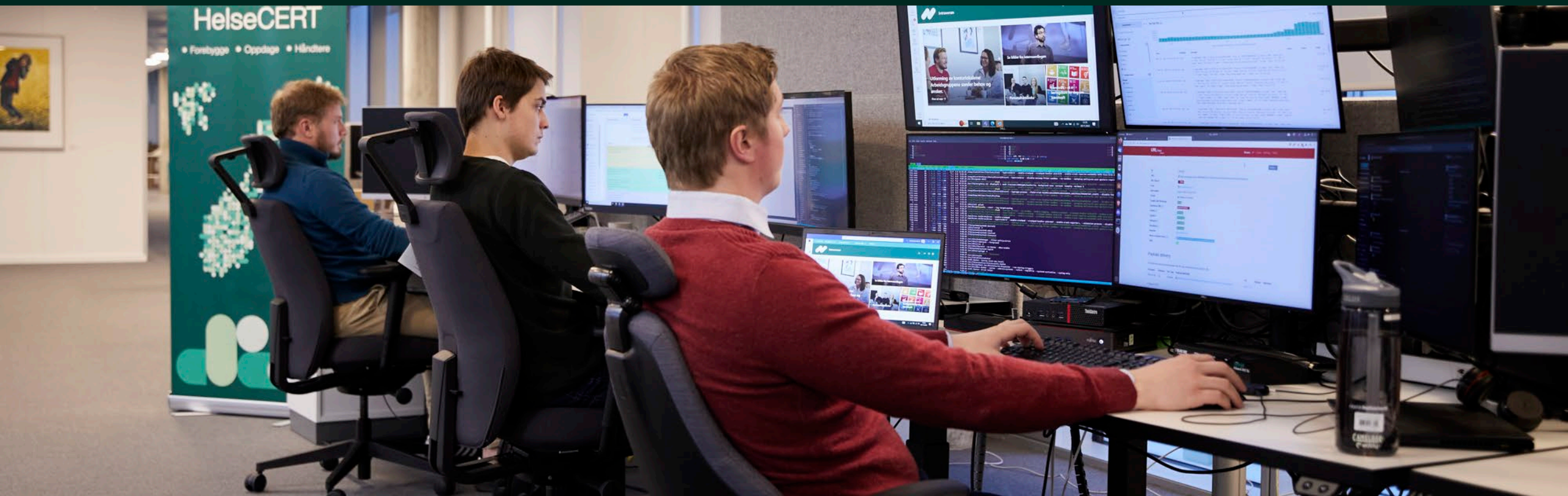


Cybertrusler og tilstand

Dimensjonerende og statlige

Hans Kristian Strømme
Helse- og KommuneCERT

NOKIOS
23. oktober 2025

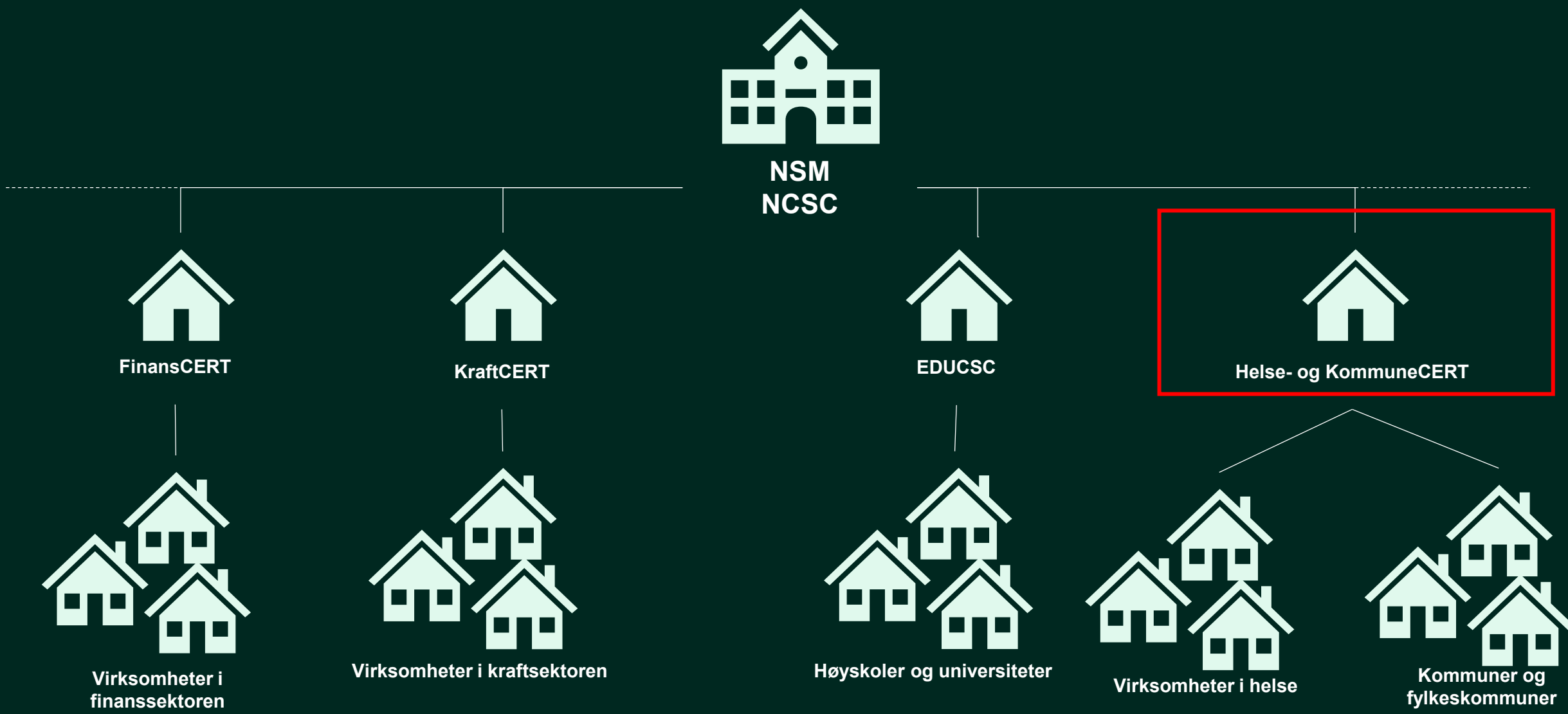


Agenda

- Hvem er jeg og vi
- Trusselbildet i cyberdomenet
 - Dimensjonerende – ransomware
 - Statlige – Kina, Russland
- Tilstanden "der ute"
- Anbefalinger



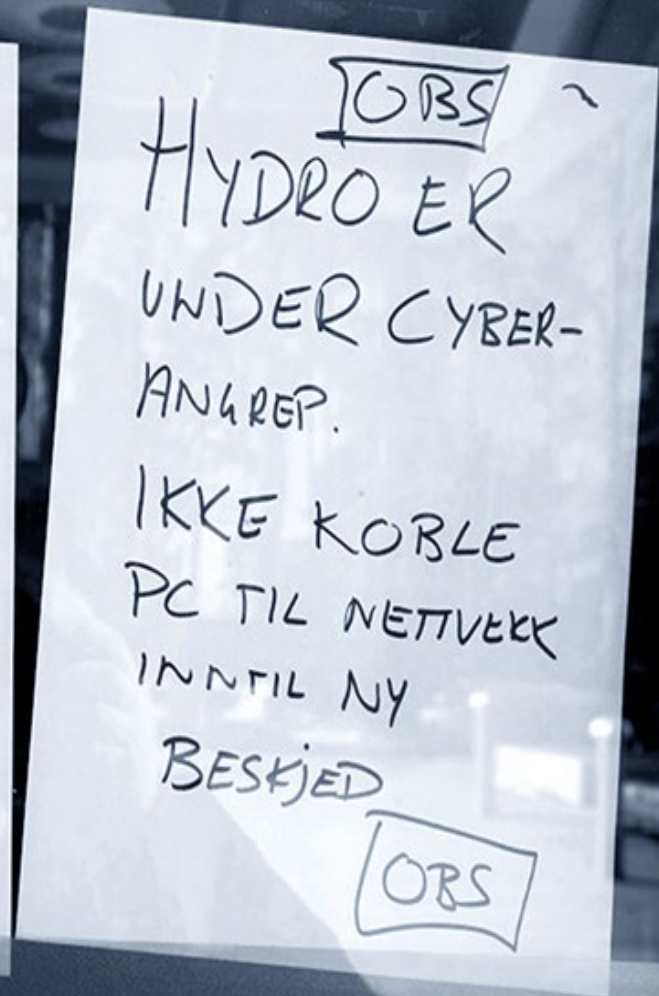
Sektorvis responsmiljøer



Helse- og KommuneCERT

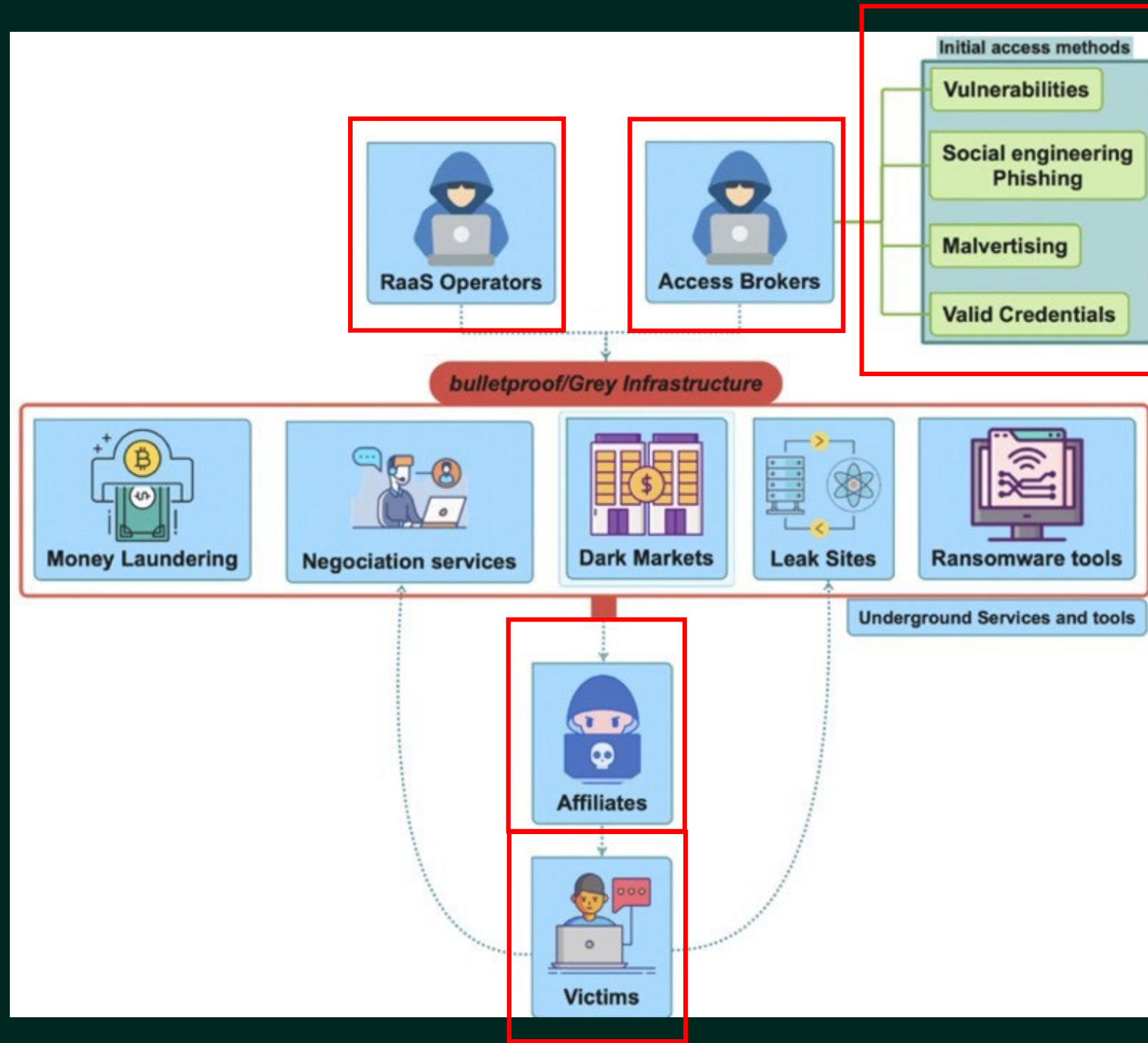
- Sektorvis responsmiljø (SRM) for helse- og kommunesektoren
- HelseCERT etablert i 2011
- KommuneCERT fra 1.12.2023
- 32 ansatte
- Helse- og KommuneCERT er en felles enhet.
- Forebygge, oppdage, håndtere tilsiktete cyberhendelser
- Helse- og Kommunesektor sikrere

Trussel - dimensjonerende



Opportunistic

- Økosystem
- Spesialisering



Opportunistiske

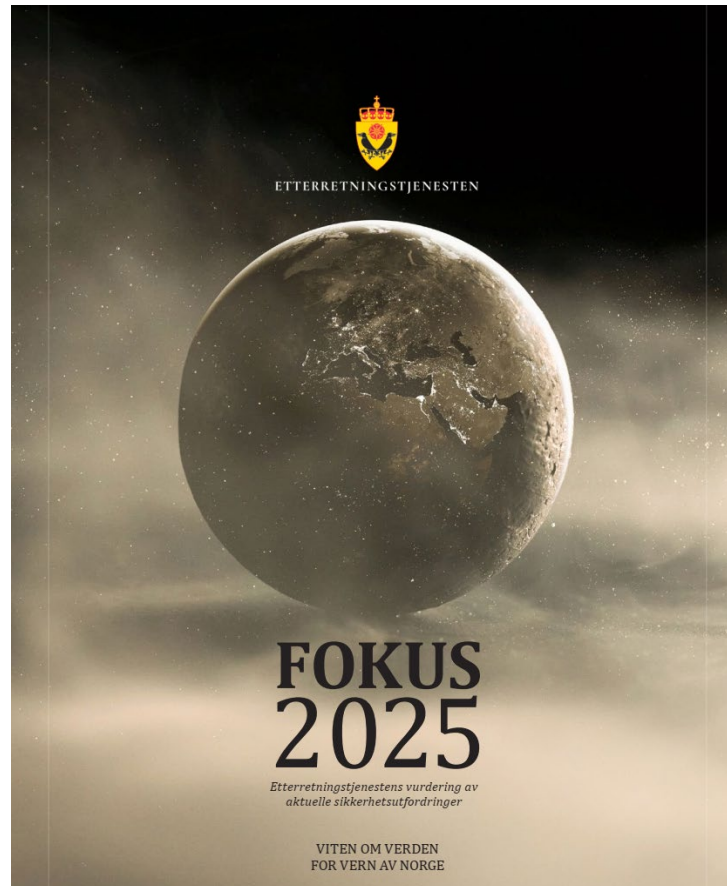
- Mål:
 - Mest mulig penger
 - For minst mulig arbeid
 - Og minst mulig (opplevd) risiko

YOU DON'T HAVE TO RUN FASTER THAN THE BEAR TO GET AWAY. YOU JUST HAVE TO RUN FASTER THAN THE GUY NEXT TO YOU



Statlige

Trusselvurderinger



Sikkerhetsutfordringer

- Sabotasjeforsøk i Norge er sannsynlig
- Vi blir utsatt for cyberangrep fra andre stater
- Infrastruktur og sårbarheter blir kartlagt av fremmede stater
- Utfordrer vår motstandsdyktighet
- Vi må sikre verdier og redusere sårbarheter
- Risikobildet krever handling

Kina

- Langsiktig

Russland

- Økende risikovilje

Kina jobber langsiktig



America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Search

Topics ▾ Spotlight Resources & Tools ▾ News & Events ▾ Careers ▾ About ▾

[Home](#) / [News & Events](#) / [Cybersecurity Advisories](#) / [Cybersecurity Advisory](#) / PRC State-Sponsored Actors Compromise and Maintain Pe...

CYBERSECURITY ADVISORY

PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure

Release Date: February 07, 2024 **Alert Code:** AA24-038A

Kina jobber langsiktig



America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Search

[Topics](#) ▾ [Spotlight](#) [Resources & Tools](#) ▾ [News & Events](#) ▾ [Careers](#) ▾ [About](#) ▾

[Home](#) / [News & Events](#) / [Cybersecurity Advisories](#) / [Cybersecurity Advisory](#) / Countering Chinese State-Sponsored Actors Compromise ...

CYBERSECURITY ADVISORY

Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System

Last Revised: September 03, 2025

Alert Code: AA25-239A

Search

and Maintain Pe...

romise and
ritical

Ukraine's airport, metro system hit by new cyber attacks

BY | KIEV | OCT 24, 2017 - 12:00 AM GMT+3 |



| Reuters Photo

Cyber attacks hit Ukraine's Odessa airport and the metro system in Kiev on Tuesday, with the state-run Computer Emergency Response Team (CERT) saying a new wave of hacks was hitting the country and asking transport networks to be on particular alert.

Ukraine's airport, metro system hit by new cyber attacks

BY | KIEV | OCT 24, 2017 - 12:00 AM GMT+3 |

The Russia-Ukraine Cyber War Part 3: Attacks on Telecom and Critical Infrastructure

March 05, 2025 | 8 Minute Read | by Pawel Knapczyk and Nikita Kazymirskyi



Cyber attacks hit Ukraine's Odessa airport and the metro system in Kiev on Tuesday, with the state-run Computer Emergency Response Team (CERT) saying a new wave of hacks was hitting the country and asking transport networks to be on particular alert.

Kina

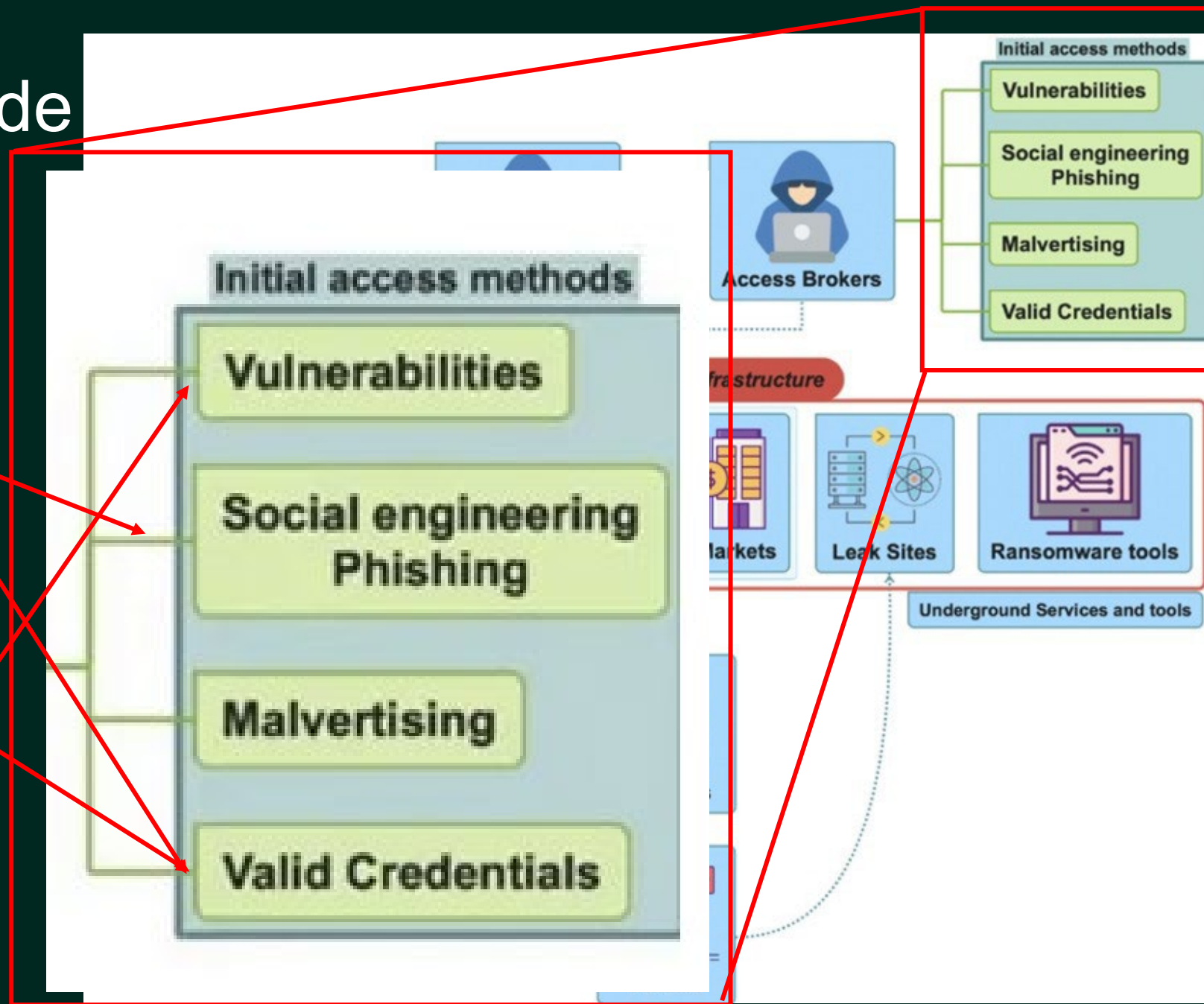
- Langsiktig
 - Strategisk posisjonering
 - Teknologi som interesserer Kina
 - Jobber målrettet etter sårbarheter som inngangsvektor

Russland

- Cyberangrep som politisk pressmiddel
- Økt risikovilje
- Destruktive angrep
 - (så langt fokusert mot Ukraina)

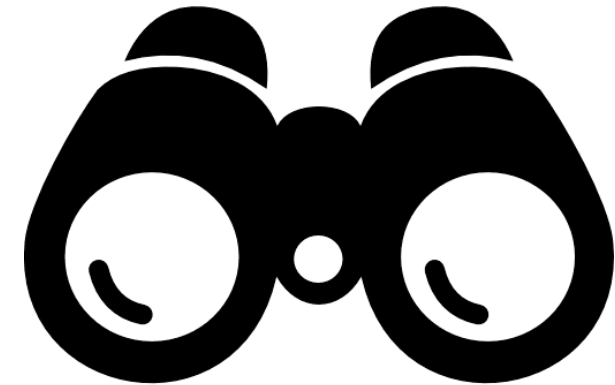
Hvordan kommer de

- Vi ser noen få vanlige inngangsvektorer
 - Phishing som omgår multifaktorautentisering
 - Kompromitterte brukernavn og passord (og manglende MFA)
 - Sårbarheter eller dårlig/manglende passord i internetteksponert utstyr



An abstract graphic on the left side of the slide. It features a large dark green square at the bottom left. Above its top-left corner is a smaller light green square. To the right of the dark green square is a medium-sized teal circle. Above the circle is a large light green square. The text is positioned to the right of these shapes.

Hvordan er tilstanden
"der ute"?



Resultater fra våre kommunetester

- Testet over 115 virksomheter så langt
 - Kommuner, fylkeskommuner, helseforetak, helseregioner
- Erfaringer
 - Stor forskjell på modenhet
 - Person- og ressursavhengig
 - Enkle tiltak er ikke gjennomført
 - Mye teknisk gjeld
- En test ender i mange tilfeller med full kompromittering

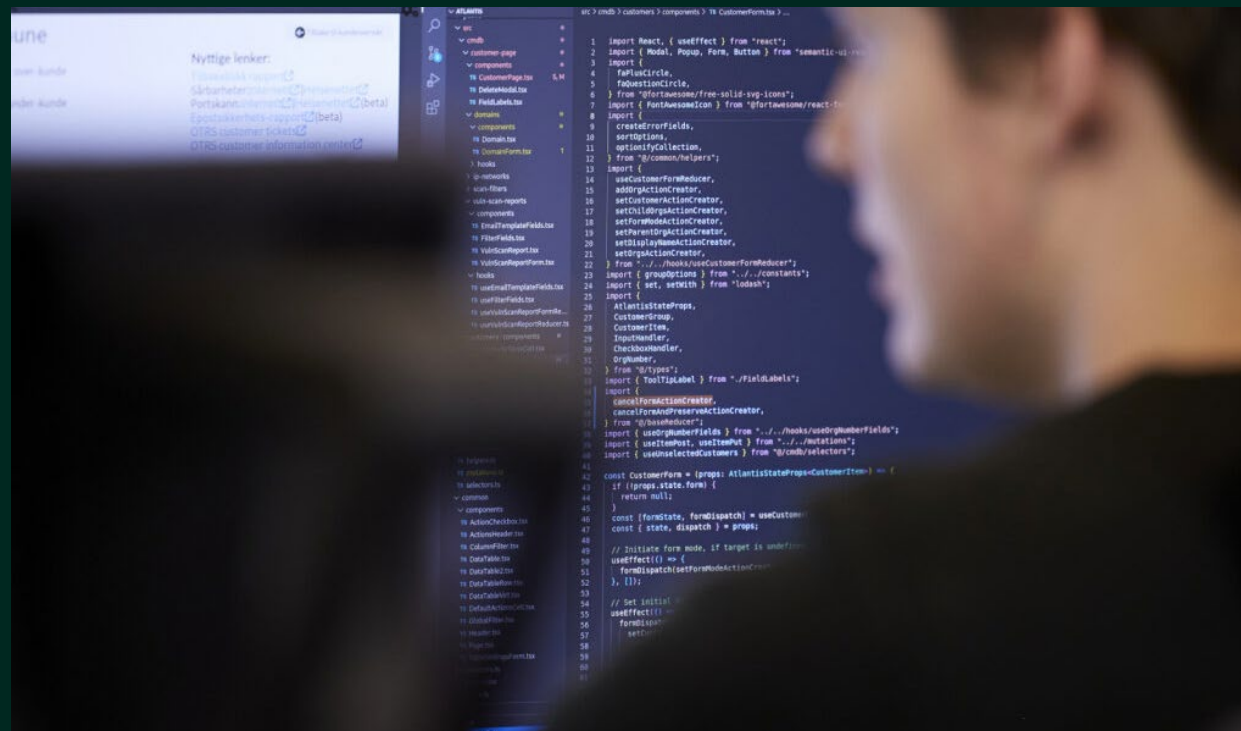
Men hva skjer etter en inntrengingstest?

- **Operativ bistand**

- Et eget team bistår våre medlemmer etter endt test
- Krever forankring i ledelsen og en forpliktelse ovenfor oss i Helse- og KommuneCERT

- **Hjelpe å utbedre funn, men også å utveksle kompetanse**

- **Vi ønsker at medlemmene skal sitte igjen med kunnskapen**



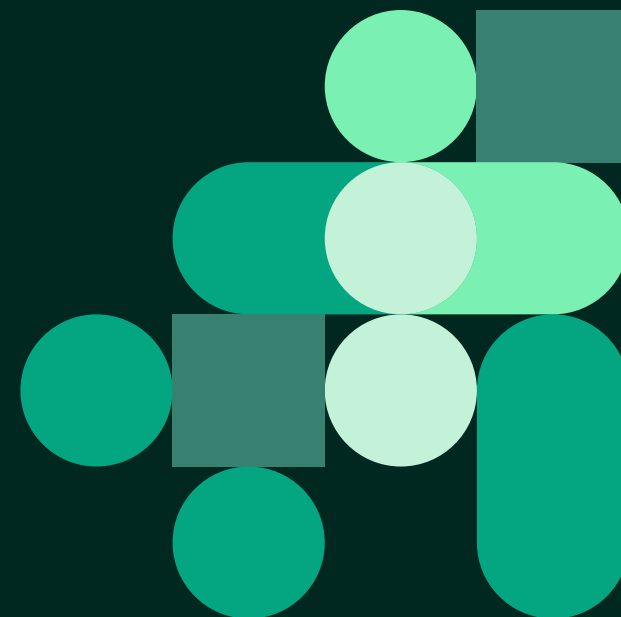
Positiv utvikling etter endt Kommunetest hos flere virksomheter

Positiv utvikling vedrørende herding

- Flere av de mest kritiske sårbarhetene blir tettet innen kort tid
- Angrepsflaten blir redusert

Kompetanseheving og bevisstgjøring

- Flere virksomheter lærer hvordan en angriper tenker
- Fremtidig sikkerhetsarbeid blir justert basert på testresultatene

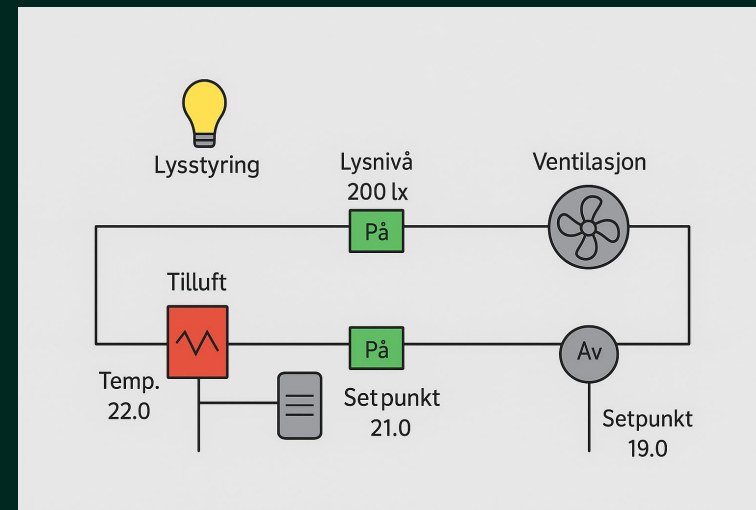


A man with short brown hair, wearing a red sweater over a white collared shirt, is seated at a desk in an office. He is looking at several computer monitors. The monitors display various software interfaces, including what appears to be a code editor with syntax-highlighted text, a document with text, and a dashboard with charts and tables. The office environment includes a grey cubicle wall in the background and a desk with various cables and a small container. A large green semi-transparent circle is positioned on the right side of the image, partially overlapping the text and the background.

Operasjonell Teknologi (OT)

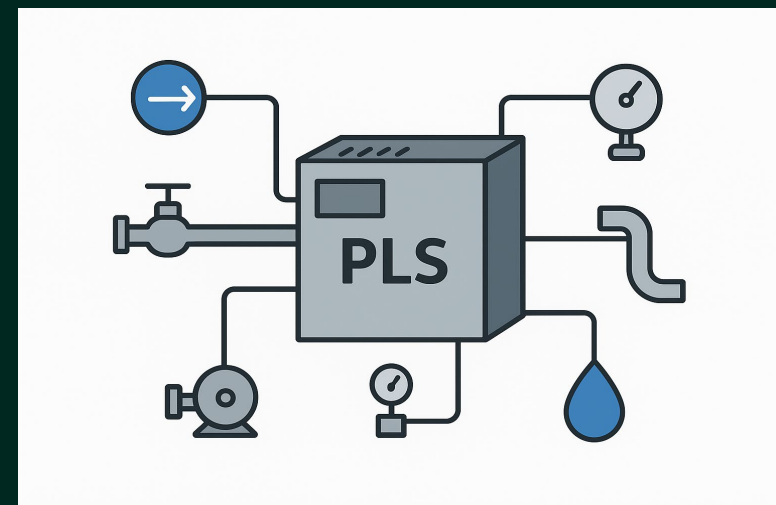
Hovedforskjellene mellom IT og OT

- OT styrer fysiske enheter
 - Eksempler er motorer/pumper, dører, ventilasjon, varme...
 - Små fabrikker til kritisk infrastruktur (vann/avløp/strøm)
- Stort fokus på "Availability". Oppetid er alltid kritisk
- Ofte nøkkelferdige løsninger med begrenset kompetanse hos eier
 - I mange tilfeller tungt avhengig av leverandør(er)
- Standard sikkerhetsoppdateringer kan knekke anleggene
 - skreddersydde løsninger og programvare



Helse- og KommuneCERTs arbeid rundt OT/VA

- › Sommeren 2025 jaktet vi etter eksponerte OT-systemer på internett
- › Avdekket mange hundre OT-enheter, noen av disse tilhørende VA, men også kraftverk
- › Noen var uten passord og andre benyttet seg av fabrikkpassord
- › Ofte var ikke systemeier klar over eksponeringen da vi varslet
- › Besøk på vannverk: Kritiske sårbarheter internt, og på internett.
- › Kommunene er ofte ikke klar over tilstanden på anleggene, da leverandørene drifter og vedlikeholder det meste selv



**Hvor involvert er du
angående tredjepartsleverandører og deres
sikkerhetsrutiner i ditt OT-anlegg?**



Vaksinasjon – tiltak og forebyggende aktivitet

HVORDAN ØKE VÅR MOTSTANDSDYKTIGHET?

Anbefalinger

- Implementer phishingresistent autentisering på eksponerte tjenester
 - Spesielt viktig på M365
- Ha kontroll på angrepsflate. Hvilke systemer har du på internett?
- Ha oversikt over egne systemer og sørg for at de blir driftet.
- Gjennomfør grunnleggende sikkerhetsherding.
- Still krav til leverandører.



Helse- og KommuneCERT

for helse- og kommunesektoren

post@helsecert.no

