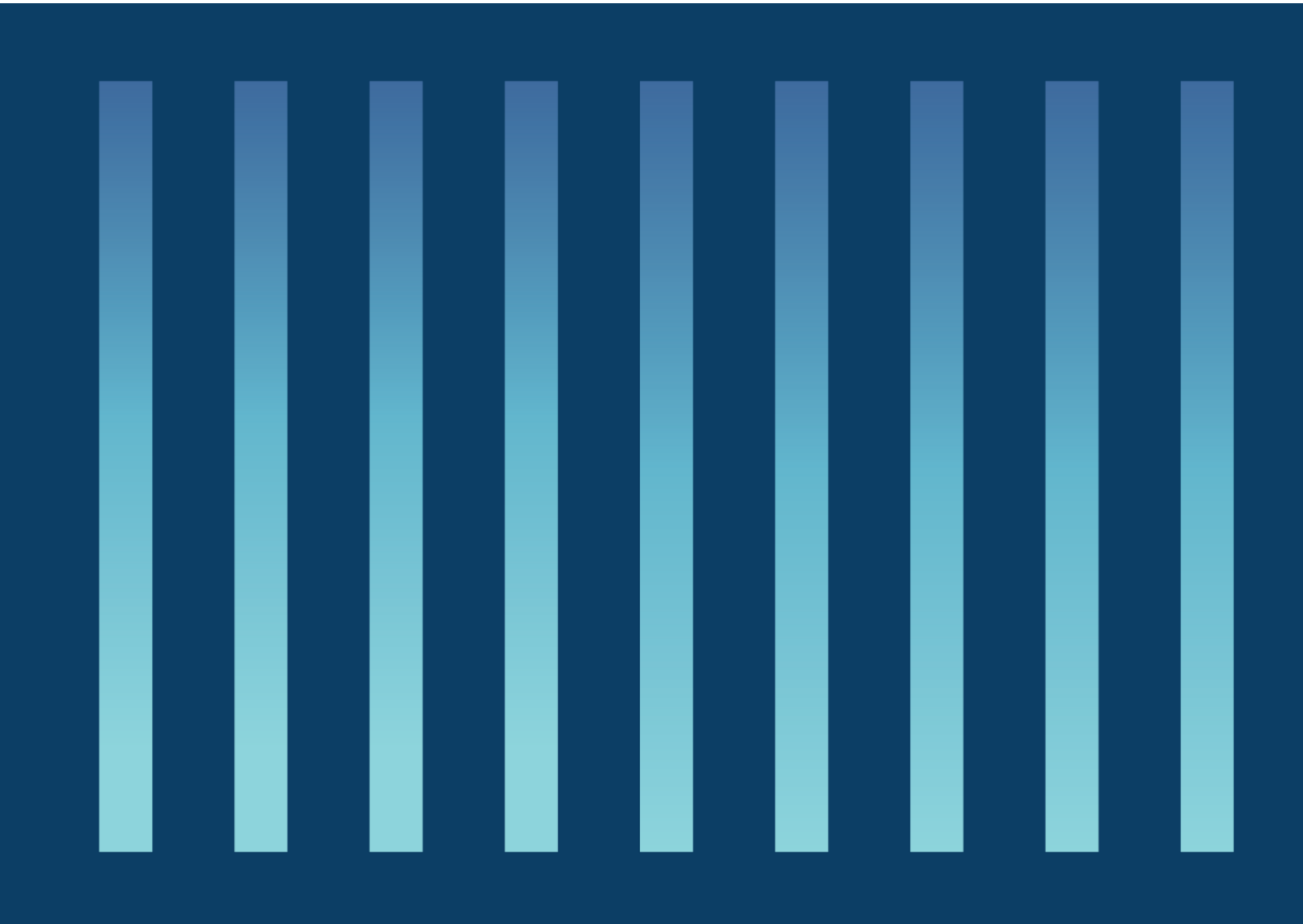
NASJONAL
SIKKERHETSMYNDIGHET

Risiko 2021 - helhetlig sikring mot sammensatte trusler

Dokumentet er et sammendrag av NSMs årlige risikorapport. Endelig versjon publiseres i midten av mars 2021.



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.

Risikobildet

Norge står overfor et komplekst risikobilde der fremmede stater ved hjelp av et bredt utvalg virkemidler forsøker å utnytte sårbarheter i funksjoner, virksomheter og systemer. Sammensatte trusler er en risiko for norske sikkerhetsinteresser.

NSM vurderer de viktigste utfordringene i risikobildet å være følgende:

- **Det digitale risikobildet er skjerpet**
- **Pandemien har gitt økt risiko**
- **Sammensatte trusler gjør oss sårbare**

Det digitale risikobildet vurderes som skjerpet. Den raske teknologiske utviklingen gir stor samfunnsnytte i form av velferd, trygghet og verdiskaping. Samtidig er det svært krevende å følge opp sikkerhetsarbeidet i samme takt. Som resultat oppstår nye sårbarheter. Dataangrepet mot Stortinget høsten 2020 er én av flere alvorlige hendelser den siste tiden som illustrerer trusselaktørenes kapasitet og vilje til å ramme norske virksomheter – selv våre mest sentrale institusjoner. Hendelsene NSM håndterer, viser fortsatt at tiltakene i NSMs grunnprinsipper for IKT-sikkerhet beskytter mot de aller fleste digitale angrep.

Pandemien har forsterket det eksisterende risikobildet. Det er blant annet økt press mot enkelte sektorer og samfunnsfunksjoner, som helsesektoren, nye sårbarheter som følge av hjemmekontor og endrede arbeidsmønstre, økt risiko for uønskede strategiske investeringer og omfattende global påvirkning og desinformasjon.

Sammensatte trusler, ofte omtalt som hybride trusler, rammer på tvers av sektorer og nivåer. Sikkerhetsloven ble modernisert for to år siden, og lovens virkeområde ble utvidet blant annet for å demme opp for slike trusler.

Til høsten er det stortings- og sametingsvalg. NSM samarbeider med Etterretningstjenesten, PST og Kripos gjennom Felles cyberkoordineringssenter (FCKS) for å sikre valggjennomføringen og gi sikkerhetsfaglige råd til norske politiske partier.

Nasjonale sårbarheter

Inntil sikkerhetsloven er fullt implementert og operasjonalisert, er forutsetningene for å oppnå forsvarlig sikkerhetsnivå mangelfulle. Sikkerhetslovens virkeområde ble utvidet blant annet for å demme opp for sammensatte trusler. Slik virkemiddelbruk rammer på tvers av sektorer og nivåer og gjør skillet mellom stats- og samfunnssikkerhet mindre tydelig, skriver Etterretningstjenesten i *Fokus 2021*. I dette bildet vet vi at det finnes verdier som har betydning for grunnleggende nasjonale funksjoner, men som ennå ikke er identifisert eller sikret på en forsvarlig måte.

Et helt sentralt tiltak for å motvirke sammensatte trusler og sørge for helhetlig sikring av skjermingsverdige verdier er å fortsette implementeringen av sikkerhetsloven med kraft og styrke.

Mangelfull oversikt over verdikjeder og avhengigheter mellom virksomheter og tjenester på tvers av sektorene utgjør også en nasjonal sårbarhet i denne sammenhengen.

Det er sentralt at slike avhengigheter kartlegges tilstrekkelig, herunder mellom sivile virksomheter og Forsvaret, som ledd i operasjonaliseringen av sikkerhetsloven.

Strategiske investeringer fra fremmede stater kan få negative konsekvenser for nasjonale sikkerhetsinteresser. Det er vanskelig å skille mellom investeringer som utføres på bakgrunn av rent kommersielle hensyn, og strategiske investeringer som gir fremmede makter tilgang på informasjon, ressurser og infrastruktur, eller som gir mulighet til å påvirke beslutninger. Økonomiske ringvirkninger av covid-19 forsterker risikoen for at norske virksomheter som forvalter slike verdier, kan komme i feil hender.

NSM anbefaler at departementer, sektormyndigheter og virksomheter i utsatte sektorer settes bedre i stand til å avdekke sammensatte trusler og annen sikkerhetstruende virksomhet. Ved begrunnet mistanke om sikkerhetstruende virksomhet skal NSM varsles.

Digitaliseringen av Norge skjer raskt, med utvikling av ny teknologi og nye løsninger både i statsforvaltningen og i det private. Flere virksomheter har forsert egne digitaliseringsplaner som følge av covid-19-pandemien. Dagens beslutninger skaper fremtidige utfordringer dersom sikkerhetsløsninger ikke er godt nok ivaretatt. Når ny teknologi og ny funksjonalitet skal implementeres, må det velges løsninger som gir bedre sikkerhet – både på kort og lang sikt.

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.

Sårbarheter i virksomheter og samfunnsfunksjoner

Rask utvikling av skytjenester og datasentre utfordrer evnen til å skape helhetlige digitale sikkerhetsløsninger. Utstrakt bruk av skytjenester og store, sentraliserte datasentre innebærer stort potensial for effektivisering og, for den enkelte virksomhet, ofte bedre sikkerhet i det daglige. Samtidig medfører det behov for gode risikovurderinger, ny kunnskap og en betydelig konsentrasjonsrisiko for viktige samfunnsfunksjoner.

Virksomheter som har behov for skyløsninger og tjenester fra datasenter, må sette seg godt inn i hvordan dette påvirker deres digitale sikkerhet. NSM anbefaler å legge rådene i temaheftet *Sikkerhetsfaglige anbefalinger ved tjenesteutsetting* til grunn for slike vurderinger.

Behovet for åpenhet og internasjonalt samarbeid i akademiske miljøer innebærer sårbarhet for at fremmede etterretningstjenester kan utnytte blant annet legitimt forskningssamarbeid for å skaffe sensitiv informasjon og teknologi fra norsk forskning. Norske forsknings- og høykompetansemiljøer innen flere fagfelt er av stor interesse for fremmed etterretning.

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.

Sårbarheter i systemer og strukturer

Kjente sårbarheter utnyttes fortsatt av trusselaktører for å få tilgang til systemer og nettverk. Ofte er det tekniske sårbarheter som utnyttes. 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.

Lange digitale verdikjeder utgjør alvorlige sårbarheter for IKT-systemer. Dersom man ikke har kontroll på verdikjedene og IKT-systemene ikke har tilstrekkelig autonomi, kan bortfall av funksjon lenger ut i verdikjeden ramme systemets funksjon. Trusselaktører kan også utnytte sårbarheter i verdikjeder for å få tilgang til informasjon og funksjonalitet i systemer som understøtter viktige samfunnsfunksjoner eller behandler sensitiv informasjon.

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.

For øvrige tiltak: Se *Risiko 2021* når den publiseres på www.nsm.no 11. mars 2021.

Nasjonal sikkerhetsmyndighet

Postboks 814
1306 Sandvika

postmottak@nsm.no
www.nsm.no