn i 2023

NSM gjennomfører årlig tilsyn med utvalgte virksomheter som er underlagt sikkerhetsloven. Hensikten er å styrke det forebyggende sikkerhetsarbeidet og kontrollere at kravene i sikkerhetsloven er oppfylt.

I et av tilsynene i 2023 avdekket NSM eksempelvis at det ikke var etablert adgangskontroll til et lokale for gradert tale. Som konsekvens kunne personell uten autorisasjon fritt bevege seg på egenhånd i lokalet. Slike sikkerhetshull gjør det langt enklere for uvedkommende å eksempelvis utplassere avlyttingsutstyr på områder som er ment for sikkerhetsgraderte samtaler. Et effektivt tiltak for å redusere risikoen for innsidere er å etablere både fysiske og digitale autorisasjonsskiller.

Tilsynsfunn fra 2023 viser totalt sett at de viktigste forbedringsområdene er knyttet til identifisering av skjermingsverdige verdier og å få oversikt over hvilke avhengigheter virksomhetene har. NSM anbefaler virksomheter å fokusere det forebyggende sikkerhetsarbeidet rundt disse områdene. En forutsetning for et godt sikkerhetsarbeid er at virksomheter vet hva de skal beskytte, og mot hvilke trusler.

Virksomheter som er underlagt sikkerhetsloven, kan også få tilgang til graderte risiko- og trusselvurderinger fra etterretnings-, overvåknings- og sikkerhetstjenestene. Det styrker muligheten til å innføre sikringstiltak som reflekterer et oppdatert risikobilde. Virksomhetens avhengigheter bør kartlegges som en del av virksomhetens arbeid med å skaffe situasjonsforståelse. Dette kan være informasjons- og kommunikasjonssystemer, transportselskaper eller andre underleverandører, som kan utgjøre en sårbarhet.

Anette Ask/Forsvaret

NSM/Ilja Hendel

Et felles arbeid for å kartlegge Norges verdier

Det er gjort viktige fremskritt innen nasjonal verdikartlegging siden 2022. Flere grunnleggende nasjonale funksjoner er blitt identifisert, som «evne til å ivareta datalagring og prosesseringskapasitet i Norge», «transport av gass i rør til Europa» og «kontroll med utvinning av petroleum på norsk sokkel». Dermed har utvalgte virksomheter som understøtter disse funksjonene, blitt underlagt sikkerhetsloven. Det gir virksomhetene et utvidet sett med virkemidler til å sikre sine verdier, som sikkerhetsklarering av personell og tilgang på graderte trussel- og risikovurderinger fra myndighetene. Det bidrar til å sikre egen drift og til å opprettholde grunnleggende nasjonale funksjoner, som kommer samfunnet til gode.

Tross fremskritt i nasjonal verdikartlegging, gjenstår fremdeles mye arbeid med å utpeke og sikre viktige verdier. Verdikartlegging er en dynamisk prosess som må tilpasses gjeldende risikobilde.

Grunnleggende nasjonale funksjoner

Grunnleggende nasjonale funksjoner er tjenester, produksjon og andre former for virksomhet som er av en slik betydning at et helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser (jf. sikkerhetsloven § 1-5 nr. 2). Per februar 2024 er det pekt ut 48 grunnleggende nasjonale funksjoner. Se oversikt på nsm.no.

Hvem sikrer din kraftleveranse?

Virksomheten din bør ha en plan for hvordan den er sikret tilgang på elektrisk kraft gjennom hele krisespennet. I en akutt situasjon er det mange som har behov for både kraft og etterfylling av drivstoff. Hvor sikre er da deres egne forsyningslinjer? Dersom virksomheten er underlagt sikkerhetsloven og har behov for kraft utover det som kan sikres med egenberedskap, må avhengigheten kartlegges og meldes inn til overordnet departement og NSM.

Avhengigheter med betydning for nasjonal sikkerhet

For å oppnå effektiv verdiskapning i samfunnet er verdi- og leverandørkjeder på tvers av sektorer og landegrenser helt nødvendig. Samtidig må det skapes høyere bevissthet om at dette er avhengigheter som kan utnyttes på bekostning av nasjonale sikkerhetsinteresser.

Mange virksomheter som understøtter grunnleggende nasjonale funksjoner og som selv er underlagt sikkerhetsloven, har avhengigheter til private bedrifter som ikke er underlagt sikkerhetsloven. Eksempler på sistnevnte er bedrifter som utvikler eller produserer teknologi knyttet til petroleumssektoren, satellitter, droner eller kryptografi. Disse bedriftene både benytter og er avhengige av leverandører utenfor Norges grenser. Så lenge bedriftene ikke er underlagt sikkerhetsloven, har de heller ikke utvidede juridiske verktøy eller informasjon som kan bidra til å sikre virksomhetens verdier. Grunnleggende nasjonale funksjoner kan dermed være avhengige av leveranser fra virksomheter med et ukjent sikkerhetsnivå og med ukjente sårbarheter.

Virksomheter underlagt sikkerhetsloven skal selv melde fra til myndighetene om hvilke avhengigheter de har. Manglende kartlegging av avhengigheter fører til at det er ukjent for egen virksomhet hvilke andre bedrifter som er kritisk for ens egen drift og produksjon. Manglende kartlegging gjør det også vanskelig å forutse leveranseproblemer eller å oppdage at en leverandør har byttet underleverandør.

Et bytte av underleverandør hos en leverandør kan virke uproblematisk, men kan i ytterste konsekvens føre til at informasjon eller tilganger ender opp hos trusselaktører uten at virksomheten selv har mulighet til å avdekke det. For å avdekke konsentrasjonsrisikoen i egne leverandørkjeder er det viktig at virksomheter kartlegger egne avhengigheter til andre virksomheter.

Virksomheter som understøtter grunnleggende nasjonale funksjoner i ulike samfunnsområder, fra beredskap og helse til elektronisk kommunikasjon og finans, kan ha betydelige avhengigheter til land som utgjør en etterretningstrussel mot Norge. Kompromittering av slike leverandørkjeder kan få store konsekvenser for ivaretakelsen av grunnleggende nasjonale funksjoner og nasjonale sikkerhetsinteresser. I tillegg kan trusselaktører benytte bortfall av eller stans i leveranser til virksomheter som et politisk pressmiddel.

Verdikjede

En verdikjede beskriver ressurser, prosesser og aktiviteter som inngår i produksjonen av en vare eller tjeneste. Aktivitetssettet til en produksjonsbedrift kalles en verdikjede. Leverandørkjeden er den delen av verdikjeden som omfatter aktiviteter utført av ulike leverandører og eventuelle underleverandører.

Norsk Romsenter/T. Abrahamsen/Illustrasjon

Konsekvenser ved bortfall av satellittbaserte tjenester

Satellittbaserte tjenester bidrar til betydelig effektivisering og bedre sikkerhet på mange områder. Samtidig har mange funksjoner i samfunnet betydelige avhengigheter til slike tjenester, både som brukere og som sluttbrukere gjennom andre tjenester. Forstyrrelser eller bortfall kan raskt få betydelige konsekvenser for samfunnets og totalforsvarets evne til å fungere.

Satellittbaserte tjenester er viktige for Forsvaret, sivil- og militær luftfart, navigasjon, helsetjenester, finansielle tjenester, politi, rednings- og nødetater, i tillegg til andre samfunnsfunksjoner. De spiller en avgjørende rolle i nordområdene, der økt militær- og sivil aktivitet krever styrket nasjonal og alliert situasjonsforståelse. Satellittbaserte tjenester er blant annet viktige bidrag i å hevde norsk suverenitet, til overvåking av havområdene og for sikker kommunikasjon.

Den omfattende avhengigheten viser hvor sårbart samfunnet er dersom viktige satellittbaserte tjenester forstyrres eller går ned. Av den grunn er det viktig for norske virksomheter å kartlegge hvilke satellittbaserte tjenester de er avhengige av for å opprettholde egen produksjon og aktivitet.

Virksomheter bør også vurdere hvordan reserveløsninger, annen funksjonalitet, rutiner eller prosedyrer kan erstatte et eventuelt bortfall. Det gjelder særlig virksomheter som er avhengige av satellittbaserte tjenester for presis posisjon, navigasjon og tid (PNT).

Andøya Spaceport

Andøya Spaceport ble offisielt åpnet november 2023, og er den første operative romhavnen på det europeiske fastlandet.

Romhavnen gir Norge en nasjonal oppskytingskapasitet som svært få andre land har. Den vil være en viktig strategisk ressurs for både sivil og militær oppskyting av satellitter fra Europa, og et nasjonalt bidrag i alliert romsatsing gjennom NATO. Dette styrker Norges evne til å opprettholde viktige satellittbaserte tjenester gjennom krisespekteret.

Regjeringen har bevilget 300 millioner kroner over en toårsperiode (2024-2025) for å dekke militære behov og styrke sikkerheten ved Andøya Spaceport.

Kritisk infrastruktur og verdier må sikres

Beskyttelse av kritisk infrastruktur krever helhetlig sikring som reduserer sårbarheter som trusselaktører kan utnytte. I ytterste konsekvens kan kritiske ytelser til befolkningen eller Forsvarets evne til å forsvare norsk territorium bortfalle. Norske virksomheter bør blant annet være bevisst på risikoen knyttet til sikkerhetstruende økonomisk virkemiddelbruk, sikkerhetstruende bruk av droner og innsidevirksomhet.

Anskaffelser må ses i sammenheng med konsentrasjonsrisiko

NSM advarer mot konsentrasjonsrisikoen i samfunnet. Det gjelder både avhengigheten til enkeltland i enkeltanskaffelser og det totale omfanget av enkeltlands teknologi og leveranser i norske virksomheters leverandørkjeder.

Når anbud og anskaffelser vektlegger pris over sikkerhet, utgjør det en sårbarhet som kan utnyttes. Etterretningstjenesten vurderer at myndighetene i Kina subsidierer næringslivsaktører for å vinne anbudskonkurranser i vestlige land. Rimelig kinesisk teknologi blir da et naturlig valg for flere virksomheter, også i Norge. Det åpner også opp for at Kina får eksportert teknologi med skjulte bakdører som kan utnyttes til etterretningsvirksomhet. Skjulte bakdører er svært krevende å avdekke. Teknologi som er koblet til internett, kan være særlig utsatt for slik utnyttelse.

Kinesisk lovgiving pålegger kinesiske virksomheter å utlevere informasjon til kinesisk etterretning, og å rapportere oppdagede sårbarheter til myndighetene. Bruk av eksempelvis kinesisk videokonferanseutstyr kan derfor gi økt risiko for at sensitiv eller gradert informasjon tilflyter kinesisk etterretning. NSM har publisert råd for bedre sikkerhet på mobile enheter, som anbefaler å legge enheter utenfor møterommet dersom det skal gjennomføres sensitive samtaler.

Tilsvarende bør internettilkoblede videokonferansesystemer eller annet utstyr som utgjør en risiko, kobles fra internett når møterommet skal benyttes til å diskutere sensitiv informasjon. NSM erfarer at en del virksomheter ikke gjør innledende sikkerhetsvurderinger, men går rett på en anskaffelse. Dette skaper sårbarheter som trusselaktørene kan utnytte. Når anskaffelsen er gjort, kan det være for sent å ta grep.

Det er viktig å gjøre grundige sikkerhetsvurderinger i forkant av anskaffelser av utstyr som skal behandle sensitiv eller gradert informasjon. For sikkerhetsgraderte anskaffelser etter sikkerhetsloven gjelder egne regler.

Olav Standal Tangen/Forsvaret

Fire råd for sikrere innkjøp og anskaffelser

1. **Gjør gode risikovurderinger**
   Kjenn virksomhetens verdier, sårbarheter og eventuelle trusler. Gode risikovurderinger gir informasjon om hvilke krav som bør inn i kontrakten. Besitter virksomheten verdier som skal beskyttes etter sikkerhetsloven, er det egne regler for anskaffelsesprosessen. Oppdragsgivere som foretar offentlige anskaffelser, bør i større grad vekte sikkerhet i anskaffelsen.
2. **Ha riktig kompetanse rundt bordet**
   Både oppdragsgiver og personer med kompetanse innen anskaffelser, avtaler og helhetlig sikkerhet må delta i utarbeidelsen og vurdering av anskaffelsen. Bruk av leverandører og underleverandører krever at du ser på sikkerhet med nye øyne, da det er underleverandører som må gjøre nødvendige tiltak for å redusere sårbarheter. Dette betyr at det er et større behov for avtalekompetanse som sikrer gode kontrakter som etablerer kontroll gjennom hele leverandørkjeden.
3. **Ta inn gode sikkerhetsklausuler i kontraktene**
   Kontrakten er det viktigste virkemiddelet til å sikre kontroll med underleverandørene. Situasjonsbildet er dynamisk, og sikkerhetssituasjonen kan endre seg raskt. Kontrakten bør gi et handlingsrom for å håndtere endringer i verdi, sårbarheter og trussel, både på oppdragsgiver- og leverandørsiden.
4. **Følg opp leverandørforholdet**
   Bli kjent med leverandøren, og etabler mekanismer som sikrer en god oppfølging av kontrakten. Kontraktene bør blant annet inneholde varslingsplikter ved endringer i eierskapsstrukturen og sikkerhetstruende hendelser. For at dette skal ha effekt, må det være etablert et system for å håndtere varsler.

Hensyn til nasjonal sikkerhet blir viktigere i offentlige anskaffelser

Den kinesiske droneprodusenten DJI Technology er både svartelistet og sanksjonert av amerikanske myndigheter siden henholdsvis 2017 og 2021. Bakgrunnen er hensynet til nasjonal sikkerhet og selskapets koblinger til det kinesiske forsvaret. Andre kinesiske selskaper på svartelisten er Huawei Technologies og halvlederprodusenten SMIC.

Storbritannia la i 2023 ned et forbud mot å bruke den kinesiske videoovervåkningsprodusenten Hikvision ved sensitive områder som forsvars- og etterretningsinstallasjoner. USA la ned et fullstendig forbud mot import og salg av Hikvision året før. Sannsynligheten for at sensitiv informasjon tilflyter kinesisk etterretning trekkes frem som begrunnelse av britiske og amerikanske myndigheter.

Oppkjøp og investeringer som nasjonal sikkerhetsrisiko

Norge skal være et attraktivt land for utenlandske investeringer. Det er viktig for norsk økonomi. Samtidig må sikkerhetstruende økonomisk virkemiddelbruk forhindres.

Stater som utgjør en sikkerhetstrussel mot Norge, benytter seg av sikkerhetstruende økonomisk virkemiddelbruk. PST forventer at både Russland og Kina vil benytte seg av oppkjøp og investeringer i norske virksomheter for å oppnå tilgang på varer, tjenester og teknologi. Slike økonomiske transaksjoner gir potensielt innflytelse over, eller tilgang til, en verdi på en måte som direkte eller indirekte kan skade nasjonale sikkerhetsinteresser.

For å redusere konsentrasjonsrisikoen og begrense sikkerhetstruende økonomisk virksomhet, har flere vestlige land begynt å føre en strategi om å redusere eventuell avhengighet til Kina innenfor kritiske sektorer som forsvar, elektronisk kommunikasjon (ekom) og energi. Det betyr at virksomheter innenfor disse sektorene, som allerede har avhengigheter til Kina, fremover vil måtte planlegge for å finne alternative leverandører.

Kinesiske oppkjøp av teknologibedrifter er blitt gjenstand for strengere regulering i Europa, i takt med økt sikkerhetsbevissthet. Ifølge Etterretningstjenesten søker kinesiske aktører tilgang på teknologi og kunnskap i Norge. Det gjelder særlig innen fagfelt med flerbrukspotensial, det vil si teknologi som kan anvendes til både sivile og militære formål. Norske virksomheter som driver med forskning, utvikling eller produksjon av navigasjonssystemer, kryptologi, atomteknologi, kunstig intelligens eller bioteknologi kan være særlig utsatt for blant annet sikkerhetstruende økonomisk virksomhet.

Slike aktiviteter brukes for å få innpass i beslutningsprosesser eller tilgang til sensitiv informasjon, teknologi og kompetanse. Strategisk posisjonering og innflytelse kan også være en motivator. Aktivitetene er ikke nødvendigvis ulovlige, men kan brukes for å nå noen av de samme målene som ved ulovlig etterretningsvirksomhet, ifølge PST. Det kan undergrave nasjonal sikkerhet.

Det finnes en rekke eksempler på kinesiske oppkjøp og investeringer i utenlandske selskaper med kompetanse og teknologi som er av relevans for Kinas forsvarsmodernisering. Ifølge Etterretningstjenesten stanset Tyskland og Storbritannia i 2022 kinesiske oppkjøpsforsøk av henholdsvis anlegg og firma for halvlederproduksjon. Økt bevissthet rundt sikkerhetstruende økonomisk virkemiddelbruk kan bidra til at kinesiske forsøk på oppkjøp og investeringer blir mer fordekt og dermed vanskeligere å avdekke.

Helene Sofie Thorkildsen/Forsvaret

Samtidig fører vestlige sanksjoner mot Russland til at russiske myndigheter i større grad enn tidligere benytter tredjeland for å tilegne seg teknologi og komponenter. I sum kan dette bidra til en økning i antall skjulte og fordekte investeringer og anskaffelsesforsøk mot norske virksomheter. Ifølge PST er selskapene som benyttes som mellomledd for å skjule sluttbrukeren, i økende grad europeiske selskaper.

NSM oppfordrer alle privatpersoner og virksomheter til å utvise årvåkenhet og til å varsle myndighetene om mistenkelige forhold. *Se hvordan du varsler NSM bakerst i rapporten.*

NSM er nasjonalt kontaktpunkt for motvirkning av sikkerhetstruende økonomisk virksomhet

Hovedoppgaven er å koordinere arbeidet med å forhindre, avdekke og håndtere sikkerhetstruende økonomisk virkemiddelbruk.

NSM har mottatt flere saker og henvendelser siden kontaktpunktet ble opprettet i 2021. NSM ser at sakene treffer bredt. I forsvarssektoren er mange av sakene knyttet til bruk av utenlandske leverandører. For petroleums- og ekom-sektoren er direkteinvesteringer den vanligste problemstillingen. Totalt er det flest saker i sivile sektorer.

NSM foretar nærmere undersøkelser i tilfeller hvor det mistenkes at økonomisk virkemiddelbruk kan medføre risiko for nasjonale sikkerhetsinteresser. Etterretningstjenesten og PST bidrar inn i NSMs risikovurderinger.

Det er trolig mørketall når det gjelder slike saker. Henvendelsene og sakene NSM mottar, gir ikke fullstendig oversikt over sikkerhetstruende økonomisk virkemiddelbruk i Norge.

Innsidevirksomhet

Den sikkerhetspolitiske situasjonen gjør innsiderisikoen i private og offentlige virksomheter enda mer aktuell. Statlige trusselaktører har i 2024 mer å vinne og mindre å tape på å utnytte også menneskelige sårbarheter for å få tilgang på verdifull informasjon. Norske virksomheter er ikke skjermet for denne utviklingen.

I takt med at den digitale sikkerheten blir bedre i mange virksomheter, blir enkeltmennesket en stadig viktigere inngangsport til skjermingsverdige objekter og infrastruktur. Metodene flere etterretningstjenester bruker, er sofistikerte og utspekulerte. De kan være krevende å avdekke. Imidlertid vil gode personellmessige, fysiske, organisatoriske og digitale sikringstiltak redusere risikoen for at innsidere gjør skade på virksomheten og nasjonal sikkerhet.

Det ble avslørt en rekke innsidere i flere vestlige land i 2022 og 2023. Mange av disse hadde høy sikkerhetsklarering i betrodde stillinger og tilgang til svært sensitiv informasjon. Sakene som er avdekket, viser tydelig hvordan fremmede etterretningstjenester aktivt bruker innsidere som et virkemiddel. Det vil være naivt å tro at det ikke finnes innsidere i betrodde stillinger også her i Norge, enten de er bevisste eller ubevisste innsidere. Kunnskapen i virksomheter om hva en innsider er, hvordan de opererer og trusselbildet rundt innsidevirksomhet er for lav. Det øker risikoen for innsidere i norske virksomheter.

Den sikkerhetspolitiske situasjonen gjør at enkeltvirksomheter har fått større betydning for nasjonal sikkerhet enn tidligere. Blant annet bidrar sanksjoner og isolasjon fra vestlige land, ifølge Etterretningstjenesten, til at Putin-regimet i økende grad må benytte fordekte metoder for å skaffe informasjon, varer og teknologi. Forståelsen av at fremmede etterretningstjenester vil forsøke å utnytte personell i andre virksomheter og sektorer enn tidligere bør styrkes.

Sikkerhetsklarering av personell er et viktig virkemiddel for virksomheter som er underlagt sikkerhetsloven. Det er mange nye sikkerhetstiltak som skal tas i bruk på kort tid, samtidig som kompetansen i virksomheten skal styrkes, når virksomheter blir underlagt loven. NSM erfarer at dialog med etterretnings-, overvåknings- og sikkerhetstjenestene om trussel, sårbarheter og tiltak er et viktig hjelpemiddel i startfasen. Å forstå hvordan økt usikkerhet i samfunnet, økende konfrontasjon mellom ulike verdenssyn og andre faktorer kan påvirke individers personellmessige sårbarheter, er viktig for virksomheter som skal utøve sikkerhetsmessig ledelse for klarert personell.

NSM/Ilja Hendel

Innsidevirksomhet

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

Den bevisste og ubevisste innsideren

Den bevisste innsideren er en person som med forsett utnytter egne legitime tilganger for ondsinnede formål – på vegne av seg selv eller andre. Personen kan være drevet av egne motiv som misnøye, hevn, ideologi, økonomi eller annet. Det kan også være en person som er rekruttert eller i verste fall presset av en statlig eller ikke-statlig trusselaktør. En ubevisst innsider er en som uforvarende videreformidler informasjon som ikke skulle vært videreformidlet, eller skjødesløst lar være å forholde seg til sikkerhetskrav og sikkerhetsoppdateringer.

Svensk brødrepar dømt for spionasje

To iranskfødte brødre i Sverige ble dømt for grov spionasje til fordel for den russiske militære etterretningstjenesten GRU i 2023. Den eldste broren ble dømt til livstid i fengsel. Han hadde i flere år jobbet for det svenske etterretningspolitiet Säpo og den svenske militære etterretnings- og sikkerhetstjenesten Must. Den yngste broren ble dømt til ni år og ti måneders fengsel. Ifølge tiltalen har de to spionert for GRU siden 2011. Begge nekter straffskyld.

Personelloppfølging reduserer innsiderisiko

Jack Teixeira, en IT-spesialist i det amerikanske forsvaret, ble i 2023 siktet for å ha delt graderte forsvarsdokumenter om Russlands krig mot Ukraina, samt annen gradert informasjon i chattegrupper på sosiale medier. Dette er en av de mest alvorlige, *kjente* lekkasjene av hemmeligstemplet informasjon i USA på mange år. Teixeira nekter straffskyld.

Etterforskningen avdekket at en bedre personelloppfølging av Teixeira kunne ha stanset lekkasjene tidligere. 15 kolleger av Teixeira fikk disiplinære sanksjoner av det amerikanske luftforsvaret for forsømmelig oppfølging av Teixairas mistenkelige oppførsel.

NSM/Tija Hendel

Risikoreduserende tiltak i ansettelsesprosesser til stillinger som ikke krever sikkerhetsklarering

NSM får mange spørsmål om hvilke grep virksomheter bør foreta når de ikke har adgang til å sikkerhetsklarere personell. Tiltakene under kan bidra til å styrke personellsikkerheten for virksomheter generelt.

- Ta stilling til hvilke verdier som finnes i virksomheten, og hvilke stillinger som skal forvalte eller ha tilgang til verdiene. Selv om virksomheten ikke forvalter skjermingsverdig informasjon, infrastruktur eller objekt, så kan den ha annen sensitiv informasjon som er interessant for trusselaktører.
- Ta stilling til hvilke egenskaper ansatte bør ha – også i et sikkerhetsmessig perspektiv – i rekrutteringsprosesser.
- Egenskaper vedrørende sikkerhet bør skrives inn i utlysningsteksten dersom dette er relevant. Det gjør at sikkerhet kan være et naturlig tema under intervju og i utvelgelsesprosess. Skriv utlysningsteksten sammen med virksomhetens HR- eller juridiske avdeling.
- Utlysningstekster skal være i samsvar med relevant regelverk, for eksempel diskrimineringslovgivningen.
- Still spørsmål om sikkerhet under intervjuet. Sørg for at kandidaten er sikkerhetsbevisst i tråd med interne retningslinjer.
- Sikre risikoreduserende tiltak for stillinger, for eksempel ved bruk av bakgrunnssjekk.
- Ved ansettelse – gi opplæring i virksomhetens sikkerhetsreglement og retningslinjer. Når retningslinjene om sikkerhet er en del av grunnopplæringen, sørger virksomheten for at medarbeiderne får kunnskap om, og forholder seg til, lovgivning og interne retningslinjer. Det gir også et signal om at virksomheten og ledelsen setter sikkerhet og sikkerhetskultur høyt.
- Utøv god sikkerhetsstyring og legg til rette for en god sikkerhetskultur. Følg opp medarbeiderne. Sørg for at personellsikkerheten har oppmerksomhet i hele ansettelsesforholdet.

Sensorforbudssoner

Over hele Norge finnes det militære og andre installasjoner og anlegg som krever beskyttelse mot overvåkning og kartlegging av hensyn til rikets sikkerhet.

Ved og rundt slike installasjoner og anlegg er det ulike restriksjoner, som adgangsbegrensninger, fotoforbud på bakken og forbud mot fotografering/filming fra luften og bruk av andre luftbårne sensorer.

Skal du fly med drone? Sjekk først oversikt over sensorforbudsområder på nsm.no.

Droner som trussel mot kritisk infrastruktur

I Norge har NSM, politiet, Avinor og Forsvaret i samarbeid testet ut systemer for å oppdage droner ved ulike lokasjoner. Det er avdekket betydelig høyere droneaktivitet enn forventet på stedene hvor systemene har vært utplassert.

Droner kan benyttes til å utøve både etterretning, sabotasje og terrorvirksomhet. I tillegg til å samle inn informasjon kan droner relativt enkelt påføre skade på kritisk infrastruktur og andre viktige funksjoner. Krigen i Ukraina har vist at kommersielt tilgjengelige droner brukes til etterretning, og at de med enkelhet kan modifiseres til å bli angrepsdroner.

Droner kan benyttes til etterretningsvirksomhet også i Norge. De kan kartlegge status, detaljer, rutiner og sårbarheter ved norske skjermingsverdige områder og objekter.

Kommersielt tilgjengelige droner skal ikke benyttes rundt kritisk infrastruktur eller skjermingsverdige områder. Planløsninger og oversikt over skjermingsverdig infrastruktur kan ha høy verdi for enkelte trusselaktører. Selv upubliserte bilder, video og lydopptak kan tilflyte uvedkommende.

NSM har avdekket at entreprenører har tatt i bruk kommersielt tilgjengelige droner ved byggeaktivitet ved skjermingsverdige objekter. I forbindelse med boligsalg er skjermingsverdige anlegg blitt ulovlig fotografert av droneoperatører som tar luftfoto til boligannonser. I enkelte tilfeller har bildene blitt lastet opp i boligannonser på internett.

Det er for de fleste opplagt at å overlevere bilder av skjermingsverdige anlegg til en fremmed etterretningstjeneste er både alvorlig og ulovlig, men konsekvensene av å fly en kommersiell drone over slike anlegg er potensielt de samme for nasjonal sikkerhet.

Droneaktivitet har også ved flere anledninger ført til at luftrommet over store områder i Norge har blitt stengt i perioder. Håndheving av uønsket dronebruk forutsetter definerte sensorforbudsområder. Det er en utfordring at det ikke er utpekt flere sensorforbudssoner i Norge slik at det blir ulovlig å fly med drone over kritisk infrastruktur med stor betydning for nasjonal sikkerhet.

Luftbårne sensorsystemer

Luftbårne sensorsystemer er et samlebegrep for utstyr som kan innhente informasjon om bakken fra luften. Det mest åpenbare er droner, fly og helikopter med foto- eller filmkamera, men omfatter også annet avansert utstyr, slik som IR-sensor, laserskanner eller radar.

Sikkerheten i cyberdomenet må styrkes

Cyberoperasjoner har blitt hverdagskost for både offentlige og private virksomheter. Derfor må virksomhetene gjøre det de kan for å forhindre, avdekke og håndtere sikkerhetstruende hendelser.

Sentrale utviklingstrekk i cyberdomenet

Det er en evig kamp mellom utviklingen av nye angrepsmåter og utviklingen av sikkerhetstiltak. Noen sentrale utviklingstrekk i cyberdomenet er utnyttelsen av nulldagssårbarheter, cyberoperasjoner som rammer nær sagt alle samfunnssektorer og en gjennomgående profesjonalisering av angrepene.

Nulldagssårbarheter

Sommeren 2023 ble det kjent at 12 norske departementer var blitt kompromittert gjennom bruk av såkalte nulldagssårbarheter. «Regjeringen står under angrep», sa statsministeren med henvisning til kompromitteringene. En avansert trusselaktør hadde over lengre tid tilgang til flere deler av departementenes nettverk. Nulldagssårbarheter er vanskelig å beskytte seg mot. Men det hjelper alltid å følge grunnleggende tiltak, som å segmentere nettverk, installere sikkerhetsoppdateringer så raskt som mulig, og ha orden på loggfiler. *Se NSMs grunnprinsipper for IKT-sikkerhet på nsm.no for mer informasjon.*

Tjenestenektangrep rammer mange sektorer

Høyteknologi, næring og offentlig forvaltning er fortsatt de mest utsatte samfunnsområdene for cyberoperasjoner i alle former, totalt sett. Forsvarsindustrien har også vært rammet av cyberoperasjoner – noen av dem svært alvorlige. Etterretningstjenesten påpeker at russiske aktører er ute etter informasjon om norsk politikkutforming, særlig innen forsvars-, utenriks- og sikkerhetspolitikk samt nordområdene, Svalbard og energisektoren.

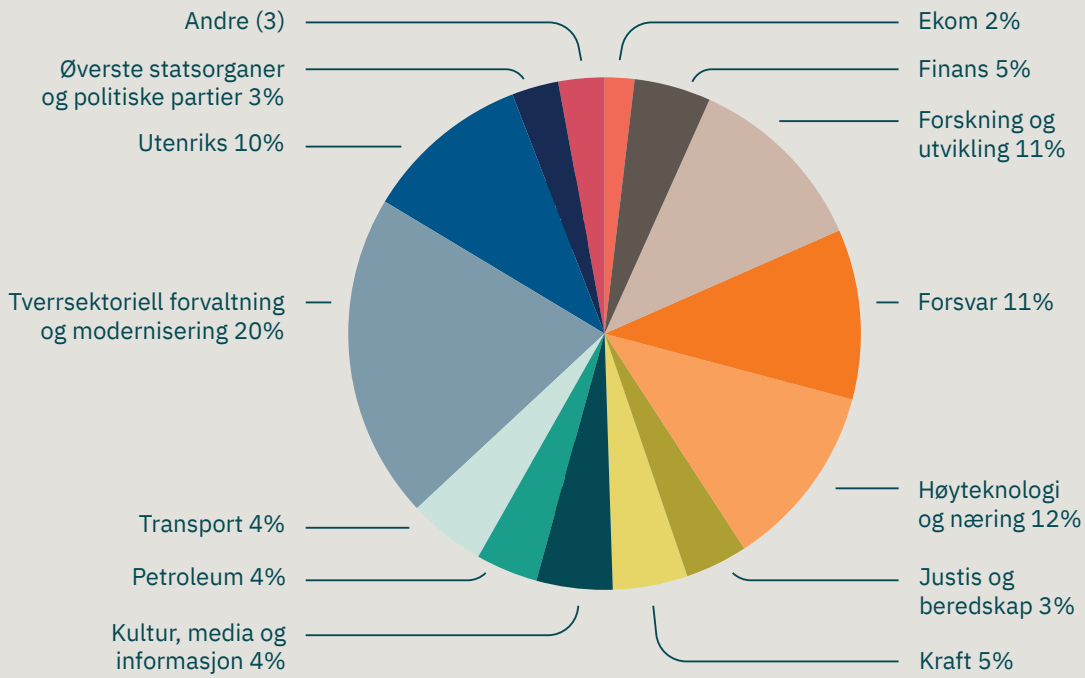
I 2023 har en rekke tjenestenektangrep fra pro-russiske aktører truffet virksomheter i transport-, finans- og helsesektoren. Flere av virksomhetene i disse sektorene har ikke tidligere vært rammet av angrep i dette omfanget. I mange av de mindre alvorlige tjenestenektangrepene mot forsvarsindustrien oppgir russiskspråklige hacktivister selv at motivasjonen for angrepene er Norges rolle som støttespiller for Ukraina.

Profesjonalisering av angrep

Internasjonalt beskriver cybersikkerhetsorganisasjoner at alle ledd i en angrepskjede profesjonaliseres; fra sårbarhetsskanning og *phishing*-kampanjer til løsepengeangrep, tjenestenektangrep og stjålne brukernavn og passord.

Også i Norge er det tegn til profesjonalisering av angrep. Eksempelvis har kvaliteten på *spearphishing* nådd et urovekkende høyt nivå. Alle mennesker kan bli lurt i et svakt øyeblikk, selv den mest årvåkne. NSM forventer at utviklingen innenfor kunstig intelligens vil skape ytterligere forbedringer og dermed enda større utfordringer. Teknologiutviklingen vil muliggjøre økt automatisering og en type spredning av svindel, desinformasjon og spionasje på måter som de færreste fullt ut forstår rekkevidden av.

Figur 2:
Prosentandel av registrerte cyberhendelser per samfunnssektor siden sommeren 2022



Cyberoperasjoner kan skade kritisk infrastruktur

Cyberoperasjoner begrenser seg ikke nødvendigvis til det digitale domenet. De kan i verste fall føre til alvorlige fysiske skader på kritisk infrastruktur og personell.

De siste årene er det avdekket ondsinnede cyberverktøy som er tilpasningsdyktige til styring- og kontrollsystemer som brukes i kritisk infrastruktur i flere sektorer. Slike systemer brukes også i Norge. Styring og kontroll av kraftproduksjon, kraftdistribusjon samt produksjon og leveranse av olje og gass utføres i stor grad av operasjonell teknologi og industrielle kontrollsystemer. Robustheten til barrierer og sikringsløsninger skal forhindre at slike cyberverktøy treffer de industrielle kontrollsystemene. Risikoen knytter seg til de enorme konsekvensene som kan utløses, dersom en avansert trusselaktør skulle velge å bruke slike potensielle kapasiteter.

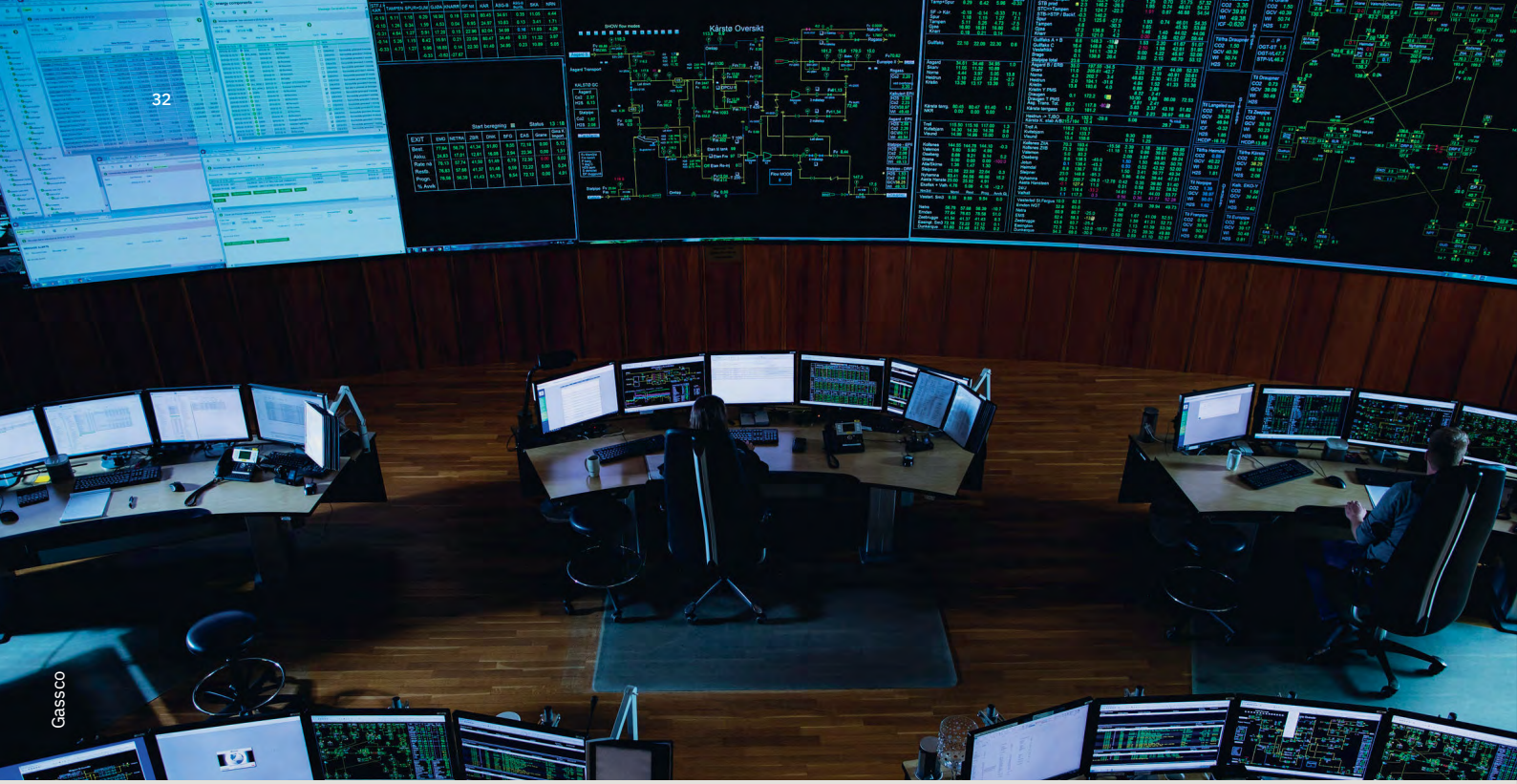
Fjerntilgang til industrielle kontrollsystemer gir økt tilgjengelighet for smart vedlikehold og produksjonsoptimaliseringer. Disse fjerntilgangene må sikres med gode tiltak for å hindre at trusselaktører får tilgang til sårbar operasjonsteknologi i kritisk infrastruktur i samtlige sektorer nasjonalt. I praksis er grensene mellom tradisjonell IT og operasjonell teknologi i ferd med å viskes ut ved at det eksponeres større digitale flater til operasjonell teknologi. Økning i anvendelse av fjernaksess samt tilgjengeliggjøring av sanntidsdata fra operasjonell teknologi til IT medfører økt risiko. Dette øker angrepsflatene mot operasjonell teknologi, som ikke har samme modenhet i beskyttelse som IT.

Spesielt utsatt er sårbarhetsflater som kritisk infrastruktur har mot internetteksponerte tjenester. Disse eksponerte flatene er det avgjørende å sikre. I ytterste konsekvens kan virksomheten utsettes for spionasje, sabotasje eller rettsstridig overtakelse som kan forstyrre for eksempel energiforsyningen av gass til Europa eller kraftforsyningen nasjonalt.

Virksomheter må øke motstandsdyktigheten og ta i bruk robusthet i hele livssyklusen til digitale systemer som er anvendt i kritisk infrastruktur i Norge. Dette betyr blant annet å sørge for at OT-systemer ikke blir stående sårbare over tid, men er oppdatert på lik linje med IT-systemer.

Nulldagssårbarheter

Nulldagssårbarheter er sårbarheter i programvare som noen får kunnskap om før produsenten, leverandøren eller brukerne av programvaren. Begrepet nulldagssårbarhet spiller på at man har 0 dager til å forberede seg på utnyttelse av sårbarheten.



Gassco

Operasjonell teknologi (OT)

Operasjonell teknologi og industrielle kontrollsystemer anvendes i flere sektorer. Der styrer eller overvåker slike systemer viktige fysiske prosesser eller funksjoner i verdikjeden. Disse systemene har både ulik størrelse og kompleksitet alt etter hvilke fysiske prosesser de overvåker og styrer. Slike systemer finnes blant annet innen petroleum, kraft og energi, luftfart, sjøfart, samferdsel eller annen infrastruktur.

Cyberoperasjoner mot kritisk infrastruktur

Ukraina har blitt utsatt for cyberoperasjoner rettet mot kritisk infrastruktur gjentatte ganger. Operasjoner mot energisystemer har ved flere anledninger ført til strømutfall i store områder. I desember 2023 år ble Ukrainas største telekom-operatør Kyivstar utsatt for en omfattende cyberoperasjon. IT-infrastruktur ble stengt ned og millioner av brukere mistet mobil- og internettdekning. Flyalarmer som varsler befolkningen om missil- og droneangrep, ble også rammet. Angrepet omtales som den største cyberoperasjonen mot Ukraina siden Russland startet en fullskala angrepskrig i februar 2022.

Tidligere hendelser som løsepengeangrepet mot Colonial Pipeline i USA i 2021 medførte betydelige samfunnskonsekvenser, da distribusjon av drivstoff stanset opp. Tilsvarende fikk SolarWinds-angrepet i 2020 nasjonale konsekvenser da norske kraftselskaper ble berørt.

Alle disse hendelsene viser kompleksiteten i systemer og nettverk i kritisk infrastruktur, og hvor store samfunnskonsekvenser cyberoperasjoner kan medføre.

I førsteutgaven av denne rapporten sto det at et cyberangrep mot Ukraina i februar 2023 førte til strømutfall i store områder. Dette medfører ikke riktighet, og er rettet i denne versjonen.

Kostnaden av å bli rammet av cyberoperasjoner

Selv om cyberoperasjoner er noe som foregår i det digitale domenet, så er kostnadene og konsekvensene høyst håndgripelige. Cyberoperasjoner og kriminell aktivitet i cyberdomenet kan forårsake nedetid, produksjonsstopp og tap av kundedata, patenter og omdømme. Andre uventede skader kan bli svært omfattende. Dette kan føre til store økonomiske tap eller konkurs for den rammede virksomheten.

Globalt er det anslått at cyberkriminalitet i 2024 vil ha en prislapp på 100.000 milliarder kroner, eller tilsvarende litt over seks oljefond, ifølge den globale statistikkplattformen Statista. Det innebærer mer enn en dobling siden 2020, og det er ventet at kostnadene vil øke ytterligere de nærmeste årene.

Kostnaden av cyberoperasjoner eller cyberkriminalitet mot enkeltbedrifter avhenger blant annet av angrepets alvorlighet og virksomhetens verdier og omsetning. Sekundæreffekter kan være vel så vanskelige å forutse. Eksempelvis kan lekkasje av persondata føre til GDPR-bøter på tosifrede millionbeløp. Mange uønskede digitale hendelser, både cyberoperasjoner og kriminell aktivitet, rammer små bedrifter. De er ofte mer sårbare og minst rustet til å håndtere konsekvensene av et angrep. Gjenopprettelsestiden kan derfor være lang. Selv om bedriftene er små, kan de være viktige leverandører og underleverandører til virksomheter som råder over kritisk infrastruktur og understøtter grunnleggende nasjonale funksjoner. Nettopp derfor er det så viktig at den nasjonale motstandskraften i cyberdomenet involverer både store og små virksomheter på tvers av sektorer og i hele landet.

Hva koster cyberoperasjoner bedriften din?

De færreste ofrene av cyberoperasjoner eller kriminell aktivitet i cyberdomenet oppgir i ettertid hva det har kostet. Noen norske tilfeller er imidlertid offentlig kjent, og kan gi en indikasjon.

Rammede bedrifter (i norske kroner):
Tomra i 2023: 200 millioner
Knut Malmberg AS (rørlegger) i 2023: 10 millioner
Nortura i 2021: 36 millioner
Amedia i 2021: anslagsvis 30 millioner
Hydro i 2019: 800 millioner

NorSIS blir en del av NSM

Fra 2024 er Norsk senter for informasjonssikring (NorSIS) en del av NSM. Overdragelsen er en viktig milepæl i NorSIS' innsats for å bidra til en sikker digital hverdag for befolkningen og små- og mellomstore bedrifter i Norge. NorSIS har lenge arbeidet dedikert med å styrke digital kompetanse gjennom veiledning, opplæring og nettverksbygging, og drifter blant annet tjenesten slettmeg.no.

Kunstig intelligens i påvirkningsoperasjoner

Selv om kunstig intelligens (KI) ikke er noe nytt, har det vært en eksplosiv utvikling innen generativ kunstig intelligens som ChatGPT og andre grunnmodeller det siste året. Grunnmodeller omfatter blant annet store språkmodeller (LLM) som eksempelvis ChatGPT baserer seg på, men også modellene som brukes til å generere *deepfakes* som lyd eller bilde.

Kunstig intelligens har gitt trusselaktører nye muligheter til å påvirke nyhetsbildet og meninger verden over. KI-genererte og naturtro video, bilder, lyd og tekst kan brukes til å påvirke, forvirre og destabilisere samfunn som en del av påvirkningsoperasjoner. Samtidig er slike påvirkningsoperasjoner vanskelig å oppdage og forhindre i et åpent demokrati som Norge, hvor det er ønskelig og positivt med meningsmangfold i det offentlige ordskiftet.

Hensikten med påvirkningsoperasjoner er ikke nødvendigvis å spre et spesifikt budskap, men heller å bidra til mistillit til media, undergraving av demokratiske prosesser og polarisering av samfunnet.

Forebyggende tiltak er blant de viktigste virkemidlene mot denne typen påvirkningsoperasjoner. Blant annet er en kildekritisk og opplyst befolkning og redaktørstyrte medier viktige for den nasjonale motstandskraften mot påvirkningsoperasjoner. Bruk av troverdige kilder for å verifisere informasjon er viktig før informasjonen deles og spres videre via sosiale medier.

Bruk av kunstig intelligens kan øke cyberaktørers kapasitet, slik at de kan ramme flere mål med færre ressurser. Svært sofistikerte *spearphishing*-operasjoner kan for eksempel gjennomføres i større skala enn tidligere. Masseutsendelser av skadevare har hittil vært forbeholdt *phishing*-kampanjer som har vært relativt enkle å gjennomskue. Masseutsendelser av *spearphishing*-kampanjer kan derimot øke faren for at verdier knyttet til nasjonale sikkerhetsinteresser rammes.

Årets ord

Språkrådet kåret *KI-generert* til årets ord i 2023.

Kåringen begrunnes med at kunstig intelligens er blitt allemannseie, og at det har gitt mange nye sammensatte ord med forkortelsen KI.

Adjektivet *KI-generert* er en av de mest brukte sammensetningene og betyr «laget med kunstig intelligens».

Risiko 2024 omtaler blant annet KI-teknologi, KI-modeller, KI-løsning – og ikke minst KI-generert.

Kilde: språkrådet.no

NSM/Ilja Hendel

Spamouflage-nettverk

Tenketanken Australian Strategic Policy Institute (ASPI) avslørte i oktober 2023 et koordinert nettverk av ca. 2000 falske sosiale medier-profiler som publiserte falsk informasjon om den canadiske statsministeren Justin Trudeau og over 50 andre politikere i Canada. Over 15.000 innlegg ble publisert på X (tidligere Twitter), Facebook og YouTube. Politikerne ble fremstilt som løgnere og korrupte, de ble beskyldt for å ha utenomekteskapelige forhold og å neglisjere familiene sine, og det ble fremsatt falske påstander om deres barns seksuelle legning.

Når fabrikkerte nyheter og sosiale medier-innlegg blir kamuflert som ekte nyheter og spres raskt på internett, ofte ved hjelp av falske profiler og bots, er det viktig at flest mulig mottagere kan bruke sunn skepsis og god kildekritikk.

Løgnerens utbytte

De som sprer fabrikkerte nyheter og *deepfakes*, bidrar til et informasjonsmiljø hvor alt *kan* være falskt, og derfor er det ingenting som *må* være ekte. Ubeleilige fakta kan dermed avfeies som usannheter. Et slikt informasjonsmiljø gjør det enklere for uredelige aktører å unngå kritikk og ansvarliggjøring for hendelser eller påstander som faktisk er sanne. Dette kalles *løgnerens utbytte*.

Løgnerens utbytte tjener særlig de som driver uærlig spill og vil unnslippe kritikk for uetisk eller ulovlig virksomhet, enten det dreier seg om korrupsjon, valgfusk, menneskerettighetsbrudd eller folkerettsstridige krigshandlinger.

Begrepet løgnerens utbytte ble først tatt i bruk av jusprofessorene Chesney og Citron (2019).

Kunstig intelligens og cybersikkerhet

Én av fordelene med kunstig intelligens er at den i mange tilfeller klarer å oppdage sammenhenger i data som mennesker ellers ikke klarer å oppdage. Kunstig intelligens har imidlertid begrensninger, som å forstå kontekst. KI-teknologi er heller ikke løsningen på alle problemer, men komplementerer andre verktøy og kan blant annet være et nyttig hjelpemiddel for cyberanalytikere.

Skal din virksomhet gå til innkjøp av KI-programvare for oppgaver i cybersikkerhet, må du kjenne til begrensningene for hva kunstig intelligens kan gjøre, tenke nøye gjennom hva slags problem du ønsker å løse og vite at KI-løsningen du får faktisk løser problemet. Det er også vesentlig at KI-løsningen ikke får tilgang til sensitive opplysninger som deretter tilflyter andre, for eksempel ved at opplysningene inngår i leverandørens videre trening. Når viktig arbeid overlates til kunstig intelligens, kan det bidra til uklarhet omkring ansvarsforhold og hvem som garanterer for sikkerhet og trygghet.

Bakdører og ondsinnet påvirkning

Kunstig intelligens i seg selv har blitt et nytt mål for cyberoperasjoner som utnytter helt nye typer sårbarheter.

Eksempelvis kan en tredjepart tjenesteleverandør plante en kryptografisk bakdør i modellen den er satt til å trene på vegne av en kunde. Bakdøren vil være umulig å oppdage i etterkant og kan bare utnyttes av den som kjenner til den hemmelige nøkkelen. En bakdør kan plasseres inn gjennom manipulasjon av programvaren som utfører treningen, eller direkte med hensikt av leverandøren selv. Bakdører kan også oppstå gjennom forgiftning av treningsdata, altså at noen med vilje prøver å villede kunstig intelligens-modellen ved å fôre den feil data. Målet med en bakdør kan være å påvirke modellen til å endre adferd i bestemte situasjoner, som å utføre en uønsket handling, eller lekke sensitiv informasjon den er trent på.

Virksomheter må være varsomme ved kjøp av treningssett fra en tredjepart, da manipulasjon med treningssettet kan få målrettede effekter i modellen. Virksomheter bør også tenke nøye gjennom om modellen er trent med sensitiv data, før de deler tilgang til modellen med andre.

Kunstig intelligens som en sårbarhet i seg selv

Teknologiselskapet Samsung la ned midlertidig forbud mot å bruke generative KI-modeller som ChatGPT for sine ansatte våren 2023. Bakgrunnen var frykt for at sensitiv informasjon skulle komme på avveie. Ansatte hadde brukt ChatGPT for å utbedre egne kildekoder og til å lage en intern presentasjon som inneholdt sensitive markedsdata. Kildekodene og markedsdataen ble dermed tilgjengeliggjort for OpenAI, selskapet bak ChatGPT, og potensielt for andre sluttbrukere av tjenesten.

Nytt i 2024

NIS-direktivet blir innført

NIS-direktivet gjennomføres i norsk rett gjennom ny lov om digital sikkerhet (digitalsikkerhetsloven).

NIS stiller krav til forebyggende digital sikkerhet hos virksomheter som leverer samfunnsviktige eller digitale tjenester innen en rekke ulike sektorer. Virksomhetene blir også pålagt en varslingsplikt ved alvorlige hendelser som rammer deres nettverk eller informasjonssystemer, og som er egnet til å forstyrre leveransen av en samfunnsviktig tjeneste.

Digitalsikkerhetsloven stiller grunnleggende krav om forsvarlig sikkerhet i nettverk og informasjonssystemer som ligger til grunn for leveransen av en samfunnsviktig tjeneste. Sikkerhetstiltakene skal være risikobaserte, som igjen forutsetter at virksomheten utarbeider risikovurderinger av nettverk og informasjonssystemer. Virksomheter som er underlagt sikkerhetsloven, er allerede underlagt krav til forsvarlig sikkerhet.

Forprosjekt for nasjonal skytjeneste

Sentrale IKT-tjenester bør være under tilstrekkelig nasjonal kontroll. Norske virksomheter bør blant annet vurdere bruk av datasentre i Norge, og i hvilken grad alle lag i en tjeneste kan, bør eller må driftes utelukkende av personell i Norge. Alle virksomheter bør inkludere beredskap som en faktor, og ha et langsiktig perspektiv for å sikre robuste tjenester.

NSM har gjennomført en konseptvalgutredning for en nasjonal skytjeneste på oppdrag fra Justis- og beredskapsdepartementet. Basert på NSMs anbefalinger, har regjeringen besluttet å forbedre regelverket for skytjenester, og å realisere et såkalt kombinasjonskonsept med en lukket skytjeneste basert på kommersielle leverandører.

NSM har fått i oppdrag å iverksette et forprosjekt for å videreføre arbeidet med en nasjonal skytjeneste.

Grunnprinsipper for IKT-sikkerhet kommer på engelsk

Grunnprinsippene kan brukes til å løfte sikkerhetsnivået i virksomheten generelt og sikkerhetskompetansen hos den enkelte spesielt. Prinsippene gir råd for å beskytte informasjonssystemer, data og tjenester mot uautorisert tilgang, skade eller misbruk. Prinsippene er relevante for alle norske virksomheter, både offentlig og privat, og bør benyttes av virksomheter med ansvar for samfunnskritiske funksjoner.

I løpet av 2024 kommer grunnprinsippene for IKT-sikkerhet på engelsk.

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 varselet.

NSM/Ilja Hendel

Design:Tank

NASJONAL
SIKKERHETSMYNDIGHET

Postboks 814,
1306 Sandvika
Tlf. 67 86 40 00

24/00150
nsm.no/risiko2024
www.nsm.no