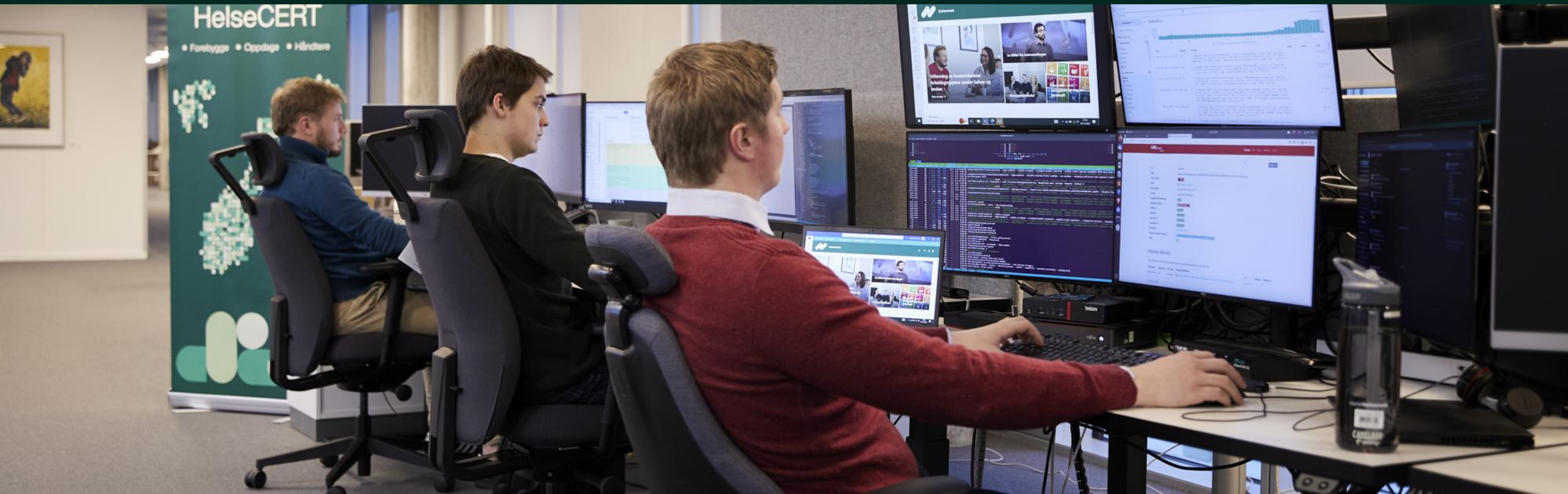
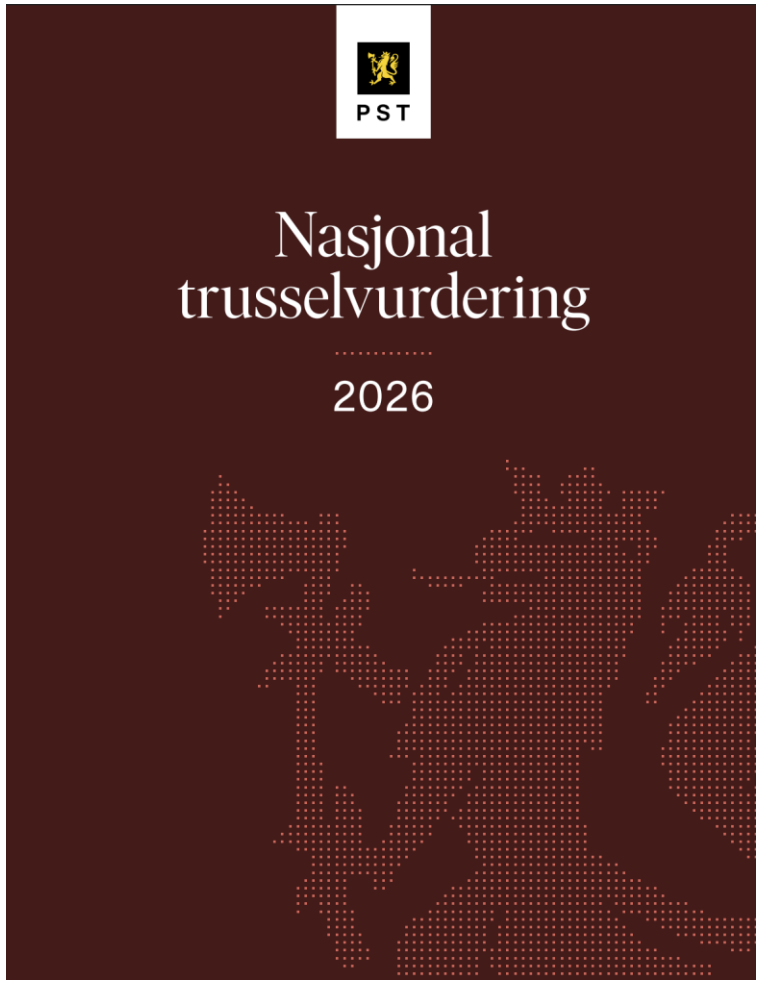
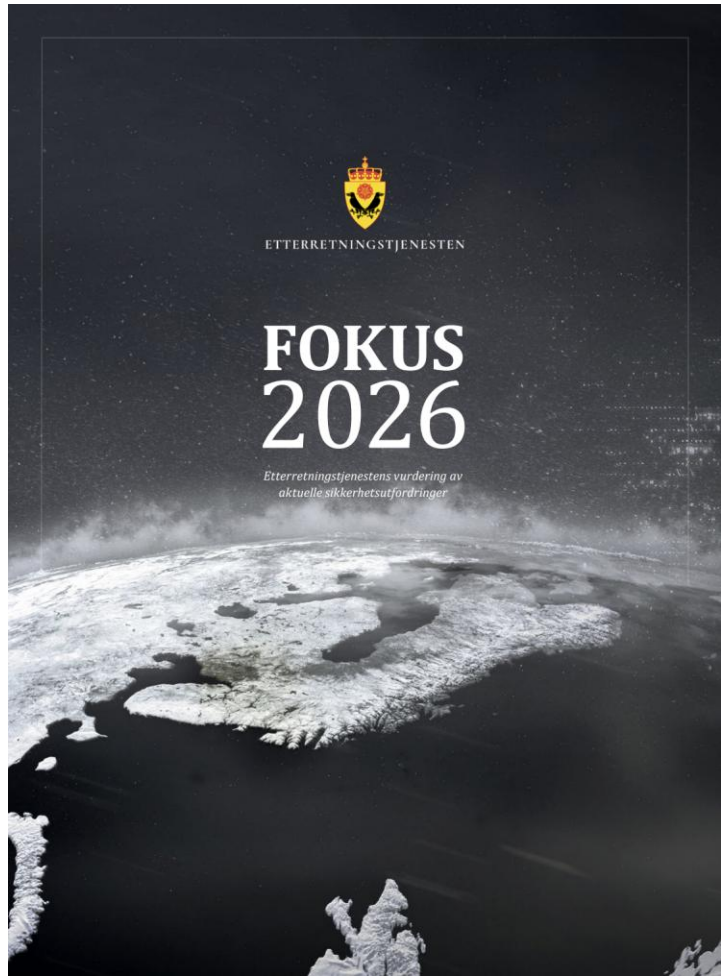
Norsk helsenett

Helse- og kommuneCERT
Forebygge, oppdage og håndtere



Nasjonale rapporter





Sikkerhetsutfordringer

- Sabotasjeforsøk i Norge er sannsynlig
- Vi blir utsatt for cyberangrep fra andre stater
- Infrastruktur og sårbarheter blir kartlagt av fremmede stater
- Høy aktivitet fra kriminelle aktører

- Utfordrer vår motstandsdyktighet
- Vi må sikre verdier og redusere sårbarheter
- Risikobildet krever handling!

Midtøsten

- NSM - ingen vesentlig endring – kan endres raskt
- Vi kan rammes gjennom leverandører
- Tiltak anbefales fra NSM:
  - Tiltak for å motvirke bortfall
  - Styrke sikkerhetskompetansen
  - Bevisstgjøring hos ansatte
  - Varsle hendelser til responsmiljøer

Iverksett tiltak i forbindelse med konflikten i Midtøsten

Publisert: 16.03.2026 Oppdatert: 16.03.2026

NSM følger situasjonen i Midtøsten tett og jobber kontinuerlig med å formidle bevissthet rundt risiko og sårbarheter for norske virksomheter. NSM råder norske virksomheter til å iverksette tiltak i forbindelse med konflikten.

ALERT

CISA Urges Endpoint Management System Hardening After Cyberattack Against US Organization

Release Date: March 18, 2026

CISA is aware of malicious cyber activity targeting endpoint management systems of U.S. organizations based on the March 11, 2026 cyberattack against U.S.-based medical technology firm Stryker Corporation, which affected their Microsoft environment.[1] To defend against similar malicious cyber activity, CISA urges organizations to harden endpoint management system configurations using the recommendations and resources provided in this alert. CISA is conducting enhanced coordination with federal partners, including the Federal Bureau of Investigation (FBI), to identify additional threats and determine mitigation actions.

To defend against similar malicious activity that misuses legitimate endpoint management software, CISA urges organizations to implement Microsoft's newly released best practices for securing Microsoft Intune the principles

Helse- og KommuneCERT

Trusler

- Økonomisk motivert kriminalitet
  - Digital utpressing/løsepengevirus
  - Fakturasvindel og andre svindelforsøk.
- Økning i trussel fra fremmede starter
  - Etterretning
  - Forskingsdata og helsedata
  - Beredskap og krisehåndteringsevne
  - Kritisk infrastruktur

https://helsecert.no

TLP:CLEAR

Hendelser

- Store r
  - Se we
- Det er
- Mange
- Ofte er
- Angrip
- Ikke va

Helse- og kommuneCERT

> Webinarer fra Helse- og kommuneCERT

Resultat av godt cybersikkerhetssamarbeid

Informasjonen som varslene er basert på kommer primært fra NSRs samarbeidspartnere, som Helse- og KommuneCERT, Nordic Financial CERT, og Nasjonal sikkerhetsmyndighet.

– Vi kan ikke få fullrost samarbeidet mellom disse aktørene nok. Her samarbeider ulike cybersikkerhetssentre med sine nisjekapasiteter, som gjør at man i sum får avverget mange alvorlige digitale angrep mot norske bedrifter. Det er unikt, sier Johannessen.

uneCERT

er

t. omittert M365-

elp

etstiltak

ramide

> Herdeguider for M365 conditional access

TLP:CLEAR

AiTM phishing - omfang

- Januar 2026: 105 som ble kompromittert
- Februar 2026: 241 som ble kompromittert
- Mars 2026: 176 som ble kompromittert (tall pr 26.03)

- 2025: ca 1200 som ble kompromittert

- Dette er hendelser vi har sett og er kjent med.

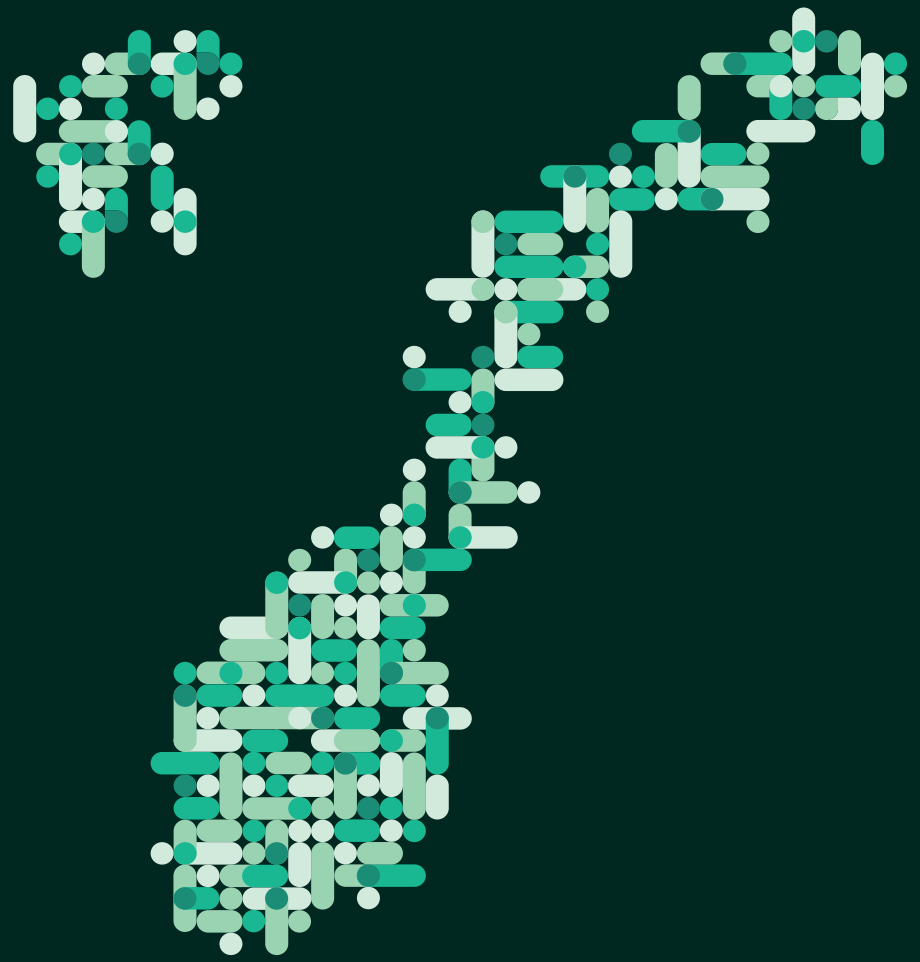
DDoS under Stortings- og Sametingsvalg 2025

- Vi fulgte med på mållister og varslet medlemmene våre løpende.
- Vår vurdering gjennom uken var at helsesektor ville forbli urørt, men at kommuner ville fortsatt være mål.
- Gruppen som sto bak er fornøyd med å få oppmerksomhet, reell konsekvens betyr mindre.
- Vi er ikke kjent med større konsekvenser utover noe nedetid.

Opportunistiske angrep

- Mange av angrepene er ikke målrettede.
- Mange blir rammet fordi de kan bli rammet!
- Sårbare systemer eksponert på internett er særlig utsatt.
- AiTM-phishing

Situasjonen i kommuneNorge



- Inntrengingstest av medlemmer
- Gjennomføres på en uke
- Tester motstandsdyktigheten
- Sjekker både intern og ekstern IT, men ofte mest fokus på det interne
- Testet over 120 virksomheter så langt
  - Kommuner, fylkeskommuner, helseforetak, helseregioner

Resultater fra våre kommunetester

- Teknisk gjeld
  - Mange AD-miljøer er satt opp for mange år siden
- Sikkerhet ligger utenfor daglig drift
  - Blir ikke fulgt opp
- Enkle tiltak er ikke gjennomført
- Person- og ressursavhengig
- Stor forskjell på modenhet
- En test ender i mange tilfeller med full kompromittering

Utfordringer med oppfølging

- Flere kommuner sliter med å følge opp funnene våre
- Ulike grunner:
  - Manglede ressurser
    - Rekrutteringsproblemer
    - Slunkne kommunekasser
  - Manglende kompetanse
  - Manglende prioritering fra kommunen
  - Travel hverdag, ofte mye som skal fikses opp i
  - Frykt for at endringer brekker ting
- Hjelper lite om vi kommer med alle funnene om det ikke rettes opp i!

Herding – ny tjeneste

- **Herding – operativ bistand og veiledning**
  - Kartlegger deres motstandsdyktighet
  - Prioritert tiltaksliste
  - Konkrete veiledere for hvert tiltak
  - Tilgjengelig fra portal.helsecert.no

Vaksinasjon – tiltak og forebyggende aktivitet

HVORDAN ØKE VÅR MOTSTANDSDYKTIGHET?

Anbefalinger

- **Implementer «Solid innlogging**
  - Spesielt viktig på M365
  - Fjerner risikoen for AiTM-phishing
  - Se veileder på helsecert.no
    - Krev FIDO2-autentisering – eller:
    - Kombiner passord med godkjent enhet – eller:
    - Kombiner passord med godkjent IP

- **Ta i bruk vår Herdingstjeneste!**
  - Gratis test av deres motstandsdyktighet
  - Gir en prioritert liste over herdingstiltak
  - Steg for steg veileder
  - Kom i gang på portal.helsecert.no!

- Bestill **gratis** inntrengingstest etter Herding

Norsk helsenett

Helse- og KommuneCERT

for helse- og kommunesektoren

Gunnar.Johansen@nhn.no

post@helsecert.no