



2025-10-30 07:00 CET

Telenor advarer i ny nordisk sikkerhedsrapport: Stigende risiko for cyberangreb, sabotage og desinformation

Mens Norden står over for øget geopolitisk spænding og accelererende digitale trusler, offentliggør Telenor i dag sin årlige rapport Nordic Digital Security 2025. Opfordringen lyder på at arbejde hen mod en stærkere, mere samlet regional tilgang til sikkerhed og beredskab.

I [en ny rapport](#) fremhæver Telenor de accelererende fysiske og digitale trusler samt den voksende indbyrdes afhængighed mellem kritiske tjenester som energi og digital infrastruktur. Derfor opfordrer selskabet regeringer og

erhvervsliv til at handle i fællesskab for at opbygge større nordisk modstandskraft, der beskytter samfund, økonomier og borgere.

“Det kræver både strategisk udsyn og praktisk samarbejde at sikre, at vores digitale infrastruktur kan modstå sikkerhedstruslen i dag og i fremtiden. Vi skal investere i fælles løsninger, der styrker robustheden på tværs af Norden,” siger Lars Thomsen, administrerende direktør i Telenor Danmark, og fortsætter:

“Styrken i den nordiske model ligger i tillid, tæt samarbejde og stærk digital infrastruktur. Men for at forblive robuste skal vi forbinde disse styrker på tværs af grænser, harmonisere rammer, dele information og forberede os sammen.”

Dette sætter nordisk robusthed på prøve

Baseret på Telenors seneste åbne trusselsvurdering og indsigter fra sikkerhedseksperter på tværs af Norden, fremhæver rapporten de mest presserende risici og handlinger, der kræves for at styrke beredskabet i regionen:

- **Hybride trusler ændrer det nordiske sikkerhedslandskab.** Statsstøttede og kriminelle aktører udvisker grænserne mellem cyberangreb, sabotage og desinformation – hvilket gør det vanskeligt at skelne mellem uheld og bevidste angreb.
- **Kritisk infrastruktur er nu en strategisk slagmark.** Søkabler, mobilnetværk og cloud-infrastruktur understøtter alt fra nationalt forsvar til finansiell stabilitet. At afbøde forstyrrelser kræver koordinering på tværs af grænser og klare ansvarsfordelinger mellem regeringer og erhvervsliv.
- **Vejrrelaterede forstyrrelser tester robustheden i realtid.** Stormen Amy og andre strømafbrydelser i regionen har vist, hvor hurtigt kommunikationen kan svigte, når energiforsyningen afbrydes – og hvordan redundans kan forhindre kaskadeeffekter.
- **Datasuverænitet bliver et afgørende spørgsmål.** Placering og styring af data er nu centrale emner, der får regeringer og organisationer til at investere i suveræne eller regionalt styrede cloud-løsninger til følsomme arbejdsopgaver.
- **Nordisk alignment er essentielt.** Fælles situationsbillede, harmoniserede rammer og fælles øvelser er nødvendige for at

opfylde NATOs robusthedsmål og sikre, at Norden kan handle som én under kriser.

“Robusthed bygges ikke fra den ene dag til den anden. Det kræver langsigtede investeringer, forberedelse og koordinering mellem regeringer, operatører og industrier. De nordiske lande har allerede stærke nationale systemer, men en krise tager ikke hensyn til grænser eller national autonomi. For at beskytte vores kritiske funktioner må vi handle som region. Det betyder forudsigelig finansiering, harmoniserede rammer og fælles nordiske kapabiliteter, så vi kan forberede os og reagere sammen, når det virkelig gælder,” siger Lars Thomsen.

De største sikkerhedsrisici i 2025

Rapporten udpeger seks hovedkategorier af trusler, der former det nordiske sikkerhedslandskab i 2025, og som Telenor skal forberede sig på:

- Destruktive cyberangreb
- Sabotage af digital og fysisk infrastruktur
- Udenlandsk påvirkning og desinformationskampagner
- Efterretningsoperationer rettet mod kritiske systemer
- Økonomisk motiveret organiseret cyberkriminalitet
- Avancerede internetsvindelnumre

“Dette er ikke abstrakte risici,” påpeger Telenor-direktøren: “De er en del af det daglige trusselsbillede, som teleselskaber og andre leverandører af kritiske tjenester skal være forberedt på at håndtere.”

En nordisk opfordring til handling

I rapporten udsender Telenors nordiske selskaber en fælles opfordring til regeringer og erhvervsliv i Norden med det formål at styrke den regionale robusthed:

- **Gør robusthed til en nordisk prioritet** – løft sikkerhed og beredskab til et fælles regionalt rammeværk.
- **Harmoniser rammer og regler** – tilpas sikkerhedsgodkendelser, rapporteringskrav og robusthedsstandarder.
- **Styrk fælles kapabiliteter** – forbedr informationsdeling og fælles

- incident response på tværs af grænser.
- **Byg redundans og afklar roller** – sørg for klare støtteprotokoller og backup-infrastruktur i driften.
- **Skalér og øv sammen** – gennemfør regelmæssige nordiske robusthedsøvelser.

Om Nordic Digital Security 2025-rapporten

Rapporten er Telenors årlige vurdering af sikkerhedssituationen i Norden, udarbejdet af Telenors sikkerhedsekspertgruppe. Den indeholder analyser af det udviklende trusselsbillede, nye angrebsmetoder, fremkomsten af kognitiv krigsførelse og sårbarheder i søkabler og kritisk infrastruktur. Den fremhæver også erfaringer fra nylige kriser og deler anbefalinger til, hvordan regeringer og operatører kan styrke totalberedskabet og opbygge varig robusthed i hele Norden.

Den fulde Nordic Digital Security 2025-rapport kan læses her:www.telenor.com/nordics/ds25

Telenor hjælper danskerne med at skabe gode forbindelser via mobil og internet. Vores mål er at skabe sammenhæng i vores kunders digitale liv og i det danske samfund. Derfor investerer vi hvert år massivt i innovation og i udvikling af den danske teleinfrastruktur.

Telenor er en del af Telenor-koncernen, som opererer i hele Norden og i Asien, og på verdensplan hjælper vi 186 millioner kunder med at kommunikere. I Danmark er vi ca. 900 medarbejdere, har 38 butikker fordelt over hele Danmark og gør hver dag vores yderste for at gøre det nemt for vores kunder at kommunikere og sikre deres forbindelse på både mobil og internet. I Danmark er CBB Mobil også en del af Telenor-familien. Du kan læse mere om os på www.telenor.dk.

Kontaktpersoner



Telenors pressetelefon

Pressekontakt

info@telenor.dk

25 600 800