NASJONAL
SIKKERHETSMYNDIGHET

RISIKO 2021

– helhetlig sikring mot sammensatte trusler

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

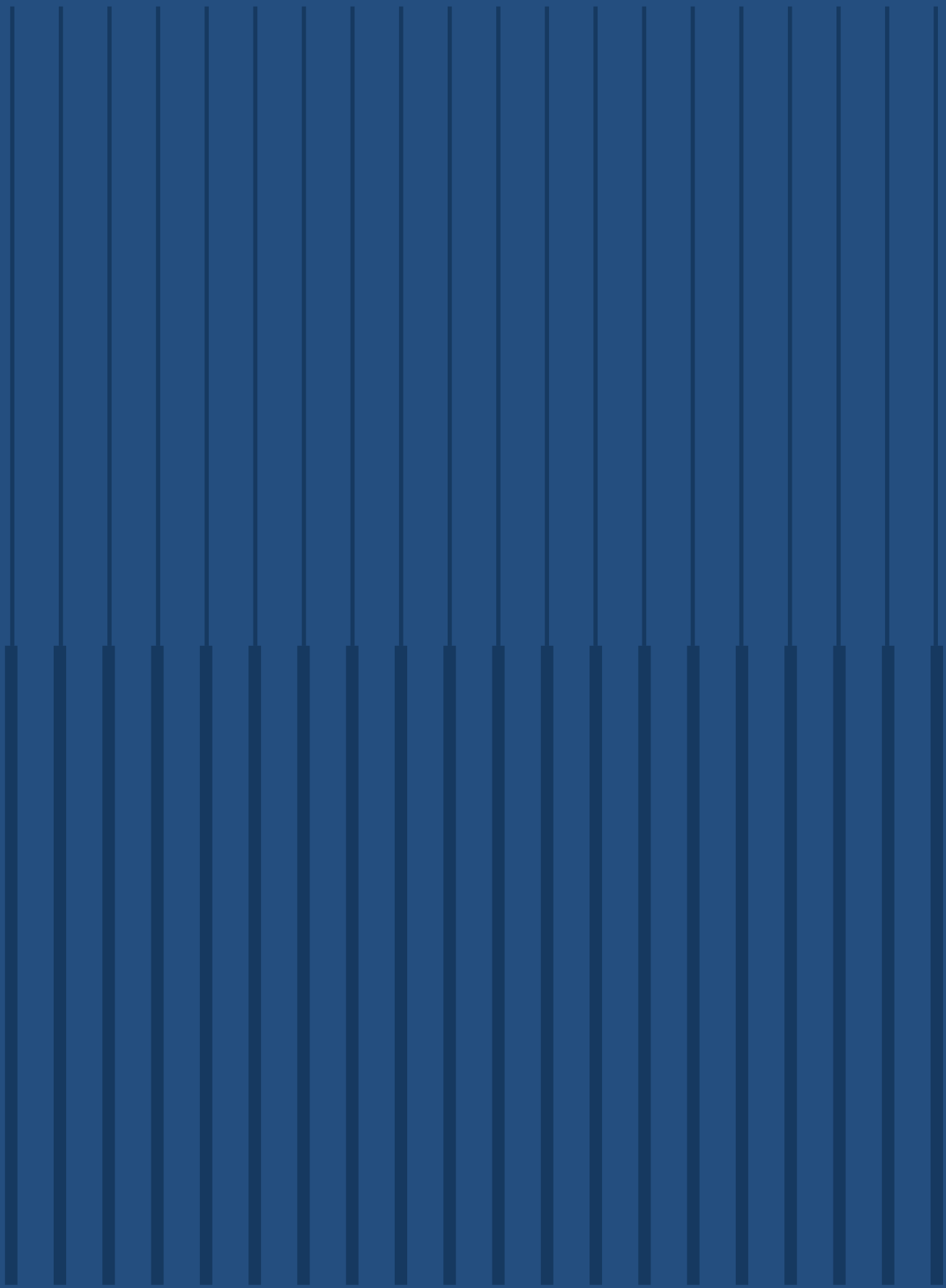
Nasjonal sikkerhetsmyndighet (NSM) er Norges fagmyndighet for forebyggende nasjonal sikkerhet. Direktoratet gir råd om og gjennomfører tilsyn og andre kontrollaktiviteter knyttet til sikring av informasjon, systemer, objekter og infrastruktur av nasjonal betydning. NSM har også et nasjonalt ansvar for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

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

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

Innhold

RISIKO 2021 | **Design:** HyperRedink **Trykk og distribusjon:** RK grafisk



Forord

Det siste året har vi levd med tiltak som har kostet oss mye som enkeltindivider, virksomheter og samfunn. Ingen har vært uberørt av covid-19-pandemien, og for noen har kostnadene vært ekstra store. Når vi nå forhåpentligvis begynner å se enden på pandemien, kan vi si at de fleste tiltakene har virket. Også i et sikkerhetsperspektiv.

Mange næringer er hardt rammet, og det er for tidlig å konkludere om de langsiktige økonomiske konsekvensene. Så langt ser det ut til at verdikjedene som understøtter viktige samfunnsfunksjoner og nasjonal sikkerhet, har blitt påvirket i mindre grad enn fryktet. Dette skyldes blant annet omstillingsevnen både myndighetene og næringslivet har vist det siste året. Pandemien har også illustrert viktigheten av samvirke mellom myndigheter og virksomheter i en krise. Slik sett har den lært oss mye om nasjonal krisehåndteringsevne og samtidig tydeliggjort noen sårbarheter.

Et viktig moment i så måte er betydningen av et godt samarbeid med internasjonale samarbeidspartnere og ikke minst hvor avhengige vi er av å kunne ha tillit til viktige leverandører. Mange verdi- og leverandørkjeder strekker seg utover landets grenser, og dersom en tilspisset sikkerhetspolitisk krise skulle inntreffe, må vi kunne stole på at leveransene ikke stopper. Derfor er det viktig at vi både som myndigheter og virksomheter kartlegger og tar innover oss egne avhengigheter. En avhengighet er en potensiell sårbarhet.

I løpet av det siste året har vi også opplevd flere cyberangrep. Et av disse rammet det norske demokratiets høyborg. Angrepet på Stortingets e-post-systemer minner oss om alvorligheten i det komplekse risikobildet vi står overfor. Håndteringen av hendelsen og norske myndigheters offentlige attribusjon av trusselaktøren viser imidlertid også at vi har fått på plass en sterk, nasjonal håndteringsevne på det digitale området. Siden den nasjonale CERT-funksjonens spede begynnelse for rundt 20 år siden har det blitt lagt stein på stein i dette arbeidet. I dag står Nasjonalt cybersikkerhetssenter (NCSC) og Felles cyberkoordineringssenter (FCKS) i spissen for en bred nasjonal innsats.

Prinsippene som NCSC og FCKS er tuftet på – samvirke, varsling og informasjonsdeling – er sentrale ikke bare innenfor det digitale domenet, men også for å håndtere sammensatte trusler i stort. En moderne og utvidet sikkerhetslov er et meget viktig verktøy for å redusere risiko for sikkerhetstruende virksomhet. Når departementene nå operasjonaliserer sikkerhetsloven innenfor sine ansvarsområder, står samvirkeprinsippet helt sentralt for å binde sammen sikkerhetsarbeidet mellom sektorene, det offentlige og private og sivil og militær side. Slik kan vi skape helhetlig sikring mot sammensatte trusler.

Foto: Cicilie S. Andersen

Kjetil Nilsen
Direktør NSM

Om rapporten

Risiko 2021 beskriver sårbarheter i virksomheter og på nasjonalt plan, hvordan trusselaktørene kan utnytte dem og hvilken risiko dette medfører. Rapporten omtaler også hvordan virksomhetene og myndighetene bør redusere sårbarheter for å gjøre trusselaktørenes jobb vanskeligere.

Risiko 2021 henvender seg til ledere og personell med sikkerhetsoppgaver i alle sektorer. Målet med rapporten er å gi virksomhetene bedre forutsetninger for å sette sikkerhetsarbeidet i en bredere kontekst. Dette er spesielt viktig for virksomheter underlagt sikkerhetsloven, men også for andre virksomheter.

Risikobildet

Norge står overfor et komplekst risikobilde der fremmede stater og andre aktører ved hjelp av et bredt utvalg virkemidler forsøker å utnytte sårbarheter i funksjoner, virksomheter og systemer.

NSM vurderer de viktigste utviklingstrekkene i risikobildet å være følgende:

1. Det digitale risikobildet er skjerpet
2. Tydeligere risiko knyttet til sammensatte trusler
3. Covid-19-pandemien har forsterket det eksisterende risikobildet

Disse tre faktorene henger nært sammen og reflekterer endringer i både sårbarhets- og trusselbildet og utviklingen i verdier av nasjonal betydning. Rask digitalisering endrer og skaper nye samfunnsverdier. De lange, digitale verdikjedene som dannes for å understøtte tjenester og funksjoner i samfunnet, medfører samtidig nye sårbarheter og avhengigheter trusselaktører kan utnytte. Dette resulterer i et skjerpet digitalt risikobilde.

Sammensatte trusler har det siste tiåret gjort skillet mellom stats- og samfunnssikkerhet mer utydelig. Globalt har vi sett flere eksempler på maktbruk og påvirkning som bidrar til å tydeliggjøre risikoen innenfor dette området. I denne sammenheng blir blant annet investeringer fra fremmede stater benyttet som et virkemiddel for å oppnå strategiske målsettinger. Summen av disse sårbarhetene og endringene gir et mer komplekst risikobilde i møte med sammensatte trusler i konstant utvikling.

Covid-19-pandemien har bidratt til å forsterke dette risikobildet. Pandemien har medført raskere digitaliseringstakt på flere områder. Den har skapt ny dynamikk i verdensøkonomien, som har gitt rom for strategiske investeringer, og brakt med seg en global *infodemi*[1,2] som gjør det ekstra krevende å skille faktiske opplysninger fra desinformasjon og påvirkningskampanjer.

Skjerpet digitalt risikobilde

Det digitale situasjonsbildet i 2020 var preget av et høyere aktivitetsnivå mot norske virksomheter og institusjoner sammenlignet med tidligere år. Vi ser ingen tegn til at dette avtar. Fremmede stater og kriminelle aktørers kapasitet til å gjennomføre nettverksoperasjoner med alvorlige konsekvenser for Norge er høy, og NSM vurderer det digitale risikobildet som skjerpet sammenliknet med i fjor.

Digitaliseringen er en viktig driver i samfunnsutviklingen og bidrar til vår velferd, trygghet og verdiskaping. Den teknologiske utviklingen fører imidlertid til at sårbarhetsflaten øker. Et dynamisk og komplekst sårbarhetsbilde gjør det utfordrende å tilpasse sikkerhetstiltakene raskt nok. Store samfunnsverdier legges over i det digitale domenet, og ny teknologi og bruksmønstre skaper nye muligheter i det digitale rom som trusselaktører vil utnytte.

Store samfunnsverdier legges over i det digitale domenet, og ny teknologi og bruksmønstre skaper nye muligheter i det digitale rom som trusselaktører vil utnytte.

Leverandørkjedeangrep mot SolarWinds

I desember i fjor ble det kjent at et sofistikert og svært omfattende dataangrep hadde rammet den amerikanske programvareleverandøren SolarWinds og deres kunder. Det som gjør angrepet spesielt, er at trusselaktøren har klart å etablere en «bakdør» i programvaren SolarWinds Orion, som så har blitt med i programvareoppdateringer som SolarWinds selv har tilgjengeliggjort for sine kunder. Dermed har over 18.000 virksomheter installert en offisiell og tilsynelatende sikker oppdatering fra selskapet, men med en sårbarhet som kun trusselaktøren visste om. Programvaren benyttes til styring av informasjons-systemer og er svært utbredt i hele verden.

Angrepet omtales som et leverandørkjedeangrep, fordi trusselaktøren har lyktes i å ramme ikke bare SolarWinds selv, men selskapets store kundebase. Konsekvensene er derfor omfattende og potensielt svært alvorlige. Det er bekreftet at blant andre amerikanske myndighetsorganer og store teknologiselskaper er rammet. Her hjemme vet vi at flere virksomheter har installert en ondsinnet versjon av SolarWinds Orion. NSM har så langt ikke sett aktiv utnyttelse av bakdøren hos norske virksomheter, men understreker at arbeidet med å kartlegge omfanget av kampanjen i Norge fortsetter.

Stadig nye digitale og internettilkoblede produkter, såkalte IoT[3]-enheter, tas i bruk i den enkeltes hverdag og virksomheters nettverk. Felles for slike enheter er at de gjør hverdagen enklere og mer effektiv. Et aspekt ved IoT-enheter er imidlertid at de ofte har ulike former for sensorer som samler inn data. Slike sensorer kan brukes for å effektivisere og forbedre funksjoner og tjenester for samfunnet, eksempelvis i smartby-prosjekter. Samtidig kan de medføre konsekvenser vi ikke er bevisst, noe som gjør det vanskelig å identifisere tiltak. Dersom en trusselaktør får tilgang til store mengder data fra slike sensorer, herunder mobile sensorer, kan det utnyttes som en svært effektiv etterretningsmetode.

Skytjenester og datasentre bidrar til å effektivisere og gir for mange virksomheter bedre sikkerhet enn man er i stand til å oppnå gjennom egne driftsmiljøer. De fleste virksomheter er avhengige av digitale komponenter eller tjenester som ofte leveres fra eller har forgreininger til utlandet. Lange, digitale verdikjeder kan gjøre både hver enkelt virksomhet og viktige samfunnsfunksjoner sårbare.

SolarWinds-saken, som ble kjent i desember 2020, viser hvilke ringvirkninger sårbarheter i ett innslagspunkt kan ha. En rekke virksomheter verden over er rammet av hendelsen, der en trusselaktør har installert bakdører i en svært utbredt programvare (SolarWinds Orion) og deretter klart å utnytte disse. Så langt

har vi ikke sett tegn til utnyttelse av sårbarheten hos norske virksomheter.

NSM ser at digitale operasjoner blir mer sofistikerte og komplekse. Som følge av dette blir hendelseshåndtering i økende grad tid- og ressurskrevende. I løpet av 2020 har NSM NCSC bistått i håndteringen av flere større hendelser, deriblant datainnbruddet på Stortinget. Hendelsene spenner bredt både i omfang, alvorlighetsgrad og mål.

Kartlegging, informasjonsinnhenting, datainnbrudd og andre digitale operasjoner utføres av både statlige og kriminelle trusselaktører mot norske virksomheter. NSM vurderer fortsatt at virksomheter innen offentlig forvaltning, forsvars-, petroleums-, ekom[4]- og kraftsektoren er risikoutsatt. Det samme gjelder for romvirksomhet og maritim produksjon og teknologi. Det siste året har også risikoen økt for samferdsel, forskning og høyere utdanning og helse. Risikonivået forventes å vedvare i 2021.

Tydeligere risiko knyttet til sammensatte trusler

Sammensatt virkemiddelbruk benyttes for å fremme et lands interesser på bekostning av et annet lands interesser. Hensikten er å utnytte sårbarheter for å styrke egen posisjon eller svekke motparten. Etterretningstjenesten og PST beskriver i sine åpne vurderinger et sammensatt trusselbilde som rammer på tvers av sektorer og dermed utfordrer sikkerhetsarbeidet både nasjonalt, i sektorene og i den enkelte virksomhet.

Fordi truslene rammer på tvers av sektorer, nivåer og domener, utfordres den nasjonale evnen til å vedlikeholde et samordnet nasjonalt situasjonsbilde som fanger opp og setter hendelser i sammenheng. Det er også krevende å utvikle gode tiltak mot sammensatte trusler fordi de utnytter sårbarheter som følger med de mest fundamentale

Østre Toten kommune rammet av løsepengevirus

I januar ble Østre Toten kommune rammet av et løsepengevirus kjent som «PYSA». Dataangrepet satte flere av kommunens systemer ut av drift og gjorde ulike tjenester hos kommunen utilgjengelige. Følgelig måtte kommunen planlegge analoge løsninger for drift, og mange oppgaver måtte håndteres manuelt.

Det aktuelle løsepengeviruset er kjent brukt i lignende angrep mot lokale myndigheter i Frankrike samt i andre hendelser. NSM ser en generell økning i denne typen økonomisk motivert kriminalitet og har tidligere gitt råd om hvordan virksomheter kan beskytte seg mot løsepengevirus. Disse gjelder fortsatt.[5]

Avanserte trusselaktører har omfattende ressurser til rådighet, og dersom målet er viktig nok, vil de lete til de finner veien inn.

verdiene i et liberalt demokrati. Vårt åpne og tillitsbaserte samfunn er dermed sårbart for sammensatte trusler.

Et aktuelt eksempel på dette er norsk forskning og høyteknologi, som er ettertraktet innenfor flere fagområder. På den ene siden er det behov for åpenhet, kompetanse fra utlandet og internasjonalt samarbeid, mens det på den andre siden er risiko for at verdifull informasjon havner i fremmed etterretnings hender. Enkelte typer informasjon kan i verste fall misbrukes til våpenutvikling eller på annen måte ha negative konsekvenser for Norges eller alliertes sikkerhet. Forskningsmiljøenes egenart med hensyn til tett samarbeid på tvers av landegrenser og sektorer gjør verdivurderingen av informasjon vanskelig, særlig når det gjelder hva som anses å være kunnskap som bør beskyttes av hensyn til nasjonal sikkerhet.

Et annet eksempel på denne balansegangen er ønsket om utenlandske investeringer i Norge sett opp mot risikoen for strategiske investeringer som truer nasjonale sikkerhetsinteresser. Det er flere tilfeller både internasjonalt og i Norge der selskaper med ulik grad av tilknytning til stater med kjent etterretningsinteresse kjøper opp, investerer i eller på annen måte involverer seg i virksomheter, eiendom og infrastruktur. Formålene med slik aktivitet kan være mange – skaffe sensitiv informasjon og teknologi, påvirke beslutningsprosesser eller få innpass i markeder som ellers ikke er tilgjengelige for den aktuelle staten. Målet kan også være å kunne kontrollere viktige samfunnsfunksjoner. Det er krevende å skille slike strategiske investeringer med illegitime hensikter fra ordinær investeringsaktivitet foretatt ut fra rene kommersielle hensyn.

Flere og mer alvorlige digitale angrep mot norske virksomheter det siste året, som angrepet mot Stortinget (se side 12), innebærer risiko for at trusselaktører får tak i informasjon som potensielt kan brukes i fremtidige påvirkningsoperasjoner eller utpressingsforsøk. Avanserte trusselaktører har omfattende ressurser til rådighet, og dersom målet er viktig nok, vil de lete til de finner veien inn. Samtidig ser vi at det ofte er kjente sårbarheter som utnyttes, noe som understreker betydningen av å være på tå hev i sikkerhetsarbeidet. Utover de direkte konsekvensene av en hendelse krever håndteringen store ressurser av virksomhetene som rammes og myndighetene som bidrar. Det medfører at andre hendelser kanskje ikke avdekkes eller må nedprioriteres, i tillegg til at annen aktivitet og produksjon blir skadelidende.

I kjølvannet av covid-19-pandemien har det fulgt omfattende desinformasjon og påvirkningsoperasjoner fra enkelte stater. Heller ikke vi i Norge er immune mot slik påvirkning, og det kan være krevende både for den enkelte og for myndighetene å oppdage illegitim påvirkningsaktivitet

i et uoversiktlig mediebilde som i økende grad preges av ikke-redaksjonelle medier. 2021 er et valgår, og i Fokus 2021 skriver Etterretningstjenesten at stortings- og sametingsvalget «er et nærliggende tilfelle der Norge kan bli utsatt for forsøk på påvirkning», med henvisning til valgpåvirkning i andre land.

Det siste året har også økt sikkerhetspolitisk spenningsnivå i nordområdene bidratt til å forsterke risikobildet, og Norge sitter i perioden 2021–22 i FNs sikkerhetsråd. Dette innebærer at norsk forsvars-, utenriks- og sikkerhetspolitikk samt forhold rundt nordområdeforvaltningen i enda større grad vil være av interesse for fremmede stater. Totalt sett betyr det at risikobildet knyttet til sammensatte trusler har blitt enda mer komplekst og omfattende.

Covid-19-pandemien har forsterket eksisterende risikobilde

Covid-19-pandemien har forsterket det eksisterende risikobildet. Dette knytter seg til flere forhold. Det er økt press mot enkelte sektorer og samfunnsfunksjoner (for eksempel helse og ekom). Risiko for uønskede strategiske investeringer har økt, og covid-19 benyttes i global påvirkning og desinformasjon. Det har også oppstått nye personellmessige og IKT-sårbarheter som følge av endrede arbeidsmønstre og raskere digitalisering. Deler av helsesektoren har fått høyere verdi som følge av sin avgjørende rolle i håndteringen av covid-19-pandemien.

De økonomiske ringvirkningene av covid-19-pandemien endrer dynamikken i globale og nasjonale markeder og fører til at mange bransjer sliter og virksomheter står i fare for å gå konkurs. Gjeldtyngede og konkurstruede virksomheter av betydning for viktig infrastruktur og forsyningssikkerhet, eksempelvis kraftselskaper, teleselskaper, havner og flyplasser, kan fremstå som tilgjengelige og attraktive investeringsobjekter for trusselaktører med et langsiktig ønske om kontroll over viktig infrastruktur.

Personlige forhold som dårligere økonomi, dødsfall i nær familie og

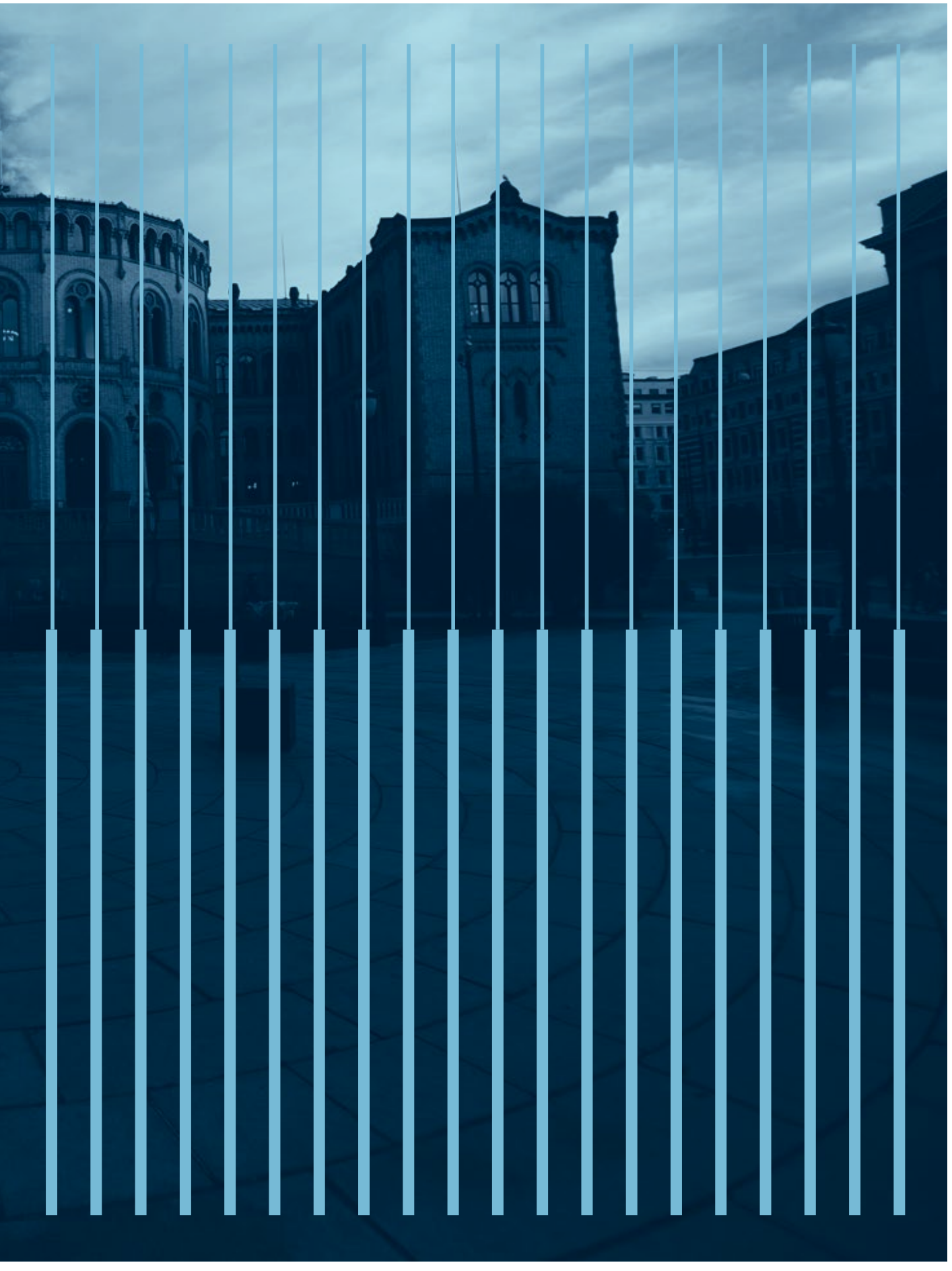
Datainnbruddet på Stortinget og konsekvensene av et cyberangrep

I fjor høst ble det kjent at Stortinget var rammet av et alvorlig datainnbrudd, som del av en omfattende nettverkskampanje som rammet virksomheter i flere land. Hendelsen er spesiell fordi det er den første gangen norske myndigheter offentlig har attribuert et slikt angrep til et annet land. PSTs etterforskning konkluderte med at det var sannsynlig at den russiske, militære etterretningstjenesten GRU stod bak.

Metoden trusselaktøren brukte, såkalt brute-force-angrep, innebærer automatisert gjetting av passord på et stort antall e-post-kontoer. Forsøkene fortsetter til de lykkes eller til de blir avvist av sikkerhetsløsninger. Det er dermed stor sannsynlighet for at slike angrep blir avdekket, og de kan karakteriseres som støyende og lite sofistikerte.

Konsekvensene av et cyberangrep kan være mange. Den direkte konsekvensen kan være at aktøren får tilgang til sensitiv informasjon, som både kan ha etterretningsverdi i seg selv og videre benyttes i påvirkningsforsøk. I tillegg kan aktøren i enkelte tilfeller oppnå tilgang til systemer som kan utnyttes i et mer langsiktig perspektiv.

Samtidig binder slike hendelser opp store ressurser og kapasitet hos virksomhetene som rammes, og hos myndighetene som er involvert i håndteringen. Cyberangrep kan også bidra til å undergrave befolkningens tillit til myndighetenes evne til å sikre viktige institusjoner og samfunnsfunksjoner. Som ledd i sammensatt virkemiddelbruk er dermed cyberangrep en metode som innebærer lav risiko for aktøren og potensielt høy effekt på flere måter.



Covid-19-pandemien har gjort sårbarhetsbildet tydeligere med hensyn til norske virksomheters avhengigheter og leverandørkjeder.

generell usikkerhet i samfunnet øker risiko for at personell gjør bevisste eller ubevisste valg til fordel for trusselaktører. Ved permitteringer og oppsigelser er det risiko for at personell som har vært sikkerhetsklarert eller autorisert for tilgang til skjermingsverdige verdier, utsettes for tilnærming fra utenlandske etterretningstjenester. Slike sårbarheter øker sjansene for at fremmed etterretning kan lykkes med sin tilnærming. Covid-19-pandemien har også gjort sårbarhetsbildet tydeligere med hensyn til norske virksomheters avhengigheter og leverandørkjeder. Når virksomheter som har roller i nasjonal beredskap og krisehåndtering er avhengige av sårbare leverandørkjeder som strekker seg ut av landet, har det betydning for Norges krisehåndteringsevne. Informasjon om Norges krisehåndteringsevne er lettere tilgjengelig nå under pandemien enn i en normalsituasjon. PST skriver i sin ugraderte trusselvurdering at fremmede etterretningstjenester kan bruke slik informasjon til å svekke norsk beredskap i en fremtidig konfliktsituasjon.

Covid-19-pandemien har akselerert den raske digitale transformasjonen, der tjenester gjøres tilgjengelig på nett. Mange virksomheter har på kort tid utvidet sin bruk av skytjenester, hjemmekontor- og fjerntilgangsløsninger for å holde produktiviteten oppe. Det er krevende å opprettholde sikkerhetsnivået når utviklingen går så raskt, med et dynamisk og uoversiktlig sårbarhetsbilde. Trusselaktører tilpasser seg endrede situasjoner raskt og utnytter sårbarheter som oppstår. Raske endringer medfører behov for økt årvåkenhet og bevisstgjøring rundt IKT-sikkerhet. I tillegg til de tekniske løsningene har pandemien ført til endret mønster i samhandling, noe som har gitt rom for sosial manipulasjon. Ulike aktører utnytter blant annet covid-19-tematikk i svindelforsøk og digitale operasjoner, som for eksempel i phishing-kampanjer mot norske virksomheter. NSM forventer at trenden med phishing-forsøk hvor vaksine blir brukt som tema, vil fortsette.

Verdier av betydning for risikobildet

Det skapes stadig nye verdier av betydning for samfunnet, blant annet i form av nye digitale tjenester og funksjoner. Verdibildet er i konstant utvikling, på samme måte som trussel- og sårbarhetsbildet. Det siste året er en god illustrasjon på dynamikken i verdibildet, der både virksomheter og myndigheter har måttet omstille drift, produksjon og digitale løsninger for å opprettholde sine leveranser og tjenester.

Når vi i dag snakker om verdier av betydning for nasjonal sikkerhet og det nasjonale risikobildet, finnes disse på tvers av sektorene og i form av samfunnsfunksjoner, virksomheter, infrastrukturer og systemer. Noen av disse er identifisert som grunnleggende nasjonale funksjoner og skjermingsverdige verdier etter sikkerhetsloven fordi de anses å ha en så viktig funksjon for nasjonal sikkerhet at de krever ekstra beskyttelse.

Det nasjonale risikobildet favner imidlertid videre enn virksomhetene som omfattes av sikkerhetsloven og de verdiene som er utpekt som skjermingsverdige. Trusselaktørenes mål følger ikke nødvendigvis vår nasjonale verdivurdering. Verdier som i et slikt bredere risikoperspektiv kan ha betydning for nasjonale sikkerhetsinteresser, må også beskyttes.

Som følge av digitalisering og større avhengigheter på tvers av samfunnsfunksjoner, samt utvikling i trusselaktørenes metoder for å påvirke disse

verdiene, er det tradisjonelle skillet mellom stats- og samfunnssikkerhet i dag mindre tydelig. For å fange opp de store samfunnsmessige og teknologiske endringene de siste to tiårene, samt i større grad kunne demme opp for sammensatte trusler, ble virkeområdet utvidet da en modernisert sikkerhetslov trådte i kraft i 2019.[6]

Implementering av sikkerhetsloven fortsetter

Implementering av sikkerhetsloven er en nasjonal verdikartlegging. Det er gjort et betydelig arbeid med departementenes identifisering av grunnleggende nasjonale funksjoner, men arbeidet er en kontinuerlig prosess fordi samfunnsutviklingen og andre endringer i risikobildet kan føre til behov

Det nasjonale risikobildet favner videre enn virksomhetene som omfattes av sikkerhetsloven og verdier som er utpekt som skjermingsverdige.

for justeringer. Inntil sikkerhetsloven er fullt implementert og operasjonalisert, er forutsetningene for å oppnå forsvarlig sikkerhetsnivå mangelfulle. Det er derfor viktig at arbeidet med å identifisere grunnleggende nasjonale funksjoner og kartlegge avhengigheter gis tilstrekkelig prioritet, slik at verdier med betydning for nasjonale sikkerhetsinteresser kan sikres.

Det er til enhver tid viktig at de riktige objektene, infrastrukturene og informasjonssystemene blir utpekt og korrekt klassifisert. Mangelfull eller uriktig identifisering av verdier vil føre til feilprioritering med hensyn til hva som skal skjermes og beskyttes. Dette åpner for feilaktig prioritering av ressurser og kapasiteter innen sikkerhetstiltak for norske virksomheter.

I løpet av 2021 skal de fleste virksomheter underlagt sikkerhetsloven ha gjort vurderinger knyttet til avhengigheter og rapportert disse inn til NSM. Dette gir verdifull innsikt i hvilke avhengighetskoblinger som potensielt er sårbare, og gir innspill til hvordan departementene og virksomhetene bør prioritere arbeid med forebyggende sikkerhet.

For å redusere sårbarhetene avhengighetene skaper, **forutsetter NSM at virksomhetene kartlegger og vurderer hvilke avhengigheter de har til andre virksomheter og tjenester. Virksomheter underlagt sikkerhetsloven plikter å rapportere om egne avhengigheter til NSM.** For å bistå virksomhetene i dette arbeidet har NSM utarbeidet *Håndbok i kartlegging og vurdering av avhengigheter*, som ble publisert ved årsskiftet.

Lov om nasjonal sikkerhet baserer seg på risikovurderinger for å identifisere sikkerhetstiltak og er således mer kompetansekrevende enn den forrige sikkerhetsloven. Dette medfører et større behov for å sette virksomhetene underlagt sikkerhetsloven i stand til å gjennomføre sikkerhetsstyring

Hva betyr forsvarlig sikkerhetsnivå?

Sikkerhetsloven gir fleksibilitet i hvordan virksomheter kan oppnå et forsvarlig sikkerhetsnivå. Helhetlig og balansert sikring innebærer en kombinasjon av sikkerhetstiltak innen ulike disipliner (menneskelige, elektroniske, fysiske og organisatoriske). Virksomhetens vurdering av risiko i henhold til sikkerhetsloven danner grunnlaget for å fastsette sikkerhetstiltak.

Forsvarlig sikkerhetsnivå oppnås når risikovurderingen ikke lenger viser uakseptabel negativ effekt for en eller flere grunnleggende nasjonale funksjoner. Uakseptabel negativ effekt avhenger av hvilken grunnleggende nasjonal funksjon det gjelder og den sikkerhetstruende virksomheten den kan være utsatt for, samt virksomhetens rolle i opprettholdelsen av funksjonen.

Økt fleksibilitet innebærer at det stilles høyere krav til sikkerhetsfaglig kompetanse i virksomhetene.

generelt og risikovurdering spesielt. Dersom virksomhetene mangler relevant kompetanse om forebyggende sikkerhet, utgjør det en sårbarhet. Hvilke fagområder innen forebyggende sikkerhet virksomheten faktisk trenger kompetanse på, avhenger av virksomhetens natur og hvilke verdier den forvalter.

Sikkerhetsloven stiller krav til at virksomhetene skal oppnå forsvarlig sikkerhet. Virksomheten må selv, på bakgrunn av en risikovurdering, vurdere hvilke tiltak som er hensiktsmessige, nødvendige og relevante for å oppnå lovens krav om forsvarlig sikkerhetsnivå. I risikovurderingen skal det tas hensyn til hvilken sikkerhetstruende virksomhet den skjermingsverdige informasjonen, informasjonssystemene, objektene og infrastrukturen kan bli utsatt for og sannsynligheten for slik aktivitet.

For å motvirke sammensatte trusler og sørge for helhetlig sikring av skjermingsverdige verdier må:

- **departementene fortsette arbeidet med å identifisere virksomheter som er av vesentlig betydning for de grunnleggende nasjonale funksjonene, og de virksomhetene som er av avgjørende betydning skal underlegges sikkerhetsloven**
- **virksomhetene underlagt sikkerhetsloven følge opp lovens krav til risikovurderinger og etablering av forsvarlig sikkerhetsnivå.**

Hva er grunnleggende nasjonale funksjoner (GNF)?

Grunnleggende nasjonale funksjoner (GNF) er definert som «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.

GNF er funksjoner som, hvis de faller helt eller delvis bort, har betydning for statens evne til å ivareta landets suverenitet, territorielle integritet, demokratiske styreform og overordnede sikkerhetspolitiske interesser.

Gjennom å identifisere GNF defineres deler av sikkerhetslovens virkeområde. Departementenes identifisering av disse funksjonene er en forutsetning for å finne frem til objekter, infrastruktur og andre verdier av betydning for statens evne til å ivareta nasjonale sikkerhetsinteresser.[7]

For mer informasjon, se NSMs temaside om GNF på nsm.no.[8]

Nasjonale sårbarheter på strategisk nivå

Situasjonsbildet for sammensatte trusler

Samtidige og komplekse hendelser i ulike domener og på tvers av sektorene setter det nasjonale sikkerhetsarbeidet på prøve. Hendelser binder opp kapasitet og ressurser, noe som kan bety at andre hendelser ikke avdekkes eller må nedprioriteres. NSM har tidligere belyst at underrapportering av sikkerhetstruende virksomhet utgjør en sårbarhet.[9] Slike varsler er et viktig informasjonsgrunnlag for det nasjonale situasjonsbildet for sammensatte trusler.

Lange verdikjeder og økende avhengigheter har ført til flere potensielle sårbarheter og et større mulighetsrom for bruk av sammensatte virkemidler. Gråsoner innen ulike områder (for eksempel diplomatiske, militære, økonomiske, etterretningsmessige og juridiske) kan utnyttes slik at de forsterker den samlede effekten på verdien som trusselaktøren søker å påvirke. Eksempelvis kan virkemidler som utnytter økonomiske, juridiske og kommersielle gråsoner kombineres for å oppnå strategiske mål, slik det beskrives på side 21.

Påvirkningsoperasjoner gjennom medier benyttes av trusselaktører for blant annet å skape splid og redusere borgeres tillit til egne myndigheter. Utfordringen med slik aktivitet ligger i hvordan vi forebygger, oppdager og håndterer subversiv og fordekt påvirkning i form av mediekampanjer og desinformasjon mot utvalgte personer og målgrupper.

Som et åpent samfunn er vi sårbare. Den informasjonen vi ser i det offentlige rom, sosiale medier eller på nyhetssider kan lett bli endret av forfalsking, halvsannheter og lignende, og det kan være vanskelig å ivareta tilstrekkelig kildekritikk. Risikoen for misbruk av åpen informasjon vil være vanskelig å redusere tilstrekkelig uten å svekke våre demokratiske verdier. Det er derfor viktig å ivareta og bygge oppunder den åpne samfunnsdebatten.

Det kan være vanskelig for befolkningen å skille mellom saker som er oppkonstruert av fremmede stater eller fremstilles på en tendensiøs måte, og faktiske opplysninger. Det hviler derfor et stort ansvar på redaksjonelle medier for å fremstille saker balansert og være tydelige på bruk av kilder og kildehenvisninger.

For å kunne identifisere sammensatte trusler og iverksette nødvendige mottiltak er det sentralt at norske myndigheter etablerer og opprettholder et samordnet nasjonalt situasjonsbilde. Et slikt bilde bør blant annet baseres på varsling, rapportering og samvirke mellom myndigheter og virksomheter. I dette arbeidet må også media og andre relevante sivile aktører involveres.

Sikkerheten ved stortings- og sametingsvalget 2021

Norge har et velfungerende og stabilt demokratisk system og et samfunn preget av åpenhet. Det bidrar til robusthet og et godt utgangspunkt for å stå imot forsøk på slik påvirkning av innenrikspolitiske prosesser. Samtidig må vi være forberedt på påvirkningsforsøk fra fremmede stater.

Russland har tidligere gjennomført påvirkningsoperasjoner både mot europeiske og amerikanske valg. Så langt synes det ikke å være registrert samme aktivitet ved det amerikanske presidentvalget i 2020. Det er likevel grunn til å forvente forsøk på slik påvirkning også i tiden fremover.

Gjennomføringen av valg, fra valgkampstart til det endelige resultatet offentliggjøres, kan berøres av de samme sårbarhetene som andre digitale prosesser, selv om valgprosessen ikke bare er digital. Nettverksoperasjoner kan være rettet mot selve gjennomføringen av valg, men aktiviteten kan også styres av mer langsiktige mål. Nettverks- og påvirkningsoperasjoner kan også brukes i kombinasjon med hverandre.

Stortinget ble rammet av en omfattende nettverkskampanje høsten 2020, hvor trusselaktøren lyktes i å hente ut informasjon fra brukere. I andre land har det vært tilfeller hvor stjålet sensitiv informasjon senere har blitt misbrukt i påvirkningsoperasjoner og press mot enkeltpersoner.

For å øke robustheten til den digitale valggjennomføringen bistår NSM med testing og kvalitetssikring av valgsystemer, deriblant tilpassede løsninger tiltenkt brukt ved stemmegivning hjemmefra ved karantene eller isolat som følge av covid-19-sykdom. Resultatene vil rapporteres til Valgdirektoratet, som har gode rutiner for å utbedre eventuelle sårbarheter i forkant av valget.

NSM, Etterretningstjenesten og PST har i fellesskap utarbeidet sikkerhetsråd og veiledning til partiene som stiller til valg. Formålet er å øke listekandidatenes bevissthet om uønsket påvirkning og å gjøre kandidatene bedre rustet til å motstå denne type påvirkning. NSM, Etterretningstjenesten, PST og Kripos samarbeider tett for å sikre felles situasjonsforståelse og koordinerer tiltak for å sikre valggjennomføringen.

Det kan være vanskelig å skille strategiske oppkjøp med illegitime hensikter fra ordinær porteføljeforvaltning foretatt ut fra rene kommersielle hensikter.

Strategiske investeringer fra fremmede stater

Investeringer fra utenlandske foretak bidrar til verdiskaping i Norge og er helt nødvendig for mange virksomheter og arbeidsplasser. Imidlertid kan strategiske investeringer fra land vi ikke har et sikkerhetsmessig samarbeid med, som Russland og Kina, få negative konsekvenser for nasjonale sikkerhetsinteresser. Dette kan for eksempel være tilfelle dersom det dreier seg om kjøp av eiendom eller investeringer i virksomheter som utvikler teknologi, bygger ut infrastruktur eller forvalter naturressurser.

Strategiske investeringer brukes som metode for blant annet å skaffe innpass i prosesser og beslutninger og tilgang til sensitiv informasjon, teknologi og kompetanse. Denne typen aktivitet kan gi legitim tilgang til informasjon og teknologi som kan benyttes for illegitime formål. Slike investeringer kan også bidra til å posisjonere egne selskaper i et strategisk viktig marked.

Etterretningstjenesten beskriver eksempelvis i årets og tidligere Fokus-rapporter hvordan denne typen aktivitet er en sentral del av Kinas silkevei-initiativ, for å styrke landets globale posisjon. Silkevei-konseptet omfatter kommunikasjons-, samferdsels- og energiinfrastrukturutbygging, og utlånsvirksomhet og investeringer, både til og fra Kina. Infrastrukturutbygging og investeringer forventes å være gunstige for Kinas økonomi, og prosjektene skaper en avhengighet til Beijing som kan gjøre mottaker-landene mer mottakelige for politisk press. 5G-nettverk, fiberkabler og smartby-systemer kan styrke Kinas etterretningskapasitet og mulighet for målrettet og kraftfull påvirkning.

Strategiske investeringer og oppkjøp kan skje gjennom stråselskaper og komplekse selskapsstrukturer og kan dermed være vanskelig å avdekke. Det kan være vanskelig å skille strategiske oppkjøp med illegitime hensikter fra ordinær porteføljeforvaltning foretatt ut fra rene kommersielle hensyn.

For virksomheter som omfattes av sikkerhetsloven, kan slike utfordringer håndteres gjennom bestemmelsene om eierskapskontroll i sikkerhetsloven. Bestemmelsene gir regjeringen mulighet til å stanse eller sette vilkår for erverv av virksomheter som er underlagt loven, dersom ervervet «kan medføre ikke ubetydelig risiko for at nasjonale sikkerhetsinteresser blir truet».[10]

Strategiske investeringer og oppkjøp vil imidlertid kunne representere en betydelig nasjonal risiko selv om investeringene som gjøres og virksomhetene som kjøpes opp, ikke er omfattet av sikkerhetsloven. Det er utfordrende for myndighetene å holde oversikt og oppdage aktiviteten i tide i slike tilfeller, og denne utfordringen skjerpes ved at leverandørkjeder blir lengre og mer uoversiktlige.

EOS-tjenestene jobber i nært fellesskap

for å avdekke og anbefale tiltak mot uønskede strategiske investeringer. **Evnen til å avdekke og varsle om sikkerhetstruende virksomhet må styrkes i alle sektorer, og det må etableres mekanismer for analyse, informasjonsutveksling og samhandling. Dette vil bidra til at kunnskap og erfaringer fra alle sektorer benyttes til å identifisere forebyggende tiltak. NSM vil fortsette arbeidet med å gi informasjon, råd og veiledning for å sette sektormyndigheter i stand til å utøve sitt ansvar.**

Sårbare verdikjeder og avhengigheter på tvers av landegrenser

Flere grunnleggende nasjonale funksjoner ivaretas av virksomheter som har lange, uoversiktlige verdikjeder og dermed en rekke avhengigheter på tvers av sektorer og landegrenser. Mangelfull oversikt over verdikjeder og avhengigheter mellom virksomheter og tjenester på tvers av sektorene utgjør en nasjonal sårbarhet i denne sammenheng.

Avhengigheter til underleverandører utgjør en sårbarhet for norske virksomheter fordi den selv ikke har kontroll over tjenester eller leveranser som er nødvendige for virksomhetens funksjon. Slike avhengigheter kan for eksempel være strøm, kjøling, bredbånd eller skytjenester. Dersom underleverandøren blir rammet av en hendelse og leveransen reduseres eller bortfaller, kan dette få direkte konsekvenser for virksomheten.

Dersom virksomheten er av vesentlig eller avgjørende betydning for en grunnleggende nasjonal funksjon, kan bortfallet eller redusert funksjonalitet få konsekvenser for nasjonale sikkerhetsinteresser. Grunnleggende nasjonale funksjoner kan dermed arve sårbarheter i leverandørkjedene til norske virksomheter. Leverandørkjeder som involverer virksomheter med tilknytning til land vi ikke har sikkerhetsmessig samarbeid med, gjør det utfordrende å følge opp sikkerhetsrelevante forhold.

Trusselaktører kan for eksempel utnytte programvare- og tjenesteleverandører for å få innpass i systemene til selskapets kunder. Leverandørkjedeangrep, hvor aktøren rammer en tredjepart eller tilgrensende virksomhet, forekommer også i Norge. NSM observerer at virksomheter lengre nede i verdikjedene rammes av sikkerhetstruende virksomhet, enten som mål i seg selv eller som ledd i å

Man kan stille spørsmål ved skytjenestenes sikkerhet i en tilspisset sikkerhetspolitisk situasjon.

nå mål høyere opp i verdikjedene. Angrep som rammer leverandørkjeder, er en økende risiko.

Det er viktig at virksomheter kartlegger virksomhetens plass i verdikjeden(e) og vurderer egne avhengigheter jevnlig. Virksomheter som er av avgjørende betydning for grunnleggende nasjonale funksjoner, bør ta høyde for en eventuell tilspisset sikkerhetspolitisk situasjon i sine risikovurderinger. Uten et godt oversiktsbilde blir det vanskelig å vurdere hvordan sårbarheter i andre deler av verdikjeden kan påvirke sikkerhetstilstanden i egen virksomhet. **Dette gjelder også for Forsvarets avhengighet av sivile virksomheter.**

Nasjonal digital infrastruktur

Digitaliseringen går raskt, og sikkerhet må være del av planleggingen før ny funksjonalitet skal implementeres. En utfordring på nasjonalt nivå er at utviklingen av dagens digitale løsninger har skjedd gradvis, og uten en tydelig overordnet strategi for hvordan tjenestene skal ivareta nasjonale behov, herunder i krise og krig. Et overordnet mål bør være at fremtidens teknologi bidrar til effektivisering i samfunnet samtidig som sikkerheten ivaretas. Sikkerhetsløsninger for fremtidens nasjonale digitale tjenester må planlegges nå.

Skyteknologi er et eksempel på viktig ny teknologi som har stort potensial for å effektivisere og rasjonalisere virksomhetenes IKT-portefølje, og som er tatt i bruk i svært mange virksomheter de seneste årene. Skytjenesteleverandørene leverer ofte mer innovative og sikrere løsninger enn det enkelte virksomheter selv har kapasitet og kompetanse til.

Imidlertid kan man stille spørsmål ved tjenestenes sikkerhet i en tilspisset sikkerhetspolitisk situasjon. De store skytjenesteleverandørene er hovedsakelig lokalisert i utlandet og baserer seg til dels på digital infrastruktur som krysser mange landegrenser og som er sårbar for sabotasje, ødeleggelse og sikkerhetspolitiske endringer. Disse leverandørene er også kommersielle aktører som vil kunne ha andre prioriteringer enn å opprettholde viktige norske samfunnsfunksjoner. Det bør derfor gjennomføres grundige verdi- og risikovurderinger når det vurderes bruk av skytjenester for viktige samfunnsfunksjoner.

NSM har gjennom FoU-aktivitet de siste årene sett på hvordan nye teknologier skaper muligheter for IKT-modernisering og digital transformasjon samtidig som sikkerheten ivaretas. Virtualisering, skyteknologi (cloud native) og 5G er fremvoksende teknologier som vil bli sentrale i svært mange av samfunnets IKT-utviklingsprosjekter i årene fremover, men også disse teknologiene vil kreve helhetlige sikkerhetsløsninger.

Samlet sett har teknologiene potensial til å gi oss moderne IKT-plattformer med nødvendig geografisk dekning, mobilitet, interoperabilitet, robusthet og smidighet.

Sikkerhetsløsninger for fremtidens nasjonale digitale tjenester må planlegges nå.

Plattformene vil kunne understøtte lokal tilgjengelighet og autonomi, og slik bidra til at Norge har nødvendig datakraft for viktige samfunnsfunksjoner når krisen inntreffer. Rammene for hvordan vi nasjonalt tar i bruk denne teknologien legges nå, og vil gi føringer for hvordan vi kan utnytte mulighetene de gir oss i fremtiden.

Myndighetene bør derfor søke å identifisere strukturelle, langsiktige grep som sørger for at innføring av ny teknologi og funksjonalitet hever sikkerheten for viktige samfunnsfunksjoner. Et eksempel på et slikt grep er et overordnet digitalt målbilde for viktige samfunnsfunksjoner. Arbeidet med målbildet bør ta utgangspunkt i internasjonale standarder og andre nasjoners (USA, EU) relevante rammeverk og arkitekturer på området. For å oppnå nødvendig interoperabilitet og gjenbruk på tvers bør disse IT-plattformene ha en *felles digital grunnmur* basert på felles grunnleggende arkitekturprinsipper.

NSM ANBEFALER:
1. Etablering av et nasjonalt, digitalt målbilde: En overordnet beskrivelse på myndighetsnivå av hvordan vi ønsker å bruke teknologiene i fremtiden.

Det er behov for i større grad å løfte utvikling av IKT-tjenester og IKT-basert samhandling ut av den enkelte etat og virksomhet for å sikre helhetlig satsing og gevinstrealisering på tvers. Et fremtidsrettet nasjonalt digitalt målbilde på strategisk nivå bør tydeliggjøre hvordan vi sikrer at virksomheter og etater har tilgang til nødvendige applikasjoner og tjenester både når og hvor de trenger dem. Det bør være et sentralt mål at en applikasjon/tjeneste som er utviklet av en virksomhet kan gjenbrukes av andre der behovene er sammenfallende. Tjenestene må være interoperable og fleksible slik at de fortløpende kan tilpasses gjeldende behov og legge til rette for samvirke på tvers av virksomheter og sektorer. Hensikten er å fokusere og harmonisere innsatsen på utvalgte viktige områder, for eksempel samlet bruk av virtualisering, cloud native, 5G, IoT og lignende.

- Et relevant eksempel på interoperabilitet og samvirke er nødetatenes bruk av operative IKT-tjenester: Den lokale branntjenesten som er først fremme på skadestedet kan dele sensorinformasjon og video direkte til AMK (akuttmedisinsk kommunikasjonssentral), som dermed får nødvendig grunnlag for å prioritere bruk av kritiske ressurser – eksempelvis sende ut nødvendig personell og materiell.

Et nasjonalt målbilde vil kunne detaljeres og operasjonaliseres ytterligere i virksomhetenes egne og mer detaljerte målbilder.

NSM mener også det er behov for en «nasjonal transportplan» for IKT. På samme måte som veiinfrastruktur

NSMs grunnleggende arkitekturprinsipper

Det er behov for et *overordnet digitalt målbilde* for IT-plattformene til virksomheter som understøtter viktige samfunnsfunksjoner. For å oppnå nødvendig interoperabilitet og gjenbruk på tvers bør disse IT-plattformene ha en felles digital grunnmur basert på felles grunnleggende arkitekturprinsipper. NSMs grunnleggende arkitekturprinsipper for IT-plattformer til viktige samfunnsfunksjoner gir et bidrag til dette målbildet:

1. Plattformene er **virtualiserte og skybaserte** *(cloud native)*.
2. Plattformene støtter **smidig utvikling**, **DevOps** og **XaaS/XaC**.
3. Plattformene er **åpne** og **standardbaserte**, inkludert **5G-baserte** der det er relevant.
4. Plattformene er **leverandørnøytrale** og har **høy tjenestemobilitet**.
5. Plattformene støtter ***enterprise*-skala**-virtualisering og cloud native (ende-til-ende).
6. Plattformene støtter ende-til-ende ***multi-tenancy*** (flerbruk).
7. Plattformene har nødvendig **mobilitet, lokal tilgjengelighet** og **autonomi**.

Spredningen av data og kunnskap kan ha en utilsiktet sikkerhetspolitisk konsekvens for Norge og vårt kunnskapsforsprang om Arktis.

planlegges sentralt og ikke av den enkelte virksomhet, bør også IKT-systemer på overordnet nivå planlegges sentralt.

2. Norge trenger en felles digital grunnmur. Den digitale grunnmuren skal skape et felles teknisk fundament som sikrer at vi oppnår målbildet.

Et felles teknisk fundament bør blant annet baseres på åpne standarder, interoperabilitet og samhandling. Kritiske ressurser og applikasjoner kan ikke være låst til proprietære produkter, leverandører eller skyer, de må til enhver tid være tilgjengelige ved at de fleksibelt kan flyttes mellom ulike tjenestetilbydere.

- Eksempel: Brannmannen har tilgang til de sentrale skytjenestene ute på skadestedet via 5G-nettet. Tjenestene er interoperable med de andre nødetatene slik at brannmannen kan samvirke med AMK-operatøren på redningssentralen.

Den digitale grunnmuren bygges stein for stein ved at alle følger de samme arkitekturprinsippene (se også side 25).

Ved å etablere et sett med felles grunnleggende arkitekturprinsipper vil man kunne bidra til at virksomheter som understøtter viktige samfunnsfunksjoner arbeider mot det samme overordnede digitale målbildet og får etablert et universelt og åpent kjøremiljø for tjeneste-applikasjoner, økt variantbegrensning og lokal datakraft.

NSM anbefaler at myndighetene intensiverer arbeidet med å etablere nasjonale og internasjonale digitale løsninger som gir nødvendig sikkerhet i fremtiden. Alle samfunnets funksjoner er avhengig av dette.

Nordområdene – økt betydning og økt risiko

Strategisk posisjonering i forhold til ressurser og kontroll over nordområdene fører til økt militær og sivil aktivitet. Dette innebærer blant annet omfattende forskningsaktivitet som er nødvendig for videre utvikling og ivaretakelse av nordområdene, men som kan medføre utfordringer for ivaretakelse av nasjonale sikkerhetsinteresser.

I dag ser vi en økende interesse i nordområdene fra flere hold. Norge som nøkkelland i Arktis, med grense til Russland og som alliert til USA, er derfor en viktig deltaker i utviklingen og opprettholdelsen av det sikkerhetspolitiske bildet i nord.

Internasjonalt forskningssamarbeid er avgjørende for å forstå klimakrisen samt dynamiske og sårbare økosystemer i nord. Omfattende internasjonal polarforskning i nordområdene har gjort regionen mindre eksklusiv.[11] Data og kunnskap fra regionen om blant annet dybder og bunnforhold, oseanografi, vær- og isforhold samt kunnskap om naturelementer som påvirker militære operasjoner i Arktis, blir i økende grad delt mellom institusjoner verden over. Spredningen av slik data og

kunnskap kan imidlertid ha en utilsiktet sikkerhetspolitisk konsekvens for Norge og vårt kunnskapsforsprang om Arktis. I tillegg vil tilstedeværelse av andre lands forskningsmiljøer i Arktis gi dem en mulighet til å hevde sine interesser, på bekostning av norske interesser.

Flere aktører vier også forskningsprosjekter til å finne hull og problematisere norsk lovgivning i nordområdene. Dette kan ha konsekvenser for norsk nordområdeforvaltning.

Mindre havis kombinert med høyere råvarepriser og ny teknologi har medført økt skipsfart i Arktis. Betraktninger rundt en mulig fremtidig kamp om uregulerte ressurser i nordområdene får internasjonal oppmerksomhet. Nordområdene prioriteres høyt av blant andre Russland, Kina og USA, og regionen forventes å bli viktigere i økonomisk sammenheng grunnet ressursforekomster og transport. Utfordringer knyttet til økt internasjonal interesse og innflytelse i nordområdene kan bidra til at situasjonen i våre nærområder blir mer uforutsigbar og at Norges eksklusive rett til naturressursene utenfor Svalbard blir utfordret.

Samtidig øker den militære betydningen i nordområdene. En del av usikkerheten i regionen er knyttet til Kinas vekst og intensjoner i nord. Kina gjennomfører samordnede øvelser med Russland, noe som er med på å øke kinesisk evne til å operere i Arktis.

Regjeringen la frem den nye nordområdemeldingen i november 2020. Den gir en oppdatert analyse av den utenriks- og sikkerhetspolitiske situasjonen i nordområdene.[12]

Et samordnet nasjonalt situasjonsbilde innenfor sammensatte trusler, som omtales på side 19, omfatter også både militær og ikke-militær aktivitet i nordområdene.

Sårbarheter i virksomheter og samfunnsfunksjoner

Skytjenester og datasentre

Bruk av skytjenester[13] er utbredt blant norske virksomheter og har kommet for å bli. Når gamle og utdaterte IKT-systemer skal byttes ut, tas skytjenester stadig oftere i bruk. I fremtiden vil det også være flere IKT-tjenester som kun vil bli levert som en skybasert tjeneste. Overgangen til og bruken av skytjenester kan imidlertid medføre nye sårbarheter som vi enda ikke har full oversikt over. Lengre og mer uoversiktlige verdikjeder, sammenkobling av «gammel» og «ny» teknologi og avhengigheter til utlandet fører til et mer uoversiktlig risikobilde. I tillegg innebærer det en risiko for at store mengder data og tjenester konsentreres på ett sted.

Skytjenester innebærer i praksis lengre og mer komplekse verdikjeder. Store internasjonale skytjenesteleverandører har datasentre i flere ulike land og er som regel avhengige av en rekke underleverandører. En underskog av skybaserte tjenester vokser frem, og disse er ofte leverandørspesifikke. Dette innebærer at virksomheten kan bli «låst» og må fortsette å bruke den spesifikke leverandøren. Alt dette er med på å skape et uoversiktlig bilde av avhengigheter og verdikjeder for virksomheten selv.

Kompleksiteten kan også øke hvis virksomheten bruker og integrerer tjenester fra ulike skytjenesteleverandører kombinert med noe «lokalt» fra eget datasenter. Eldre IKT-tjenester, som ikke er laget for skyløsninger, kan medføre økt sårbarhet når de kobles til skyen. Rask utvikling av skytjenester og datasentre utfordrer evnen til å skape helhetlige digitale sikkerhetsløsninger. NSM erfarer at flertallet av uønskede hendelser relatert til skytjenester skyldes feilkonfigurasjon eller feil bruk av skytjenesten. Skytjenester må derfor brukes riktig, noe som krever kompetanse og ressurser.

Ved å tjenesteutsette IKT-systemer som bærer viktige samfunnsfunksjoner, eksempelvis i form av skytjenester, kan vi komme til å svekke vår nasjonale beredskapsevne. Virksomheter som benytter skytjenesteleverandører med datasentre i utlandet, får dermed de fysiske installasjonene underlagt et annet lands jurisdiksjon. I tillegg vil kommunikasjonen til og fra datasentre kunne gå gjennom ett eller flere transittland. Ved eskalering i krisespennet kan det tenkes scenarioer hvor skytjeneleverandøren blir nødt til å omprioritere ressurser i henhold til vertslandets egne beslutninger, herunder nedprioritering av support og lagrings-/prosesserings-/nettverkskapasitet. Dette er realiteter som virksomheten må ta hensyn til i sin egen beredskapsplanlegging, og som er viktig i arbeidet med vår samlede nasjonale beredskap.[14]

Skytjenester vil være vesentlig for realisering av fremtidens teknologi og vil utgjøre sentrale byggeklosser for morgendagens digitaliserte samfunn.

Det er helt avgjørende at virksomheter

er bevisst risikoen ved bruk av skytjenester og konsekvensene ved et eventuelt bortfall, både for egen del og i et samfunnssikkerhetsperspektiv. Summen av norske virksomheters «skyavhengighet» utgjør en betydelig del av den samlede risikoen for samfunnet.

NSM mener at det bør prioriteres å etablere nasjonale robuste og redundante datasenter- og skyløsninger som kan tilbys virksomheter som forvalter skjermingsverdige verdier og ivaretar viktige samfunnsfunksjoner.

Virksomheter som har behov for å ta i bruk skyløsninger og tjenester fra datasenter, må sette seg godt inn i hvordan dette påvirker deres digitale sikkerhet og gjøre gode verdi- og risikovurderinger i forkant. NSM har utarbeidet temaheftet *Sikkerhetsfaglige anbefalinger ved tjenesteutsetting* og anbefaler å legge disse rådene til grunn for slike vurderinger.

Brukerkonti, autentisering og passord

Manglende oversikt og kontroll på identiteter og tilganger utgjør en sårbarhet for virksomheter. NSM erfarer at en del virksomheter mangler kontroll på brukerkonti. Det innebærer risiko for at personer som ikke lenger skal ha tilgang til virksomhetens IKT-systemer, kan tilegne seg uautorisert tilgang for å sabotere, modifisere eller hente ut informasjon fra disse IKT-systemene. Problemstillingen omfatter både konti til enheter, systemprosesser og tilganger til IKT-systemer og applikasjoner.

Passordsikkerhet er en vedvarende utfordring, til tross for at stadig flere virksomheter stiller strengere krav til kvaliteten på passord. Sterke passordregimer er viktig, og det er viktigere å lære brukere å sette gode og sterke passord enn å kreve at brukere skifter passord ofte. NSMs erfaringer viser at passord som må byttes ofte, blir svakere fordi brukere lager enklere

Ansvarsdeling ved bruk av skytjenester

Virksomheten har ansvar for sikring av egne verdier, også ved bruk av skytjenester, og vil selv ha et delansvar avhengig av hva slags tjenestemodell som benyttes:

- Software-as-a-service (Saas): Virksomheten har selv ansvar for å sikre data og tilgangsstyring.
- Plattform-as-a-service (PaaS): Virksomheten har selv ansvar for å sikre data, tilgangsstyring og programvare/applikasjoner.
- Infrastructure-as-a-service (IaaS): Virksomheten har selv ansvar for å sikre data, tilgangsstyring, programvare/applikasjoner, operativsystem og nettverkstrafikk.

Enkeltpersoner blir manipulert og utnyttet på en kynisk måte der vedkommendes skjebne har liten betydning målt mot nasjonale etterretningsbehov.

passord eller benytter mønstre som er enkle å huske. Mennesker er vanedyr, og erfaring tilsier at vi gjenbruker passord fordi det gjør det lettere å huske. Et tidligere eksponert passord kan prøves flere steder, og én tapt konto kan fort bli flere. Å gjenbruke passord mellom brukerkonti med ulikt tilgangsnivå eller å gjenbruke passord på private og jobb-relaterte konti, svekker virksomhetens sikkerhet.

NSMs grunnprinsipp for IKT-sikkerhet punkt 2.6.7

Bruk multi-faktor autentisering, som smartkort, sertifikater eller engangspassord, for å autentisere brukere.

Implementer som et minimum multi-faktor på brukerkontoer som har tilgang til kritiske data eller systemer, samt for brukere med driftsoppgaver. Der multi-faktor autentisering ikke støttes, bør brukerkontoer bli pålagt å bruke sterke passord på systemet.

Benytt biometri (for eksempel fingeravtrykk) på klienter som benyttes mye i det offentlige rom (passord-inntasting kan bli observert/filmet). Merk at det kan være personvernutfordringer med hensyn til biometri.

For å redusere sårbarheter knyttet til passord anbefaler NSM virksomheter å ta i bruk multi-faktor pålogging, i tråd med rådene i NSMs grunnprinsipper for IKT-sikkerhet.

NSM anbefaler også at virksomheter har gode rutiner for å fjerne ansattes tilganger til virksomhetens IKT-systemer når arbeidsforholdet avsluttes.

Innsidere

Fremmede stater forsøker å skaffe seg tilgang til informasjon fra norske myndigheter og virksomheter som kan benyttes for å sikre egne interesser. Etterretningstjenesten og PST påpeker at trusselaktører fra fremmede stater søker innpass i næringslivet samt i teknologitunge virksomheter og forskningsmiljøer. Når trusselaktørenes informasjonsbehov ikke dekkes av legitim innhenting, kan de benytte spionasje. Spionasje kan for eksempel gjennomføres ved rekruttering av innsidere. Innsideren kjenner virksomhetens rutiner, prosesser og sårbarheter og kan benytte kunnskapen for å skade virksomheten til fordel for annen virksomhet, stat eller til egen vinning.[15] Skaden en innsider kan påføre verdiene våre, er store.[16] Det er derfor viktig at utsatte miljøer, virksomheter og institusjoner etablerer tiltak for å redusere innsiderrisikoen.

Det kan være flere grunner til at en person begår innsidevirksomhet. Vedkommende kan være motivert av

egne interesser eller bli påvirket av en ekstern aktør som har til hensikt å forlede, rekruttere eller presse. Det forekommer også tilfeller hvor innsideraktivitet begås uten at det ligger en klar motivasjon bak, men hvor personens adferd utsetter virksomhetens verdier for risiko. Når fremmed etterretning står bak, kan enkeltpersoner bli manipulert og utnyttet på en kynisk måte der vedkommendes skjebne har liten betydning målt mot nasjonale etterretningsbehov.

Det er kjent at utenlandske etterretningstjenester retter sin aktivitet blant annet mot norske forskningsmiljøer. Norge har ledende forsknings- og utviklingsmiljøer innen en rekke områder, og både næringsliv og forskere forvalter kunnskap, kompetanse, personell og utstyr som andre stater ønsker å tilegne seg.

Informasjon knyttet til forskning og utvikling kan gi både økonomiske og militære fortrinn,[17] og andre staters militære kapasitet vil kunne styrkes gjennom å skaffe seg norsk flerbruksteknologi og -kompetanse.[18] Forskningsmiljøer og enkeltpersoner med spisskompetanse innen områder av interesse for fremmede stater kan derfor være særlig attraktive etterretningsmål og sårbare overfor innsidere. Likevel kan det kan være vanskelig å oppdage tilfeller der fremmede etterretningstjenester forsøker å utnytte legitimt forskningssamarbeid.

For Norges posisjon innen forskning og utvikling er åpenhet, økt mangfold og samarbeid på tvers av landegrenser helt avgjørende for fremskritt innen denne sektoren. Dette er også viktig for Norge, jf. *Langtidsplan for forskning og høyere utdanning*, og forskere søker samarbeid med de fremste forskningsmiljøene, uavhengig av geografi.[19] [20]

I en situasjon hvor flyt av informasjon er nødvendig for å løse oppgaver, er det ofte utfordrende å se hva som kan deles fritt, og hva som bør beskyttes. Lav bevissthet knyttet til verdiene innen forskning og utvikling utgjør derfor en sårbarhet. Flere forsknings- og utviklingsmiljøer arbeider med både ugradert, sensitiv og sikkerhetsgradert informasjon. Det kan være krevende å navigere i et slikt landskap – noe som

Hva er en innsider?

En innsider forstås som 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 kunnskapen og tilgangen for å utføre handlinger som påfører virksomheten skade eller tap. Innsideaktivitet kan gjennomføres direkte og på egenhånd, eller på vegne av en ekstern aktør. Eksterne aktører kan være statlige, ikke-statlige eller andre enkeltindivider. Disse aktørene kan søke å utnytte personer med tilgang til en virksomhets eller stats verdier for å oppnå egne mål.

Enkeltindivider med vide tilganger i et informasjons-system kan endre og hente ut store mengder informasjon uten at det blir oppdaget.

Eksempel på innsidevirksomhet

Seniorforsker i NASA tilknyttet Kinas Thousand Talents Program

Meyya Meyyappan, senior-forsker hos NASA med mer enn 320 publikasjoner i vitenskapelige tidsskrifter, sa seg i januar i år skyldig i å ha løyet om sin tilknytning til Kina gjennom det kinesiske Thousand Talents Program. Gjennom sin stilling innen «Exploration Technology» og forskningsfelt innen nanoteknologi og romteknologi var Meyyappan underlagt strenge rapporteringsrutiner og restriksjoner omkring samarbeid, eksterne arbeidsoppdrag og det å motta penger eller kompensasjon fra andre. Likevel valgte Meyyappan å la seg rekruttere til Thousand Talents Program og hadde professorat ved universiteter i Kina, Japan og Sør-Korea som han holdt skjult for sin arbeidsgiver. Ved direkte spørsmål om sin tilknytning valgte Meyyappan å lyve om forholdene. Dommen faller i juni 2021.[21] [22]

krever god kompetanse og bevissthet knyttet til hvilke verdier som må beskyttes. Mens forretningshemmeligheter av åpenbar økonomisk betydning og forsvarshemmeligheter tradisjonelt beskyttes godt, er implementering av sikkerhetstiltak ikke kommet like langt innen sektorer som driver forskning og utvikling.

NSM anbefaler at myndigheter og forskningsinstitusjoner samarbeider tettere om bevisstgjøring og kompetanseheving om risiko knyttet til fremmed etterretning i forsknings-, utviklings- og teknologimiljøer. Flere risikoreduserende tiltak bør vurderes.

Digitalisering har medført at sårbarheter knyttet til nøkkelpersonell og annet etterretningsutsatt personell har økt, som følge av at enkeltindivider med vide tilganger i et informasjonssystem kan endre og hente ut store mengder informasjon uten at det blir oppdaget.

Menneskebasert etterretningsaktivitet kjennetegnes ved at den er svært vanskelig å oppdage. Ansatte og nøkkelpersonell i etterretningsutsatte virksomheter kan være sårbare for tilnærming, dersom de ikke er kjent med trusselbildet og at de selv kan være mål for fremmede etterretningstjenester.

NSM anbefaler virksomhetene å ha en systematisk og helhetlig tilnærming til risikoreduserende tiltak

Risikoreduserende tiltak mot innsidevirksomhet

1

Skap et helhetlig system for å styrke personellsikkerheten.

Dette innebærer å vurdere den menneskelige faktoren i alle deler av sikkerhetsarbeidet og innarbeide mulige konsekvenser av innsidevirksomhet i virksomhetens risikovurdering.

2

Ivareta personellsikkerheten før, under og etter ansettelse.

Dette innebærer å sikre at risikoreduserende tiltak iverksettes i alle ledd av ansettelsesprosessen, herunder bruk av bakgrunnssjekk.

3

Sørg for at virksomheten har tilstrekkelig sikkerhetskompetanse og -ressurser.

Dette er nødvendig for å kunne beskytte virksomhetens verdier mot innsidevirksomhet, men også for at virksomheten skal settes i stand til å følge opp sårbarheter som oppstår hos ansatte.

4

Legg til rette for en god sikkerhetskultur.

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

5

Håndter hendelser, evaluer tiltak og lær av erfaringene.

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

For mer informasjon, se NSMs temarapport *Innsiderisiko*.

Eksempel på innsidevirksomhet

Professor dømt for spionasje og tyveri

Hao Zhang, professor ved Tianjin-universitetet i Kina, ble i september 2020 dømt til 18 måneders fengsel for økonomisk spionasje og tyveri fra to amerikanske selskaper til fordel for Kina. Han skal i perioden 2010 til 2015 ha stjålet informasjon om akustiske filtre brukt i mobiltelefoner og annen teknologi. I 2006 tok Zhang sin PhD ved University of South California og startet deretter i firmaet Skyworks (et av de fornærmede selskapene). Zhang ble pågrepet i 2015 da han deltok på en konferanse i USA.[23 24 25 26]

mot innsidevirksomhet. Se i denne sammenheng NSMs grunnprinsipper for personellsikkerhet.

Sikkerhetsbevissthet, forankring og iverksetting av tiltak i virksomheter

Funn fra NSMs tilsyn indikerer at det fremdeles er mange virksomheter der sikkerhetsarbeidet ikke er tilstrekkelig forankret i virksomhetens ledelse. NSM erfarer at mange virksomheter har manglende kompetanse på gjennomføring av risikovurderinger. Manglende kunnskap om risiko bidrar til dårligere sikkerhetsstyring og en svakere sammenheng mellom risikoreduserende tiltak og faktisk risikobilde. Funn fra tilsyn viser at der hvor styringssystemet for sikkerhet har en solid forankring i ledelsen og er godt dokumentert, gir det tydelige positive konsekvenser for sikkerhetsbevisstheten og iverksetting av sikkerhetstiltak i virksomheten.

NSMs kontrollaktivitet i virksomheter underlagt sikkerhetsloven viser noe økt oppmerksomhet om sikkerhetsarbeid knyttet til skjermingsverdige verdier. Likevel gjenstår mye arbeid før sikkerhetsloven fullt ut etterleves i sektorer og virksomheter. Manglene i virksomhetenes sikkerhetsarbeid skyldes blant annet at behovene for beskyttelse av virksomhetenes skjermingsverdige verdier og deres betydning for nasjonal sikkerhet ikke sammenfaller med virksomhetenes dimensjonering av sikkerhetsarbeidet etter egne behov. Mange virksomheter risikovurderer verdier av betydning for sine kjerneoppgaver og ikke i tilstrekkelig grad verdier som har betydning for nasjonal sikkerhet. Konsekvensen er at knappe ressurser blir brukt på forebyggende sikkerhetstiltak som ikke nødvendigvis fungerer etter sin hensikt eller i samspill med hverandre.

En stadig tilbakevendende mangel hos flere er utilstrekkelig håndtering av uønskede hendelser, herunder manglende ekstern varsling blant annet til NSM og andre myndigheter.

NSM erfarer at det er en klar

Det er risiko for at utstyr og produkter produsert i andre land kan kontrolleres, overvåkes eller settes ut av drift av leverandøren...

sammenheng mellom sikkerhets-engasjerte ledere og sikkerhetstilstanden i virksomheten. Det er helt avgjørende for å etablere god sikkerhet at ledere er involvert og tar ansvar for det forebyggende sikkerhetsarbeidet. Der ledelsen er fraværende i sikkerhetsspørsmål, blir avstanden til sikkerhetsarbeidet fort stort, og det blir vanskeligere å få besluttet, gjennomført og evaluert relevante tiltak.

NSM har gjennom tilsyn sett flere eksempler hvor virksomhetene ikke i tilstrekkelig grad har identifisert og fordelt alle nødvendige roller for å ivareta sikkerhetsarbeidet. I flere tilfeller har enkeltpersoner holdt mange roller, og nødvendig kompetanse og rutiner har ikke vært dokumentert i virksomhetenes styringssystem. Dette gjør sikkerhetsarbeidet svært personavhengig og sårbart ved frafall av nøkkelpersonell med høy sikkerhetskompetanse. Funn fra tilsyn viser at en formalisering av enkeltpersoners kompetanse i rutiner og prosedyrer har positive effekter for virksomhetenes sikkerhetsarbeid.

Sikkerhet i anskaffelser

Etterretningstjenester har gjennom alle år utnyttet leveransekjeder for å få tilgang til informasjon eller for å få kontroll på verdier. Det må derfor gjøres risikovurderinger for anskaffelser som kan påvirke grunnleggende nasjonale funksjoner eller andre viktige samfunnsfunksjoner. Når man gjennomfører anskaffelser, kan man gjøre seg avhengig av produsenten. Dette fører med seg risiko, særlig der det er snakk om materiell produsert i land som Norge ikke har et sikkerhetsmessig samarbeid med.

Det er risiko for at utstyr og produkter produsert i andre land kan kontrolleres, overvåkes eller settes ut av drift av leverandøren dersom de ønsker det, selv etter at materiellet er tatt i bruk av norske virksomheter. Dette kan få store konsekvenser for nasjonale sikkerhetsinteresser dersom materiellet brukes til å understøtte viktige samfunns-funksjoner. For å sikre at funksjonalitet i materiell og systemer som understøtter viktige samfunnsfunksjoner ivaretas ved en eventuell tilspisset sikkerhetspolitisk situasjon, er det nødvendig å ha kontroll på avhengigheter som går utenfor landets grenser.

NSM er kjent med at det i 2020 har vært gjennomført anskaffelser der materiell til skjermingsverdige verdier er blitt produsert i land som representerer en etterretningstrussel mot Norge, eller levert av virksomheter med tilknytning til et slikt land. Felles for disse anskaffelsene er at det ikke er gjennomført risikovurderinger i forkant av anskaffelsene eller at risikovurderingene er mangelfulle, og sikkerhet har derfor ikke blitt vurdert som et vesentlig kriterium ved valg av leverandør. Det har heller ikke blitt iverksatt tilstrekkelige kompenserende tiltak for å hindre at materiellet tilrettelegges for bruk i

Fremmede stater kan etablere tilgang til norsk skjermingsverdig informasjon.

etterretningsinnhenting. Resultatet kan bli at fremmede stater etablerer tilgang til norsk skjermingsverdig informasjon eller andre skjermingsverdige verdier, eller at det blir svært utfordrende å hindre slik tilgang når materiellet skal tas i bruk.

For virksomheter underlagt sikkerhetsloven er det krav om å gjennomføre risikovurderinger som en del av forberedelsene til anbudsprosesser, slik det fremgår av sikkerhetsloven § 9-4. Det er vesentlig at operative krav til materiell eller tjenester som skal anskaffes, er godt kjent for miljøene som gjennomfører anbudsprosessene. Dette gjelder både for nye anskaffelser og ved fornyelse av eksisterende avtaler. Operative krav, eierskapsstrukturer eller trusselbildet kan eksempelvis ha endret seg siden forrige avtaleinngåelse.

Sårbarheter ved systemer, infrastruktur og objekter

Utnyttelse av kjente digitale og menneskelige sårbarheter

Kjente sårbarheter utnyttes fortsatt av trusselaktører for å få tilgang til systemer og nettverk. Fremdeles er det mennesker som utgjør en av de største sårbarhetene og som vitende eller uvitende tilrettelegger for et vellykket datainnbrudd. Trusselaktører utnytter også kjente tekniske sårbarheter. Eksempler på dette er feil i nettverks-, klient- eller server-konfigurasjon, svake autentiseringsmekanismer, svak styring av rettigheter og manglende sikkerhetsoppdatering. Mangelfull logging gjør det vanskelig å få full oversikt over omfanget av en hendelse.

Manglende oppdateringer av systemer og tjenester kan gi en aktør uautorisert tilgang til virksomhetens systemer. Direkte innbrudd i sårbare, internetteksponerte tjenester er en vanlig inngangsvektor. NSM har bistått flere virksomheter i håndteringen av hendelser der manglende oppdateringer er direkte årsak til at systemer har blitt kompromittert.

Mange virksomheter mangler oppdatert oversikt over egne systemer og nettverk, og dermed hvor virksomhetens verdier befinner seg. Nye systemer «legges oppå» eldre systemer, noe som kan introdusere nye sårbarheter i overgangene mellom systemene som det er vanskelig å ha kontroll over. Økende avhengighet til komplekse verdi- og leverandørkjeder gjør det utfordrende å ha oversikt over den totale sårbarhetsflaten.

Gode logger er et nødvendig virkemiddel for å avdekke og håndtere hendelser og sikre IKT-systemer. Manglende logging gjør det teknisk umulig å få full oversikt over hendelsen og omfanget av kompromitteringen. Samtidig vil mangel på logging utgjøre en sårbarhet som kan utnyttes av innsidere fordi virksomheten ikke vil ha tilstrekkelig kontroll på aktiviteten i IKT-systemene. Dette er også relevant dersom virksomheten tjenesteutsetter, og **det er viktig at virksomheten har god tilgang til egne logger og informasjon i tilfelle de utsettes for uønskede hendelser.**

NSM ser gjennom hendelseshåndtering at menneskelige sårbarheter utnyttes for å få tilgang til IKT-systemer. Selv om bevisstheten om phishing-aktivitet ser ut til å øke, gjør mer målrettede forsøk det vanskelig for mottakeren av en skreddersydd e-post å la være å åpne skadelige vedlegg eller lenker. Bruk av e-post som inngangsvektor lykkes fortsatt, og NSMs inntrengingstester viser at utsendelse av phishing-e-poster fremdeles er en svært effektiv metode for å komme på innsiden av virksomheters informasjonssystemer. Ofte er det nærmest umulig for en person som har det som sine daglige arbeidsoppgaver å ta imot tilbud, søknader eller lignende fra personer og virksomheter, å skille legitime henvendelser fra illegitime dersom ikke virksomhetens systemer fanger det opp.

Tjenestene vi etter hvert blir avhengige av, vil kunne manipuleres eller falle bort.

Informasjonssystemer er sårbare for angrep fra innsiden. Følgelig er personellsikkerhet en sentral sikkerhetsbarriere. En innsider vil i mange tilfeller kunne utføre betydelig sikkerhetstruende virksomhet i informasjonssystemer, ofte uten at dette blir fanget opp av virksomheten. Innsidere har som regel tillit i virksomheten, og terskelen for å anse mistenkelig aktivitet som skadelig er ofte høy. **Økt sikkerhetsbevissthet og god sikkerhetskultur er derfor viktig også for å redusere risiko for innsidevirksomhet.**

Det er ofte enkle tiltak som kan beskytte IKT-systemer mot utnyttelse av kjente sårbarheter. **Virksomhetene må ha grunnleggende deteksjonsevne og evne til å agere på mistenkelig aktivitet i sine digitale systemer. NSM anbefaler også å etablere et sentralt styrt regime for sikkerhetsoppdatering og en helhetlig sikkerhetsarkitektur i tråd med NSMs grunnprinsipper for IKT-sikkerhet.**

IoT, sensorer og «smarte byer»

Det blir stadig større variasjon i krav til tjenester og til integrasjon mellom tjenester. Samtidig omgir vi oss i økende grad med «smarte» produkter som er knyttet til internett og samler inn ulike typer data om brukere og om omgivelsene. Dette gjør at kompleksiteten i samfunnet øker og dermed også sårbarhets- og angrepsflaten. En aktør med intensjon og kapasitet vil gå minste motstands vei for å få tilgang til et informasjonssystem eller til informasjon. En digital verdikjede er derfor ikke sterkere enn det svakeste punktet.

«Tingenes internett» er et eksempel på dette. IoT er en samlebetegnelse for alle tingene vi omgir oss med som kan kobles til internett og dermed snakke med omgivelsene. Gjennom sensorer i IoT-produkter kan det samles inn store mengder data som kan brukes til blant annet å styre trafikkavvikling, kraftforsyning, vann- og avløpsfunksjoner, avfallshåndtering, helsetjenester og andre funksjoner i samfunnet.

Antallet sensorer, og sensorenes teknologiske kapasitet, øker raskt. Denne informasjonen har bred kommersiell anvendelse, og nye tjenester basert på blant annet stordataanalyse og datasyn (computer vision) er i utvikling. Eksempler på sensorer er mobiltelefoner, smartklokker, strømmålere, elektroniske dørlåser og alarmsystemer, satellitt-

Hva er phishing?

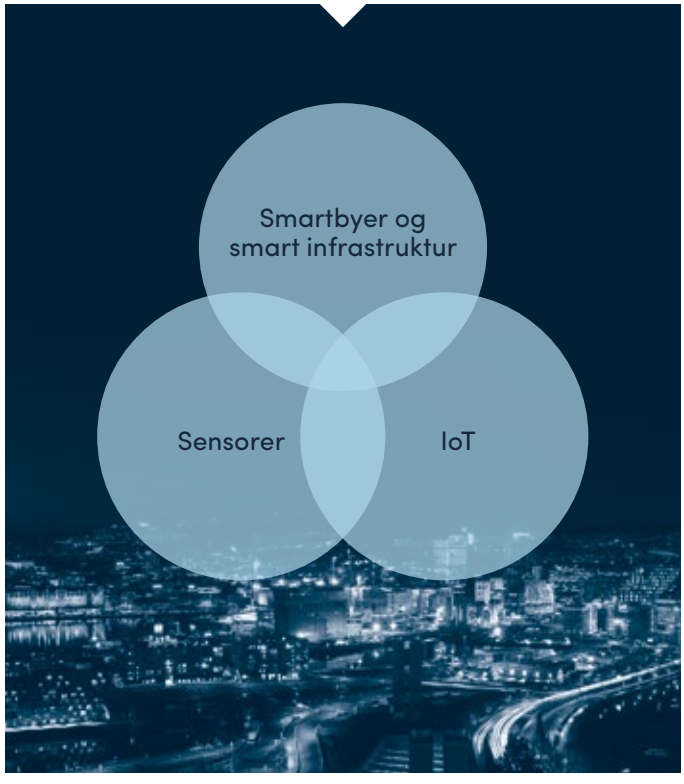
Phishing innebærer å utnytte en ansatt for å skaffe seg uautorisert tilgang til en virksomhets IKT-systemer. Phishing kan gjøres på ulike måter. De vanligste metodene er ved å lure en mottaker til å oppgi påloggingsdetaljer eller å få mottaker til å laste ned skadevare via vedlegg eller lenke i en e-post. Dette kan gi aktøren tilgang til systemet for videre kompromittering.

og flybilder, action-kameraer, droner, overvåkningskameraer og trafikkameraer og nye avanserte kjøretøy.[27] Sammenstilling og analyse av data fra ulike sensorer danner grunnlaget for den raske utviklingen innen autonome systemer, smart infrastruktur, smarte byer og mer. Sensorene bidrar til effektivisering av tid og ressurser, men sensorbruk er i liten grad regulert. De kan medføre konsekvenser vi ikke er bevisst, noe som gjør det vanskelig å identifisere tiltak. Dette fører til at sikkerhetsarbeidet blir hengende etter.

Data fra mobile sensorer og IoT-produkter danner grunnlaget for «smarte byer» – urbane områder hvor dataene sammenstilles og analyseres for å effektivisere og forbedre ressurser og tjenester. Digitalisering og utvikling av «smarte byer» er ment å gjøre fremtidens byer mer bærekraftige, effektive og trygge. Ulike tjenesteområder, teknologier og datakilder vil integreres, slik at data kan deles av offentlige organer, private bedrifter, FoU-aktører og organisasjoner i sivilsamfunnet. «Smartby»-løsninger er under utprøving i flere norske kommuner.

Vi som individer vil i liten grad kunne begrense hvilke data som samles inn om oss og hvilke «smarte» enheter som kan brukes som kilder. I et sikkerhetsperspektiv vil det være risiko for at store mengder informasjon blir tilgjengelig for en trusselaktør. Det er også risiko for at trusselaktører etablerer kapasitet til å påvirke samfunnsfunksjoner gjennom «smart» infrastruktur og «smart by»-løsninger. Tjenestene vi etter hvert blir avhengige av, vil kunne manipuleres eller falle bort.

Det meste av «smart»-teknologien utvikles i utlandet, og det er risiko for at enkelte utenlandske teknologiselskaper vil kunne få svært dominerende posisjoner regionalt eller nasjonalt. Økt kompleksitet og antall sammenkoblinger, ukjente avhengigheter, begrensninger i kompetanse og evne til effektiv hendelseshåndtering vil kunne gi store



Ved en programvareoppdatering kan det introduseres ondsinnet programvare.

utfordringer for sikkerhet i «smarte byer».

Kommunal sektor og sektormyndigheter må settes i stand til å gjennomføre risikovurderinger og stille krav når «smart by»-prosjekter etableres slik at sikkerheten i viktige samfunnsfunksjoner ivaretas.

Myndighetene må få bedre oversikt over hvilke data fra sensorer som samles inn, lagres og sammenstilles, samt hvem som har tilgang til dataene. Videre må det vurderes hvilke tiltak som skal iverksettes for å ivareta personvern og nasjonal sikkerhet.

Sårbarheter ved adgangskontroll

NSM erfarer at enkelte virksomheter har mangelfull fysisk sikkerhet. NSMs inntrengingstestere har ved flere anledninger fått tilgang til sikre soner ved blant annet å produsere falske eller kopiere adgangskort eller ved at dører som skulle vært en del av sikkerhetsbarrieren, står åpne.

Adgangskort gir fysisk tilgang til virksomheters lokaler. Generelt har mange stor tillit til andre som har adgangskort, og holder gjerne opp døren for en travel «kollega» med adgangskort rundt halsen, til tross for at personene aldri tidligere har møttes. Slik kan uvedkommende ta seg inn i bygninger gjennom såkalt «tail-gating».

Adgangskort og tilhørende PIN-kode er også lette å få tak i og beskyttes ofte for dårlig. Mange bærer adgangskortet synlig utenfor arbeidsplassen, uten å tenke på at en trusselaktør da kan få kunnskap om virksomhetens adgangskort og utnytte det til å forfalske kort. PIN-koden kan også enkelt gjøres kjent for uvedkommende ved at den ikke skjermes tilstrekkelig av den enkelte når den brukes på utsiden av bygg.

NSM ser også en tendens til at fysiske sikringstiltak er bedre ivaretatt på virksomhetenes hovedkontor enn ved andre fysiske lokasjoner eller stasjoner. Når virksomhetens avdelinger er koblet til samme informasjonssystem, kan mindre beskyttede lokaler og stasjoner lett bli et svakt punkt hvor uvedkommende får tilgang til virksomhetens systemer. Sikkerheten blir aldri bedre enn det svakeste ledd.

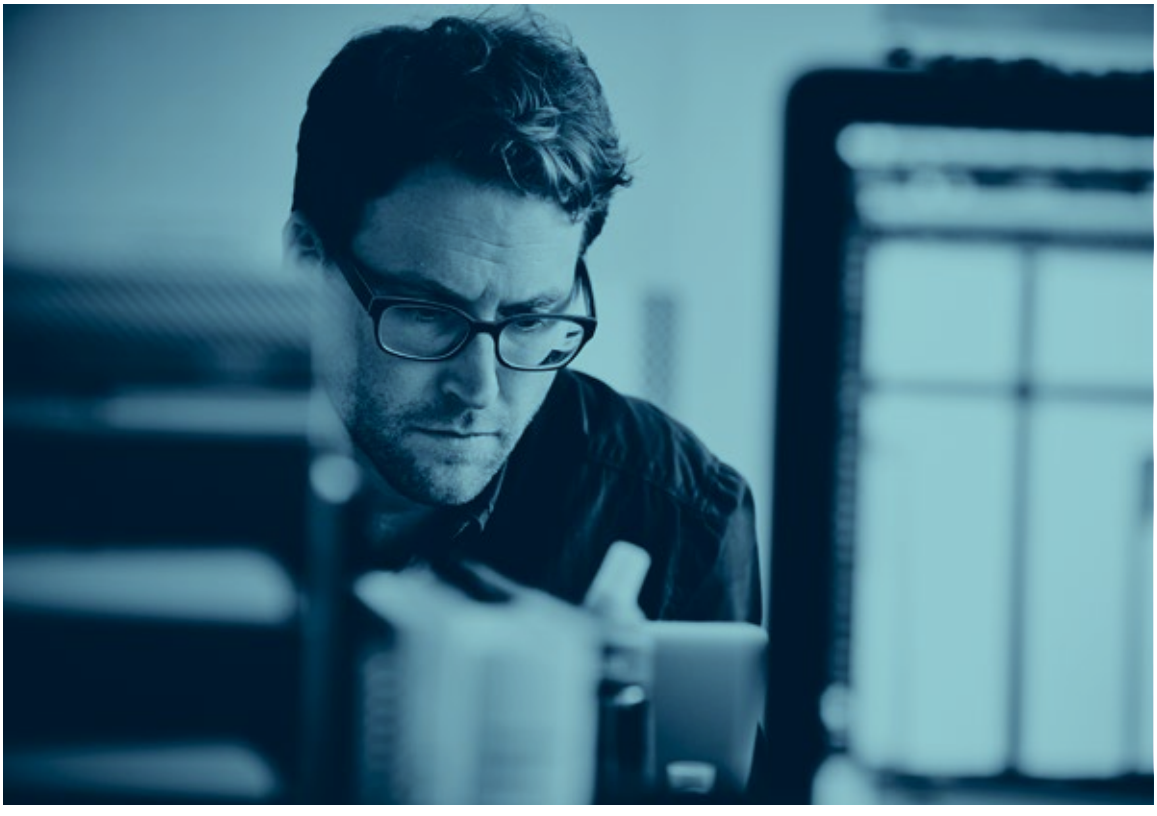
Adgangskontrollsystemer som skal sikre bygg, kan også ha digitale sårbarheter. Digitale kortlesere inneholder programvare som må oppdateres. Ved en programvareoppdatering kan det introduseres ondsinnet programvare som gjør det mulig å hente ut data fra kortleseren eller på annen måte manipulere denne. Hverken beskyttelse av kortet eller PIN-koden vil beskytte virksomheten mot en aktør med slike intensjoner. I dette tilfellet vi det være viktig å kunne stole på leverandørkjeden for kortleseren.

Et elektronisk kortlesersystem gir mulighet for effektiv adgangskontroll med tilgangsstyring og loggføring. Utfordringene nevnt over vitner imidlertid om at fysiske og elektroniske sikringstiltak, som adgangskort og adskilte soner, ikke fungerer dersom de ikke implementeres i sammenheng med andre forebyggende

tiltak. Dette kan føre til en «falsk sikkerhet» i virksomhetene, og det er viktig å være bevisst hvilke eventuelle nye sårbarheter dette kan medføre dersom systemene ikke understøtter hverandre på ønsket måte. **For å oppnå helhetlig sikring er man avhengig av at de fysiske, elektroniske, menneskelige og organisatoriske tiltakene fungerer sammen og understøtter hverandre.**

For at de fysiske sikkerhetstiltakene skal kunne virke etter sin hensikt, må personell tilknyttet virksomheten ha tilstrekkelig kunnskap om tiltakene for å sørge for at de ikke blir omgått eller manipulert. Dette krever opplæring og bevisstgjøring av de ansatte i alle deler av virksomheten.

NSM anbefaler virksomhetene å legge NSMs grunnprinsipper for fysisk sikkerhet til grunn når nye fysiske sikringstiltak skal vurderes og implementeres.



Anbefalte tiltak

NSM gir råd om forebyggende tiltak på strategisk nivå til sine overordnede departementer.

Anbefalte tiltak for å motvirke risiko som er sektorspesifikk vil inngå som del av dialogen mellom NSM og de respektive departementer.

Nasjonal sikkerhet ivaretas først og fremst gjennom virksomhetenes sikkerhetsarbeid – særlig av virksomheter som er av avgjørende betydning for grunnleggende nasjonale funksjoner og som behandler sikkerhetsgradert informasjon. NSMs anbefalinger om tiltak på virksomhetsnivå kommuniseres blant annet gjennom råd, veiledninger og kurs.

NSM anbefaler at alle virksomheter følger NSMs grunnprinsipper for IKT-sikkerhet. Grunnprinsippene er et godt utgangspunkt for å oppnå forsvarlig digital sikkerhet.

NSM lanserte høsten 2020 grunnprinsipper også innenfor fysisk sikkerhet, personellsikkerhet og sikkerhetsstyring. NSMs grunnprinsipper innen de ulike fagområdene følger samme oppbygging og gir virksomhetene nyttige råd om hvilke prinsipper som bør legges til grunn for å oppnå forsvarlig sikkerhet.

For ytterligere informasjon om råd, veiledninger og kurs besøk oss på www.nsm.no.

Følgende tiltak er presentert tidligere i rapporten:

IKT-SIKKERHET

For å oppnå nødvendig interoperabilitet og gjenbruk på tvers bør IT-plattformene tilknyttet viktige samfunnsfunksjoner ha en felles digital grunnmur basert på felles grunnleggende arkitekturprinsipper. (Se side 24-26). NSM anbefaler:

1. Etablering av et nasjonalt, digitalt målbilde: En overordnet beskrivelse på myndighetsnivå av hvordan vi ønsker å bruke teknologiene i fremtiden.
2. Norge trenger en felles digital grunnmur. Den digitale grunnmuren skal skape et felles teknisk fundament som sikrer at vi oppnår målbildet.

NSM anbefaler at myndighetene intensiverer arbeidet med å etablere nasjonale og internasjonale digitale løsninger som gir nødvendig sikkerhet i fremtiden. Alle samfunnets funksjoner er avhengig av dette. (Se side 24-26).

NSM mener at det bør prioriteres å etablere nasjonale robuste og redundante datasenter- og skyløsninger som kan tilbys virksomheter som forvalter skjermingsverdige verdier og ivaretar viktige samfunnsfunksjoner. (Se side 29).

Virksomheter som har behov for å ta i bruk skyløsninger og tjenester fra datasenter, må sette seg godt inn i hvordan dette påvirker deres digitale sikkerhet og gjøre gode verdi- og risikovurderinger i forkant. NSM har

utarbeidet temaheftet *Sikkerhetsfaglige anbefalinger ved tjenesteutsetting* og anbefaler å legge disse rådene til grunn for slike vurderinger. (Se side 29).

For å redusere sårbarheter knyttet til passord, anbefaler NSM virksomheter å ta i bruk multi-faktor pålogging, i tråd med rådene i NSMs grunnprinsipper for IKT-sikkerhet. (Se side 30).

NSM anbefaler at virksomheter har gode rutiner for å fjerne ansattes tilganger til virksomhetens IKT-systemer når arbeidsforholdet avsluttes. (Se side 30).

NSM anbefaler at virksomheten har god tilgang til egne logger og informasjon i tilfelle de utsettes for uønskede hendelser. (Se side 37).

Virksomhetene må ha grunnleggende deteksjonsevne og evne til å agere på mistenkelig aktivitet. NSM anbefaler også å etablere et sentralt styrt regime for sikkerhetsoppdatering og en helhetlig sikkerhetsarkitektur i tråd med NSMs grunnprinsipper for IKT-sikkerhet. (Se side 38).

Økt sikkerhetsbevissthet og god sikkerhetskultur er viktig for å redusere risiko for innsidevirksomhet. (Se side 38).

PERSONELLSIKKERHET

NSM anbefaler at virksomheter har gode rutiner for å fjerne ansattes tilganger til virksomhetens IKT-systemer når arbeidsforholdet avsluttes. (Se side 30).

NSM anbefaler at myndigheter og forskningsinstitusjoner samarbeider om bevisstgjøring og kompetanseheving om risiko knyttet til fremmed etterretning i forsknings-, utviklings- og teknologimiljøer. Flere risikoreduserende tiltak bør vurderes. (Se side 32).

NSM anbefaler virksomhetene å ha en systematisk og helhetlig tilnærming til risikoreduserende tiltak mot innsidevirksomhet. Se i denne sammenheng NSMs grunnprinsipper for personellsikkerhet. (Se side 32-34).

FYSISK SIKKERHET

For å oppnå helhetlig sikring er man avhengig av at de fysiske, elektroniske, menneskelige og organisatoriske tiltakene fungerer sammen og understøtter hverandre. (Se side 41).

For at de fysiske sikkerhetstiltakene skal kunne virke etter sin hensikt, må personell tilknyttet virksomheten ha tilstrekkelig kunnskap om disse for å sørge for at de ikke blir omgått eller manipulert. Dette krever opplæring og bevisstgjøring av de ansatte i alle deler av virksomheten. (Se side 41).

NSM anbefaler virksomhetene å legge NSMs grunnprinsipper for fysisk sikkerhet til grunn når nye fysiske sikringstiltak skal vurderes og implementeres. (Se side 41).

SAMMENSATTE TRUSLER

For å kunne identifisere sammensatte trusler og iverksette nødvendige mottiltak er det sentralt at norske myndigheter etablerer og opprettholder et samordnet nasjonalt situasjonsbilde. Et slikt bilde bør blant annet baseres på varsling, rapportering og samvirke mellom myndigheter og virksomheter. I dette

NSM skal varsles ved mistanke om sikkerhetstruende virksomhet.

arbeidet må også media og andre relevante sivile aktører involveres. (Se side 19).

Evnen til å avdekke og varsle om sikkerhetstruende virksomhet må styrkes i alle sektorer, og det må etableres mekanismer for analyse, informasjonsutveksling og samhandling. Dette vil bidra til at kunnskap og erfaringer fra alle sektorer benyttes til å identifisere forebyggende tiltak. NSM vil fortsette arbeidet med å gi informasjon, råd og veiledning for å sette sektormyndigheter i stand til å utøve sitt ansvar. (Se side 22).

Kommunal sektor og sektormyndigheter må settes i stand til å gjennomføre risikovurderinger og stille krav når «smart by»-prosjekter etableres slik at sikkerheten i viktige samfunnsfunksjoner ivaretas. (Se side 40).

Myndighetene må få bedre oversikt over hvilke data fra sensorer som samles inn, lagres og sammenstilles, samt hvem som har tilgang til dataene. Videre må det vurderes hvilke tiltak som skal iverksettes for å ivareta personvern og nasjonal sikkerhet. (Se side 40).

KARTLEGGING AV VERDIER OG AVHENGIGHETER

NSM forutsetter at virksomhetene kartlegger og vurderer hvilke avhengigheter de har til andre virksomheter og tjenester. Virksomheter underlagt sikkerhetsloven plikter å rapportere om egne avhengigheter til NSM. (Se side 16).

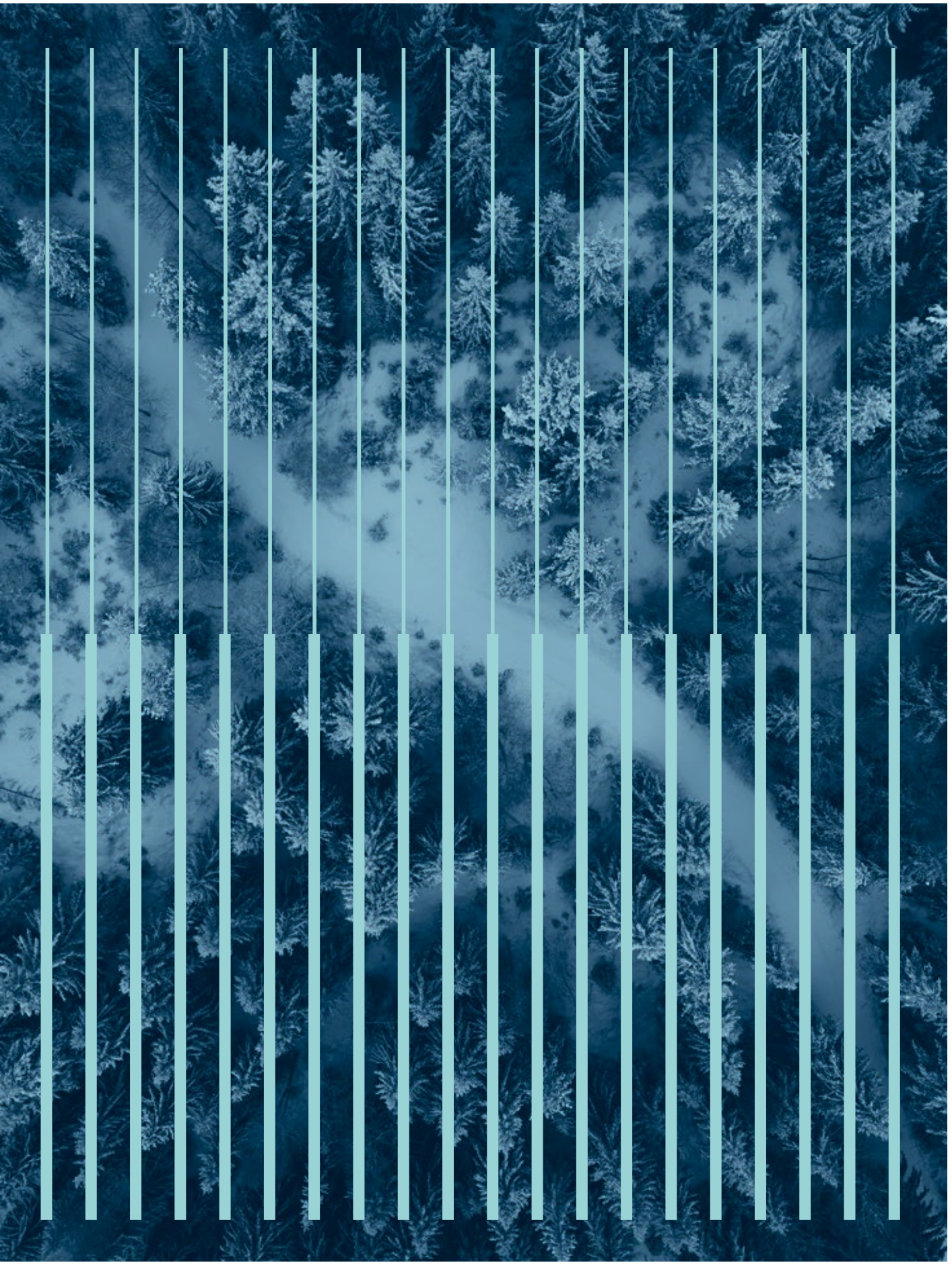
Departementene må fortsette arbeidet med å identifisere virksomheter av vesentlig betydning for de grunnleggende nasjonale funksjonene og at disse underlegges sikkerhetsloven. (Se side 17).

Virksomhetene underlagt sikkerhetsloven må følge opp lovens krav til risikovurderinger og etablering av forsvarlig sikkerhetsnivå. (Se side 17).

Det er viktig at virksomheter kartlegger virksomhetens plass i verdikjeden(e) og vurderer egne avhengigheter jevnlig. Virksomheter som er av avgjørende betydning for grunnleggende nasjonale funksjoner bør ta høyde for en eventuell tilspisset sikkerhetspolitisk situasjon i sine risikovurderinger. Dette gjelder også for Forsvarets avhengighet av sivile virksomheter. (Se side 23.)

ANSKAFFELSER

For virksomheter underlagt sikkerhetsloven er det et krav å gjennomføre risikovurderinger som en del av forberedelsene til anbudsprosesser, slik det fremgår av sikkerhetsloven § 9-4. Det er vesentlig at operative krav til materiell eller tjenester som skal anskaffes er godt kjent for miljøene som gjennomfører anbudsprosessene. (Se side 36).



Fotnoter

[1] Begrepet «infodemi» ble brukt av WHO i februar 2020. Begrepet referer til en overflod av mer eller mindre pålitelig informasjon, desinformasjon, falske nyheter, rykter og konspirasjonsteorier som gjør det vanskelig for folk å finne pålitelige kilder og riktig veiledning når de trenger det https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200202-sitrep-13-ncov-v3.pdf

[2] https://www.nupi.no/Skole/HHD-Artikler/2020/Korona-og-falske-nyheiter-Ein-infodemi

[3] Internet of Things, tingenes internett, består av et nettverk av enheter utstyrt med elektronikk og programvare som fører til at enhetene kan kommunisere seg imellom og i nettverk.

[4] Elektronisk kommunikasjon.

[5] https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/losepengevirus

[6] Prop. 153 L (2016–2017) Lov om nasjonal sikkerhet.

[7] NSMs Veileder i departementenes identifisering av grunnleggende nasjonale funksjoner. https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker-til-sikkerhetsloven/veileder-i-departementenes-identifisering-av-grunnleggende-nasjonale-funksjoner/om-denne-veilederen/

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

[9] Sikkerhetstruende virksomhet er i sikkerhetsloven definert som tilsiktede handlinger som direkte eller indirekte kan skade nasjonale sikkerhetsinteresser. Det omfatter blant annet spionasje, sabotasje og terror, i tillegg til handlinger som har som mål å undergrave eller påvirke norske myndigheters styringsevne.

[10] Jf. sikkerhetsloven § 10-3.

[11] Pedersen, Thorbjørn (2019), Internasjonal polarforskning gjør flere land i stand til å operere med militære styrker i Arktis. Dette er uheldig for Norge. Kronikk i Aftenposten 3. mai 2019. https://www.aftenposten.no/meninger/kronikk/i/AdRlGq/internasjonal-polarforskning-gjoer-flere-land-i-stand-til-aa-operere-med

[12] Meld. St. 9 (2020–2021) Mennesker, muligheter og norske interesser i nord. https://www.regjeringen.no/no/dokumenter/meld.-st.-9-20202021/id2787429/

[13] Begrepet «sky» og «skytjenester» favner vidt og benyttes for en rekke ulike teknologier, forretningsmodeller og leverandørkonstellasjoner. Nasjonal strategi for bruk av skytjenester omtaler skytjenester som: «... skalerbare tenester som blir leverte over nett. Den viktigaste forskjellen på skytenester og meir tradisjonell tenesteutsetting er forretningsmodellen, der kunden berre betaler for den kapasiteten han har brukt. Målet er å tilby kostnadseffektive, sikre, skalerbare IT-tenester til kundane.». https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-bruk-av-skytenester/id2484403/

[14] Meld. St. 9 (2020–2021) Mennesker, muligheter og norske interesser i nord. https://www.regjeringen.no/no/dokumenter/meld.-st.-9-20202021/id2787429/

[15] NSM (2019), Tema-rapport. Innsiderisiko. https://nsm.no/regelverk-og-hjelp/rapporter/temarapport-om-innsidere/temarapport-om-innsidere

[16] NSM, Kronikk. «Er utenlandske etterretningstjenester amatører?» 7.1.2021.

[17] NSM, Kronikk. «Er utenlandske etterretningstjenester amatører?» 7.1.2021. https://nsm.no/aktuelt/kronikk-er-utenlandske-etterretningstjenester-amatorer

[18] Etterretningstjenesten, Fokus 2021

[19] Meld. St. 4 (2018–2019), Langtidsplan for forskning og høyere utdanning 2019–2028.

[20] Tall fra Nordisk institutt for studier av innovasjon, forskning og utdanning (NIFU) viser at 39 prosent av doktorandene våren 2020 var utenlandske statsborgere.

[21] https://www.nasa.gov/centers/ames/research/2009/Meyya_Meyyappan.html [nasa.gov]

[22] https://www.justice.gov/usao-sdny/pr/senior-nasa-scientist-pleads-guilty-making-false-statements-related-chinese-thousand [justice.gov]

[23] https://www.justice.gov/opa/pr/chinese-citizen-convicted-economic-espionage-theft-trade-secrets-and-conspiracy [justice.gov]

[24] https://www.bloomberg.com/news/articles/2020-06-26/chinese-professor-found-guilty-of-trade-secret-theft-espionage [bloomberg.com]

[25] https://www.bloomberg.com/news/articles/2020-09-01/chinese-professor-gets-18-months-in-prison-for-theft-espionage [bloomberg.com]

[26] https://www.justice.gov/usao-ndca/pr/chinese-citizen-sentenced-economic-espionage-theft-trade-secrets-and-conspiracy [justice.gov]

[27] NSM (2020) 13 råd om sikkerhet på mobile enheter: https://nsm.no/aktuelt/13-rad-om-sikkerhet-pa-mobile-enheter

NASJONAL SIKKERHETSMYNDIGHET

Postboks 814, 1306 Sandvika

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