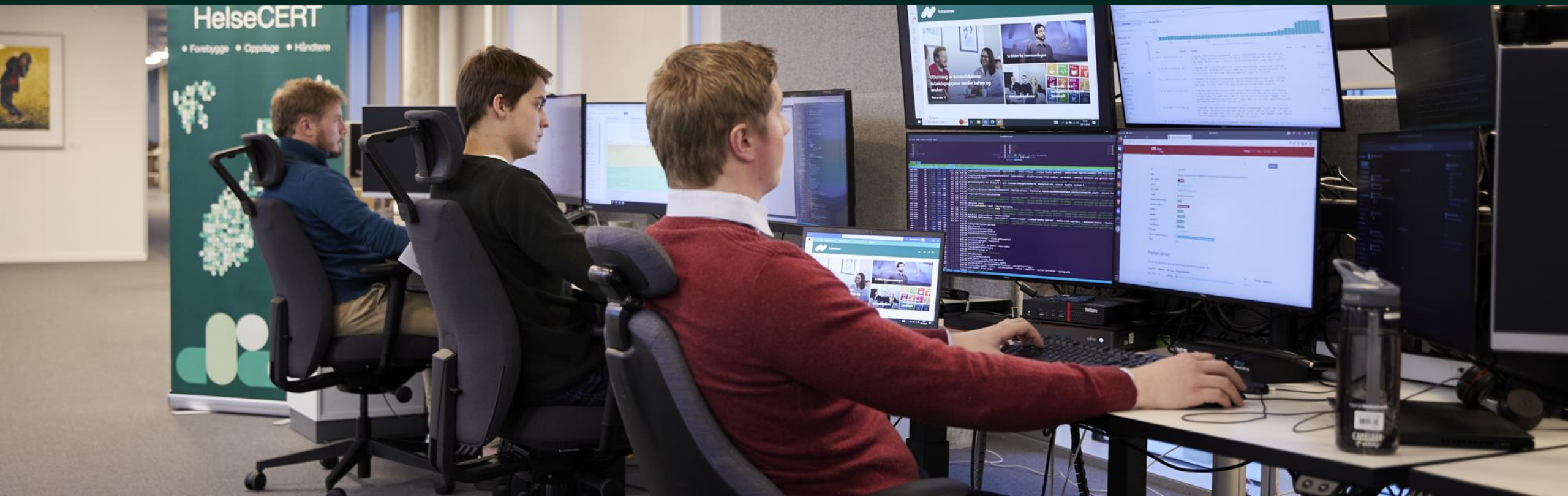
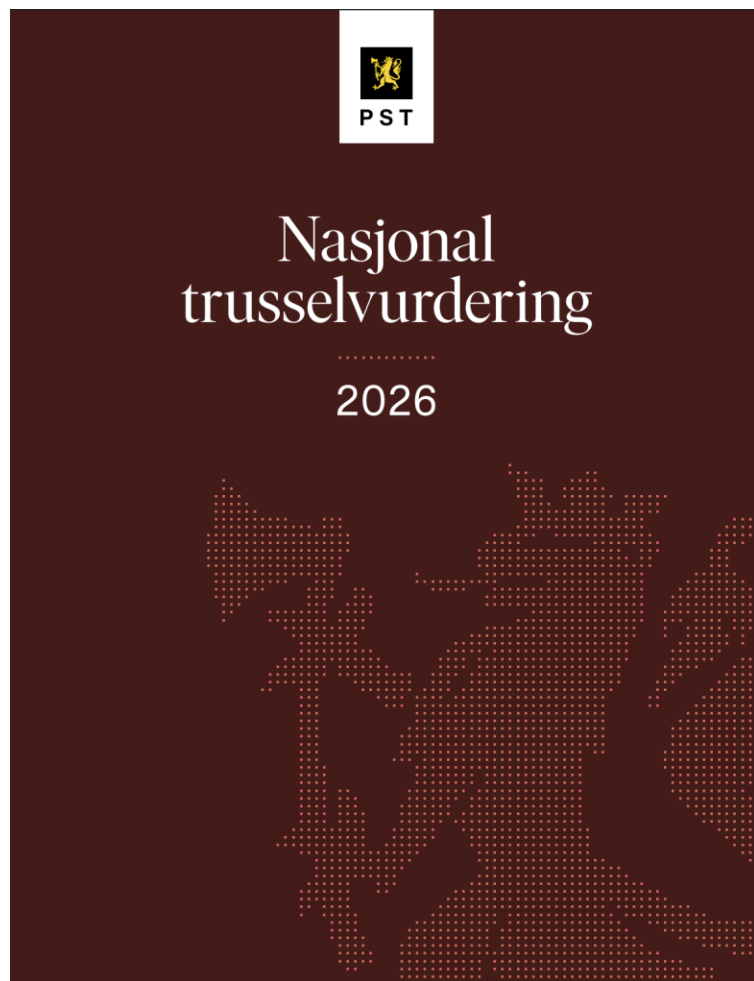


Helse- og kommuneCERT

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!



Risiko 2026

Dagens valg – morgendagens risiko

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.

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](#)²; the principles

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



Statlige aktører

- Statlige aktører utgjør de mest omtalte aktørene.
- Høyest evne til å gjennomføre angrep av alle typer aktører.
- Har som regel store støtteapparat.
- Flere mulige motiv
 - Spionasje
 - Sabotasje
 - Profitt
 - Forskningsdata og helsedata

Økonomisk motiverte kriminelle

- Står for brorparten av aktivitet vi ser mot medlemmene våre.
- Komplisert økosystem med tjenester som kjøpes og selges.
 - Hvis det kan tilbys som en tjeneste, selges det.
 - Økende profesjonalisering, men profesjonalisering er ikke nytt.
- Den største trusselen i denne kategorien er ***utpressingsaktører***.
- Drives av profitt, sjelden av ideologi.

Phishing

- Store mengder varsler
- Se webinaret vårt
- Det er en del AI
- Mange pålogging
- Ofte en forsinke
- Angripere bruke
- Ikke vær avheng

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.

ksjon.

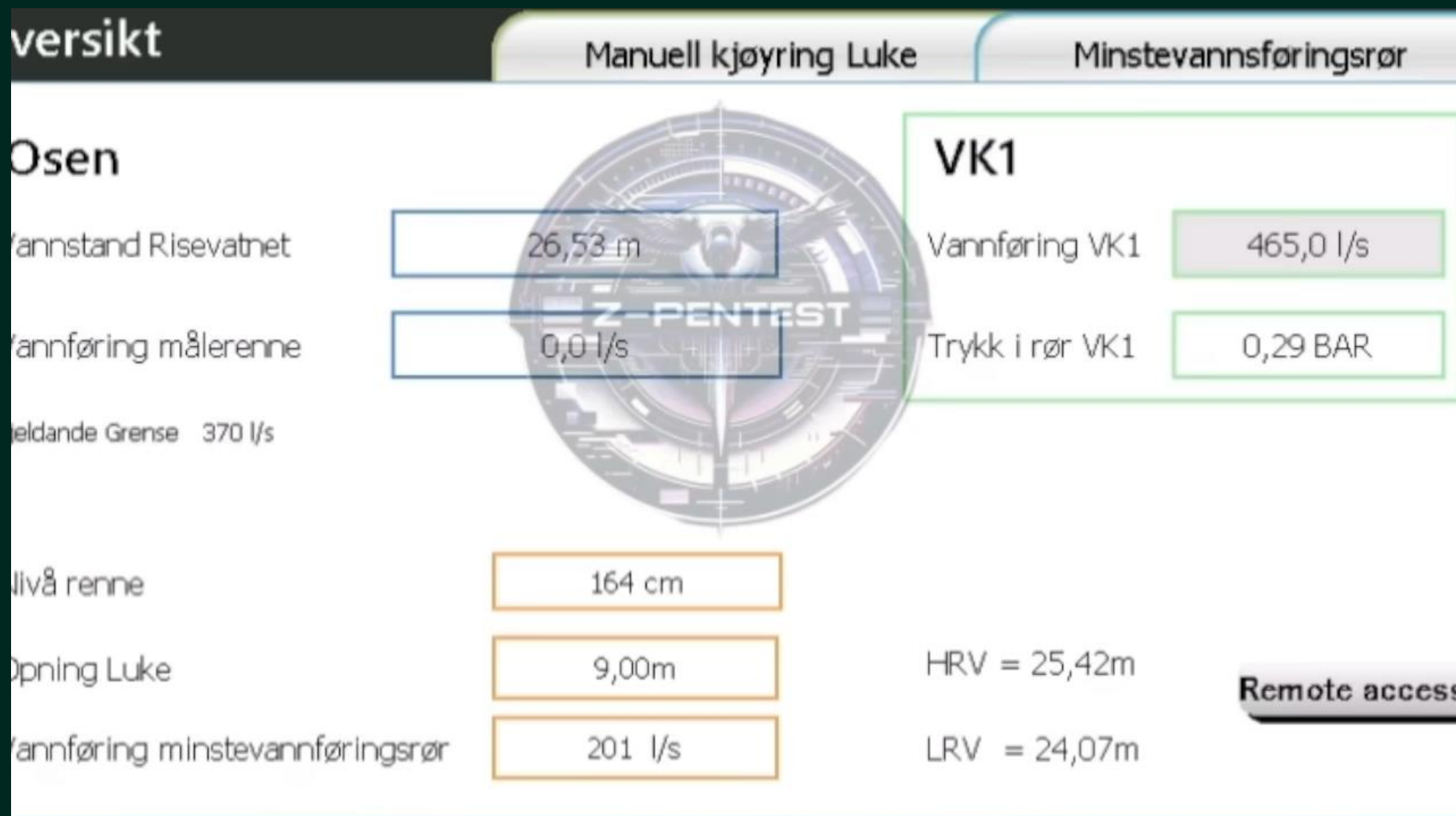
AiTM phishing - omfang

- 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.

Hacktivister

- En cyberaktivist som *begår kriminelle handlinger*
- Paradigmeskifte i aktiviteten februar 2022
 - Jevn aktivitet mot vestlige mål - også Norge
- Nytt skifte gjennom 2025 med fokus på Operasjonell Teknologi (OT)
 - Gruppene annonserer gjerne kompromitteringene ved å publisere video fra OT-systemene på Telegram.
 - Mot slutten av 2025 begynte flere grupper å publisere bilder og videoer fra webkamera.
 - Disse meldingene legges ofte ut med provoserende tekster med negative karakteristikker av et lands befolkning.

Z-Pentest Alliance



OT-funn i Norge

- Avdekket flere hundre OT-systemer på internett.
- En stor andel av systemene er uten passord, med svakt passord eller fabrikkpassord.
- Vi finner alt mulig av systemer direkte tilgjengelig på internett
 - Byggetekniske systemer
 - Vannforsyning
 - Oppdrettsanlegg
 - Kraftverk

Hacktivister

- Hvis vi fant så mange systemer, hvorfor har ikke hacktivistene funnet de?
- De norske systemene har enn så lenge druknet i mengden.
- Når disse gruppene får et påskudd for å prioritere Norge må vi forvente at disse systemene finnes av gruppene.
- Metodene og tjenestene vi har brukt for å finne disse systemene er fritt tilgjengelige for alle.
- Når gruppene får kontroll på et system endrer de på **ALT**.
- Merk at hacktivist er mindre sofistikerte enn statlige aktører og andre kriminelle.

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

Hva er vi redd for?

- Infrastruktur blir ikke mindre komplekst.
- Angrep går oftere og oftere på identitet og utnytter legitime tilganger på en måte som
 - Kan virke troverdig, eller
 - Er vanskelig eller umulig å oppdage med eksisterende logger.
- Mer utnyttelse av legitim infrastruktur
- Raskere utnyttelse av nye metoder enn en presset sikkerhetsbransje klarer å følge med på

Forenklede vurderinger

- Helsesektoren vil bli utsatt for spionasje- og påvirkningsoperasjoner
- Helsesektoren er attraktive mål for økonomisk motiverte kriminelle
- Hacktivister har ingen spesiell interesse i helsesektoren

Helse- og KommuneCERT for helse- og kommunesektoren

Gunnar.Johansen@nhn.no

post@helsecert.no

