

NSM hever det nasjonale cyberrisikonivået til HØYT

Publisert: 27.10.2026

Oppdatert: 27.10.2026

For første gang deler NSM nasjonalt cyberrisikonivå åpent og ugradert. Et høyt risikonivå krever at norske virksomheter iverksetter forebyggende tiltak umiddelbart.

NSM deler derfor en større tiltakspakke til alle norske virksomheter. Se nederst i artikkelen.

- NSM har ikke gått offentlig ut med denne typen vurderinger tidligere. Vi gjør dette nå fordi det er helt nødvendig å styrke både motstandsdyktigheten og evnen til å håndtere cyberoperasjoner i norske virksomheter, forteller NSM-direktør Arne Christian Haugstøyl.

Nasjonalt cyberrisikonivå

- NSM vurderer risiko i cyberdomenet mot norske offentlige og private virksomheter kontinuerlig.
- Nivået spenner mellom SVÆRT LAVT, LAVT, MODERAT, HØYT og EKSTREMT HØYT.
- Nivået MODERAT anses som normaltstand i cyberdomenet, der cyberoperasjoner mot norske virksomheter forventes.
- Bedre grunnsikring i norske virksomheter bidrar til å senke det nasjonale risikonivået.

Samfunnskritisk infrastruktur risikoutsatt

Forsvarssektoren, forsvarsindustrien og romsektoren er utsatt for høy risiko i cyberdomenet. Det gjelder også samfunnskritisk infrastruktur og tjenesteleverandører til virksomheter av betydning for nasjonal sikkerhet.

NSM ser at disse stadig blir utsatt for kartlegging, kompromitteringsforsøk og kompromitteringer, løsepengevirusangrep og tjenestenektangrep.

- Vi har det siste halve året sett en tredobling av vellykkede cyberoperasjoner mot norske virksomheter. Flere av disse har hatt alvorlige konsekvenser og medfører fortsatt et skadepotensial for nasjonal sikkerhet, sier Haugstøyl.

Teknologiutviklingen påvirker risikonivået

Rask eskalering i bruk av kunstig intelligens (KI) er med på å påvirke situasjonen. KI kan brukes offensivt ved gjennomføring av cyberoperasjoner.

Bruk av språkmodeller og agentiske KI-systemer i cyberoperasjoner utgjør en alvorlig risiko mot norske virksomheter. Selv om dette ikke per nå er dokumentert i Norge, påvirker skadepotensialet det nasjonale cyberrisikonivået.

- KI analyserer store mengder data, og finner sårbarheter raskere enn det mennesker har vært i stand til. Disse åpner for nye muligheter for cyberangrep i hyppigere tempo og større volum. Det betyr at risikoen øker, og tempoet for å utføre sikkerhetstiltak må opp, sier Haugstøyl.

Iverksett tiltak

NSM deler en større tiltakspakke som alle norske virksomheter må sette seg inn i. Tiltakene er ikke nye, mange er å finne i NSMs grunnprinsipper for IKT-sikkerhet. I tillegg er tiltak som phishing-resistent flerfaktoraутентisering, herding, god logging og avdekking, samt oppdatering og utfasing av enheter for å sikre opprettholdelse av samfunnskritisk infrastruktur trukket frem.

Det samme er risikostyring for leverandørkjeder, kartlegging av enheter og programvare, og validering av at sikkerhetstiltak virker etter hensikten.

- Dagens digitale risikobilde krever at det iverksettes flere tiltak, både menneskelige, tekniske og organisatoriske. Når virksomheter iverksetter tiltak bidrar de ikke bare til motstandsdyktigheten i egen organisasjon, men de bidrar også til å ta ned det nasjonale cyberrisikonivået, understreker Haugstøyl.

Tiltakspakke for å bedre norsk grunnsikring ved høyt cyberrisikonivå
Den digitale motstandsdyktigheten til norske virksomheter må opp. Dagens digitale risikobilde krever at det iverksettes flere tiltak, både menneskelige, tekniske og organisatoriske. NSM deler derfor åpent tiltak vi forventer at norske virksomheter iverksetter.

Sikkerhetstiltakene som skal sikre verdier, må være robuste og tilpasset det til enhver tid gjeldende trussel- og risikobildet. Tiltak må herdes, og ytterligere tiltak må kunne iverksettes ved økt trussel og risiko.

NSM fremhever avslutningsvis 21 relevante tiltak fra NSMs grunnprinsipper for IKT-sikkerhet som er relevante for alle norske virksomheter. Tiltakene øker den enkeltes virksomhets motstandsdyktighet og ikke minst evne til å håndtere cyberoperasjoner.

Start med cybersjekk.no. Her får dere et konkret bilde på sikkerhetstilstanden i egen virksomhet og konkrete råd om hvilke tiltak dere begynner med.

Anbefalte tiltak fra NSM

For opprettholdelse av samfunnskritisk infrastruktur

NSM anbefaler bruk av [phishing-resistent flerfaktoraутентisering](#), herding, god logging og avdekking, samt oppdatering og utfasing av enheter.

I tillegg anbefaler NSM implementering av soner og konduiter med autentisering og styring av nettverkstrafikk. Det anbefales også å begrense tilgjengelig programvare på enheter i slike soner avhengig av etablert sikkerhetsnivå og implemente tilstrekkelig tilgangskontroll.

Videre anbefales det å etablere som et minimum et opprettholdbart system som kan drifte funksjonen, selv under en hendelse.

NSM erfarer at trusselaktører utnytter tekniske sårbarheter i samfunnskritisk infrastruktur. Selv om denne infrastrukturen ikke er skjermingsverdig, har den betydning for opprettholdelse av grunnleggende behov og funksjoner i samfunnet.

Risikostyring for leverandørkjeder

Virksomheter bør etablere helhetlig risikostyring av egne leverandørkjeder. Risikostyringen må omfatte opprinnelsen av råvarer, komponenter, deler, tjenester og programvare, og også hvilken informasjon som flyter andre veien i leverandørkjedene i form av bestillinger med spesifikasjoner og krav. Det må stilles krav til at alle leverandører har forsvarlig sikkerhetsstyring, og at alle leverandører stiller tilsvarende krav til underleverandørene sine.

Kartlegging av leverandørkjeder for digitale tjenester og programvare bidrar til å etablere hensiktsmessig overvåking og forsvarlige sikkerhetstiltak i virksomhetens digitale infrastruktur.

NSM er kjent med at cyberoperasjoner også rammer virksomheter som er underleverandører til virksomheter som har betydning for nasjonal sikkerhet. Det kan være forsøk fra trusselaktør på å få tilgang til andre virksomheter høyere opp i en leverandør- eller verdikjede.

Kartlegg enheter og programvare

Tiltakene i prinsipp 1.2 i NSMs grunnprinsipper for IKT-sikkerhet bør følges opp med bruk av hensiktsmessige verktøy. En mulighet er å bruke NIST Common Platform Enumeration (CPE) for denne kartleggingen, for å være i stand til raskt å identifisere om og hvor nye sårbarheter kan være eksponert i virksomhetens digitale infrastruktur.

Kartleggingen er også viktig for å etablere hensiktsmessig overvåking for å detektere sikkerhetstruende hendelser eller unormal aktivitet. Dette vil også styrke evnen til rask respons for å redusere konsekvensene av en sikkerhetstruende hendelse.

Valider at sikkerhetstiltak virker etter hensikten

Virksomhetens tekniske infrastruktur og de risikoreducerende sikkerhetstiltak kan være komplekse. Det er viktig å verifisere at sikkerhetstiltak er korrekt iverksatt og å validere at sikkerhetstiltaket virker etter hensikten.

Et eksempel er tilgangsstyring med flerfaktoraутентisering (MFA) og totrinnsپا logging som må være motstandsdyktig for forsøk på omgåelse ved sosial manipulering eller phishing.

Øvrige tiltak fra NSMs grunnprinsipper for IKT-sikkerhet

- 1.2.3 Kartlegg enheter i bruk i virksomheten.
- 1.2.4 Kartlegg programvare i bruk i virksomheten.
- 1.3.3 Kartlegg roller og ansvar i virksomheten knyttet til IKT-sikkerhet.
- 2.1.2 Kjøp moderne og oppdatert maskin- og programvare.
- 2.1.9 Ta ansvar for virksomhetens sikkerhet også ved tjenesteutsetting.
- 2.2.1 Etabler og vedlikehold en helhetlig sikkerhetsarkitektur.
- 2.2.3 Del opp virksomhetens nettverk etter virksomhetens risikoprofil.
- 2.3.1 Etabler et sentralt styrt regime for sikkerhetsoppdatering.
- 2.3.2 Konfigurer enheter slik at kun kjent programvare kjører på dem.
- 2.3.3 Deaktiver unødvendig funksjonalitet
- 2.3.7 Endre alle standardpassord på IKT-produktene før produksjonssetting.
- 2.4.1 Etabler tilgangskontroll på flest mulige nettverksporter.
- 2.5.1 Styr dataflyt mellom virksomhetens inndelte nettverksoner.
- 2.6.4 Minimer rettigheter til sluttbrukere og spesialbrukere.
- 2.6.5 Minimer rettigheter på drifts-kontoer.
- 2.6.7 Bruk flerfaktoraутентisering.
- 2.9.1 Legg en plan for regelmessig sikkerhetskopiering av alle virksomhetsdata.
- 2.9.3 Test sikkerhetskopier regelmessig.
- 3.2.3 Avgjør hvilke deler av IKT-systemet som skal overvåkes.
- 3.2.4 Beslutt hvilke data som er sikkerhetsrelevant og bør samles inn.
- 4.1.1 Etabler et planverk for hendelseshåndtering.

For flere tiltak se til [NSMs grunnprinsipper for IKT på nsm.no](https://nsm.no), IEC62443/NEK 820 og NIST SP 800-82.

NSM minner om viktigheten av å tenke helhetlig sikkerhet. Se gjerne også til NSMs grunnprinsipper for sikkerhetskultur, personellsikkerhet og fysisk sikkerhet for ytterligere tiltak.

Forbehold: Tiltakene fra NSM fjerner ikke all risiko for cyberoperasjoner, men det både øker virksomhetens evne til å håndtere situasjonen og kan redusere konsekvensene av en cyberoperasjon.