NSM



Risiko 2026

Dagens valg – morgendagens risiko



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

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

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

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

Om rapporten

Risiko 2026 beskriver sårbarheter trusselaktører kan utnytte i virksomheter og i samfunnet, og hvilken risiko dette innebærer. I rapporten peker NSM på hvordan myndigheter og virksomheter bør beskytte seg mot truslene som Etterretningstjenesten og PST beskriver i sine årlige trusselvurderinger.

Målet med NSMs risikovurdering er å gi virksomheter bedre forutsetninger for å etablere og opprettholde et forsvarlig sikkerhetsnivå i lys av det nasjonale risikobildet. Dette gjelder alle virksomheter, men spesielt for virksomheter omfattet av sikkerhetsloven eller digitalsikkerhetsloven. Rapporten inneholder anbefalte tiltak som virksomheter kan iverksette for å beskytte seg mot spionasje, sabotasje, terror og sammensatte trusler. Årets rapport er tilgjengelig på nsm.no/risiko2026.

Innhold

Forord 7

Sammendrag 8

Et sammensatt risikobilde 10

Norges rolle i det sikkerhetspolitiske bildet 10

Europeisk opprustning påvirker norske virksomheter 12

Teknologisk utvikling skaper nye risikoområder 13

Forebyggende sikkerhetsarbeid 14

Sikkerhetsstyring styrker nasjonal sikkerhet 14

Gode rutiner for sikkerhetsmessig ledelse og personellsikkerhet er avgjørende 17

Fysisk sikring må tilpasses trussel- og risikobildet 20

Viktigheten av innsikt i eierstrukturen 22

Det digitale risikobildet 24

Trender i cyberdomenet det siste året 24

Operasjonell teknologi som del av angrepsflaten 28

Bruk av usikker protokoll er utbredt 30

Kjente sårbarheter i nettverksutstyr blir utnyttet 31

Sikkerhet i anskaffelser 32

Norske virksomheter kan bidra til å redusere risiko i leverandørkjeder 32

Omfattende bruk av et fåtall utenlandske skytjenester 35

Satellittsystemers avhengigheter 36



Forord



Foto: Ole Berg-Rusten/NTB

2026 er totalforsvarsåret. Målet er å styrke Norges evne til å forebygge og håndtere sikkerhetspolitiske kriser og krig. NSM oppfordrer virksomheter til å styrke egen sikkerhet, oppdatere beredskapsplaner, og ikke minst øve.

Totalforsvaret er summen av landets sivile og militære ressurser. Det handler om samarbeid og gjensidig støtte mellom Forsvaret og det sivile samfunnet for å ivareta nasjonens sikkerhet i fred, krise og krig. Totalforsvarskonseptet handler ikke bare om de sivile virksomhetene som understøtter Forsvaret direkte, men også alle virksomhetene som skal sørge for at samfunnet fungerer mest mulig normalt gjennom hele krisespekteret og i verste fall gjennom en krig.

Regjeringen har i den nasjonale sikkerhetsstrategien slått fast at vi må gjøre samfunnet mer motstandsdyktig. Dette har vi de beste forutsetninger for å lykkes med i Norge, men det krever innsats.

Både den sikkerhetspolitiske situasjonen og trusselbildet, som Etterretningstjenesten og Politiets sikkerhetstjeneste beskriver, er krevende. Trusselaktørene tar stadig større sjanser og metodene blir mer sofistikerte. For norske virksomheter holder det ikke å forstå trusselbildet. Det som skaper motstandsdyktighet er langsiktig og systematisk sikkerhetsarbeid. Iverksett konkrete tiltak for å beskytte deres viktigste verdier. Reduser konsekvenser av eventuelle ondsinnede handlinger som rammer dere. Etabler redundans og reserveløsninger.

Etterretningstjenesten understreker at Russland er forberedt på en varig konflikt med Vesten. Det er lett å føle på avmakt med et dystert trusselbilde, men det er det motsatte av dette som kreves nå. Selv om trusselbildet kan variere, er langsiktig forebyggende sikkerhetsarbeid helt avgjørende for et motstandsdyktig Norge.

Bruk Risiko 2026 til å drive god sikkerhetsstyring. Det er helt nødvendig at norske virksomheter har, eller får på plass, styringssystem som inkluderer organisatoriske, fysiske, tekniske og menneskelige tiltak. Det må følges opp med kontinuerlig forbedring gjennom opplæring, øvelser og ikke minst lærdommer fra hendelser, for å sikre at virksomheten oppnår et forsvarlig sikkerhetsnivå. Valgene dere tar i dag avgjør morgendagens risiko.

Arne Christian Haugstøyl
Direktør



Sammendrag

Forebyggende sikkerhetsarbeid er helt avgjørende i et omskiftelig trusselbilde. Der trusselnivået kan variere over tid, ligger behovet for risikoreduserende tiltak fast. Det er vesentlige mangler i det forebyggende sikkerhetsarbeidet til virksomheter i Norge. Disse sårbarhetene går igjen på tvers av sektorer. I Risiko 2026 beskriver NSM flere mangler virksomheter bør rette.

Kjenn dine verdier. Reduser sårbarheter. Bygg reserveløsninger. Konsekvensene av en uønsket hendelse kan bli de samme, enten årsaken er en trusselaktør eller en tilfeldig, teknisk eller menneskelig feil. Virksomheter må redusere risikoen for at hendelser setter dem og leveransene deres ut av spill. Videre må virksomheter ha god beredskap for reserveløsninger og reparasjon for å gjenopprette et forsvarlig sikkerhetsnivå i etterkant av en hendelse.

Norske virksomheter må holde fokus på verdier virksomheten rår over – det være seg objekter, infrastrukturer, informasjon eller informasjonssystemer. Verdiene er utgangspunktet for å identifisere og håndtere risiko. Sikkerhetsstyring er det viktigste verktøyet virksomheter har for å oppnå og opprettholde forsvarlig sikkerhet. Styringen må omfatte alle fagområder, fra digital og fysisk sikkerhet til personellsikkerhet og sikkerhetskultur. Sikkerhet er et lederansvar. Ivareta ansatte ved å sikre at de har nødvendig kunnskap om sitt sikkerhetsmessige ansvar.

NSM ser at cyberoperasjoner fortsatt rammer bredt. Både små og store virksomheter på tvers av ulike sektorer må være forberedt på å håndtere hendelser i cyberdomenet. Når trusselaktører kontinuerlig utvider sin verktøykasse, øker behovet for forebyggende tiltak som begrenser konsekvensene når en hendelse inntreffer. Digitalsikkerhetsloven skjerper kravene til digital sikkerhet for virksomheter i både offentlig og privat sektor. Virksomheter som er tilbydere av samfunnsviktige tjenester har varslingsplikt innen 24 timer ved alvorlige hendelser.

Dersom virksomheter er avhengige av en enkelt leverandør, eller leverandører fra samme land, oppstår det som kalles konsentrasjonsrisiko. Norske virksomheter er på flere samfunnsområder avhengig av produkter, teknologi og tjenester fra andre land. Fornybar energi, moderne kjøretøy og skytjenester er noen få eksempler. Det er ikke den enkelte anskaffelsen som er problemet, men det er det samlede omfanget som er en nasjonal utfordring. Trusselaktører kan bruke denne avhengigheten mot norske virksomheter. Fotfeste i det norske markedet kan blant annet utnyttes til å utøve politisk eller økonomisk press.



Et sammensatt risikobilde

Russlands fullskalainvasjon av Ukraina har endret sikkerhetssituasjonen i Europa betydelig. Samtidig driver teknologisk og samfunnsmessig utvikling fram nye risikoområder. Det sikkerhetspolitiske bildet skjerper kravene til beredskap og forebyggende sikkerhet i totalforsvaret. Norges nasjonale sikkerhetsstrategi setter felles retning for sikkerhetsarbeidet.

Norges rolle i det sikkerhetspolitiske bildet

Den sikkerhetspolitiske situasjonen har de seneste årene vært preget av vedvarende spenninger. Krig og konflikt rammer flere kontinenter. Stormaktsrivalisering, teknologisk utvikling og raske omveltninger setter de ytre rammene for risikobildet i 2026.

Forholdet mellom USA og Europa er i endring. Dette skaper usikkerhet innen både transatlantisk handel, og sikkerhets- og forsvarssamarbeid. Europeiske land må i større grad ta kostnaden av å ivareta sikkerhet og stabilitet på kontinentet. Endringer i amerikanske prioriteringer og NATO-landenes nye mål om å bruke fem prosent av brutto nasjonalprodukt på forsvar og sikkerhet, legger stort press på europeisk forsvarsindustri. Norsk forsvarsindustri har over tid bygd opp unik kompetanse og teknologi, blant annet innen kommandosystemer, autonome systemer, missilsystemer, undervannsteknologi og materialteknologi. Enkelte norske virksomheter er verdensledende på sitt område. Norges rolle som forsvarsleverandør til Ukraina medfører blant annet økt risiko for uønsket aktivitet i cyberdomenet.

Etterretningstjenesten vurderer at Russland fortsatt ønsker å gjennomføre operasjoner for å undergrave eller påvirke holdninger og beslutninger i europeiske land. Disse operasjonene kan bli flere, og mer alvorlige, dersom forholdet til Europa forverres. PST forventer at russiske etterretningstjenester i 2026 vil bruke et bredt spekter av virkemidler mot Norge. Dette inkluderer påvirkningsoperasjoner, cyberoperasjoner og rekruttering av menneskelige kilder. Sivile fartøy vil også benyttes for kartleggingsforsøk langs norskekysten. Eventuelle russiske sabotasjeforsøk i Norge vil mest sannsynlig rettes mot mål knyttet til støtte til Ukraina, men det kan også ramme sivil infrastruktur, ifølge PST.

PST trekker videre frem at Norge står overfor en betydelig etterretningstrussel fra Kina. Kinesiske sikkerhets- og etterretningstjenester har økt sine evner til å operere i Norge, både når det kommer til cyberoperasjoner og innhenting via menneskelige kilder. Ifølge Etterretningstjenesten øker Kina handlingsrommet mot europeiske land ved å utnytte kontrollen de har i verdikjeder for eksempel innen forsvarsindustri og det grønne skiftet. Virksomheter som inngår samarbeid med kinesiske selskaper trenger derfor en særlig årvåken tilnærming. Risikoreduserende tiltak må iverksettes på bakgrunn av konkrete risikovurderinger som tar hensyn til trusselbildet, verdier og sårbarheter.

Som følge av det sikkerhetspolitiske bildet må det norske totalforsvaret tilpasses nye rammebetingelser og endrede krav til beredskap og forebyggende sikkerhet. Norges første nasjonale sikkerhetsstrategi fra mai 2025 setter felles retning for sikkerhetsarbeidet. Tre prioriteringer er at Norge skal styrke forsvarsevnen og samtidig bidra til europeisk sikkerhet i rammen av NATO. Videre må samfunnet bli mer motstandsdyktig mot alvorlige trusler. I tillegg skal Norge styrke landets økonomiske sikkerhet gjennom økt konkurranseevne, reduserte sårbarheter og økonomisk samarbeid med allierte og partnere.

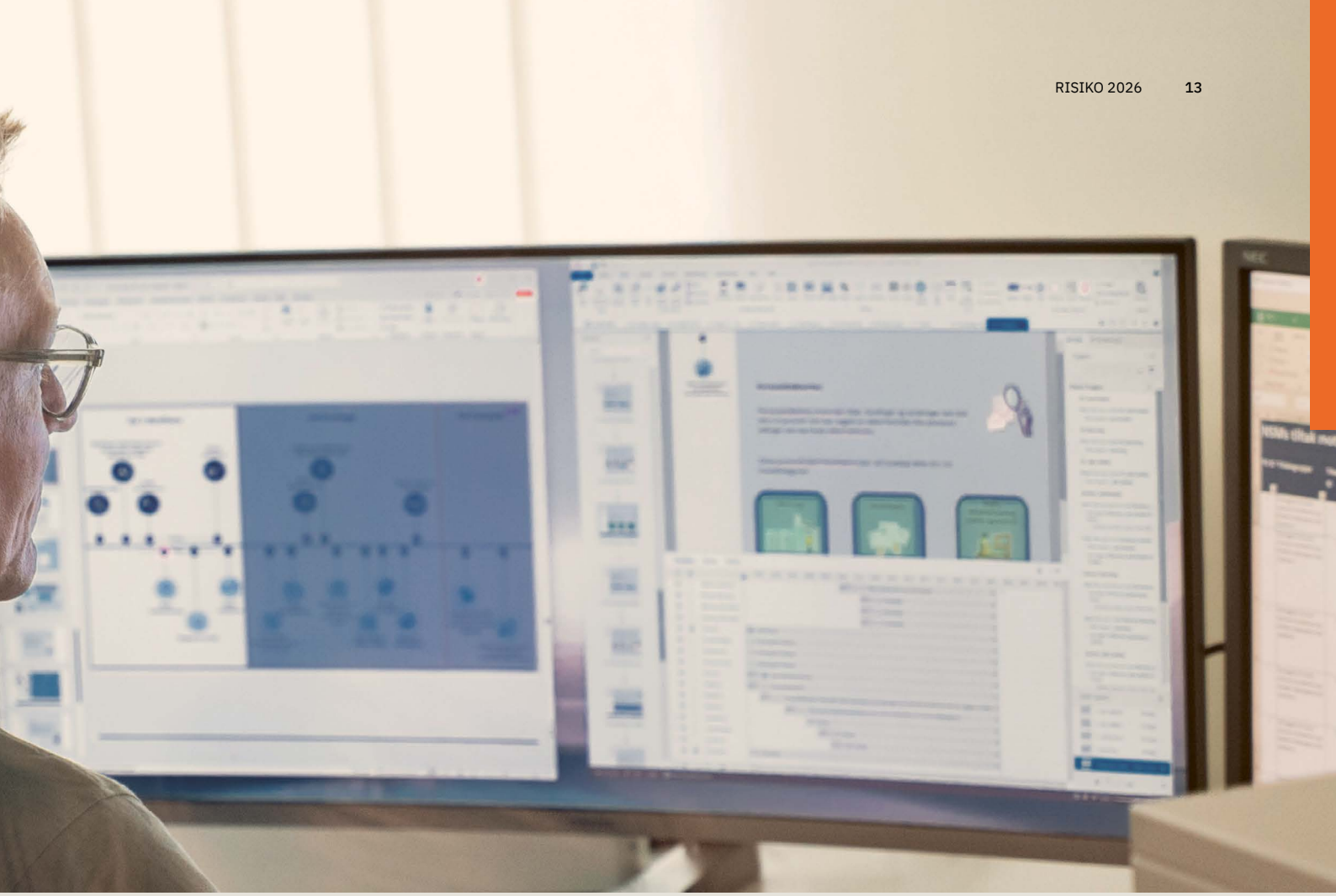

NORGE



Europeisk opprustning påvirker norske virksomheter

Den kraftige opptrappingen av både norsk og europeisk forsvarsevne medfører store og komplekse investeringer de neste årene. Når større deler av samfunnet understøtter forsvar og nasjonal sikkerhet, blir også flere virksomheter aktuelle mål for spionasje, sabotasje og sammensatte trusler. Det stiller strenge krav til sikkerheten i alt fra sivile underleverandører og administrative IKT-systemer til våpensystemer og kampmateriell. Det er derfor enda viktigere at både offentlige og private virksomheter prioriterer sikkerhet i utvikling, anskaffelser og drift, til tross for tidspress og krav om kostnadseffektivitet.

«Hvis du jobber innenfor avansert teknologi i dag så er du ikke nødvendigvis interessert i geopolitikk, men geopolitikk er definitivt interessert i deg», sa Ken McCallum, sjef for den britiske innenlands etterretnings- og sikkerhetstjenesten MI5 i 2023. Det gjelder fortsatt. En liten norsk bedrift som for eksempel produserer deler til forsvarsmateriell er ikke lenger bare en av mange underleverandører til Forsvaret, men en del av det europeiske opprustningsprosjektet.



Teknologisk utvikling skaper nye risikoområder

En rekke hendelser i 2025 bidro til å forsterke betydningen av teknologi som sikkerhetspolitisk drivkraft. Et eksempel er at kinesiske trusselaktører skal ha gjennomført den første cyberoperasjonen tilnærmet fullstendig orkestrert av kunstig intelligens (KI). Når ny teknologi blir tilgjengelig, åpner det for nye former for ondsinnet virkemiddelbruk – enten det er med mål om å påvirke, spionere eller sabotere. Utviklingen gir kompetente aktører flere muligheter til å gjennomføre cyberoperasjoner. Samtidig får også mindre kompetente aktører evne til å gjennomføre operasjoner som tidligere krevde høyere teknisk kompetanse. Både NSM og PST forventer at norske virksomheter i løpet av 2026 blir utsatt for cyberoperasjoner hvor KI-verktøy spiller en viktig rolle.

Norge blir stadig mer avhengig av teknologi fra noen få dominerende aktører – enten det er i nasjonale romprogram, fornybar energi eller skytjenester. Nye teknologiplattformer som kommersielle droner og moderne kjøretøy kommer ofte med omfattende, integrerte sensorsystemer som kan samle inn store mengder informasjon. Det er derfor viktig at norske virksomheter tenker gjennom hvordan de benytter slike teknologier. Det brede spekteret av åpne og fordekte virkemidler, som benyttes av land som Russland og Kina, krever at norske myndigheter og virksomheter har en helhetlig tilnærming til sikkerhet.

Forebyggende sikkerhetsarbeid

Virksomheter over hele landet forvalter verdier av betydning for Norges nasjonale sikkerhet. NSMs kontroller har avdekket flere mangler i sikkerheten til virksomheter underlagt sikkerhetsloven. Gjentatte utfordringer i ulike sektorer er beskrevet her for at virksomheter, enten de er underlagt sikkerhetsloven eller ikke, kan bruke dem til å forbedre det forebyggende sikkerhetsarbeidet i egen virksomhet.

Sikkerhetsstyring styrker nasjonal sikkerhet

Sikkerhetsstyring er virksomheters viktigste verktøy for å oppnå og opprettholde forsvarlig sikkerhet. Dette handler om de aktivitetene som er nødvendige for å beskytte virksomheters verdier mot uønskede hendelser. For å oppnå forsvarlig sikkerhet må virksomhetene ha oversikt over verdiene sine og være kjent med hvilke avhengigheter, sårbarheter og trusler som påvirker disse. Virksomhetsledere har ansvaret for sikkerhetsstyringen, og må derfor legge til rette for, og følge opp, at virksomhetene sikrer sine verdier godt nok. Et godt sikkerhetsarbeid gjør virksomhetene mer motstandsdyktige, samtidig som det bidrar til å styrke nasjonal sikkerhet.

NSM gjør jevnlig tilsyn av virksomheter underlagt sikkerhetsloven. Dessverre viser tilsyn mangler i virksomheters styringssystemer for sikkerhet. Enkelte funn går igjen i flere sektorer. En utfordring NSM altfor ofte ser er at virksomheters ansatte er blitt tildelt roller i sikkerhetsarbeidet som de enten ikke er klar over eller har ressurser og kompetanse til å ivareta. Resultatet er at sikkerhetsarbeidet ikke blir godt nok fulgt opp. Konsekvenser kan være at avvik og sikkerhetstruende virksomhet heller ikke blir identifisert og rapportert, slik at nødvendige tiltak ikke blir iverksatt.

Virksomheter har gjerne etablert grunnsikringstiltak, det vil si tiltak som skal bidra til et forsvarlig sikkerhetsnivå i en normaltilstand. NSM har gjennom tilsyn avdekket at virksomheter i mange tilfeller ikke har gjennomført tester, kontroller eller øvelser av sikkerhetstiltakene. Det er viktig å sjekke at tiltakene fungerer som tiltenkt, og at de blir korrekt iverksatt dersom en hendelse skulle oppstå.

Virksomheter underlagt sikkerhetsloven skal i tillegg til grunnsikring, også planlegge og forberede påbyggingstiltak som raskt kan iverksettes dersom risikonivået øker. Eksempel på påbyggingstiltak kan være skjerpet adgangskontroll, større sikkerhetssone rundt bygninger og aktivering av midlertidige reserveløsninger for å redusere konsekvenser ved en uønsket hendelse. NSMs funn viser imidlertid at virksomhetene ofte mangler slike planer. Det er alvorlig når sikkerhetspolitisk uro og usikkerhet kan endre risikobildet raskt.

Dersom en uønsket hendelse inntreffer er det viktig at det er utarbeidet beredskapsplaner for å håndtere hendelsen og for å gjenopprette et forsvarlig sikkerhetsnivå i etterkant av hendelsen. Dette innebærer blant annet å identifisere og beskrive hvilke eksterne ressurser virksomheter trenger støtte fra – og koordinere med disse i forkant, under og etter en hendelse.



Verdier, avhengigheter og forsvarlig sikkerhet

Verdier kan være informasjon som forretningshemmeligheter eller kundelister som virksomheter ikke ønsker å dele med andre. Virksomheter underlagt sikkerhetsloven har ansvar for å beskytte informasjon, informasjonssystemer, objekter eller infrastruktur som kan ha betydning for nasjonale sikkerhetsinteresser.

Avhengigheter kan omfatte andre virksomheter, funksjoner eller tjenester en virksomhet er avhengig av for å kunne fungere.

Forsvarlig sikkerhet innebærer at virksomheter gjennom systematisk sikkerhetsstyring og risikovurderte tiltak beskytter skjermingsverdige verdier mot sikkerhetstruende virksomhet, i tråd med kravene i sikkerhetsloven og forskriftene.

Anbefalinger til virksomheter for å styrke sikkerhetsstyringen

- Sørg for at sikkerhetsstyringen er integrert i virksomhetens overordnede styringssystem.
- Hold oppdatert oversikt over verdier og avhengigheter samt sårbarheter og trusler som påvirker disse verdiene.
- Ha tydelige beskrivelser av ansattes roller, ansvar og myndighet innen sikkerhet, og sørg for at disse er godt kjent i virksomheten.
- Gå jevnlig gjennom sikkerhetstiltakene og bruk øvelser til å sjekke at de er hensiktsmessige.
- Planlegg påbyggingstiltak og tiltak som reduserer skadefølgene ved en uønsket hendelse, og øv også på disse tiltakene.
- Gjennomfør jevnlig risikovurderinger slik at sikkerhetstiltakene er tilpasset trussel- og risikobildet.
- Gjør dere kjent med ressurser for tester og øvelser, som NSMs cybersjekk.no, DSBs øvingsbank på dsb.no/ovelser samt diskusjons- og spilløvelser hos sektormyndigheter.


BØRSEN
TILBYGGET
1909-1910
2

Gode rutiner for sikkerhetsmessig ledelse og personellsikkerhet er avgjørende

NSM har gjentatte ganger observert at svakheter ved personellsikkerhetsarbeidet i norske virksomheter har ført til økt risiko for innsidere og tap av verdier. Dette skyldes ofte mangelfull kompetanse om personellsikkerhet, mangler ved sikkerhetsmessig ledelse av personellet og svakheter i den interne kommunikasjonen om ansattes sårbarheter og håndtering av disse.

Sikkerhetsmessig ledelse bidrar til å redusere, avdekke og håndtere innsiderisiko, og består av en rekke tiltak som dialog, håndtering av sårbarheter, opplæring og holdningsskapende arbeid. Sikkerhetsloven pålegger virksomheter oppgaver knyttet til autorisasjon og oppfølging av ansatte. Selve autorisasjonsprosessen skal bidra til tillitsbygging mellom autorisasjonsansvarlig og den autoriserte.

En forutsetning for god personellsikkerhet er både god ledelse og sikkerhetskultur. Ledere har et stort ansvar for at ansatte har kunnskap om hvilket sikkerhetsmessig ansvar de har. En viktig del av dette er å gi ansatte trygghet til å si ifra om egne sårbarheter og eventuelle feil de har gjort. På denne måten hindrer ledelsen at sårbarheter hos den enkelte får utvikle seg. Økonomiske utfordringer og tilknytning til land som PST mener utgjør en etterretningstrussel mot Norge, er eksempler på personellsikkerhetsmessige sårbarheter. Disse kan utvikle seg over tid uten god nok oppfølging, og kan gi økt risiko for innsidevirksomhet.

Mangelfull kommunikasjon internt om forhold som påvirker autorisert personell kan også føre til utfordringer. Flere enheter i en virksomhet, som HR- eller økonomiavdelingen, kan ha viktig informasjon som autorisasjonsansvarlig trenger for å vurdere den enkeltes sikkerhetsmessige skikkethet og autorisasjon. Tydelige rutiner og prosedyrer for intern utveksling av relevant informasjon tar bort usikkerhet og uklare ansvarsforhold når det gjelder å følge opp sårbarheter hos de ansatte og hendelser i virksomheten.

Rekruttering av kilder

PST vurderer at rekruttering av kilder er en sentral del av fremmede staters etterretningsvirksomhet i Norge. Personell med tilgang til sensitiv eller gradert informasjon er spesielt utsatte. Russland og Kina har økt bruken av digitale kanaler som sosiale medier for rekruttering, men benytter også fysiske metoder som etterretningsoffiserer under diplomatisk dekke.

Personellsikkerhet

Personellsikkerhet bidrar til å håndtere risikoen som oppstår når mennesker er involvert i produksjon, håndtering og beskyttelse av virksomhetens verdier. Personellsikkerhets-tiltakene gjør ansatte mer robuste, og bidrar til at de forstår egen rolle i sikkerhetsarbeidet og beskyttelse av virksomhetens verdier.



Betydningen av god sikkerhetsmessig ledelse

Hvorfor er egentlig sikkerhetsmessig ledelse så viktig? NSM har satt sammen et fiktivt scenario basert på enkeltsaker i personellsikkerhet for å illustrere kjente problemstillinger.

«Ola Nordmann» er ansatt i en virksomhet underlagt sikkerhetsloven, og blir samboer med en person fra et land som PST vurderer at utgjør en høy etterretningstrussel mot Norge. «Ola» er klarert og autorisert for nivå HEMMELIG, og arbeider med sensitive fagområder av stor interesse for landet samboeren kommer fra. Virksomheten har imidlertid ikke bevisstgjort de ansatte om risikoen en slik relasjon kan medføre, eller etablert klare rutiner for å melde fra om relevante sikkerhetsforhold. Etablering av samboerskap er et forhold som «Ola» skal varsle autorisasjonsansvarlig om. Det gjør han ikke.

«Ola» introduseres for samboerens venner fra hjemlandet. En av disse viser seg å være spesialist innen samme fagområde som «Ola». Etter en tid inviteres «Ola» til et samarbeid, og blir spurt om å holde et foredrag i utlandet. «Ola» ser på dette som en mulighet til å utvide eget kontaktnett og reiser til utlandet hvor han treffer flere som er interesserte i arbeidet hans.

Vel hjemme forteller «Ola» om reisen til kollegaer. Først da ringer varselklokkene hos autorisasjons-ansvarlig. Hva betyr denne interessen for «Ola» og hans arbeid? Er det tilfeldig, eller er det fremmede etterretningstjenester som viser interesse for «Ola» og arbeidet hans?

Både virksomheten og «Ola» står nå i en krevende og uoversiktlig situasjon. Denne kunne trolig vært unngått dersom personellsikkerhet hadde vært en tydelig del av virksomhetens styringssystem, og den enkeltes ansvar og plikter hadde blitt fulgt opp gjennom bevisstgjøring og god sikkerhetsmessig ledelse. Relevante momenter ville vært:

- at «Ola» er av interesse for utenlandsk etterretningstjeneste
- betydningen av samboerens tilknytning til høyrisikoland
- risiko for eksponering av eget arbeid
- metodene til fremmede etterretningstjenester
- hvilke sikkerhetsmessige relevante forhold som skal varsles til den autorisasjonsansvarlige



Anbefalinger til virksomheter for å styrke arbeidet med personellsikkerhet

- Fokuser på god kompetanse om personell-sikkerhet i virksomheten.
- Gjør dere kjent med NSMs håndbok i autorisasjon og NSMs grunnprinsipper i personellsikkerhet.
- Gjør autorisasjonskurs obligatorisk for alle som har et ansvar knyttet til autorisasjon og sikkerhetsmessig ledelse av personell. Sivil klareringsmyndighet (SKM) tilbyr kurs for virksomheter underlagt sikkerhetsloven.
- Integrer personellsikkerhet i styringssystemet for sikkerhet. Styringssystemet bør inkludere hvordan informasjon om enkeltpersoners sårbarheter internt i virksomheten skal formidles og behandles på tvers av organisatoriske skiller eller rollefordelinger.
- Ledere må legge til rette for en kultur som bygger tillit mellom ansatte og autorisasjonsansvarlige.
- Bevisstgjør ansatte om virksomhetens verdier, og tydeliggjør hvilken informasjon som kan deles internt og eksternt.
- Sørg for at alle i virksomheten er klar over plikten til å varsle om forhold som kan påvirke sikkerhetsmessig skikkethet.

Fysisk sikring må tilpasses trussel- og risikobildet

Dersom en virksomhet oppdager fysiske sårbarheter, er det viktig at de straks iverksetter tiltak for å utbedre dette, eller etablerer kompenserende tiltak frem til utbedringen er på plass. Grunnsikring, påbyggingstiltak, skadebegrensning og gjenoppretting bør være en del av virksomheters fysiske sikkerhet. Ifølge PST kan russisk etterretning se seg tjent med å utføre sabotasjeaksjoner mot mål i Norge i 2026. Eiendom og logistikkinfrastruktur knyttet til støtte til Ukraina, samt sivil infrastruktur, trekkes frem som mest sannsynlige mål for slike aksjoner.

Verdier kan tilsynelatende være godt sikret, men dersom sikkerhetstiltakene ikke er oppdatert og tilpasset aktuelle trusler, er ikke forsvarlig sikkerhet oppnådd. Dette gjelder også dersom det er innført sikkerhetstiltak som ikke er basert på en helhetlig risikovurdering. For at fysiske sikkerhetstiltak skal være effektive må tiltakene være tilpasset dagens trussel- og risikobilde.

NSM har gjentatte ganger oppdaget svakheter i virksomheters fysiske sikkerhetstiltak. Det gjelder blant annet rom eller lokaler og rutiner for gradert tale samt beskrivelse av funksjon og begrensninger for alarmanlegg og kameraovervåkning. I tillegg er det oppdaget svakheter knyttet til tidsregnskap for tilgang til virksomheters sikkerhetsgraderte informasjon. Tiden det tar for en virksomhet å detektere, verifisere og reagere på en hendelse må være kortere enn tiden det tar for en trusselaktør å få tilgang til verdiene.

For å oppnå forsvarlig sikkerhet må de ulike sikkerhetstiltakene ses i forhold til hverandre. Ofte er det gjensidige avhengigheter mellom ulike tiltaksområder. God digital sikkerhet alene er for eksempel ikke tilstrekkelig dersom de fysiske sikkerhetstiltakene er mangelfulle. I tillegg blir fysiske sikkerhetstiltak, i likhet med digitale, utdaterte og mindre motstandsdyktige ettersom trusselaktørene stadig utvikler nye og mer effektive verktøy og teknikker.

Synlige adgangskort utenfor virksomheten

Dersom adgangskort er synlige utenfor virksomheten reduseres effekten av slike kort som sikkerhetstiltak. Trusselaktører som får kjennskap til adgangskort og deres utforming kan med enkle midler lage falske kopier av kortene, og benytte dem for å få fysisk adgang til virksomheten.

Luftbårne droner utfordrer virksomheters fysiske sikkerhet

Luftbårne droner er blitt allemannseie. De er mobile, lett tilgjengelige, meget utberedt og kan opereres med en grad av anonymitet, noe som kan utfordre virksomheters fysiske sikkerhet og drift. Droner kan benyttes til flere ulike formål:

- Informasjon kan innhentes ved å ta bilder, filme eller på annen måte kartlegge objekter, infrastruktur, rutiner, signaler og bevegelse.
- Kartlegging og responstesting av kapasitet kan for eksempel foregå ved å skape en hendelse og observere reaksjonen.
- Påvirkning ved å skape usikkerhet og frykt.
- Droner kan også benyttes til anslag; enten ved å bruke dronen som våpen, videre ved å slippe, avfyre eller plassere våpen, eller ved å forstyrre virksomhetenes drift.

Alle som eier eller forvalter skjermingsverdige verdier må identifisere hvilken risiko droner utgjør, og iverksette tiltak som skjermer og beskytter disse verdiene mot uønskede hendelser.



Synne Nilsson / Forsvaret

Dronedeteksjonssystemer

Etterretningstjenesten og PST rapporterer at fremmede etterretningstjenester har intensjon og kapabilitet til å gjennomføre avanserte etterretningsoperasjoner mot norske verdier. Dronedeteksjonssystemer er effektive for å avdekke og håndtere uønsket droneaktivitet, men dronedeteksjonssystemer med sensorer utplassert nær skjermingsverdige verdier kan ha sårbarheter som kan utnyttes av ondsinnede aktører.

For noen virksomheter er dronedeteksjonssystemet avgjørende for sikker drift. Manipulasjon eller bortfall av systemet kan få omfattende konsekvenser. Virksomheter underlagt sikkerhetsloven må i slike tilfeller vurdere hvordan de kan oppnå og ivareta et forsvarlig sikkerhetsnivå.

Selv om systemet ikke er av avgjørende betydning for virksomhetens drift, kan det fortsatt utgjøre en sårbarhet som trusselaktører kan utnytte dersom systemet innhenter skjermingsverdig informasjon fra omgivelsene. Ved utplassering av dronedeteksjonssystemer bør både systemeier og berørte virksomheter ta høyde for dette i sine risikovurderinger. Om man er usikker bør NSM kontaktes for å bistå i vurderingen.

Anbefalinger til virksomheter for å styrke den fysiske sikkerheten

- Gjennomfør risikovurderinger og etabler mål for den fysiske sikringen.
- Gi tilstrekkelig prioritet og ressurser til arbeidet med fysisk sikkerhet.
- Gjør dere kjent med NSMs veileder og grunnprinsipper for fysisk sikkerhet.
- Kombiner flere fysiske sikringslag som ytre barrierer, adgangskontroll, alarm og indre låser for å forlenge tiden det tar for uvedkommende å få tilgang til verdiene.
- Ha prosedyrer og ressurser for deteksjon, reaksjon og håndtering av sannsynlige sikkerhetstruende hendelser.
- Gjennomfør tester av virksomhetens fysiske sikkerhetstiltak regelmessig. NSM kan på forespørsel gjennomføre fysiske inntrengingstester i virksomheter underlagt sikkerhetsloven.



Viktigheten av innsikt i eierstrukturen

Et oppkjøp av en virksomhet, anskaffelser eller andre økonomiske virkemidler kan gi tilganger og rettigheter til å påvirke viktige verdier. Sikkerhetstruende økonomisk virksomhet omfatter alle økonomiske transaksjoner som enten direkte eller indirekte kan medføre en risiko for at nasjonale sikkerhetsinteresser blir truet.

NSM er nasjonalt kontaktpunkt for varsler om sikkerhetstruende økonomisk virksomhet. Flere av henvendelsene NSM har mottatt i 2025 gjelder Private Equity-fond. Slike fond investerer ofte i sektorer der forvalter av fondet har spesialisert kompetanse, og hvor målet er å restrukturere og optimalisere selskaper for å øke verdien av selskapet. Eierstrukturer i slike fond kan være uoversiktlige. Private Equity-fond i seg selv er ikke en indikator på sikkerhetstruende virksomhet, men utilstrekkelig informasjon om eierstrukturer og reelle rettighetshavere gjør det vanskeligere å avdekke hvem som har innflytelse over selskapet. Reelle rettighetshavere vil alltid være fysiske personer.

For å unngå uønsket påvirkning eller teknologioverføring er det viktig å være klar over hvem som har innflytelse over selskapet. Eiere kan påvirke virksomhetens strategi og beslutninger, noe som kan tilrettelegge for sikkerhetstruende aktivitet innen eksempelvis cyberdomenet, fysisk sikkerhet og personellsikkerhet. Virksomheter bør derfor kartlegge hvem som har reell innflytelse. Dersom det ikke lar seg gjøre, bør virksomheten vurdere kompenserende tiltak.

Eierskapskontroll i sikkerhetsloven

Sikkerhetsloven kapittel 10 om eierskapskontroll er et verktøy for å kontrollere eierskapet i virksomheter som er av betydning for nasjonale sikkerhetsinteresser. Kontrollen skal hindre at slike virksomheter kommer i hendene på aktører som kan utgjøre en sikkerhetstrussel. Det er meldeplikt ved oppkjøp av kvalifiserte eierandeler. Også andre forhold som kan gi betydelig innflytelse over en virksomhet kan utløse meldeplikt.



Rapport om skjult eierskap i Norge

Norge har et register for reelle rettighetshavere for å motvirke hvitvasking, terrorfinansiering og økonomisk kriminalitet. Rapporteringspliktige virksomheter hadde frist til 31. juli 2025 for å registrere seg. En undersøkelse utført av Tax Justice Norge i 2025 viste at registeret inneholder et stort antall ufullstendige registreringer som kan redusere påliteligheten av dataene. Videre kan begrensninger i tilgangen og brukervennligheten i registeret bidra til å svekke formålet om åpenhet. Rapporten belyser momenter i eierskapsstrukturer som kan være relevant i et sikkerhetsperspektiv.

Kilde: Tax Justice Norge. 2025. Skjult eierskap i Norge – Analyse av det nye eierregisteret.

Anbefalinger til virksomheter for motvirkning av sikkerhetstruende økonomisk virkemiddelbruk

- Virksomheter underlagt sikkerhetsloven må gjøre seg kjent med kapittel 10 i sikkerhetsloven om eierskapskontroll og med eierskapskontroll-forskriften.
- Søk informasjon og bygg kompetanse for å kunne vurdere om økonomiske transaksjoner kan utgjøre en risiko for nasjonal sikkerhet.
- Hold oversikt over økonomiske bindinger og gjør jevnlige vurderinger av hvilken risiko disse kan medføre.
- Hvis det er usikkerhet om hvem som er reelle rettighetshavere, bør virksomheten innføre risikoreduserende tiltak.

Det digitale risikobildet

Cyberoperasjoner rammer fortsatt bredt i det norske samfunnet. Både små og store virksomheter på tvers av ulike samfunnssektorer må bygge motstandsdyktighet mot digitale angrep. Det handler om å være godt rustet, både teknisk og organisatorisk, for å håndtere trusselaktører som stadig blir mer sofistikerte. Digitalsikkerhetsloven skjerper kravene til digital sikkerhet for flere virksomheter.

Trender i cyberdomenet det siste året

Mange av cyberhendelsene NSM har observert i 2025 er knyttet til sosial manipulasjon, slik som phishing. NSM ser økende bruk av mer avanserte former for phishing der flerfaktorautentisering ikke lenger gir tilstrekkelig beskyttelse. Trusselaktører benytter stadig mer sofistikerte teknikker for å framstå som legitime avsendere, ofte gjennom e-post, tekstmeldinger eller meldinger på sosiale medier. Formålet er som regel å manipulere mottakeren til å avsløre sensitiv informasjon, gi tilgang til systemer eller installere skadelig programvare. En tydelig utvikling globalt er bruken av kunstig intelligens som støtteverktøy i slike kampanjer, blant annet for å generere mer overbevisende og målrettet innhold.

Løsepengeangrep er en av de mest utbredte angrepsmetodene mot norske virksomheter. Skadepotensialet er stort fordi angrepene blir stadig mer sofistikerte. Angripere bruker avanserte metoder for å få tilgang til virksomheters data, noe som kan føre til tap av sensitiv eller skjermingsverdig informasjon. I tillegg er det ved flere tilfeller observert såkalt «dobbelt utpressing», der angriperne ikke bare krypterer data, men også truer med å offentliggjøre sensitiv informasjon dersom løsepenger ikke betales.

Løsepengeangrep mot en norsk tjenesteleverandør

En norsk tjenesteleverandør ble i 2025 rammet av et løsepengeangrep der en større mengde data fra bedriftens kvalitets- og virksomhetssystem ble hentet ut. Det samme systemet benyttes av en rekke offentlige og private kunder, også flere som er omfattet av sikkerhetsloven. Et angrep mot en tjenesteleverandør kan få betydelige konsekvenser for kundene, spesielt ved hendelser der sensitiv eller skjermingsverdig informasjon kommer på avveie. Dette viser hvor viktig det er å vurdere hvilken informasjon som blir lagt i et system som driftes av en tredjepart. Kompromittert informasjon kan potensielt benyttes til videresalg på det mørke nettet, til dobbelt utpressing eller i framtidige cyberoperasjoner.


NSM



NSM gjennomførte i 2025 flere inntrengingstester i statlige virksomheters kontorsystemer. I de aller fleste tilfellene fikk NSM fullstendig kontroll over virksomhetens informasjonssystem. Flere av de samme sårbarhetene gikk igjen på tvers av virksomheter og sektorer. Det var blant annet manglende eller ingen segmentering av roller, svake administratorpassord, bred gjenbruk av passord for lokaladministratorer og svakheter i oppsett av sertifikater og infrastruktur for sertifikater. I flere tilfeller gjorde virksomhetenes mangel på applikasjonskontroll det mulig for NSM å gjennomføre angrep mot virksomhetens IT-systemer. NSM utfører kun tester etter anmodning fra virksomheter som er underlagt sikkerhetsloven.



Cybersjekk.no

Cybersjekk fra NSM gir virksomheter et raskt overblikk over virksomhetens sikkerhetstilstand og følger opp med konkrete tiltak for å bedre sikkerhetsnivået ytterligere. Alle virksomheter har ansvar for den digitale sikkerheten hos seg selv. Cybersjekk er tilgjengelig for alle norske virksomheter, og bidrar til å bedre sikkerheten mot både cyberkriminalitet og cyberoperasjoner. Test tjenesten på cybersjekk.no.

- Det er mulig å svare på hele eller deler av sjekken og få anbefalinger knyttet til disse delene. Cybersjekk kan også benyttes gjentatte ganger. Etter hvert som virksomheter får på plass sentrale sikkerhetstiltak, vil de få forslag til tiltak som forsterker sikkerheten ytterligere.
- Cybersjekk bygger på grunnprinsippene for IKT-sikkerhet og ytterligere digitale råd fra NSM.
- NSMs grunnprinsipper for IKT-sikkerhet er tiltak for å beskytte informasjonssystemer mot uautorisert tilgang, skade eller misbruk. Tiltakene tar for seg kartlegging og beskyttelse av egne systemer, og tiltak for å oppdage og håndtere hendelser.

Slik fungerer tjenesten

- Spørsmålene er organisert i 11 kategorier.
- Virksomheter kan velge å svare på alle eller utvalgte kategorier.
- Virksomhetene får forslag til de viktigste tiltakene for virksomheten å innføre basert på svarene de har oppgitt.
- En del av kategoriene krever en viss kjennskap til oppbygging og forvaltning av virksomhetens IKT-systemer, og kan være lettere å besvare med hjelp fra en IKT-ansvarlig eller IKT-sikkerhetsansvarlig.
- Første kategori handler om ledelse, og NSM oppfordrer ledere til å svare her. Dersom de ikke kan svaret, er det et svar i seg selv. Sikkerhet er et lederansvar.
- Virksomhetens opplysninger forlater aldri datamaskinen som brukes for å gjøre undersøkelsen. Dette gjør det enklere for virksomheten å holde oversikt over hvor deres egne opplysninger blir av.

Operasjonell teknologi som del av angrepsflaten

Operasjonell teknologi (OT) utgjør den digitale ryggraden i noen av samfunnets viktigste prosesser, som styring av kraftproduksjon, vann- og avløpssystemer, transportsystemer og industriproduksjon. Cyberoperasjoner som rammer OT og industrielle styringssystemer kan sette sentrale produksjonsprosesser ut av spill. I ytterste konsekvens kan slike angrep føre til alvorlige ulykker, driftsstans eller hindre leveranser som samfunnet er helt avhengig av.

I motsetning til informasjonsteknologi (IT), som i hovedsak dreier seg om behandling av informasjon, handler OT om styring av fysiske prosesser og funksjoner. Mange OT-systemer er bygget på teknologi som en gang ble designet uten fokus på cybersikkerhet. Disse har ofte vært i drift i mange tiår. Når disse systemene eksponeres for internett eller integreres med moderne IT-systemer, åpner det for en rekke sårbarheter. Angrepsflater oppstår ofte gjennom fjernaksess, utilstrekkelig segmentering mellom IT og OT, manglende logging og overvåking eller manglende oppdatering av programvare.

Tjenestenektangrep mot IT-systemer kan indirekte påvirke OT-systemer. Enten kan tilgangen på kritiske IT-systemer som vedlikeholdssystemer og prosedyrer bli utilgjengelige, eller så kan OT-systemer rammes direkte hvilket kan føre til prosessforstyrrelser eller produksjonsstans. Mange OT-systemer er ikke motstandsdyktige mot tjenestenektangrep. Samtidig krever denne typen angrep tilnærmet ingen teknisk kompetanse hos trusselaktøren, og kan utføres av omtrent hvem som helst. Det kan også kjøpes som en tjeneste fra en tredjepart for en lav kostnad. Tjenestenektangrep handler gjerne om oppmerksomhet snarere enn å påføre skade, men kan likevel få alvorlige konsekvenser.

Norge innførte digitalsikkerhetsloven i oktober 2025 for å styrke det helhetlige arbeidet med digital sikkerhet i både offentlig og privat sektor. Loven gjelder for en del offentlige og private tilbydere av samfunnsviktige tjenester innenfor områdene energi, transport, helse, vannforsyning, bank og finansmarkedsinfrastruktur og digital infrastruktur. Loven gjelder ikke bare tradisjonelle IT-systemer, men omfatter også operasjonell teknologi. Dette innebærer at OT-sikkerhet må inngå i det helhetlige digitalsikkerhetsarbeidet på lik linje med øvrige digitale systemer.

Cyberoperasjon mot et norsk damanlegg

I mai 2025 oppfordret NSM norske virksomheter om å styrke egen sikkerhet på bakgrunn av observert aktivitet mot OT-systemer tilknyttet digital infrastruktur i Norge. Eksempelvis ble et av OT-systemene til et damanlegg i Bremanger i 2025 utsatt for en cyberoperasjon. NSM delte oppfordringen åpent for at også virksomheter som ikke er underlagt sikkerhetsloven skulle kunne iverksette tiltak.

Ifølge PST gjennomførte en pro-russisk hacktivistgruppe cyberoperasjonen i Bremanger. Gruppen fikk tilgang til et kontrollpanel gjennom fjernaksess og skal ha gjort endringer på innstillingene i systemet. Hendelsen førte til at ventilene i damanlegget stod åpne i fire timer og slapp ut omkring 500 liter vann i sekundet. Utover dette fikk hendelsen tilsynelatende begrensede fysiske og økonomiske konsekvenser. Slike cyberoperasjoner kan imidlertid få alvorlige konsekvenser dersom infrastrukturen som rammes har betydning for samfunnsviktige leveranser.



Hvordan varsle om hendelser etter digitalsikkerhetsloven?

Virksomheter, enten de tilbyr samfunnsviktige tjenester eller digitale tjenester, skal varsle myndighetene om hendelser som virker betydelig inn på leveransen. Slike hendelser kalles gjerne alvorlige hendelser.

Tilbyder skal, uten unødig opphold og uten hinder av taushetsplikt, varsle om hendelser som virker betydelig inn på tjenesteleveransen. Loven avgrenser dette til hendelser med negativ virkning på sikkerheten i nettverk og informasjonssystemer. Årsaken til hendelsen er uten betydning. Den er heller ikke avgrenset til cyberdomenet.

Det er utarbeidet et eget varslingsskjema som virksomhetene kan benytte. Dette er tilgjengelig på nsm.no. Alle tilbydere skal varsle tilsynsmyndigheten i egen sektor med kopi til NSM.

Tilbydere av samfunnsviktige tjenester har disse fristene for å varsle og følge opp varsler:

- **første varsel** innen 24 timer etter at virksomheten oppdaget hendelsen
- **oppdatering til myndighetene** innen 72 timer etter at virksomheten oppdaget hendelsen
- **hendelsesrapport** innen én måned etter at det første varselet ble sendt

Fristene er absolutte og gjelder også hvis hendelsen skjer hos en samarbeidspartner eller underleverandør. Virksomheter som tilbyr samfunnsviktige tjenester skal registrere at de tilbyr slike tjenester hos NSM og sektortilsynsmyndighet.



Bruk av usikker protokoll er utbredt

NSM observerer at bruken av den usikre protokollen *HTTP* for overføring av informasjon over internett fortsatt er utbredt blant norske virksomheter. Informasjon som sendes over slike ukrypterte protokoller kan leses av trusselaktører og andre. Usikker bruk av *HTTP* gjør det mulig for en såkalt angriper-i-midten å angripe både tjenesteleverandør og brukere av tjenesten. Selv i 2026 blir denne protokollen fortsatt benyttet til utvikling av tjenester og applikasjoner.

NSM har tidligere observert at brukernavn, passord og personopplysninger som navn og adresser er overført ukryptert til og fra virksomheter. NSM vurderer at det er en betydelig sårbarhet knyttet til det å sende data i klartekst over internett fordi informasjonen kan fanges opp og leses av trusselaktører. Uten bruk av kryptering er dataene sårbare for avlytting, manipulasjon og misbruk. Uavhengig av om kryptering er tatt i bruk, er det risiko knyttet til det å la tredjeparter få tilgang til informasjon om lokasjoner, interesseområder og bevegelser.

Sensitiv posisjonsdata sendt ukryptert over internett

NSM varslet høsten 2025 flere virksomheter om at de sender sensitiv posisjonsdata ukryptert over internett. NSMs funn viste at avanserte aktører kan få tilgang til geografiske koordinater som kan indikere posisjonen til brukernes enheter. Informasjonen om hvor enhetene befinner seg kan også bli eksponert gjennom oppslag av kartdata knyttet til svært avgrensede geografiske områder. Tjenester som vær- og kartoppslag er omfattet.

Kjente sårbarheter i nettverksutstyr blir utnyttet

Overvåking av egne systemer er essensielt for å kunne avdekke uvanlig eller mistenkelig aktivitet. Cyberoperasjoner gjennomført av kinesiske trusselaktører de siste årene har tydeliggjort at denne typen overvåking er nødvendig. Operasjonene følger et mønster hvor aktørene utnytter kjente sårbarheter i nettverksutstyr, får innpass i systemene og skjuler seg der over tid. På kort sikt får aktørene hentet ut store mengder informasjon, som for eksempel kommunikasjonsdata og driftsrutiner. På lengre sikt kan kinesiske trusselaktører kartlegge og etablere fotfeste i den kompromitterte infrastrukturen. På denne måten kan tilgangene benyttes til å forstyrre eller lamme tjenester ved en eventuell senere politisk eller militær konflikt. Tidlig avdekking av slike operasjoner er avgjørende for å kunne iverksette nødvendige tiltak.

Kinesiske trusselaktører skal ha kompromittert nettverk i nær 80 land

Salt Typhoon er en antatt kinesisk trusselaktør som har kompromittert nettverksenheter i USA og en rekke andre land gjennom en omfattende cyberoperasjon. Amerikanske myndigheter og internasjonale partnere beskriver operasjonen som en koordinert kampanje der angriperne har fått tilgang til nettverk, særlig innen telekommunikasjon, transport, forsvar og andre samfunnsviktige sektorer. FBI anslår at mer enn 200 amerikanske organisasjoner og nær 80 land ble berørt. Det er også observert aktivitet fra infrastruktur tilknyttet aktøren mot norske nettverksenheter.

Kilde: CISA, m.fl. 2025. Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System.

Anbefalinger til virksomheter for å redusere risikoen for cyberoperasjoner

- Reduser unødvendig eksponering av egen digital infrastruktur mot internett.
- Etabler forsvarlig segmentering mellom infrastruktur med OT og infrastruktur med IT.
- OT-infrastruktur bør i minst mulig grad være eksponert mot internett.
- Skift ut nettverksutstyr, servere og utstyr for sluttbrukere som ikke lenger mottar sikkerhetsoppgraderinger.
- Etabler en fast rutine for å regelmessig identifisere og lukke kjente tekniske sårbarheter som aktivt utnyttes.
- Bruk sikre overføringsprotokoller for å unngå at informasjon sendes i klartekst over internett.
- Etabler overvåking av egne systemer for å kunne avdekke uvanlig eller mistenkelig aktivitet. Logger må lagres sikkert og tilstrekkelig lenge slik at analyse av hendelsesforløp er mulig.
- Se NSMs grunnprinsipper for IKT-sikkerhet for flere anbefalinger knyttet til digital sikkerhet på nsm.no/gp-ikt.

Sikkerhet i anskaffelser

Norge er avhengig av teknologi og tjenester fra andre land innen flere områder. Sikkerheten må ivaretas gjennom et stadig økende antall anskaffelser. Konsentrasjonsrisiko er en nasjonal utfordring. Virksomheter bør ikke gjøre seg avhengige av én leverandør eller ett land for å kunne opprettholde sentrale funksjoner.

Norske virksomheter kan bidra til å redusere risiko i leverandørkjeder

Dersom mange virksomheter er avhengige av én leverandør, eller leverandører fra samme land, oppstår det som kalles konsentrasjonsrisiko. Dette oppstår ofte på grunn av pris, tilgjengelighet eller andre faktorer som gjør at alternativene blir begrenset. Graden av risiko for en virksomhet alene eller samfunnet i stort avhenger av det totale omfanget av anskaffelser og hva slags anskaffelser det er snakk om. Noen produkter, teknologier og tjenester tilbys bare av noen få på verdensmarkedet, og i disse tilfellene er konsentrasjonsrisiko vanskelig å unngå.

Trusselaktører kan utnytte høy konsentrasjonsrisiko til å utøve politisk og økonomisk press. Dersom trusselaktører får innpass i leverandørkjeder i en tidlig fase, kan dette utgjøre en sårbarhet på sikt. De kan for eksempel legge inn skjulte bakdører i digitale komponenter for å utnytte denne tilgangen på et senere tidspunkt. Også naturkatastrofer og andre hendelser kan påvirke leveranser og medføre mangel på komponenter som er nødvendige for samfunnsviktige systemer. Et forebyggende tiltak for virksomheter er å unngå å bli avhengige av én leverandør eller ett land for å kunne opprettholde sentrale funksjoner. Begynn med å sikre redundans for varer og tjenester virksomheten er avhengig av. Tenk langsiktig og ta høyde for at tiltak kan måtte endres i framtiden.

Det grønne skiftet

Norge går gjennom en energiomstilling med mer bruk av fornybar energi for å møte både energibehov og klimautfordringer. Kina har etablert seg som den dominerende aktøren i globale leverandørkjeder for både sol- og vindkraft. Etterretningstjenestene i Storbritannia vurderer at kinesisk teknologi brukt i britiske havvindprosjekter kan utgjøre en nasjonal sikkerhetsrisiko. I USA er udokumentert kommunikasjonsutstyr blitt oppdaget i kinesiske solcelleinvertere og batterier. Det har også blitt gjort funn av mistenkelige kinesiske komponenter i energiforsyningsnettet i Danmark.

NSM oppfordrer virksomheter til å tenke sikkerhet i alle ledd når de skal anskaffe teknologi tilknyttet vind- og solkraft, slik at sikkerheten er godt ivaretatt.



Moderne kjøretøy

I krise- eller krigssituasjoner er kjøretøy avgjørende for å ivareta nasjonale sikkerhetsinteresser. Både totalforsvaret og beredskapen i Norge er avhengige av veitransport. En bilpark dominert av få leverandører eller leverandører fra få land kan føre til alvorlige konsekvenser ved omfattende feil eller sikkerhetstruende handlinger. Et scenario er at mange kjøretøy settes ut av spill samtidig som følge av en programvarefeil hos en leverandør.

De siste årene har mange kollektivselskaper gått til anskaffelse av elektriske busser. I dette markedet er det et begrenset antall leverandører, og et større antall kinesiske busser er blitt kjøpt inn. NSM vurderer i denne saken at en enkelt anskaffelse av slike busser isolert sett ikke utgjør en sikkerhets-utfordring. Det er den totale mengden anskaffelser fra samme land eller leverandør som kan være utfordrende.

Det viktigste busselskapene kan gjøre er å vurdere hvilke krav bussene skal oppfylle, i hvilken grad de skal være en del av den lokale beredskapen og hvilket antall kjøretøy som faktisk er nødvendig for å oppfylle krav til beredskap. Samtidig trenger de bevissthet rundt og oversikt over hvordan data fra sensorer i kjøretøyene blir forvaltet. Det er også viktig at både lokale og sentrale myndigheter foretar vurderinger av hvordan busser skal bidra i en beredskapssituasjon og hvilke egenskaper det dermed er viktig at bussene har. I dette tilfellet handler det om kjøretøy, men tilsvarende problem-stilling kan gjelde andre produkter eller tjenester i andre sektorer.

Anbefalinger til virksomheter for å redusere risiko i leverandørkjeder

- Gjennomfør gode og dekkende risikovurderinger for å velge riktige sikkerhetstiltak før anskaffelser.
- Sikre at relevante krav til sikkerhet framgår av konkurransevilkår og kontrakt.
- Sikre redundante løsninger for varer og tjenester virksomheten er avhengig av, slik at manglende funksjonalitet eller tilganger raskt kan gjenopprettes eller erstattes.
- Begrens antall ledd i leverandørkjeden for å sikre økt oversikt og kontroll.



Omfattende bruk av et fåtall utenlandske skytjenester

Skybaserte løsninger har blitt en sentral del av den digitale infrastrukturen i Norge. Markedet er imidlertid i høy grad dominert av utenlandske aktører, særlig amerikanske selskaper som Amazon, Google og Microsoft. Norske virksomheter som benytter utenlandske skytjenester gir fra seg en del av kontrollen over digital infrastruktur, systemer og data som lagres og behandles i skyen. Dette svekker virksomhetenes evne til å sikre dataens konfidensialitet, integritet og tilgjengelighet.

Tekniske problemer, cyberoperasjoner eller endrede vilkår for bruk hos en stor leverandør kan få betydelige konsekvenser for virksomheter som leverer tjenester som samfunnet er avhengig av. I ytterste konsekvens kan geopolitiske konflikter gjøre det vanskelig eller umulig å bruke tjenester levert av utenlandske aktører. Stor avhengighet til utenlandske tjenester kan svekke nasjonal kapasitet og kompetanse til å utvikle, drifte og beskytte tilsvarende løsninger over tid. På lang sikt kan dette gjøre Norge enda mer avhengig, ikke bare av teknologien, men også av leverandørenes økosystemer og strategiske prioriteringer.

Nedetid i Microsoft og Amazons skytjenester

Da Microsoft og Amazon fikk betydelige drifts-problemer i skytjenestene sine i oktober 2025, førte det til store forstyrrelser for millioner av brukere globalt. Plutselig var e-post, skytjenester eller digitale verktøy utilgjengelige. Enkelte tjenester var nede i flere timer. Disse hendelsene viser risikoen ved å være avhengig av et begrenset antall skyleverandører.

Anbefalinger til virksomheter ved bruk av skytjenester

- Planlegg for å kunne bytte ut skyleverandør effektivt og med kjent ressursbruk og kostnad dersom behovet skulle oppstå.
- Vurder om det er behov for å spre tjenester hos flere leverandører for å sikre kontinuitet og redusere risiko.



Satellittsystemers avhengigheter

Det norske samfunnet er svært avhengig av satellittbaserte tjenester, som posisjon, navigasjon og tidsbestemmelse (PNT), satellittkommunikasjon og jordobservasjon. Presis tid har en helt sentral rolle i for eksempel velfungerende kraftforsyning, finansielle transaksjoner og telekommunikasjon (5G), inkludert programvareoppdateringer og sikkerhetssertifikater i digitale systemer. Dersom sentrale satellittbaserte tjenester faller bort, får det store konsekvenser for samfunnets funksjonsevne. Det får også raskt konsekvenser for totalforsvarets evne til å understøtte Forsvaret.

Satellittsystemene Norge er avhengige av har imidlertid egne kritiske avhengigheter som er helt avgjørende for å levere satellittbaserte tjenester. Blant annet er satellittsystemene avhengige av bakkebasert infrastruktur, romovervåkning og kollisjonsunngåelse, geodesi, varsling av romvær og frekvenstilgang. På alle disse områdene er norske satellittsystemer avhengige av utenlandske leverandører og tjenester, spesielt amerikanske.

For å redusere den nasjonale sårbarheten trengs en større grad av sikkerhet og redundans. Norge bør utvikle en større grad av nasjonal autonomi på relevante områder og støtte EUs initiativer og programmer som gir redundans. Det er også viktig at internasjonale normer og regelverk respekteres, spesielt i frekvenskoordinering og -bruk.

Fem sentrale avhengigheter

1. Bakkebasert infrastruktur
Satellitter er avhengige av en omfattende infrastruktur på bakken. For oppskyting er en romhavn nødvendig, og under drift trengs antennenettverk og kontroll- og datasentre. Denne infrastrukturen krever gjerne fysisk sikring og er igjen avhengig av blant annet IKT-nettverk og stabil strømforsyning. IKT-systemer og digital infrastruktur som er kritisk for operasjon av satellittene kan være sårbare for radioforstyrrelser, cyberoperasjoner og fysisk sabotasje.

2. Romovervåkning og kollisjonsunngåelse
Det går nå mer enn 15 000 satellitter i bane rundt jorden. For å unngå kollisjoner må operatørene ha tilgang på en varslingstjeneste. I dag er det amerikanske Space Track som leverer den mest helhetlige romovervåkningstjenesten. Direktoratet for romvirksomhet arbeider med å bygge opp en nasjonal tjeneste i Norge, men avhengigheten til USA vil vedvare.



Simen Rudi/ Forsvaret

3. Geodesi
Satellitter er avhengige av geodesi, som er presise målinger av jordens skiftende tyngdefelt, rotasjon og orientering i verdensrommet. En geodetisk referanseramme er en forutsetning for å kunne tilby PNT og andre rombaserte tjenester. Det globale geodesiarbeidet er basert på et frivillig samarbeid mellom vitenskapelige institusjoner og statlige etater. Sluttresultatet bygges og tilgjengeliggjøres av NASA. Kartverkets geodetiske jordobservatorium i Ny-Ålesund på Svalbard er en viktig bidragsyter til det globale geodetiske referansesystemet, særlig for nordområdene.

4. Romvær
Med jevne mellomrom blir jorden utsatt for kraftige solstormer som forstyrrer og ødelegger satellitter. I tillegg er kraftnettet, radiokommunikasjon, luftfart, sjøfart og petroleumssektoren utsatt. Hvis man klarer å forutse kraftige solstormer kan det gjøres tiltak som beskytter både satellitter og bakkebasert infrastruktur. Amerikanske Space Weather Prediction Center for romværvarsling er helt sentralt. Norge har ingen nasjonal funksjon som varsler om romvær.

5. Frekvensbruk
Radiofrekvenser er en begrenset ressurs. Det er avgjørende med global koordinering av frekvensbruk i regi av FNs International Telecoms Union (ITU) for å redusere utilsiktede forstyrrelser mellom satellitter. ITU har få reelle sanksjonsmuligheter mot land eller satellittoperatører som opererer i strid med ITUs reglement.

Anbefalinger til virksomheter som har avhengigheter til satellittbaserte tjenester

- Identifiser avhengigheter til satellittbaserte tjenester og vurder alternative løsninger for redundans.
- Virksomheter som er avhengige av PNT-tjenester bør vurdere behovet for å ta i bruk forsterket PNT, alternativ PNT eller utstyr og teknologi som beskytter mot jamming og spoofing.
- Styrk evnen til å motstå cyberoperasjoner, inkludert i satellitter, bakkestasjoner og kontrollsentre.

Bidra til å styrke det nasjonale situasjonsbildet

Uønskede hendelser må varsles til myndighetene. Varsle til politiet, PST, NSM eller andre relevante myndigheter. Lag egne rutiner for varsling i virksomheten slik at alle ansatte er trygge på hva de skal gjøre.

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

Virksomheter underlagt sikkerhetsloven er lovpålagt å varsle om sikkerhetstruende hendelser, mistanke om dette, og brudd på sikkerhetsloven. Virksomheter underlagt digitalsikkerhetsloven skal i løpet av 24 timer varsle utpekt tilsynsmyndighet med NSM i kopi om hendelser som virker betydelig inn på leveransen av de digitale tjenestene. Som privatperson kan du varsle om hendelser og observasjoner som du frykter kan skade nasjonale sikkerhets-interesser eller viktige verdier.

Hvordan varsler du NSM?

Varsle situasjons- og operasjonssenteret i NSM
e-post: **beredskap@nsm.no** / telefon: **02497 (24/7)**

For teknisk bistand ved pågående cyberhendelser,
bruk e-post: **beredskap@cert.no**

Se nsm.no/varsle for mer informasjon og varslingsskjemaer.

Sikkerhetsgradert informasjon må ikke inngå i ugraderte varsler. NSM har egne kanaler for gradert varsling fra virksomheter omfattet av sikkerhetsloven.



Foto: Ilja Hendel/NSM
Design: Tank

NASJONAL
SIKKERHETSMYNDIGHET

Postboks 814,
1306 Sandvika
Tlf. 67 86 40 00

26/00205
nsm.no/risiko2026
www.nsm.no