

Longyearbyen, Svalbard, på kveldstid.
Foto: Oriane Laromiguiere / AFP / NTB

Digital sikkerhet i en usikker verden

Cybersikkerhet er en grunnleggende forutsetning

Alle virksomheter lever med risiko. Markedsrisiko. Finansiell risiko. Operasjonell risiko. Derfor vurderer vi konsekvenser og sannsynlighet før vi investerer, ansetter eller endrer strategi. Risikovurdering er grunnlaget for god styring.

Et stort cyberangrep kan true selve eksistensen til en virksomhet. I totalforsvarsåret 2026 blir det tydeligere enn noen gang at virksomheters digitale sikkerhet er en del av Norges samlede beredskap. Under Munich Security Conference i februar vurderte G7-landene cybertrusler som den største opplevde risikoen knyttet til økonomisk krise, konflikt og klima i vår tid.

I denne rapporten ser vi nærmere på utvikling og trender innen cybersikkerhet, med innsikt fra intervjuer med flere sikkerhetsledere. Rapporten gir konkrete råd og anbefalinger på sentrale områder, med mål om å bidra til at virksomheter står digitalt robuste i en mer uforutsigbar tid.

Det digitale trusselbildet i endring

De fleste virksomheter er i dag digitale. Tjenester utvikles, produksjon styres og kommunikasjon skjer digitalt, ofte i skybaserte løsninger.

Samtidig lever vi i en tid med økende internasjonale spenninger. I årets åpne trussel- og risikovurdering pekes det på at trusler mot Norge i økende grad skjer under terskelen for væpnet konflikt, gjennompåvirkningsoperasjoner, etterretning, cyberoperasjoner og økonomisk press. Den digitale arenaen er blitt et sentralt virkemiddel i geopolitisk rivalisering. Cyberangrep brukes både av statlige aktører og kriminelle grupper som forsøker å presse virksomheter for penger.

Hva betyr dette for norske virksomheter?

Cybersikkerhet handler i stor grad om politikk og internasjonale forhold. Rivalisering mellom stormakter og avhengighet av utenlandsk teknologi påvirker risikoen for norske virksomheter. Derfor må de beskytte seg mot angrep og samtidig klare å holde driften i gang når noe skjer.

Våre viktigste anbefalinger fra denne rapporten

- Cybersikkerhet som strategi: Cybersikkerhet må integreres i strategi, investeringer og risikobeslutninger. Når det blir en del av kjernevirksomheten, styrker det både motstandskraft og konkurranseevne.
- Risikohåndtering og teknologi: Oppdater risikovurderinger, ha oversikt over viktige systemer og leverandører, og sørg for løsninger som fungerer hvis noe svikter. Vær bevisst på risiko med gammel og ny teknologi, og sikre at du har gode retningslinjer for bruken av AI.
- Planlegg og øv på drift i krise: Planlegg med forretningskontinuitet og motstandsevne også under krise. Øv jevnlig på cyberhendelser for å styrke beredskaps- og håndteringsevne.

Vi vil takke følgende ledere for at de tok seg tid til å bli intervjuet i forbindelse med arbeidet vårt:

- Bjørn Tore Markussen, Forsvaret
- Audun Jøsang, UiO
- Erik Haugland, Lyse
- Heidrun Larsen Reisæter, Posten Bring
- Tom Remberg, Bane NOR
- Ole Tom Seierstad, Microsoft Norge
- Morten Goodwin, UiA
- Lillian Røstad, Simula Research Lab
- Sokratis Katsikas, NTNU
- Esben Gudbrandsen, Statnett
- Sven Størmer Thaulow, Thaulow Technologies
- Bernt Reitan Jenssen, Ruter
- Antonio Matriadonna, Orkla ASA
- Ronny Windvik, Forsvarets forskningsinstitutt

Innhold

Cybersikkerhet er en grunnleggende forutsetning **2**

Om rapporten **4**

Trender og utvikling innenfor cybersikkerhet **5**

- Cybersikkerhet fremover: Dette sier sikkerhetslederne 6
- Bekymring i akademia: Norge kan bli hengende etter 7
- Cyberkrig i sanntid: Hva kan vi lære av Ukrainas motstandskraft? 8

Råd og anbefalinger på kritiske cybersikkerhetstemaer **10**

- Det digitale totalforsvaret: Fra idé til konkrete planer i din virksomhet 11
- Teknologi og cybersikkerhet: En kjernekompetanse i styret 13
- Skystrategi: Digital suverenitet må på agendaen 14
- Kunstig intelligens: Mulighet og trussel 15
- Kvantesikkerhet: Tenk i dag på å beskytte deg for fremtiden 16
- OT og IoT i frontlinjen: Digital sikkerhet for kritisk infrastruktur 18
- Avhengigheten av romteknologi: En trussel vi må ta på alvor 19
- Innovasjon og regulering: Fra krav til konkurransefortrinn 20

Definisjoner **21**

Om rapporten

Denne rapporten er ment for ledere, medarbeidere som jobber med cybersikkerhet, og deg som er interessert i temaet.

Rapporten er bygget opp i fire deler:

- Et sammendrag av de viktigste utviklingstrekkene og anbefalingene
- En introduksjon med et historisk bakteppe
- En seksjon med trender og utvikling innenfor cybersikkerhet
- En seksjon med råd og anbefalinger på spesifikke temaer innenfor cybersikkerhet

Vi er som samfunn og virksomheter avhengige av digitale verdikjeder. Samtidig bygger mange fortsatt på IT-løsninger utviklet for flere tiår siden. Gammel teknologi, kombinert med for lite systematisk sikkerhetsarbeid, gjør dette til en av våre største systematiske sårbarheter. Når kritiske systemer ikke oppdateres, og sikkerhetsarbeidet ikke er godt nok strukturert, øker risikoen for alvorlige hendelser. Flere fremhever at kombinasjonen av eldre teknologi og utilstrekkelige sentrale sikkerhetskontroller gjør norske virksomheter mer sårbare, og at konsekvensene ved alvorlige cyberhendelser derfor kan bli betydelige.

Verden preges av stormaktrivalisering, teknologisk kappløp og økende systemavhengighet. Sikkerhet kan derfor ikke lenger ses som et rent teknisk spørsmål.

Globale maktforhold, teknologisk eierskap og forsyningslinjer påvirker risikoen også for norske aktører. Som teknologisjef i Forsvaret, Bjørn Tore Markussen, sier: «Vi kan ikke kontrollere noe vi ikke forstår, eller forsvare noe vi ikke har tilgang til».

Robusthet og motstandskraft er avgjørende. Konkurransen mellom USA og Kina om AI og mikrobrikker påvirker aktører som er avhengige av deres skytjenester og maskinvare. Erfaringene fra Ukraina viser at motstandskraft handler om mer enn tekniske reserveløsninger. Det handler om evnen til å opprettholde drift under press.

Når fysiske systemer er koblet til internett og styres gjennom leverandøravhengige løsninger, kan cyberrisiko raskt få konsekvenser i den virkelige verden. Ruter sin sikkerhetstest som viste at elbusser kan fjernstyres, illustrerer behovet for å forstå og håndtere leverandørrisiko.

Nordområdene har fått en sentral rolle i geopolitikken. Svalbard og Arktis får større strategisk betydning, og risikoen for hybride og digitale trusler kan øke som følge av den geopolitiske utviklingen. Når avhengigheten av kritisk infrastruktur øker, blir det viktigere å garantere at disse systemene fungerer som de skal i møte med et vidt spekter av trusler og risikoer.

Cybersikkerhet må ses på som et strategisk felt på tvers av sektorer og nivåer. Risiko kan ikke fjernes, men håndteres bedre gjennom samarbeid, kunnskap og strategisk tilnærming.

Vi håper rapporten er nyttig for deg. Ta gjerne kontakt om du har spørsmål eller trenger råd.



Hans Christian Pretorius
Partner
hans.christian.pretorius@kpmg.no



Bente Hoff
Director
bente.hoff@kpmg.no



Berit Bergsli Salvesen
Senior Manager
berit.salvesen@kpmg.no

Trender og utvikling innenfor cybersikkerhet

Behovet for å beskytte virksomheter mot cybertrusler har økt i takt med økende geopolitisk uro og en forverret sikkerhetspolitisk situasjon. For å forstå utviklingen bedre har vi snakket med fremtredende sikkerhetsledere i norske virksomheter, eksperter i akademia, og leder av vår ukrainske cyber-avdeling.



Jonas Gahr Støre under Oslo Security Conference 2026.
Foto: Javad Parsa / NTB

Cybersikkerhet fremover:

Dette sier sikkerhetslederne

Sikkerhetslederne vi har snakket med peker på at AI vil dominere diskusjonen det neste året, både som mulighet og risiko. Oppmerksomheten vil i stor grad være rettet mot ny teknologi, samtidig er det mange virksomheter som fortsatt er avhengige av gamle systemer og løsninger. Norge digitaliserte tidlig, og mange av løsningene vi fortsatt bruker i dag har ikke blitt fornyet. Det er dette som skaper de største sårbarhetene. Ny teknologi kan derfor også bli en del av løsningen på problemer som har bygget seg opp over tid.

Det ventes strengere regulering innen cybersikkerhetsområdet, særlig gjennom europeiske krav som NIS2. Dette bidrar til å løfte digital sikkerhet høyere opp på toppledernivå. Flere trekker også frem behovet for sterkere digital beredskap, bedre hendelseshåndtering og mer robust digital infrastruktur hos virksomhetene.

Angrepene blir mer målrettede og sofistikerte, ofte gjennom kompromitterte brukerkontoer, leverandørkjeder eller sårbare IoT-enheter. Antallet hendelser kan øke, uten at alle nødvendigvis representerer alvorlige samfunnskriser. Samtidig anses alvorlige cyberhendelser mot kritisk infrastruktur som energi og transport som sannsynlige i en geopolitisk rivalisering, mens ny teknologi og tettere kobling mellom statlige og kriminelle aktører vil prege trusselbildet.

> AI vil dominere diskusjonen, med økende erkjennelse av at trusselaktører bruker AI kriminelt og uetisk."
>
> Audun Jøsang, forsker ved UiO

> AI vil være en viktig driver fremover og kan bidra til å sikre verdier og systemer, forutsatt riktig bruk. Samtidig vil teknologien utnyttes av trusselaktører, i et dynamisk trusselbilde der tilgjengelige verktøy tas i bruk for å nå deres mål."
>
> Erik Haugland, Direktør Sikkerhet i Lyse

> 2026 vil bli preget av fortsatt usikkerhet rundt Norges strategiske veivalg innen digital sikkerhet. Spesielt beslutningen om en nasjonal skyløsning vil fortsette å være et hett tema. Året vil bringe økt press på å ta i bruk kunstig intelligens. Jeg forventer at debatten om ansvarlighet og rettferdighet vil bli enda mer sentral. Grunnleggende sikkerhetsarbeid vil fortsatt være en flaskehals. Det hjelper lite å være skikkelig god i sikkerhet om du ikke forstår teknologien – og omvendt."
>
> Heidrun Larsen Reisæter, Konserndirektør Digital teknologi og sikkerhet i Posten Bring AS

> AI har i dag en del hype-kjennetegn, samtidig som det er en underliggende utvikling av modeller som vil gi reell forretningsverdi. Vi vil se en tydelig modning og konsolidering av AI-anvendelse de neste årene. Dette vil tydeliggjøre hva AI kan bidra med i kjerneprosesser, hvor det kan gi effektivisering, og hva som i større grad er «hype». Jeg er også svært spent på om, og eventuelt når, quantum computing blir det som spås. Samtidig nærmer noen trusselaktører seg OT-land, i alle fall OT-nær IT."
>
> Tom Remberg, CISO i Bane NOR

> Vi tror at infostealere fortsetter å dominere som effektive verktøy for datatyveri, med økt sofistikasjon og mulig støtte fra aktører som utnytter kvantefordeler på sikt, særlig knyttet til russiske miljøer. Angrepene blir mer målrettede, men i mindre volum. Samtidig ser vi større risiko for utnyttelse av zero-day-sårbarheter. I Europa kan flere cybersikkerhetssaker bli løftet direkte til toppledelsen gjennom NIS2-direktivet, med et tydeligere regime for bøter og krav som gjør at norske virksomheter «våkner», inkludert strengere krav til DPA (data processing agreements) i leverandørkjeden."
>
> Ole Tom Seierstad, National Security Officer hos Microsoft

Bekymring i akademia:

Norge kan bli hengende etter

I akademia er det flere miljøer som forsker på cybersikkerhet, og som kan gi virksomheter viktige perspektiver. De beskriver et digitalt risikolandskap som utvikler seg raskere enn samfunnets evne til å forstå, regulere og beskytte det.

Norge mangler kapasitet og kobling mellom fagmiljøer

Mange av de vi har intervjuet innen akademia peker på at Norge mangler kapasiteten som trengs for å sikre gode strukturer. Manglende sikkerhetskompetanse bremser sikker digitalisering av energi, industri, maritim sektor og helse, og etterlater et stort behov for tverrfaglige utdanningsløp som foreløpig ikke finnes i god nok bredde.

Akademia er tydelig på at dette ikke bare handler om antall studieplasser, men om innhold. AI-sikkerhet, integrasjon mellom IT og OT, industriell nettverkssikkerhet, rom- og satellittvern og avansert kryptologi er fagfelt som bør bli vesentlig sterkere i Norge enn de er i dag.

Innen AI peker flere på et misforhold mellom tempoet i trusselutviklingen og Norges evne til å henge med. De beskriver AI-forskningen i Norge som fragmentert, svakere finansiert enn i konkurrerende land og ofte rettet mot etiske spørsmål snarere enn sikkerhet og robusthet. Professor ved UiA, Morten Goodwin, mener aktivitetsnivået er for lavt: «Norge har veldig lite aktivitet sammenliknet med andre land. Vi henger bakpå, og må få opp farten».

Må se sivile og militære forskningsbehov i sammenheng

Geopolitikken har også endret forskningsagendaen. Ukrainakrigen, økt stormaktsrivalisering og nye avhengigheter til satellitter, datasentre og globale skyleverandører gjør at Norge må se sivile og militære forskningsbehov i sammenheng. Forskerne fronter et tydelig politisk ønske om å bruke sivile teknologimiljøer mer aktivt i forsvarssektoren, men dette møter kulturelle og strukturelle hindringer.

Akademia står i en skvis mellom å være så åpent som mulig, og samtidig så sikkert som nødvendig. «Åpenhet er den grunnleggende verdien», sier Lillian Røstad i Simula. «Å bruke sivil teknologikompetanse i Norge inn mot forsvarsformål er avgjørende for å lykkes». Flere påpeker også at Norges størrelse gjør selvforsyning av teknologikompetanse urealistisk. Morten Goodwin understreker behovet for samarbeid på tvers av land: «Norge er alt for lite til å stå alene. Vi er nødt til å samarbeide med resten av Europa».

Det kommer også tydelig frem at reguleringene ikke treffer godt nok. Norge har en sterk etterlevelseskultur, men en svakere tradisjon for å måle effekt. Vi får stadig flere reguleringer med mer skjerpede krav, samtidig som gapet mellom forskning, praksis og faktisk risikoreduksjon øker. «Vi ser et for stort fokus på compliance over effekt. Forskning er veldig teknisk, men det er lite forskning gjort på hva de som jobber med sikkerhet faktisk gjør i praksis», sier Lillian Røstad, CEO i Simula Research Lab.

Det svekker innovasjonsevnen.

Tydelig rolleforståelse Til tross for utfordringene, har akademikerne en tydelig rolleforståelse. De skal utvikle kunnskap, utdanne fagfolk og utfordre samfunnets teknologivalg. De skal forklare og avdekke risikoer som kan være ubehagelige for både politikk og næringsliv, fra satellittavhengighet til avhengighet av amerikanske språkmodeller og kommersielle skyleverandører.

Flere ønsker seg mer kunnskap på områder som AI, IT og OT, kvantesikkerhet, læring fra krigen i Ukraina og samspillet mellom sivil og militær sektor. Samtidig peker forskere på at områder som nordområdene, maritim sektor og romteknologi er særlig viktige for Norge. Audun Jøsang ved UiO påpeker at forskning ikke kan kurere alle våre cybertrusler. Sokratis Katsikas fra NTNU mener derfor cybersikkerheten må løftes politisk: «Jeg ber ikke først og fremst om mer penger, jeg ber om at cybersikkerhet settes på den politiske agendaen».



Den amerikanske romstasjonen Pituffik på Grønland, romteknologi er et stadig større tema i Norden.

Foto: Thomas Traasdahl / Ritzau Scanpix / NTB



Om forfatteren.

Gennadiy Reznichenko leder KPMGs cyberavdeling i Ukraina. Han har omfattende erfaring som cybersikkerhetsrådgiver for regjeringer og store bedrifter om motstandskraft, hendelsesrespons og transformasjon av cyberforsvar. Hans perspektiver er formet av år med arbeid i skjæringspunktet mellom nasjonal cyberkrigføring og sikkerhetsarbeid i virksomheter på tvers av ulike geografier.

Cyberkrig i sanntid:

Hva kan vi lære av Ukrainas motstandskraft?

Mer enn et tiår inn i Russlands hybride aggresjon, og nesten fire år inn i fullskalainvasjonen, fortsetter Ukraina å kjempe den mest teknologisk komplekse krigen i moderne historie. Det som begynte som isolerte inntrengninger i 2014, har utviklet seg til en synkronisert multidomenekonfrontasjon der cyberoperasjoner former tempoet på slagmarken, nasjonal stabilitet, offentlig moral og internasjonal sikkerhet. Denne artikkelen gir et overblikk over Ukrainas cyberkrig sett fra innsiden, og gir lærdommer som nasjoner ikke har råd til å ignorere.

Før 2022 fungerte Ukraina lenge som et testområde for russiske cybervåpen. Tidlige angrep, som innblanding i valgsystemet (2014), BlackEnergy (2015), og den beryktede NotPetya (2017), viste Kremls skifte mot systemiske forstyrrelser. Målet var klart: å undergrave tillit, destabilisere statlige institusjoner, og å teste destruktive kapabiliteter mot reelle mål. Parallelt begynte Ukraina å styrke sitt cyberfundament gjennom å vedta sin første cybersikkerhetslov (2017); danne et situasjonssenter for Cybersikkerhet (2018); opprette et samlet CERT-UA (2020; og investere i den digitale transformasjonen.

I ukene før invasjonen, den 24. februar 2022, eskalerte Russland sine cyberoperasjoner, designet for å "myke opp slagmarken". Regjeringsnettsteder ble vandalisert, dataslettende malware forkledd som ransomware ble distribuert, og storskala DDoS-angrep rammet banker og departementer. Hensikten var psykologisk; for å undergrave tillit, skape forvirring, og distrahere ledelsen før missiler og stridsvogner krysset grensen.



Bilde fra en av de lokale butikkene som ble rammet av NotPetya angrepet i Ukraina i 2017.
Foto: Brendan Hoffman / NYT / NTB

I den tidlige fasen etter invasjonen var cyberangrep tett synkronisert med fysiske angrep. Russiske enheter forsøkte å forstyrre kommando- og kontrollsystemer, energinett, satellittkommunikasjon og nødtjenester. I motsetning til den vanlige antagelsen om at flytting til skyen øker eksponeringen, ble det motsatte tilfellet for Ukraina. En rask migrering av kritiske statlige funksjoner til skyen, både innenfor og utenfor landet, ble en av de mest avgjørende defensive handlingene i krigen. Ved å distribuere data og tjenester over robuste, globale skyplattformer, sikret Ukraina kontinuitet i statsapparatet selv når fysiske datasentre var under bombardement.

Dette skiftet beskyttet kritiske registre fra ødeleggelse, muliggjorde rask gjenoppretting, og fjernet risiko for flaskehalser og svake ledd som er iboende i lokalt driftede systemer. Samtidig dukket den frivillig drevne IT-hæren opp nesten over natten, med mer enn 300 000 bidragsytere, og introduserte en ny modell for massemobilisering av cyber-kompetanse som kompletterte statens defensive kapabiliteter.

Fra 2023 til 2025 har Russlands cyberoperasjoner skiftet fra oppsiktsvekkende, destruktive angrep til mindre spektakulære, langsiktige kampanjer for å infiltrere, spionere, og skape systemiske forstyrrelser. I stedet for å stole på volum alene, søkte Russland dybde ved å kompromittere forsyningskjeder, utnytte sikre kommunikasjonslinjer, og å integrere informasjonsoperasjoner i sin bredere militærstrategi. Denne utviklingen ble understøttet av Russlands økte statlige investeringer og tydeligere strategiske prioritering, noe som produserte mer koordinerte, automatiserte, og robuste offensive cyberkapabiliteter. Etter hvert ble det tydelig at Russland beveget seg mot en moden, økosystemdrevet cyberdoktrine som angriper samfunnsfunksjoner like mye som militære mål.

Samtidig akselererte Ukraina sin egen transformasjon gjennom bredere adopsjon av Zero Trust-modellen, sterkere offentlig-privat deling av trusseletterretning, proaktiv bistand og utstrakt operativt samarbeid med statlige myndighetsorganer, og fremveksten av et cyberoperasjonssenter i Forsvarsdepartementet. Resultatet var kortere deteksjonssykluser og raskere nasjonal hendelseshåndtering.

Fremover fra 2026 kan vi forvente dypere AI-integrasjon i angrep, større synkronisering med militære operasjoner, flere ringvirkninger til NATO-land, og aktivering av sovende kompromitteringer. Slagmarken innsnevres ikke, den utvides.

Ukrainas erfaring viser at cybermotstandskraft ikke er en statisk kapasitet, men snarere en tankegang, et system, og til sist en nasjonal overlevelsesmekanisme. Andre nasjoner står nå overfor et valg: lære av Ukraina i tide, eller lære på den harde måten.

Viktige lærdommer fra Ukraina for andre nasjoner

- Cybertrusler er systemiske, ikke tekniske. De kan destabilisere samfunnet, undergrave tillit, og lamme kritiske sektorer og industrier.
- Motstandskraft krever desentralisering og raske beslutninger. Skymigrasjon og en hybrid flernasjonsmodell reddet Ukrainas digitale stat.
- Offentlig-privat samarbeid er avgjørende. Ukrainas samarbeid med Microsoft, Google, Mandiant og mange andre ble en styrkemultiplikator.
- IT/OT-konvergens må styres. Hendelser i energisektoren har vist de eksistensielle risikoene ved ubeskyttede OT-miljøer.
- Cybersikkerhet begynner med mennesker. Bevissthet, klare roller, og myndiggjorte lokale forsvarere er like viktig som teknologi.



Ukrainske soldater på frontlinjen i Donetsk.
Foto: Tyler Hicks / NYT / NTB



Råd og anbefalinger på kritiske cybersikkerhetstemaer

Cybersikkerhet spenner over flere fagfelt og er et strategisk tema for norske virksomheter. Ansvar for robusthet og drift har flyttet seg til ledelse og styre. Samtidig krever områder som IoT og kvantesikkerhet ny kompetanse. Kapitlet gir en oversikt over de viktigste områdene med anbefalinger.

Bente Hoff under årets NHO konferanse der hun presenterte funn fra KPMGs topplederrapport 2026.

Foto: Alf Simensen / NTB Kommunikasjon

Det digitale totalforsvaret:

Fra idé til konkrete planer i din virksomhet

2026 er totalforsvarsåret. Det digitale totalforsvaret har blitt en del av Norges felles beredskap. Fra å tidligere ha vært en støttefunksjon, er det digitale domenet nå en kritisk del av nasjonal motstandskraft. Som Bjørn Tore Markussen, CTO i Forsvaret påpeker, har både sikkerhetssituasjonen og krigens karakter endret seg betydelig siden 2014: «Siden 2014 har fredens natur endret seg, vi er i en hybrid fred eller en lavskala konflikt. Samtidig har krigens karakter endret seg fullstendig».

Det er ikke lenger mulig å skille skarpt mellom fred, krise og konflikt. Digitale hendelser skjer hele tiden og kan raskt eskalere. Den digitale infrastrukturen som holder Norge i gang, er den samme som kan svikte når landet trenger den mest. Flere vi har snakket med peker på et trusselbilde som krever at scenarioer revurderes og utvides.

Manglende rolleforståelse i totalberedskapen

Flere virksomheter er bevisste på at de inngår i totalberedskapen, men har begrenset forståelse for hva det konkret innebærer. KPMGs topplederrapport, «Nytt alvor», viser at kun én av tre virksomheter anser seg som en del av totalberedskapen. Utydelige roller kan føre til at risikoen for rask eskalering av digitale angrep undervurderes, samt at behovet for å kunne stenge ned systemer og raskt gå over til manuell drift ikke er tilstrekkelig ivaretatt. Som en sikkerhetsleder påpeker, bør alle virksomheter ha en «killswitch », altså evnen til å stenge ned systemer umiddelbart. Effektiv beredskap forutsetter ikke bare teknologiske løsninger, men også tydelige prosedyrer, avklarte fullmakter og evne til koordinert handling.

Norske virksomheter må diskutere og konkretisere hva robusthet faktisk betyr. Det handler ikke bare om samarbeid som en idé, men om investeringer som gjør Norge i stand til å stå i kriser. Innovasjon og vekst må balanseres med sikkerhetstiltak. Flere av de vi har snakket med sier at balansen i dag ikke er god nok, og at store deler av næringslivet ser behovet for større investeringer og mer strategisk samhandling.



Oslo Sentralstasjon. Togene er en stor del av kritisk infrastruktur og totalberedskap i Norge.
Foto: Gorm Kallestad / NTB



Digitaliserings og forvaltningsminister Karianne Tung mottar rapport om nasjonal kontroll om digital infrastruktur fra ekspertutvalget av direktør ved SimulaMet og professor ved OsloMet Olav Lysne.
Foto: Javad Parsa / NTB

Flere peker på mangel på åpne og forpliktende arenaer for samarbeid. Det er ikke mangel på aktører som har lyst til å bidra, men det mangler arenaer. «Jeg savner strategiske møteplasser», sier Erik Haugland i Lyse. Han oppsummerer det slik: «For virksomheter underlagt sikkerhetsloven så er kravene til sikkerhet uomtvistelige, mens ytterligere robusthet og redundans ofte fremmes som ambisjoner uten kommersiell gjennomførbarhet».

Samtidig understrekes behovet for koordinert innsats ved større hendelser. «Det er få i Norge som klarer å håndtere store angrep uten å involvere sektorvise responsmiljøer, myndigheter eller andre samarbeidspartnere», sier Esben Gudbrandsen i Statnett.

Behovet for en felles situasjonsforståelse blir viktig og flere mener at de hemmelige tjenestene gjør en god jobb med å beskrive situasjonen. Etter samtalene ser vi særlig én felles konklusjon; det digitale totalforsvaret blir viktigere i tiden som kommer. Dette forutsetter modernisering, investeringer og rammer som gjør samarbeid til mer enn et prinsipp. Skal vi bli digitalt robuste krever det at vi tar flere strategiske valg nå.

Hva betyr dette for norske virksomheter?

Virksomheter må modernisere, investere og tilpasse styringsmodell og praksis til et trusselbilde som er i kontinuerlig endring. Det krever både strategiske prioriteringer og operative tiltak. Rolleforståelse må kartlegges og det må etableres en sikkerhetskultur som tar innover seg alvoret i dagens hybride sikkerhetssituasjon. Bevissthet, tydelige roller, og lokalt forsvar er like viktig som teknologi.

Tre konkrete råd

1. Forstå og tren på virksomhetens rolle i totalforsvaret, slik at både ledelse og ansatte vet hva som forventes i fred, krise og konflikt.
2. Oppdater, etabler og øv på krisescenarioer.
3. Bygg robusthet gjennom forpliktende samarbeid med myndigheter, leverandører og bransjeaktører, slik at tiltak og respons fremstår helhetlige og ikke fragmenterte i en krisesituasjon.

Teknologi og cybersikkerhet:

En kjernekompetanse i styret

Mange vi snakket med trekker frem svak styrekompetanse på cyber som en utfordring. Ifølge Sven Størmer Thaulow har styremedlemmer i de fleste norske styrer begrenset forståelse for cybersikkerhet, og virksomheter styres fortsatt primært etter kommersielle og juridiske hensyn. Konsekvensen er at beslutninger om investeringer, leverandørstyring, dataarkitektur og beredskap blir tatt uten tilstrekkelig forståelse for trussellandskapet virksomheten befinner seg i. Dermed blir også ambisjoner om digital modernisering mer sårbare når styret ikke stiller tydelige krav til sikkerhet, kontinuitet og minimumsdrift.

Fra tekniske funn til beslutninger for ledelsen

Flere påpeker viktigheten av oversettelse av tekniske funn til konkrete beslutninger for ledelsen. Virksomheter må avklare hvilke prosesser som er kritiske, hvilke systemer som må holdes i drift under krise, og hvilke leverandører som kan utgjøre en systemrisiko, og ikke minst hvordan dette faktisk måles og øves i praksis.

Samtidig strekker risikoen seg på tvers av sektorer og landegrenser. Erik Haugland fremhever at sikkerhet ikke kan avgrenses til egen infrastruktur alene. Avhengigheter i verdikjeden gjør at hendelser rettet mot andre sektorer eller land likevel kan ramme norske virksomheter. Veien videre handler om å flytte tyngdepunktet fra ambisjon til gjennomføring. For virksomheter betyr det å gjøre cyber til en styrt strategisk kapasitet.



Direktør i cybersikkerhet Bente Hoff fra KPMG under årets NHO-konferanse, her presenterer hun funnene fra KPMGs topplederrapport 2026.

Foto: Alf Simensen / NTB Kommunikasjon

Hva betyr dette for norske virksomheter?

Virksomheter må ha en tydelig beredskap fra styret og helt ut i den daglige driften. Det er viktig å prioritere de mest kritiske oppgavene, stille krav til leverandører og øve jevnlig sammen med både egne ansatte og samarbeidspartnere.

Arbeidet med sikkerhetsstyring må være systematisk. Beskyttelse, oppdagelse av hendelser, håndtering og gjenoppretting må følges opp over tid. Det samme gjelder leverandøroppfølging og øvelser. Når dette gjøres godt, blir det lettere å oppfylle kravene i praksis.

Tre konkrete råd

1. Gjør cybersikkerhet til et ansvar for styret og toppledelsen.
2. Få oversikt over hva virksomheten er avhengig av, og hvem dere er avhengige av.
3. Styrk virksomhetens motstandsdyktighet gjennom målrettet arbeid med gode tekniske løsninger, tydelig organisering og klare arbeidsrutiner.

Skystrategi:

Digital suverenitet må på agendaen

Virksomheters valg av skyløsning, plattformer og teknologipartnere kan ikke lenger behandles som rene tekniske eller operative beslutninger. Det er strategiske valg med direkte konsekvenser for virksomhetens kontroll over egne verdikjeder, beslutningsgrunnlag og kontinuitet.

Konsekvensen av denne utviklingen er tydelig. Styret og toppledelsen må ta eierskap til diskusjonen om skystrategi og digital suverenitet. Valg av teknologiarkitektur må understøtte virksomhetens styringsevne. Ikke bare i normalsituasjon, men også når rammevilkårene endrer seg raskt.

Når alvorlige hendelser inntreffer, må virksomheten ha reell evne til å:

- stenge ned eller isolere tjenester
- flytte eller restrukturere kritiske systemer raskt
- endre driftsmodeller og sikkerhetsnivå
- opprettholde kontroll selv ved svikt i eksterne leveranser

Dette er ikke operative IT-spørsmål. Det er spørsmål om virksomhetskontroll og risikostyring, og dermed et klart styreansvar. De fleste norske selskaper er kjøpere av teknologi, ikke utviklere av plattformene de baserer seg på. Det skaper en asymmetrisk relasjon til globale leverandører. Man får tilgang til avanserte løsninger, men har begrenset innflytelse over hvordan teknologien utvikles, prioriteres og styres.

Hva betyr dette for norske virksomheter?

Teknologistrategi er et risikoperspektiv styret aktivt må ta stilling til, og ikke noe som kan overlates til prosjekt- eller linjenivå. En ansvarlig sky- og plattformstrategi bør bygge på tre grunnleggende prinsipper:

- Transparens. Virksomheten må forstå hvordan systemene fungerer, hvilke data som behandles, og hvilke beslutningslogikker som ligger til grunn. Uten innsikt svekkes styring, etterprøvbarhet og tillit.
- Portabilitet og exit-mulighet. Virksomheten må ha reelle muligheter til å flytte data og funksjonalitet dersom rammebetingelsene endrer seg. Exit-strategier må være teknisk, organisatorisk og kommersielt gjennomførbare, ikke bare formulert i kontrakter.
- Egen kompetanse. Evnen til å forstå og styre teknologi som påvirker virksomhetens kjernefunksjoner kan ikke outsources fullt ut. Uten intern kompetanse mister styret reell styringsevne.

Tre konkrete råd

1. Sørg for at valg av skystrategi settes på agendaen til toppledelsen i 2026.
2. Finn en strategi som sikrer beredskap og som kan opprettholde tjenester i krisesituasjoner.
3. Utnytt mulighetsrommet i ny teknologi og driftsmodeller som tilbys i markedet.

Kunstig intelligens:
Mulighet og trussel

Flere peker på at diskusjonen om AI preges av optimisme. Som tidligere CPTO i Schibsted, Sven Størmer Thaulow, uttrykker det, er vi fortsatt i en «forelskelsesfase» der mulighetene står i sentrum. Samtidig åpner AI et nytt rom for sikkerhetsutfordringer.

AI gir store muligheter, men endrer også sikkerhetsbildet raskt. Teknologien brukes nå både av angripere og av dem som skal forsvare seg. Angripere kan lage mer troverdige svindelforsøk, finne sårbarheter raskere og gjennomføre angrep i større skala. Samtidig bruker virksomheter teknologien til å oppdage avvik, prioritere varsler og støtte beslutninger i kriser. Resultatet er et kappløp der både angrep og forsvar blir mer automatiserte og tilpasningsdyktige.

Utviklingen påvirker hele totalforsvaret. Norske virksomheter må bygge kompetanse, samarbeide tettere og øve mer for å bruke AI-teknologi trygt, samtidig som de forstår hva trusselaktører kan gjøre. Mulighetene er store, men risikoen øker også. Derfor trenger virksomheter en tydelig strategi for bruk og begrensninger.

Ny utvikling innen autonome systemer øker behovet for kontroll og forståelse. Teknologien kan endre spillereglene. For ledere betyr dette at bruk av AI i sikkerhetsarbeid må være styrt, målbart og forståelig. Beslutninger med stor konsekvens må fortsatt tas av mennesker.



Forsvarsjef Eirik Kristoffersen presenterer Forsvarets nye senter for kunstig intelligens.
Foto: Ole Berg-Rusten / NTB

Hva betyr dette for norske virksomheter?

For norske virksomheter innebærer dette et behov for helhetlig styring av kunstig intelligens, der teknologi, mennesker og prosesser ses i sammenheng. Det må integreres i sikkerhetsfunksjoner på en måte som er styrt, målbar og forklarbar, og beslutninger med høy konsekvens må fortsatt forankres i tydelig menneskelig ansvar.

Samlet sett må norske virksomheter balansere bruk av kunstig intelligens grundig med forståelse av nye sårbarheter. Evnen til å kombinere innovasjon med styring, kompetansebygging og sikkerhetskontroll blir avgjørende for å opprettholde motstandskraft i et stadig mer komplekst trusselbilde.

Tre konkrete råd

1. Fastsett hva AI skal brukes til, hva det ikke skal brukes til, og hvilke risikoer virksomheten aksepterer.
2. Bygg forsvar i samme tempo som angrepene utvikler seg.
3. Integrer risiko knyttet til AI i sikkerhetsstyringen.

Kvantesikkerhet:

Tenk i dag på å beskytte deg for fremtiden

Kvanteutviklingen er i ferd med å forandre de grunnleggende forutsetningene for digital sikkerhet, og vil medføre nye sårbarheter for norske virksomheter. Teknologien vil forandre hvordan vi samler inn og analyserer data, og kvantemekanismer og -sensorer vil på sikt kunne knekke dagens krypteringskoder og muliggjøre GPS-uavhengig navigasjon.

Norske virksomheter er allerede sårbare for fremtidige kvantedatamaskiner når det gjelder sensitiv bedriftsinformasjon. Økonomiske data, investerings- og innovasjonsplaner, forskningsmateriale, kundedata og personalinformasjon vil ikke lenger være trygge om de fortsatt beskyttes med tradisjonell kryptering. En fremtidig kvantedatamaskin vil enkelt kunne knekke tradisjonelle krypteringsalgoritmer som dagens datamaskiner strever med å løse. Situasjonen blir ikke mindre alvorlig av «harvest now, decrypt later»-strategien, som innebærer at aktører allerede i dag kan lagre store mengder kryptert informasjon i påvente av kvantekapable systemer i fremtiden. Altså: Data som i dag oppfattes som godt beskyttet, kan bli fullstendig eksponert om ti eller tjue år.

Enda en utfordring handler om mangel på kompetanse. Lillian Røstad i Simula peker på at Norge er sent ute med forskning på dette området, selv om regjeringen nå har økt sin satsing vesentlig med etableringen av fire nasjonale forskningssentre innen kvanteteknologi. Samtidig har kun et fåtall virksomheter god nok fagkunnskap om postkvantekryptografi, og ansvaret for kvantesikkerhet er ofte fragmentert mellom IT, sikkerhet og ledelsen. Selv om bevisstheten rundt kvantetrusselen øker, har få virksomheter konkrete overgangsplaner eller modne strategier for kvantesikkerhet. Mange undervurderer fremdeles risikoen, eller avventer tydeligere standardisering før de setter i gang migrasjonstiltak. Samtidig øker regulatoriske krav i Europa, og også norske selskaper må regne med at forventninger knyttet til kvantesikkerhet både blir mer konkrete og bindende på sikt.



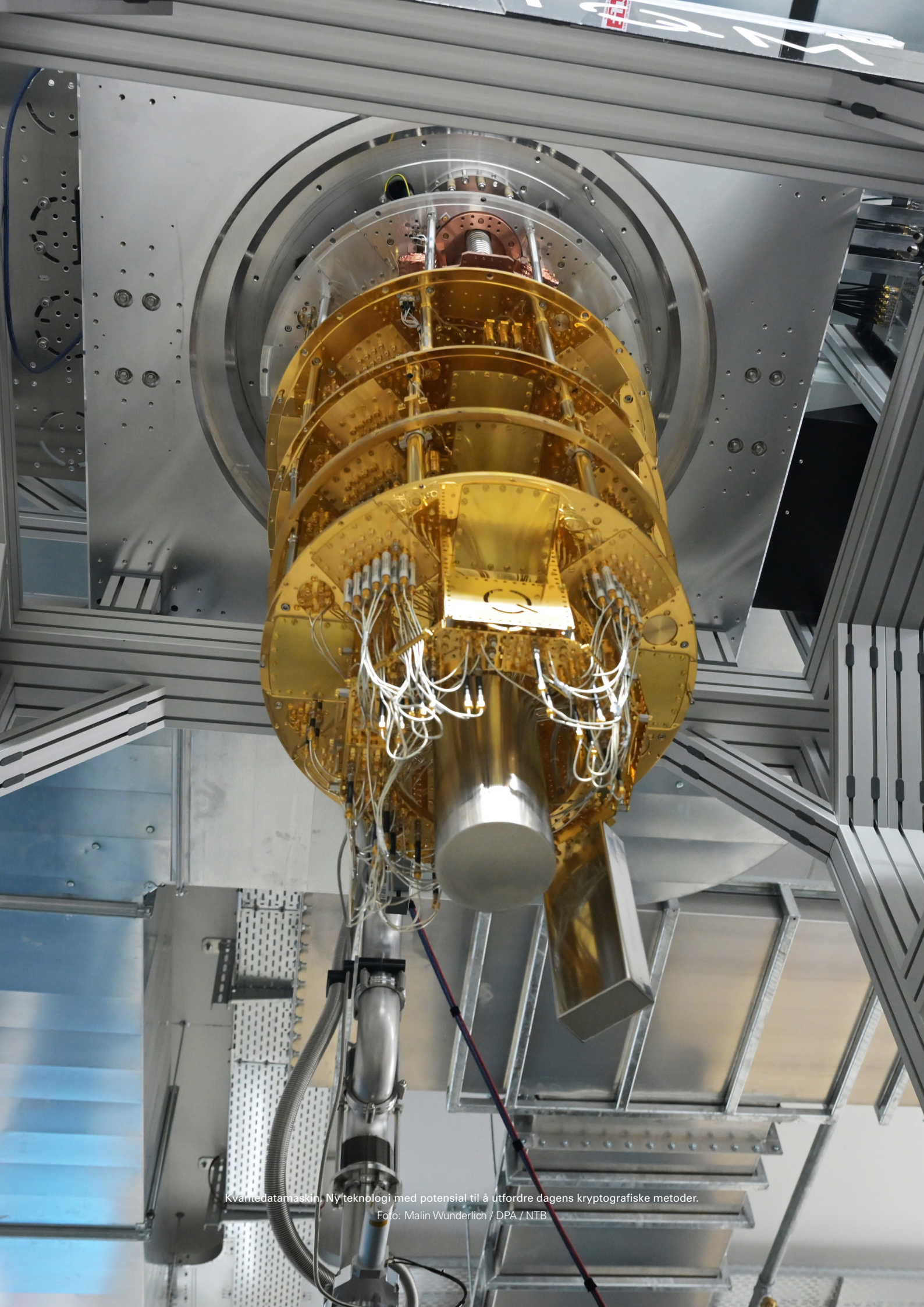
Kvantechip. Den teknologiske kjernen i moderne kvantedatamaskiner.
Foto: Malin Wunderlich / DPA / NTB

Hva betyr dette for norske virksomheter?

Når den fremtidige digitale sikkerheten avhenger av vår evne til å møte kvanteutfordringen, blir det avgjørende å ta grep raskt. Det innebærer å kartlegge kryptografiske avhengigheter, etablere en migrasjonsplan, bygge kompetanse og begynne overgangen til kvantesikre løsninger i god tid før teknologien blir en reell trussel. Særlig bør samfunnskritiske virksomheter og virksomheter som håndterer sensitive data prioritere kvantesikkerhet tidlig.

Tre konkrete råd

1. Finn ut hvor virksomheten bruker sårbar kryptering, slik at dere vet hva som må oppdateres først.
2. Etabler et tydelig ansvar for kvantesikkerhet og bygg opp nødvendig kompetanse, slik at arbeidet ikke stopper opp i organisasjonen.
3. Planlegg en gradvis overgang til kvantesikre løsninger sammen med leverandører, og bruk tid på å velge løsninger som passer virksomheten.



Kvantedatamaskin. Ny teknologi med potensial til å utfordre dagens kryptografiske metoder.
Foto: Malin Wunderlich / DPA / NTB

OT og IoT i frontlinjen:

Digital sikkerhet for kritisk infrastruktur

Digitaliseringen av kritisk infrastruktur gjør at systemer for operasjonell teknologi (OT) som styrer fysiske prosesser i kraftforsyning, helse, vann, olje og gass, transport og industri, i større grad integreres med tradisjonelle IT-miljøer.

Mer effektiv drift, bedre datagrunnlag og økt automatisering gir store gevinster. Samtidig skaper digitaliseringen nye sårbarheter. Konsekvensene av et cyberangrep er ikke lenger begrenset til tap av data eller forstyrrelser i administrative prosesser. De kan ramme samfunnet i fysisk forstand, med operasjonssvikt, miljøskader og i verste fall fare for liv. Olje og gassektoren, som både har høy digitaliseringsgrad og stor samfunnsbetydning, trekkes frem som spesielt utsatt i et eskalerende hybrid trusselbilde.

Angrepet på damanlegget i Bremanger i april 2025 viste dette tydelig. Angripere fikk tilgang til systemene og kunne endre vannføringen. Hendelsen er et klart varsel om hva som kan skje når OT-systemer manipuleres. God samhandling er avgjørende. Beskyttelse av OT-systemer er stadig viktigere, spesielt som en følge av integrasjon med IT-systemer. Samtidig øker risikoen fra IoT - alt fra sensorer til smarthus til kjøretøy. Mange enheter har svak sikkerhet, og eksperter advarer om at vi trolig vil se flere hendelser som rammer folk direkte. Sven Størmer Thaulow, tidligere CPTO og EVP i Schibsted, trekker frem at det finnes utallige IoT-enheter med svak beskyttelse, og det er sannsynlig at vi snart vil se hendelser som gjør dette tydelig for folk flest.

Han advarer mot at det er først når angrep rammer biler, smarthus eller andre fysiske enheter, at mange forstår rekkevidden av denne risikoen. IoT ser ut til å bli en av arenaene hvor det hybride trusselbildet materialiserer seg mest konkret fremover.

Parallelt skjerpes kravene til virksomheter gjennom nye EU-regler. Bedrifter må nå jobbe mer systematisk med risiko, sikkerhet og rapportering. God samhandling mellom IT og OT er blitt avgjørende for sikker og stabil drift.

Hva betyr dette for norske virksomheter?

Sikkerhet innen OT og IoT må være sentralt i virksomhetens sikkerhetsarbeid. Angrep på OT-systemer kan være særlig attraktive for de som vil skape uro. OT og IoT er ikke lenger en skjermet teknisk sone, men integrert i virksomhetens strategiske risikobilde. Dermed står det også i frontlinjen i Norges digitale robusthet.

Tre konkrete råd

1. Skaff full oversikt over OT- og IoT-systemer, avhengigheter og sårbarheter.
2. Definer tydelige prinsipper for sikker samhandling mellom IT og OT, inkludert segmentering, tilgangsstyring og overvåkning.
3. Integrer innsikt som en etablert del av virksomhetens risikostyring.



Risevatnet-dammen i Svelgen, Bremanger. Et eksempel på kritisk infrastruktur som har vært utsatt for et cyberangrep.

Foto: Arve Olav F. Solbakken / Firdaposten / NTB

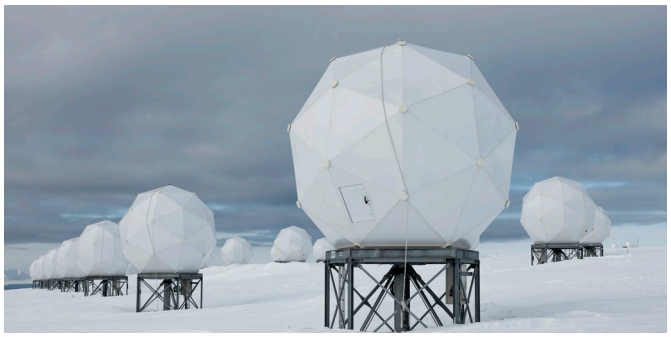
Avhengigheten til romteknologi:

En trussel vi må ta på alvor

I 2023 beskrev Totalberedskapskommisjonen romsikkerhet som evnen til å sikre stabil tilgang til satellittjenester, og tillit til signaler og data. Romsikkerhet er nå en viktig del av det digitale totalforsvaret.

Når samfunnet blir mer digitalt og avhengigheten til satellitter øker, blir også risikoen større dersom tjenester svikter, blir forstyrret eller manipulert. Både for samfunnet og for den enkelte virksomhet.

Sokratis Katsikas ved NTNU peker på at rommet lenge har vært et oversett sikkerhetsområde, til tross for hvor kritisk det er: «Norge er mer avhengig av satellitter for kommunikasjon enn mange andre land».



SvalSat på Svalbard, en sentral bakkestasjon for satellittkommunikasjon og rombasert infrastruktur.

Foto: Emile Ducke / NYT / NTB

Et trusselbilde som rammer både nasjonen og virksomhetene

Romsikkerhet og cybersikkerhet er ikke to separate domener. Angrep mot satellittsystemer kan gi umiddelbare konsekvenser for digitale tjenester, og cyberangrep kan ramme selve satellittinfrastrukturen. NSM peker i Nasjonalt digitalt risikobilde 2022 på KA-SAT-angrepet i Ukraina samme år som et tydelig eksempel. Angrepet påvirket både militær kommunikasjon i Ukraina, europeiske energitjenester og norske brukere. NSM skriver i Sikkerhetsfaglig råd 2023 at cyberangrep kan ramme satellittbaserte tjenester, og at bortfallet av satellittbaserte tjenester kan få alvorlige konsekvenser i cyberdomenet.

Denne typen hendelser viser at rominfrastrukturen ikke er en abstrakt teknologi, men en del av verdikjedene som virksomheter i alle sektorer er avhengige av. Norge har i tillegg strategisk viktig romaktivitet i Arktis, som overvåking, kommunikasjon og navigasjon for fiskeri, energi, beredskap og forsvar. Mange organisasjoner bruker satellittbaserte tjenester uten å ha dem eksplisitt identifisert som kritisk infrastruktur. Dette gjelder alt fra navigasjon og logistikkstyring til kommunikasjon, sensordata, tidsstempling og overvåking. Uten oversikt er det vanskelig å forstå konsekvensene av bortfall.

Hva betyr dette for norske virksomheter?

For virksomheter betyr dette at romsikkerhet ikke lenger er et nasjonalt ansvar alene, men også en del av virksomhetenes risiko- og beredskapsstyring. Virksomheter må være forberedt på at satellittjenester kan bli forstyrret, manipulert eller falle bort.

Det innebærer å ha alternative løsninger, gode leverandøravtaler, overvåking av tjenestene og beredskapsrutiner dersom rombasert infrastruktur svikter. Ledere må vite hvilke deler av virksomheten som er avhengige av satellittjenester, hvilke risikoer dette gir, og hvordan ansvar, kompetanse og styring skal organiseres.

Tre konkrete råd

1. Finn ut hvilke deler av virksomheten som er avhengige av satellittbaserte tjenester.
2. Lag planer for hva dere gjør hvis satellittjenester faller bort, blir forstyrret eller manipulert.
3. Integrer romsikkerhet som en del av virksomhetens helhetlige sikkerhets- og risikostyring, i tett sammenheng med cybersikkerhet.

Innovasjon og regulering:

Fra krav til konkurransefortrinn

Kravene til digital sikkerhet øker raskt. Tidligere gjaldt reguleringer bare enkelte sektorer, men dette er i ferd med å endre seg. Med den nye digitalsikkerhetsloven, DORA og nye EU-regelverk som NIS2, CER og AI Act må mange virksomheter i 2026 tilpasse seg nye krav.

For norske virksomheter betyr dette mye arbeid med å forstå og prioritere kravene. Målet er ikke bare etterlevelse, men også bedre sikkerhet og økt konkurransekraft.

Regelverkene skal styrke digital sikkerhet og tillit i Europa. Samtidig opplever mange virksomheter regelverkslandskapet som fragmentert. Sikkerhetsledere peker på ulik praktisering av NIS2 mellom europeiske land, noe som skaper utfordringer for selskaper som opererer internasjonalt. Også i Norge kan nye krav komme oppå gamle uten god samordning.

Teknologirådet peker på et tydelig geopolitisk skille: Europa bruker regulering for å skape trygghet, mens USA og Kina satser mer på innovasjon. Flere av de vi har intervjuet frykter at Norge kan bli hengende etter. Regulering er nødvendig, men Norge er ofte bedre på å regulere enn å utvikle ny teknologi.



Stortingssalen, der lover vedtas og danner grunnlaget for iverksetting av regler og styring i Norge.

Foto: Terje Pedersen / NTB

Hva betyr dette for norske virksomheter?

De nye kravene til digital sikkerhet handler ikke bare om å følge regler. Regelverkene er drivere for å forbedre sikkerhetsarbeidet og stiller ofte krav til en risikobasert tilnærming. Regelverkene vil påvirke hvordan virksomheter arbeider med risiko, dokumentasjon, sikkerhetsstyring og utvikling av teknologi.

Virksomheter som bruker kravene aktivt, kan styrke både profesjonalitet, modernisering og sikkerhetskultur. Ledelsen må sørge for at kravene blir oppfylt i tide, samtidig som reguleringene ikke hindrer utvikling og nyskaping. Målet bør være at nye regler bidrar til sterkere digital motstandskraft og bedre konkurranseevne.

Tre konkrete råd

1. Ha en helhetlig plan for nye reguleringer.
2. Bruk etterlevelsesarbeidet til å bedre sikkerheten og til å drive innovasjon.
3. Sørg for tydelig forankring i ledelsen og fremdrift.

Definisjoner

Digital Suverenitet
En nasjons eller organisasjons evne til å ha kontroll over egne data, digitale infrastrukturer, digitale tjenester og teknologiske avhengigheter.

NIS2
EUs reviderte direktiv for cybersikkerhet, som stiller krav til nettverks- og informasjonssikkerhet for virksomheter i kritiske sektorer.

CER
Søsterregelverk til NIS2. EU-direktiv som pålegger medlemsland å beskytte kritisk infrastruktur mot fysiske trusler.

AI Act
EUs lov om kunstig intelligens, som klassifiserer AI-systemer etter risikonivå og setter krav til åpenhet, sikkerhet og menneskelig kontroll.

IoT (Internet of Things)
IoT består av fysiske objekter som sensorer, kameraer og industriutstyr som er koblet til nettverk. Mange av disse er tilkoblet internett og kommuniserer data i sanntid. Teknologien er tatt i bruk i alt fra smarthjem til industri og samfunnskritisk infrastruktur.

Kvantesikkerhet
Teknologi basert på kvantefysikkens prinsipper kommer til å bryte dagens kryptering, noe som gjør kvantesikkerhet til et viktig fremtidstema.

IT vs. OT
Informasjonsteknologi (IT) håndterer data, applikasjoner og forretningsprosesser. IT skiftes ut hyppig og oppdateres ofte. Operasjonell teknologi (OT) kontrollerer og overvåker fysiske prosesser. OT kjennetegnes ofte av lang levetid og høye krav til stabil og sikker drift for å forebygge ulykker og fysisk skade. Dette innebærer at sikkerhet i OT må håndteres annerledes enn i IT, ettersom risiko for fysisk skade på mennesker, miljø og utstyr må inngå som en del av sikringsarbeidet.

Romteknologi
Teknologi som satellitter for GPS, kommunikasjon og jordobservasjon. Moderne samfunn er i stor grad avhengige av rombaserte tjenester, noe som gjør dem til en del av kritisk infrastruktur.



KPMG.no/kontakt

KPMG AS and KPMG Law Advokatfirma AS, Norwegian limited liability companies and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.