



CYBERSIKKERHET- VEIKART FOR ET TRYGGERE NORGE

Oktober 2026

Innholdsfortegnelse

Norge har kompetansen og forskningsmiljøene som trengs for å bli en ledende cybersikkerhetsnasjon. Det som mangler, er strategien, regelverket og pengene som binder dem sammen.

Sammendrag	3
1 – Hvor står Norge i 2026?	5
2 – Hva nabolandene har gjort det siste året	8
3 – Strategiske mål 2026-2030	10
4 – Strategi og nasjonalt lederskap	11
5 – Lover, regler og regulatorisk rammeverk	12
6 – Situasjonsforståelse og hendelseshåndtering	13
7 – Kommuner og lokal cyberberedskap	15
8 – Næringslivets sikkerhetsarbeid	16
9 – Motstandsdyktig infrastruktur og digital grunnmur	17
10 – Digitalt handlingsrom	19
11 – Totalberedskap og sivil motstandskraft	20
12 – Utdanning og kompetanse	21
13 – Forskning, innovasjon og samarbeid	22
14 – Budsjetttramme	24
Kilder	25

Sammendrag

Norge er sist i TEK Norges nordiske benchmark for andre år på rad.

Norden har flyttet seg det siste året. Sverige, Finland og Danmark har ny cyberlov etter NIS2 og ny eller oppdatert strategi med handlingsplan. Sverige har i tillegg satt av egne penger til kommunene. Norge har omsider fått NIS1 på plass og et budsjettløft for særlig NSM i 2027, men mangler fortsatt en gjeldende cybersikkerhetsstrategi og en NIS2-lov.

TEK Norges nordiske benchmark for 2026, utarbeidet av NyAnalyse for TEK Norge, gir Sverige 83,7 poeng, Finland 81,2, Danmark 76,0 og Norge 67,6 av 100. Sverige har tatt over førsteplassen fra Finland, som ledet i 2025. Norge ligger fortsatt sist.

Det tydeligste enkeltfunnet gjelder virksomhetene. Bare 31,5 prosent av norske foretak har dokumenterte rutiner for IKT-sikkerhet. I Danmark er andelen 59,1 og i Finland 59,4 prosent. NyAnalyse tolker dette som at norske virksomheter oftere har enkelttiltak på plass enn et systematisk og dokumentert sikkerhetsarbeid.

Det andre hovedfunnet gjelder styring og regelverk. Norge har NIS1 i kraft gjennom digitalsikkerhetsloven fra 1. oktober 2025. Finland har hatt sin NIS2-lov i kraft siden 8. april 2025, Danmark siden 1. juli 2025 og Sverige siden 15. januar 2026. NIS2 er en betydelig faktor som vil stille krav til langt flere virksomheter enn tidligere og styrke motstandskraften i samfunnet. Det er uforståelig og uheldig at vi fortsetter å bli liggende flere år etter med implementering av sentral lovgivning som Europa for øvrig for lengst har tatt i bruk.

Regjeringen foreslår i statsbudsjettet for 2027 å øke bevilgningen til Nasjonal sikkerhetsmyndighet (NSM) med 188,9 millioner kroner og å etablere et næringsberedskapsråd for cybersikkerhet. Det er riktig retning. Forslaget lukker likevel på langt nær gapet til nabolandene, fordi det mangler en strategi som binder tiltakene sammen og et regelverk på nivå med resten av Europa.

TEK Norges ti viktigste tiltak for 2027

- 1** Ny nasjonal cybersikkerhetsstrategi med finansiert handlingsplan og offentlig måling mot resultatindikatorer, vedtatt innen sommeren 2027.
- 2** NIS2- og CER-lov på høring i første halvår 2027, og fremmet for Stortinget innen utgangen av 2027.
- 3** Kommunalt cyberløft med minst 300 millioner kroner i året i øremerkede midler, felles sikkerhetsovervåking og krav til leverandørstyring.
- 4** Hjelp ved hendelser for alle små og mellomstore bedrifter, ved å utvide Næringslivets Sikkerhetsråds (NSR) cybersikkerhetssenter ut over Nærings- og fiskeridepartementets ansvarsområde, i samarbeid med blant andre TEK Norge og norske sikkerhetsselskaper.
- 5** Næringsberedskapsrådet for cybersikkerhet får mandat og ressurser til å bli et samlende punkt for hele næringslivet, og til å etablere cyberberedskapsordningen som ble varslet i totalberedskapsmeldingen.
- 6** Nordisk gjensidig anerkjennelse av sikkerhetsklareringer, slik tek-organisasjonene i Norden ber om i oppropet «A Call for Nordic Digital Resilience».
- 7** TEK Norge mener alle statlige og kommunale virksomheter som kjører kritiske tjenester i skyen bør pålegges å gjennomføre en risikoanalyse for å avklare sårbarheter og avhengigheter med forslag til konkret tiltaksplan som sentrale myndigheter må ta stilling til og medfinansiere.
- 8** Lovhjemmel for informasjonsdeling mellom NSM og private virksomheter.
- 9** Full norsk deltagelse i det nordisk-baltiske cybersamarbeidet, med egne midler.
- 10** 150 nye studieplasser i cybersikkerhet i 2027, og 500 innen 2030.

TEK Norge foreslår nye og økte midler på 2 090 millioner kroner i året, fullt innfaset fra 2028. Om lag 250 millioner kroner av dette er tidsavgrenset til 2027-2030. Rammen er beskrevet i kapittel 14.

1 – Hvor står Norge i 2026?

Nordisk benchmark 2026: Norge sist for andre år på rad

Benchmarken måler forutsetninger for cybersikkerhet i fem delområder med lik vekt: infrastruktur, forskning og utvikling, utdanning og kompetanse, sikkerhetsrutiner i næringslivet og regelverk og beredskap. Hver indikator skaleres mot beste nordiske resultat.

Land	Totalscore 2026	Rangering	Totalscore 2025	Rangering
Sverige	83,7	1	69,3	2
Finland	81,2	2	71,9	1
Danmark	76,0	3	65,9	3
Norge	67,6	4	64,1	4

Kilde: NyAnalyse for TEK Norge, «Cybersikkerhet i Norge. Nordisk benchmark» (november 2025 og oktober 2026).

Metoden er noe endret fra 2025.

Sikkerhetshendelser er tatt ut av totalscoren, fordi mørketall og ulik rapporteringspraksis gjør landtallene for usikre. Delområdene er redusert fra seks til fem. Fem av 14 variabler er oppdatert, de øvrige er videreført fra 2025, og utdanningsscoren er beregnet på en ny måte. Totalscorene for 2025 og 2026 kan derfor ikke sammenlignes direkte. NyAnalyse påpeker at Norge ville kommet noe bedre ut dersom den lave rapporterte hendelsesandelen var tatt med som i 2025. TEK Norge mener det lave tallet sier lite om sikkerhetsnivået. Vår vurdering er at Norge så langt har vært et mindre prioritert mål enn nabolandene, og at underrapporteringen av hendelser i Norge er betydelig. Næringslivets

Sikkerhetsråds Mørketallsundersøkelse 2026 viser at 18 prosent av 2 500 spurte virksomheter opplevde minst én hendelse det siste året, og at bare 12 prosent av dem anmeldte hendelsen til politiet.

Norges plass er stabil. Norge er sist både i 2025 og 2026, og sist på tre av de fem delområdene i 2026: infrastruktur, næringslivets sikkerhetsrutiner og regelverk og beredskap. Sverige leder fordi landet er best på forskning og utvikling og på utdanning og kompetanse. Sverige har også steget fra rang 41 til rang 19 i National Cyber Security Index (NCSI), noe NyAnalyse særlig knytter til gjennomføringen av NIS2.

Delområde 2026 (0-100)	Danmark	Finland	Sverige	Norge
Infrastruktur	97,5	87,1	68,7	64,1
Forskning og utvikling	27,1	65,0	100,0	50,0
Utdanning og kompetanse	65,0	55,4	77,2	66,0
Næringslivets sikkerhetsrutiner	97,5	98,4	82,2	75,3
Regelverk og beredskap (NCSI)	93,1	100,0	90,4	82,6

Kilde: NyAnalyse for TEK Norge, oktober 2026.

Fire funn som bærer veikartet

Virksomhetene mangler systematikk. 31,5 prosent av norske foretak har dokumenterte sikkerhetsrutiner, mot 59,1 i Danmark, 59,4 i Finland og 46,6 prosent i Sverige. 62,7 prosent av norske foretak har gjort ansatte kjent med sine plikter innen IKT-sikkerhet, lavest i Norden (Eurostat isoc_cisce_ra, 2024, foretak med minst ti ansatte).

Den tekniske grunnmuren har gått tilbake på ett område. Andelen norske foretak som bruker avanserte skytjenester, falt fra 68,2 prosent i 2023 til 64,8 prosent i 2025, lavest i Norden. Finland ligger på 73,1 prosent (Eurostat isoc_cicce_use, gjengitt av NyAnalyse). Rutingsikkerheten har gått motsatt vei: andelen ROA-signerte prefikser i Norge økte fra 73 til 83 prosent (Internet Society, 2025).

Kunnskapen omsettes for dårlig. Norge har 541 publikasjoner om cybersikkerhet i perioden 2021 til 2025 (OpenAlex), nest flest i Norden etter Sverige med 590. Norge har 42 patenter innen cybersikkerhet, mot 514 i Sverige. Patenttallene er ikke oppdatert siden 2025-rapporten.

Regelverket ligger etter. Norge har rang 45 globalt i NCSI med 79,17 poeng, sist oppdatert 30. september 2025. Finland har rang 2, Danmark rang 15 og Sverige rang 19. NyAnalyse

peker på manglende gjennomføring av NIS2 som hovedårsaken til at Norge ligger etter.

Hva Norge har fått på plass siden 2025

Digitalsikkerhetsloven trådte i kraft 1. oktober 2025 og gjennomfører NIS1. Regjeringen la fram den første nasjonale sikkerhetsstrategien 8. mai 2025 og Nasjonal sikkerhetsplan for digital infrastruktur 1. september 2025. Nkom oppgir at planen er foreslått finansiert med 400 millioner kroner i året.

I statsbudsjettet for 2027 foreslår regjeringen:

- 188,9 millioner kroner mer til NSM, og et næringsberedskapsråd for cybersikkerhet (Justis- og beredskapsdepartementet, 7. oktober 2026).
- 131,7 millioner kroner til digital sikkerhet, hvorav 105,7 millioner kroner til Digidirs felles løsninger og 26 millioner kroner til digital sikkerhet i kommunene (Digitaliserings- og forvaltningsdepartementet, 7. oktober 2026).
- 451,3 millioner kroner til telesikkerhet og beredskap, en økning på 40 millioner kroner. Midlene går blant annet til tre døgn reservestrøm i mobilnettene i utvalgte områder og til å klargjøre sivil infrastruktur for militære behov (Digitaliserings- og forvaltningsdepartementet, 7. oktober 2026).

Hvor står Norge?

TEK Norge støtter disse forslagene. Næringsberedskapsrådet svarer på kravet i veikartet fra 2025 om en fast samarbeidsarena mellom myndighetene og næringslivet.

Det som fortsatt mangler

Nasjonal strategi for digital sikkerhet fra 2019 er fortsatt den gjeldende cyberstrategien. TEK Norge ba i 2025-utgaven av veikartet om en ny strategi innen første halvår 2026. Den er ikke lagt fram.

NIS2- og CER-direktivet er ikke tatt inn i EØS-avtalen. Justis- og beredskapsdepartementet ga i juni 2023 DSB og NSM i oppdrag å lage utkast til høringsnotat med lovforslag for begge direktivene. Vi finner ingen høring om en slik lov per oktober 2026.

Regjeringen skrev i totalberedskapsmeldingen (Meld. St. 9 (2024-2025)) at den raskt ville starte arbeidet med å utrede en cyberberedskapsordning med myndigheter og næringsliv. TEK Norge foreslår at det nye næringsberedskapsrådet får ansvaret for å etablere ordningen.

Trusselbildet gjør etterslepet dyrere for hvert år. PST skriver i Nasjonal trusselvurdering 2026: «I 2026 forventer vi en økning i russiske cyberoperasjoner, påvirkningsoperasjoner og rekrutteringsforsøk via digitale kanaler.» NSM skriver i Risiko 2026: «Det er vesentlige mangler i det forebyggende sikkerhetsarbeidet til virksomheter i Norge.»

2 – Hva nabolandene har gjort det siste året

Tabellen viser hvor de nordiske landene står på regelverk og strategi.

	Sverige	Finland	Danmark	Norge
NIS2-lov i kraft	15.1.2026	8.4.2025	1.7.2025	Nei (NIS1 fra 1.10.2025)
CER-lov i kraft	Foreslått 1.1.2027	1.7.2025	1.7.2025	Nei
Gjeldende cyberstrategi	2025-2029	2024-2035	2026-2029	2019
Handlingsplan	91 tiltak, oppdatert mars 2026	Gjennomføringsplan, årlig oppfølging	Politisk avtale med finansiering	Ingen

Kilder: Riksdagen (SFS 2025:1506), Regeringen (prop. 2025/26:303), Finlex (124/2025 og 310/2025), Retsinformation (lov nr. 433 og 434 av 6. mai 2025), Regeringen.se (9.9.2025), regjeringen.no.

Sverige: nytt nav for cybersikkerhet og penger til kommunene

Regjeringen la fram Nationell strategi för cybersäkerhet 2025-2029 den 20. mars 2025. Handlingsplanen ble utvidet fra 72 til 91 tiltak i mars 2026. Nationellt cybersäkerhetscenter (NCSC) har fått i oppdrag å måle strategiens 13 resultatindikatorer.

Cybersäkerhetslagen (SFS 2025:1506) trådte i kraft 15. januar 2026, med krav om tidlig varsel innen 24 timer og hendelsesrapport innen 72 timer. Fra 1. juli 2026 er CERT-SE og rollen som nasjonalt kontaktpunkt etter NIS2 samlet i NCSC under Försvarets radioanstalt. En egen lov om informasjonsdeling innenfor NCSC trådte i kraft 15. juli 2026.

Budsjettet for 2026 gir en nasjonal satsing på 300 millioner svenske kroner i 2026, 350 millioner i 2027 og 400 millioner i 2028. Av dette

går 200 millioner til kommunene og 50 millioner til regionene hvert år fra 2026.

Bakgrunnen er erfaring. Angrepet mot programvareleverandøren Miljödata i august 2025 berørte minst 164 kommuner og 4 regioner, ifølge det svenske datatilsynet IMY. Myndigheten för civilt försvar meldte i mars 2026 at bare 3 av de 47 offentlige virksomhetene som har deltatt i alle fire målinger av «Cybersäkerhetskollen», har et systematisk cybersikkerhetsarbeid.

Regjeringen vedtok 28. mai 2026 en skypolicy for offentlig forvaltning med vekt på digital suverenitet.

Finland: lov på plass først, og granskning av alvorlige hendelser

Finland vedtok Kyberturvallisuusstrategia 2024-2035 den 10. oktober 2024, med en gjennomføringsplan som følges opp årlig.

Kyberturvallisuuslaki (124/2025) trådte i kraft 8. april 2025, og CER-loven (310/2025) 1. juli 2025.

Regjeringen har foreslått at Onnettomuustutkintakeskus, Finlands havarikommisjon, skal kunne granske svært alvorlige cybersikkerhetshendelser, med planlagt ikrafttredelse 1. januar 2027 (HE 71/2026).

Kyberturvallisuuskeskus hadde ved utgangen av 2025 informasjonsdelingsgrupper (ISAC) i 16 bransjer med om lag 300 deltakende organisasjoner. Senteret mottok 20 890 meldinger om cyberhendelser i 2025.

En ministergruppe la 27. april 2026 fram et veikart for digital suverenitet. Prioriteringene omfatter kontinuitet i kritiske tjenester, portabilitet, åpne grensesnitt og evnen til å bytte leverandør.

Danmark: strategi med penger og et SMB-CERT

Regjeringen og ni partier inngikk 28. januar 2026 en avtale om strategi for cyber- og informasjonssikkerhet 2026-2029. Avtalen setter av 211 millioner danske kroner i 2026 til 2029 og 33 millioner kroner årlig fra 2030. Den etablerer blant annet et offentlig-privat SMV-CERT for små og mellomstore bedrifter, et nasjonalt øvingskonsept og et sivilt

cyberprogram. Danmark har også opprettet en egen budsjettpost for Nordic-Baltic Cyber Consortium.

Beredskapsavtalen fra januar 2025 satte av 100 millioner danske kroner årlig fra 2025 til 2033 til et høyt felles cybersikkerhetsnivå. I desember 2025 prioriterte regjeringen om lag 1 milliard danske kroner over fire år til et felles døgnbemannet situasjonssenter, et cyberoperasjonssenter og et overvåkingsnettverk.

Forsvarets Etterretningstjeneste vurderte 18. desember 2025 at Russland sto bak et ødeleggende cyberangrep mot et dansk vannverk i 2024, og at gruppen bak DDoS-angrep i forkant av kommune- og regionvalget i 2025 har forbindelser til russiske myndigheter.

Hva Norge bør lære

To grep går igjen hos alle tre naboland og mangler i Norge: en lov på NIS2-nivå og en cyberstrategi fra de siste to årene med handlingsplan. Sverige har i tillegg målbare indikatorer og egne midler til kommunene. Danmark har knyttet strategien til egen finansiering og etablerer et SMB-CERT. TEK Norge mener kommunene og de små og mellomstore bedriftene er de svakeste leddene, og at Norge bør lære mest av tiltakene som er rettet mot dem.

3 – Strategiske mål 2026-2030

TEK Norge mener Norge bør ha disse målene for perioden fram til 2030:

- 1 – Ny nasjonal cybersikkerhetsstrategi med finansiert handlingsplan vedtas innen sommeren 2027, og følges opp med en årlig offentlig rapport mot målbare indikatorer.
- 2 – NIS2- og CER-lov fremmes for Stortinget innen utgangen av 2027.
- 3 – Norske bedrifters sikkerhetspraksis heves til nordisk gjennomsnitt på alle måleområder innen 2030. Andelen foretak med dokumenterte sikkerhetsrutiner er nøkkeltallet.
- 4 – Alle kommuner har et dokumentert minimumsnivå for cybersikkerhet og er knyttet til en felles sikkerhetsovervåking innen 2028.
- 5 – Statlige og kommunale virksomheter som kjører kritiske tjenester i skyen, har gjennomført en risikoanalyse og tiltaksplan innen utløpet av 2027.
- 6 – Hendelses- og krisehåndteringskapasiteten i Norge er best i Norden innen 2030.
- 7 – Norge deltar fullt i det nordisk-baltiske cybersamarbeidet, med felles øvelser og felles situasjonsbilde.

4 – Strategi og nasjonalt lederskap

Norge er det eneste av de fire landene i benchmarken som styrer etter en cyberstrategi fra før 2024.

Nasjonal strategi for digital sikkerhet er fra 2019. Siden da har Norge fått en nasjonal sikkerhetsstrategi og en sikkerhetsplan for digital infrastruktur, men ingen av dem er en cyberstrategi for hele samfunnet. Sverige har en strategi for 2025 til 2029 med 91 tiltak og 13 resultatindikatorer. Danmark har en strategi for 2026 til 2029 med egen finansiering. Finland følger opp sin strategi årlig.

TEK Norges forslag til konkrete tiltak:

4.1 Ny nasjonal cybersikkerhetsstrategi innen sommeren 2027

- Strategien skal dekke alle samfunnssektorer og forvaltningsnivåer, og bygge på en kartlegging av dagens situasjon.
- Handlingsplanen skal være finansiert, slik den danske strategien er, og oppdateres jevnlig, slik den svenske ble i mars 2026.
- Strategien bør legges fram i tide til budsjettprosessen for 2028. Målet i 2025-utgaven om en handlingsplan klar til budsjettprosessen i 2027 er ikke nådd.

4.2 Målbare indikatorer og årlig rapport

- Regjeringen bør fastsette et sett resultatindikatorer og gi NSM i oppdrag å måle dem årlig, etter modell av oppdraget det svenske NCSC fikk i oktober 2025.
- Rapporten bør være offentlig og omfatte kommunene. Den bør også sammenligne Norge med de øvrige nordiske landene.

4.3 Cybersikkerhet i budsjett- og styringsdialogen

- Tildelingsbrevene fra alle departementer bør ha eksplisitte mål for cybersikkerhet, med måleparametere som viser effekt.

4.4 Næringsberedskapsrådet for cybersikkerhet

- TEK Norge støtter regjeringens forslag om et næringsberedskapsråd. Rådet bør få et klart mandat, faste møter og representasjon fra sikkerhetsbransjen, de store digitale tjenesteleverandørene og små og mellomstore bedrifter.
- Rådet bør få i oppdrag å etablere cyberberedskapsordningen som regjeringen varslet i totalberedskapsmeldingen, innen utgangen av 2027.

5 – Lover, regler og regulatorisk rammeverk

Nabolandene har hatt NIS2 i kraft i opptil halvannet år. Norge fikk NIS1 i oktober 2025, ni år etter at direktivet ble vedtatt i EU.

NIS2 stiller krav til ledelsens ansvar, risikostyring, leverandørkjeder og rapportering innen 24 timer. Så lenge Norge står utenfor, får norske virksomheter et annet og lavere nivå enn konkurrentene i Norden. Norske konsern med virksomhet i nabolandene må forholde seg til to regimer. NyAnalyse peker på gjennomføringen av NIS2 som hovedforklaringen på Sveriges framgang i NCSI.

TEK Norges forslag til konkrete tiltak:

5.1 NIS2- og CER-lov på høring i første halvår 2027

- Høringsnotatet som DSB og NSM fikk i oppdrag å lage i 2023, bør sendes på høring senest i første halvår 2027.
- Loven bør fremmes for Stortinget innen utgangen av 2027.

5.2 Gjennomføring av CRA og KI-forordningen

- Cyber Resilience Act og KI-forordningen bør gjennomføres i takt med EU, slik at norske

leverandører av digitale produkter har de samme reglene som konkurrentene i EU.

5.3 Koordinert håndheving og tilsynsforum

- Myndighetene med ansvar for digitalsikkerhetsloven, NIS2, DORA, CRA og KI-forordningen bør pålegges et felles tilsynsforum, med felles forståelse av overlappende krav og en felles veileder.
- Regjeringen må klargjøre hvilken sektormyndighet som er kontaktpunkt for den enkelte virksomhet.

5.4 Lovhjemmel for informasjonsdeling

- Sverige har fra 15. juli 2026 en egen lov om informasjonsplikt mellom myndighetene som samarbeider i landets nasjonale cybersikkerhetssenter. Norge bør gå lenger og utrede en hjemmel som også gjør det mulig for NSM og private virksomheter å dele trusselinformasjon raskt og lovlig.

6 – Situasjonsforståelse og hendelseshåndtering

Bare 12 prosent av virksomhetene som ble rammet av en hendelse det siste året, anmeldte den til politiet, ifølge Næringslivets Sikkerhetsråds Mørketallsundersøkelse 2026.

Norge hadde færrest rapporterte sikkerhetshendelser i Norden i benchmarken for 2025, og NyAnalyse har tatt hendelsestallene ut i 2026 fordi mørketallene er store. Av virksomhetene som lot være å anmelde, mente 42 prosent at hendelsen var ubetydelig. Mørketallene gjør at ingen har et fullstendig bilde av hva som rammer norske virksomheter. Rapporteringsplikten i digitalsikkerhetsloven gjelder tilbydere av samfunnsviktige tjenester og digitale tjenester. Danmark bygger et overvåkingsnettverk som skal være fullt utbygget i 2029. Finland har informasjonsdelingsgrupper i 16 bransjer.

TEK Norges forslag til konkrete tiltak:

6.1 Lavere terskel for rapportering

- Automatiserte rapporteringsløsninger og felles standarder for beskrivelse av hendelser, slik at datagrunnlaget får høy kvalitet.
- Støtte til virksomheter som rapporterer, slik at rapportering lønner seg.

6.2 Nasjonalt sensornettverk

- NSMs sensorsystem bør moderniseres og utvides til flere private og kommunale nettverk, etter modell av det danske overvåkingsnettverket.
- Strukturerte data bør deles i standardiserte formater, slik at analysen kan automatiseres.

6.3 Informasjonsdeling med næringslivet

- NSM bør bygge bransjevis informasjonsdelingsgrupper (ISAC) for alle sektorer i NIS2, etter finsk modell, med deltakelse fra næringslivet.
- Det trengs en betrodd plattform der myndighetene deler trusselinformasjon og hendelsesinformasjon strukturert og raskt med operatørene av digital infrastruktur og sikkerhetsbransjen, innenfor gjeldende regler for gradering. Det er også anbefalingen i det nordiske oppropet.

6.4 Åpenhet og læring etter alvorlige hendelser

- Lørenskog kommune publiserte en uavhengig lærings- og forbedringsrapport etter dataangrepet i 2026. TEK Norge mener offentlige virksomheter som rammes av alvorlige hendelser, bør gjøre det samme, og at NSM bør samle og formidle lærdommene.

6.5 Tydelig rollefordeling i hendelseshåndteringen

- NSM bør ha en koordinerende rolle ved hendelser med nasjonal sikkerhetsbetydning som får konsekvenser i flere sektorer, og bistå med spesialkompetanse ved behov, også overfor virksomheter som ikke er omfattet av sikkerhetsloven.
- Virksomheter uten sektorvis responsmiljø skal fortsatt kunne melde til NSM, som så langt det lar seg gjøre viderefremidler saker til responsmiljøene eller til virksomheter i

Hendelseshåndtering

Kvalitetsordningen for håndtering av IKT-sikkerhetshendelser.

- Kripos ved NC3 bør i større grad rette ressursene inn mot alvorlig cyberkriminalitet og omfattende etterforskninger. Regjeringen bør avklare hvem som følger opp den stadig økende digitale svindelen og mindre alvorlig cyberkriminalitet.

7 – Kommuner og lokal cyberberedskap

Lørenskog kommune ble rammet av et dataangrep våren 2026. Angriperne hentet ut 1,8 terabyte data, blant annet personsensitive opplysninger.

Kommunene leverer tjenester alle er avhengige av, men har et stort antall systemer, teknisk gjeld og varierende kompetanse. Lørenskog er det ferskeste norske eksempelet. Angrepet ble oppdaget 9. mai 2026. Kommunen mistet e-post en periode, og saksbehandlingen i Nav Lørenskog ble forsinket. Deloitte gjennomgang for kommunen fant at ikke alle identifiserte risikoer og sårbarheter var fulgt opp, at sikkerhetsvarsler ikke raskt nok førte til tiltak, og at avviklingen av enkelte eldre systemer ikke var fulgt opp tilstrekkelig. Kapasitet, kompetanse og ressurser innen IKT- og sikkerhetsarbeidet var ifølge kommunen en vesentlig bidragende faktor.

I Sverige viste angrepet mot Miljödata i 2025, som berørte minst 164 kommuner, hvordan én leverandør kan bli et felles sårbart punkt for hundrevis av virksomheter. Sverige svarte med 200 millioner svenske kroner i året til kommunene og 50 millioner til regionene. Regjeringens forslag for 2027 gir 26 millioner kroner til digital sikkerhet i norske kommuner. Det er et første steg.

TEK Norges forslag til konkrete tiltak:

7.1 Øremerkede midler til kommunene

- 300 millioner kroner i året til et kommunalt cyberløft, fordelt etter innbyggertall og risiko,

og knyttet til krav om et dokumentert minimumsnivå.

7.2 Felles sikkerhetsovervåking for kommunene

- Alle kommuner bør knyttes til felles sikkerhetsovervåking, gjennom Helse- og KommuneCERT eller i samarbeid med private sikkerhetsselskaper. Mindre kommuner bør kunne kjøpe tjenesten samlet.

7.3 Leverandørstyring og konsentrasjonsrisiko

- KS og statsforvalterne bør kartlegge hvilke leverandører mange kommuner er avhengige av, og det bør stilles felles sikkerhetskrav i avtalene.

7.4 Cyber i de kommunale beredskapsrådene

- Cyberberedskap bør inn som fast tema i de kommunale og regionale beredskapsrådene, med egne cyberberedskapsteam der kommunene samarbeider regionalt.

7.5 Valgsikkerhet før kommunevalget 2027

- NSM bør få i oppdrag å styrke cybersikkerheten rundt kommune- og fylkestingsvalget i 2027, slik det svenske NCSC fikk for valgene i 2026. Danmark opplevde DDoS-angrep før kommunevalget i 2025.

8 – Næringslivets sikkerhetsarbeid

Bare 31,5 prosent av norske foretak har dokumenterte sikkerhetsrutiner. I Danmark og Finland er andelen om lag 59 prosent.

Små og mellomstore bedrifter i verdikjedene til totalforsvaret er særlig utsatt. Mange av dem faller utenfor sikkerhetsloven og digitalsikkerhetsloven, men er underleverandører til virksomheter som omfattes. De trenger praktisk hjelp, utover veiledere fra myndighetene. Næringslivets Sikkerhetsråd (NSR) er utpekt som sektorvis responsmiljø og driver et cybersikkerhetssenter for næringslivet, etablert med støtte fra Nærings- og fiskeridepartementet (NFD). Senteret dekker de delene av næringslivet som hører under NFDs ansvarsområde og ikke allerede er dekket av andre responsmiljøer. Danmark etablerer et offentlig-privat SMV-CERT for alle små og mellomstore bedrifter. Sverige gir NCSC og Myndigheten för civilt försvar i oppdrag å lage veiledning for små og mellomstore bedrifter utenfor NIS2.

TEK Norges forslag til konkrete tiltak:

8.1 Hjelp ved hendelser for alle små og mellomstore bedrifter

- Norge bør bygge videre på Næringslivets Sikkerhetsråds cybersikkerhetssenter, men bygge ut ordningen. Senteret bør utvides til å dekke små og mellomstore bedrifter i alle næringer, også utenfor NFDs ansvarsområde, med finansiering fra flere departementer.

- Hjelpen ved hendelser bør gis i samarbeid med selskaper i Kvalitetsordningen for håndtering av IKT-sikkerhetshendelser, etter modell av det danske SMV-CERT.

8.2 Sikkerhetssjekk for små og mellomstore bedrifter

- En tilskuddsordning der bedrifter får dekket deler av kostnaden ved en sikkerhetsgjennomgang og etablering av dokumenterte rutiner hos et kvalitetsmerket sikkerhetsselskap.

8.3 Kvalitetsmerking av sikkerhetsleverandører

- Det bør vurderes å innføre en kvalitetsmerking av leverandører med et grunnleggende kvalitets- og sikkerhetsnivå, etter mal av Kvalitetsordningen. Merkingen bør omfatte sikkerhetsledelse og rådgivning, sikkerhetsovervåking og sikkerhetstesting, og kan i sin enkleste form bygge på NSMs Cybersjekk.

8.4 Cyberforsikring

- Norsk næringsliv bør i større grad vurdere forsikring mot cyberhendelser. Myndighetene og forsikringsbransjen bør sammen se på hvordan forsikringsvilkår kan belønne dokumentert sikkerhetsarbeid.

9 – Motstandsdyktig infrastruktur og digital grunnmur

Norge har lavest score i Norden på infrastruktur, og andelen foretak som bruker avanserte skytjenester har falt siden 2023.

Nasjonal sikkerhetsplan for digital infrastruktur og forslaget om 451,3 millioner kroner til telesikkerhet og beredskap i 2027 er viktige grep. Regjeringen har flyttet penger fra bredbåndsutbygging til sikkerhet og oppetid i nettene. I budsjettet for 2026 foreslo regjeringen å redusere statens midler til bredbåndsutbygging gjennom fylkeskommunene fra 415 millioner kroner i 2025 til 34 millioner kroner i 2026. TEK Norge mener sikkerhet og utbygging må finansieres hver for seg, slik at det ene ikke går på bekostning av det andre. NATO-landenes mål om å bruke inntil 1,5 prosent av BNP innen 2035 på blant annet beskyttelse av kritisk infrastruktur og sivil beredskap, bør brukes til å styrke den digitale grunnmuren ytterligere.

TEK Norges forslag til konkrete tiltak:

9.1 Sikkerhetskrav i offentlige anskaffelser

- Stortinget vedtok i januar 2026 en ny § 5d i anskaffelsesloven: oppdragsgiver «kan stille krav eller kriterier i alle ledd av en anskaffelsesprosess for å ivareta sikkerhets- og beredskapshensyn», og «bør vurdere å stille slike krav i anskaffelser der det er relevant». TEK Norge ba i 2025 om en plikt. Når loven bare åpner for krav, må veiledning og praksis gjøre jobben.
- DFØ og NSM bør lage en veileder med standardkrav til cybersikkerhet, og staten bør gjøre slike krav til hovedregel i egne

anskaffelser av digitale tjenester og infrastruktur.

- Kontraktsvilkår om sikkerhet, redundans og leverandørkrav bør brukes aktivt. Det nordiske oppropet anbefaler slike vilkår framfor ny lovgivning som kan fragmentere markedet.

9.2 Styrke sikkerhet og redundans i digital infrastruktur

- Insentivordninger for private investeringer i redundans der utbyggingen ikke er kommersielt forsvarbar, som alternativ til direkte offentlig finansiering.
- Flere cybersikre forbindelser til alle deler av landet, særlig Nord-Norge og øyområdene, og reserveløsninger med nordiske partnere.
- De nordiske landene bør utrede hvordan regelverket for digital infrastruktur kan forenkles og harmoniseres, blant annet for tillatelser og saksbehandlingstid ved bygging av fiber og sjøkabler på tvers av grensene.

9.3 Drift og fjernstyring av nett på tvers av grensene

- Operatørene må kunne overvåke, styre og rute om trafikk på tvers av de nordiske grensene i sanntid. Norge bør sammen med bransjen og nabolandene utrede felles rammer for grenseoverskridende drift og fjernstyring av nett, som ivaretar nasjonal sikkerhet og krav til datalagring.

9.4 Nordisk koordinering av forsyningskjeder

- Norge bør sammen med de nordiske landene utrede tettere samordning av risikovurderinger, informasjon om kritiske avhengigheter og leverandørkrav for kritisk teknologi.
- Sivile og militære beredskapskrav til digital infrastruktur bør samordnes, også med NATO og EU, slik at operatørene får klare rammer for vertslandsstøtte og tilgang til kritiske komponenter i krise.

9.5 Sikker ruting og grunnleggende internetsikkerhet

- Andelen ROA-signerte prefikser i Norge har økt fra 73 til 83 prosent. Danmark ligger på 93 prosent. Nkom bør sette et mål om full dekning hos norske nettverksoperatører.

9.6 Beskyttelse av undersjøisk infrastruktur

- Kabelskadene i Finskebukta etter skipet Eagle S i desember 2024 førte til straffesak i Finland, med tiltale for grov ødeleggelse og grov forstyrrelse av telekommunikasjon. Norge bør sikre at overvåking, rettslig grunnlag og reparasjonsberedskap for undersjøiske kabler er på plass.

10 – Digitalt handlingsrom

NSM skriver i Risiko 2026: «Planlegg for å kunne bytte ut skyleverandør effektivt og med kjent ressursbruk og kostnad». TEK Norge mener en myndighet må få ansvar for å følge opp at det skjer.

Norge bør bruke mer skytjenester.

Benchmarken viser at norske virksomheter bruker avanserte skytjenester minst i Norden. Samtidig er markedet dominert av noen få leverandører, og NSM peker særlig på amerikanske selskaper. Svaret er skybruk med kontroll: kunnskap om hvilke avhengigheter Norge har, og evne til å bytte leverandør hvis det blir nødvendig.

Sverige vedtok en skypolicy for offentlig forvaltning 28. mai 2026. Finland la 27. april 2026 fram et veikart for digital suverenitet, med vekt på portabilitet og evne til å bytte leverandør. I Norge ble komiteens tilråding om at regjeringen kontinuerlig skulle kartlegge Norges digitale avhengigheter, forkastet i Stortinget 7. mai 2026 (Innst. 225 S (2025-2026)).

TEK Norges forslag til konkrete tiltak:

10.1 Årlig kartlegging av digitale avhengigheter

- Regjeringen bør kartlegge Norges kritiske digitale avhengigheter og rapportere til

Stortinget årlig.

10.2 Risikoanalyse og tiltak som krav for kritiske tjenester

- TEK Norge mener alle statlige og kommunale virksomheter som kjører kritiske tjenester i skyen bør pålegges å gjennomføre en risikoanalyse for å avklare sårbarheter og avhengigheter med forslag til konkret tiltaksplan som sentrale myndigheter må ta stilling til og medfinansiere.

10.3 Avklaring av nasjonal sky

- Regjeringen bør avklare formålet med en nasjonal sky og hvilke tjenester den skal dekke, før det bevilges mer penger. Norske og nordiske leverandører bør få konkurrere om oppdraget.

10.4 Nordisk samarbeid om digital suverenitet

- Norge bør samarbeide med de nordiske landene om felles krav til portabilitet og exit i offentlige skyanskaffelser, slik at kravene får tyngde overfor de store leverandørene.

11 – Totalberedskap og sivil motstandskraft

Digitale trusler er de mest aktuelle vi står overfor, og cyber må inn i alle deler av totalberedskapen.

Totalberedskapsmeldingen etablerte et nytt grunnlag for sivil motstandskraft. TEK Norge mener cyber fortsatt har for liten plass i den, og at samordningen med privat sektor er for svak. Erfaringer fra offentlige og private virksomheter i Ukraina bør brukes aktivt i det norske totalforsvaret.

TEK Norges forslag til konkrete tiltak:

11.1 Tilfluktsrom 2.0

- Kravet til tilfluktsrom bør omfatte god dekning og reservestrøm, slik at befolkningen har digital tilgang under kriser.

11.2 Befolkningsopplæring «Sikker digital hverdag»

- Myndighetene bør stå bak et opplæringstilbud til befolkningen, og samle all informasjon om digital sikkerhet og hendelser i én portal for enkeltpersoner og bedrifter.

11.3 Virksomhetsopplæring

- Norske sikkerhetsselskaper bør brukes til målrettet opplæring av virksomheter i totalforsvarets verdikjeder, i et offentlig-privat samarbeid.

12 – Utdanning og kompetanse

Norge er nest best i Norden på utdanning og kompetanse. Kompetansen når for sjelden ut i virksomhetene.

Norge har en bred studieportefølje i cybersikkerhet og andreplass på utdanning og kompetanse i benchmarken. Sverige leder med flest masterprogrammer. Søkningen viser at det er plass til flere. Fire av NTNUs toårige masterprogram innen informasjonssikkerhet, cybersikkerhet og digital sikkerhet, blant dem ett erfaringsbasert deltidsprogram, hadde 513 norske og nordiske søkere med programmet som førsteprioritet til 169 plasser i 2026 (vår sum av NTNUs søkertall). Regjeringen ga 100 nye studieplasser i IKT i 2025 og 100 i kvanteteknologi i 2026, men foreslår ingen nye plasser i cybersikkerhet for 2027.

TEK Norges forslag til konkrete tiltak:

12.1 150 nye studieplasser i cybersikkerhet i 2027, og 500 innen 2030

- 150 nye studieplasser i 2027 er på nivå med det regjeringen har gitt til IKT og kvanteteknologi tidligere. Opptappingen til 500 bør styres etter søkningen, med vekt på

praksisprogrammer mellom utdanningsinstitusjoner og næringsliv og på erfaringsbaserte masterprogram for folk i jobb.

12.2 Obligatorisk opplæring for ledere

- Obligatorisk opplæring i IKT-sikkerhet for ledelsen i alle offentlige virksomheter. NIS2 stiller tilsvarende krav til ledelsen i virksomhetene loven omfatter, og den svenske loven har gjennomført dette kravet.

12.3 Sikkerhet i skolen

- IKT-sikkerhet bør inn i læreplanen, og lærere bør få kompetanseheving i IKT-sikkerhet.

12.4 Omskolering og karriereprogram

- Danmark etablerer et sivil cyberprogram for blant annet tidligere cybervernepliktige. Norge bør utrede et tilsvarende program som bruker kompetansen fra Forsvaret i sivil sektor.

13 – Forskning, innovasjon og samarbeid

Forskning og innovasjon

Norge har nest flest publikasjoner om cybersikkerhet i Norden, men 42 patenter mot Sveriges 514.

Norge har sterke forskningsmiljøer, blant annet ved NTNU, UiO og Simula. Utfordringen er å gjøre forskning om til produkter og tjenester. Cybersikkerhet utvikles mest reaktivt og i industrien, og forskningsmiljøene trenger tilgang til reelle data og hendelser. Forskningsrådet lyste i 2026 ut 200,8 millioner kroner til flerårige prosjekter om sikkerhet, pålitelighet og motstandsdyktighet i digitale økosystemer. Til sammenligning har regjeringen satt av 150 millioner kroner årlig i minst fem år til kvanteteknologi og 132 millioner kroner årlig over fem år til forskning på forsvarsevne, sikkerhet og beredskap. Regjeringen foreslår 30 millioner kroner i 2027 til at KI Norge kan arbeide med KI-sikkerhet.

TEK Norges forslag til konkrete tiltak:

- **13.1 Økt grunnfinansiering:** 100 millioner kroner ekstra i året til forskning og innovasjon innen kryptologi og KI-sikkerhet, utover det som er satt av til kvanteteknologi. Det gir rom

for et nasjonalt forskningssenter på nivå med de nye KI-sentrene og en årlig utlysning.

- **13.2 Tett samarbeid mellom akademisk og næringsliv:** innovasjonsmidler knyttet til klynger rundt forskningsmiljøene, og bedre tilgang til reelle data og sikkerhetsklarering for forskere.
- **13.3 Videreutvikling av Norwegian Cyber Range ved NTNU Gjøvik:** det eksisterende testmiljøet ved NTNU i Gjøvik bør videreutvikles til et nasjonalt testmiljø for realistisk testing og øving, i samarbeid med Forsvaret og næringslivet.
- **13.4 KI og cybersikkerhet:** NSM bør få i oppdrag å kartlegge hvordan KI endrer trusselbildet og forsvarsevnen, slik Sverige har gjort i 2026.
- **13.5 Offentlige anskaffelser som innovasjonsverktøy:** offentlige anskaffelser bør brukes strategisk til å utvikle norsk sikkerhetsindustri.

Nordisk og internasjonalt samarbeid

Norden bør være én sikkerhetssone. Det nordisk-baltiske cybersamarbeidet er stedet å begynne.

TEK Norge står sammen med IT-Branchen i Danmark, TechSverige og FiCom i Finland bak oppropet «A Call for Nordic Digital Resilience». Oppropet har seks anbefalinger: mer

harmonisert regelverk for digital infrastruktur, en felles nordisk modell for sikkerhetsklarering, rammer for grenseoverskridende drift og fjernstyring av nett, nordisk koordinering av

forsyningskjeder, tettere samarbeid om trusselhåndtering og respons, og felles nordiske cyberøvelser. Anbefalingene er tatt inn i dette veikartet, i kapittel 6, 9 og 13.

Danmark har opprettet en egen budsjettpost for Nordic-Baltic Cyber Consortium, som skal gi felles tilgang til kommersiell trusselinformasjon og en felles plattform for datadeling mellom de nasjonale cybermyndighetene. Norge bør delta fullt og med egne midler.

TEK Norges forslag til konkrete tiltak:

- **13.6** Full deltakelse i Nordic-Baltic Cyber Consortium, med egne midler og en plan for hvordan Norge bidrar.
- **13.7 Gjensidig nordisk sikkerhetsklarering:** De nordiske landene bør straks godta hverandres personellklareringer, for eksempel ved å revidere eller supplere den nordiske sikkerhetsavtalen fra 2010 slik at den også omfatter personell, objekter og infrastruktur. På lengre sikt bør Norden få en felles klareringsmodell med like kriterier og saksbehandlingstider.
- **13.8 Dual use i forsvarsløftet:** en del av forsvarsløftet bør brukes til cybersikkerhetsprodukter med både sivil og militær nytte.
- **13.9 Felles nordisk infrastruktur og respons:** rutining av fiber og mobil på tvers av grensene, felles reserveløsninger og felles

beredskapslager for kritiske komponenter. De nordiske landene bør ta initiativ til en avtale om beskyttelse, redundans og gjenoppretting av felles digital infrastruktur, med felles eskaleringsrutiner og felles planverk for respons, og samarbeide tettere om trusselhåndtering i EU og NATO.

Øvelser

TEK Norges forslag til konkrete tiltak:

- **13.10** Nasjonal bi-årlig cyberøvelse, med «black sky»-scenarier der flere sektorer rammes av langvarige utfall.
- **13.11** Sektorvise øvelser for virksomheter under digitalsikkerhetsloven, med offentlige midler.
- **13.12** Norsk deltakelse i NATO-øvelser som Locked Shields og Crossed Swords, med en fast gruppe sertifiserte norske private selskaper.
- **13.13 Felles nordiske cyberøvelser:** Norge bør ta initiativ til avgrensede nordiske øvelser der myndigheter, forsvaret, operatører av digital infrastruktur og sikkerhetsselskaper tester samordning og beslutningslinjer ved hendelser på tvers av grensene, slik oppropet anbefaler. Danmark utvikler et nasjonalt øvingskonsept, og Finlands budsjettforslag for 2027 samler 1,5 millioner euro til samlet finansiering av cyberøvelser.

Budsjettramme

TEK Norge foreslår beløp knyttet til tiltakene over. Beløpene er ambisjoner for å nå målene i kapittel 3. Rammen er 2 090 millioner kroner i året i nye og økte midler, fullt innfaset fra 2028. Om lag 250 millioner kroner i året er tidsavgrenset til 2027-2030 og går til å bygge ut sensornettverket (kap. 6), felles sikkerhetsovervåking og utfasing av teknisk gjeld i kommunene (kap. 7), digitalt handlingsrom og avklaring av nasjonal sky (kap. 10) og videreutvikling av testmiljøet ved NTNU Gjøvik (kap. 13). Driften av det som bygges, ligger i rammen. Etter 2030 er den varige økningen om lag 1 840 millioner kroner i året.

Nye og økte årlige midler (millioner kroner)

Område	2025-utgaven	2026-utgaven
Strategi og nasjonalt lederskap (kap. 4)	50	50
Lover, regler og tilsyn (kap. 5)	20	40
Situasjonsforståelse og hendelseshåndtering (kap. 6)	80	205
Kommuner og lokal cyberberedskap (kap. 7)	Del av kap. 3	460
Næringslivets sikkerhetsarbeid (kap. 8)	Del av kap. 3, 4 og 5	150
Infrastruktur og digital grunnmur (kap. 9)	400	400
Digitalt handlingsrom (kap. 10)	Ny	75
Totalberedskap og sivil motstandskraft (kap. 11)	100	100
Utdanning og kompetanse (kap. 12)	800	250
Forskning og innovasjon (kap. 13)	400	210
Nordisk og internasjonalt samarbeid (kap. 13)	50	50
Øvelser (kap. 13)	100	100
Sum	2 000	2 090

Rammen er nye og økte midler sammenlignet med 2026. Beløpene til utdanning og forskning er satt ned fra 2025-utgaven, slik at de står i forhold til søkningen og til dagens forskningsbevilgninger. Regjeringens forslag for 2027 om mer penger til NSM, digital sikkerhet i kommunene og telesikkerhet dekker deler av kapittel 6, 7 og 9.

Dette oppdaterte veikartet bygger på de politiske beslutningene som er tatt siden 2023 og på erfaringene fra

nabolandene det siste året. Norge har kompetansen og forskningsmiljøene som trengs for å bli en ledende cybersikkerhetsnasjon. Det som mangler, er strategien, regelverket og pengene som binder dem sammen.

TEK Norge, oktober 2026

Advokat Pål Wien Espen

Direktør infrastruktur, sikkerhet og forsvar

Kilder

- NyAnalyse for TEK Norge: Cybersikkerhet i Norge. Nordisk benchmark 2026, oktober 2026.
- NyAnalyse for TEK Norge: Cybersikkerhet i Norge. Nordisk benchmark 2025, november 2025. teknorge.no
- Internet Society: ROA-signerte prefikser (IPv4), 2025. OpenAlex: publikasjoner om cybersikkerhet 2021-2025.
- Eurostat: isoc_cisce_ra (sikkerhetstiltak i foretak, 2024) og isoc_cisce_use (skytjenester, 2025).
- National Cyber Security Index, landsider for Norge, Sverige, Finland og Danmark. ncsi.ega.ee
- Justis- og beredskapsdepartementet: Ny lov om digital sikkerhet trer i kraft i dag, 1.10.2025. regjeringen.no
- Justis- og beredskapsdepartementet: Regjeringen styrker den nasjonale cybersikkerheten, 7.10.2026. regjeringen.no
- Digitaliserings- og forvaltningsdepartementet: pressemeldinger om statsbudsjettet 2027, 7.10.2026. regjeringen.no
- Nkom: Nasjonal sikkerhetsplan for digital infrastruktur, oppdatert 20.3.2026. nkom.no
- Justis- og beredskapsdepartementet: Supplerende tildelingsbrev til DSB og NSM om høringsnotat for NIS2 og CER, 8.6.2023.
- Regjeringen: EØS-notat om NIS2-direktivet. regjeringen.no
- Meld. St. 9 (2024-2025) Totalberedskapsmeldingen, pkt. 1.3. regjeringen.no
- Stortinget: Innst. 225 S (2025-2026) og votering 7.5.2026 i sak om Dokument 8:119 S (2025-2026). stortinget.no
- PST: Nasjonal trusselvurdering 2026. pst.no
- Næringslivets Sikkerhetsråd: Mørketallsundersøkelsen 2026, s. 48-50. nsr-org.no
- Nærings- og fiskeridepartementet: Etablerer nytt cybersikkerhetssenter for næringslivet, 20.8.2025. regjeringen.no
- Lørenskog kommune: pressemeldinger om IT-hendelsen og Deloitte's lærings- og forbedringsrapport, 10.9.2026. lorenskog.kommune.no
- Stortinget: Lovvedtak 26 (2025-2026) om endringer i anskaffelsesloven, § 5d. stortinget.no
- Prop. 1 S (2026-2027) Digitaliserings- og forvaltningsdepartementet, kap. 1543 post 70. regjeringen.no
- Regjeringen: Justerer pengebruken fra dekning til sikkerhet og oppetid i mobil- og bredbåndsnettene, 15.10.2025. regjeringen.no
- Digdir: Skiftende skydekke. En Skate-rapport om endringsevne i bruken av skytjenester, 2026. digdir.no
- NTNU: Søkertall 2-årige masterprogram 2026. ntnu.no
- Regjeringen: pressemeldinger om høyere utdanning og forskning i statsbudsjettene for 2025, 2026 og 2027. regjeringen.no
- Forskningsrådet: Sikkerhet, pålitelighet og motstandsdyktighet i digitale økosystemer, utlysning 2026. forskningssradet.no
- IT-Branchen, TEK Norge, TechSverige og FiCom: A Call for Nordic Digital Resilience.
- NSM: Risiko 2026, s. 8 og 35. nsm.no
- Regeringen (Sverige): Nationell strategi för cybersäkerhet 2025-2029 (20.3.2025), handlingsplan oppdatert 2026 (5.3.2026), Sveriges cybersäkerhet ska mätas (31.10.2025), Nationell satsning på cybersäkerhet (9.9.2025), Sveriges cybersäkerhetscenter får utökat ansvar (20.11.2025), Regeringen stärker cybersäkerheten inför valåret 2026 (21.11.2025), molnpolicy (28.5.2026), prop. 2025/26:303. regjeringen.se
- Riksdagen: Cybersäkerhetslag (SFS 2025:1506). Lag om uppgiftsskyldighet vid samverkan inom det nationella cybersäkerhetscentret (SFS 2026:1200). riksdagen.se
- CERT-SE: Nu samlas cyberverksamheten hos NCSC, 12.6.2026. cert.se
- IMY: Omfattande personuppgiftsincident hos Miljödata, august 2025. imy.se
- Myndigheten för civilt försvar: Fjärde Cybersäkerhetskollen, 2.3.2026. mcf.se
- Valtioneuvosto (Finland): Kyberturvallisuusstrategia 2024-2035 (10.10.2024), veikart for digital suverenitet (27.4.2026), LVM budsjettforslag 2027 (21.9.2026). valtioneuvosto.fi
- Finlex: Kyberturvallisuuslaki 124/2025 og lov 310/2025. finlex.fi
- Hallituksen esitys HE 71/2026 (Finland).
- Traficom/Kyberturvallisuuskeskus: Kyberturvallisuuden vuosi 2025, 29.1.2026, og Kybersää januar 2026.
- Helsingin käräjäoikeus: Eagle S, tiltale R706/2025/12270.
- Ministeriet for Samfundssikkerhed og Beredskab (Danmark): Aftale om strategi for cyber- og informationssikkerhed 2026-2029, 28.1.2026, og baggrundsnotat om 24/7-situationscenter, desember 2025. mssb.dk
- Folketinget: Forsvarsministerens svar på FOU spm. 116 (2024-25), 11.3.2025. ft.dk
- Retsinformation: Lov nr. 433 og 434 af 6. maj 2025.
- Forsvarets Efterretningstjeneste: Russia is responsible for destructive and disruptive cyberattacks against Denmark, 18.12.2025. fe-ddis.dk

Rapporten er utgitt
av

TEK Norge

Forfatter

Pål Wien Espen, direktør for infrastruktur, sikkerhet og forsvar
i TEK Norge

Tallgrunnlag

NyAnalyse: Cybersikkerhet i Norge. Nordisk benchmark 2026

Kontakt

pwe@teknorge.no

Grafisk

Vilde Sollien, senior kommunikasjonsrådgiver i TEK Norge

Hvem er vi?

TEK Norge representerer de bedriftene som jobber i frontlinjen av teknologiutviklingen.

Vi er en uavhengig medlemsorganisasjon for det digitale næringslivet.

Vår jobb er å opplyse og skape innsikt. Vi skal være en klar stemme i fortellingen om det digitale Norge. En veiviser å stole på gjennom et stadig mer krevende teknologisk landskap.

Kontakt
OSS

Ta kontakt:
(+47) 960 08 142
post@teknorge.no

Post og besøk:
Prinsens gate 22
0157 Oslo

TEK NORGE

