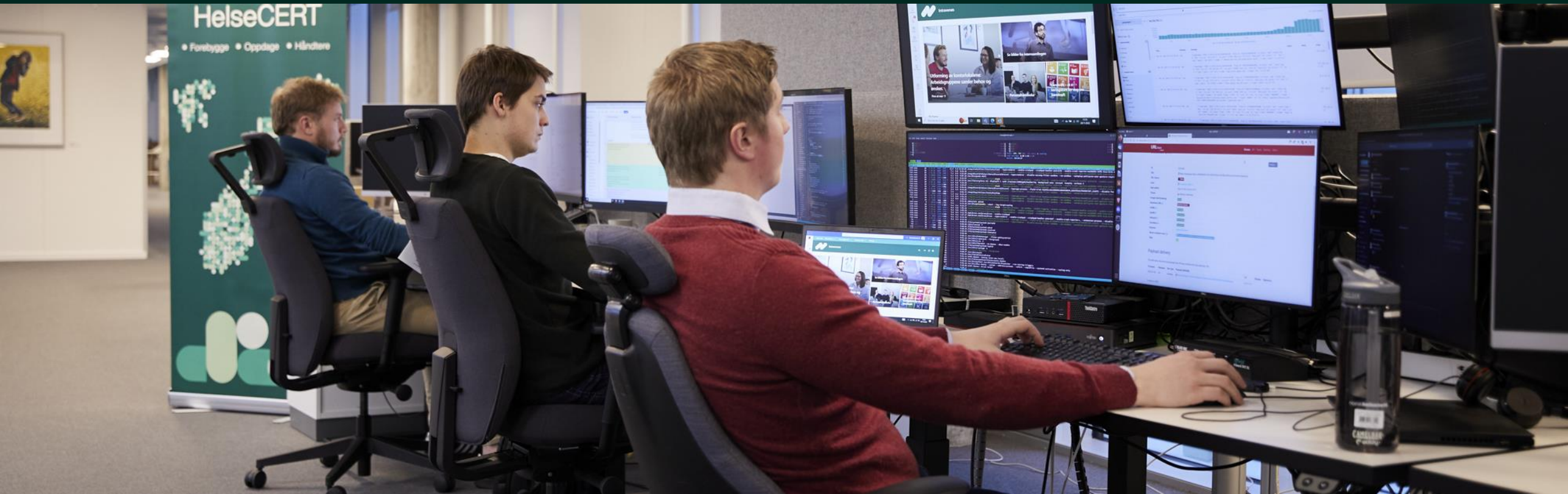
Norsk helsenett

TLP:GREEN

Helse- og KommuneCERT
Stories from the trenches



TLP:GREEN

Hvem er jeg?

- Hans Kristian Strømme
- Senior sikkerhetsanalytiker
- Helse- og KommuneCERT
  - 7+ år
- Teamleder operativt del

TLP:GREEN

Agenda

- Introduksjon
- Om Helse- og KommuneCERT
- Hendelser
  - Løvetann-phishing
  - Hvor mange sa du
  - Sårbar server, det tar vi på mandag

Limited disclosure, recipients can spread this within their community. Sources may use TLP:GREEN when information is useful to increase awareness within their wider community. Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. Note: when “community” is not defined, assume the cybersecurity/defense community.

Kort oppsummert: Du kan fortelle videre, men ikke offentlig!

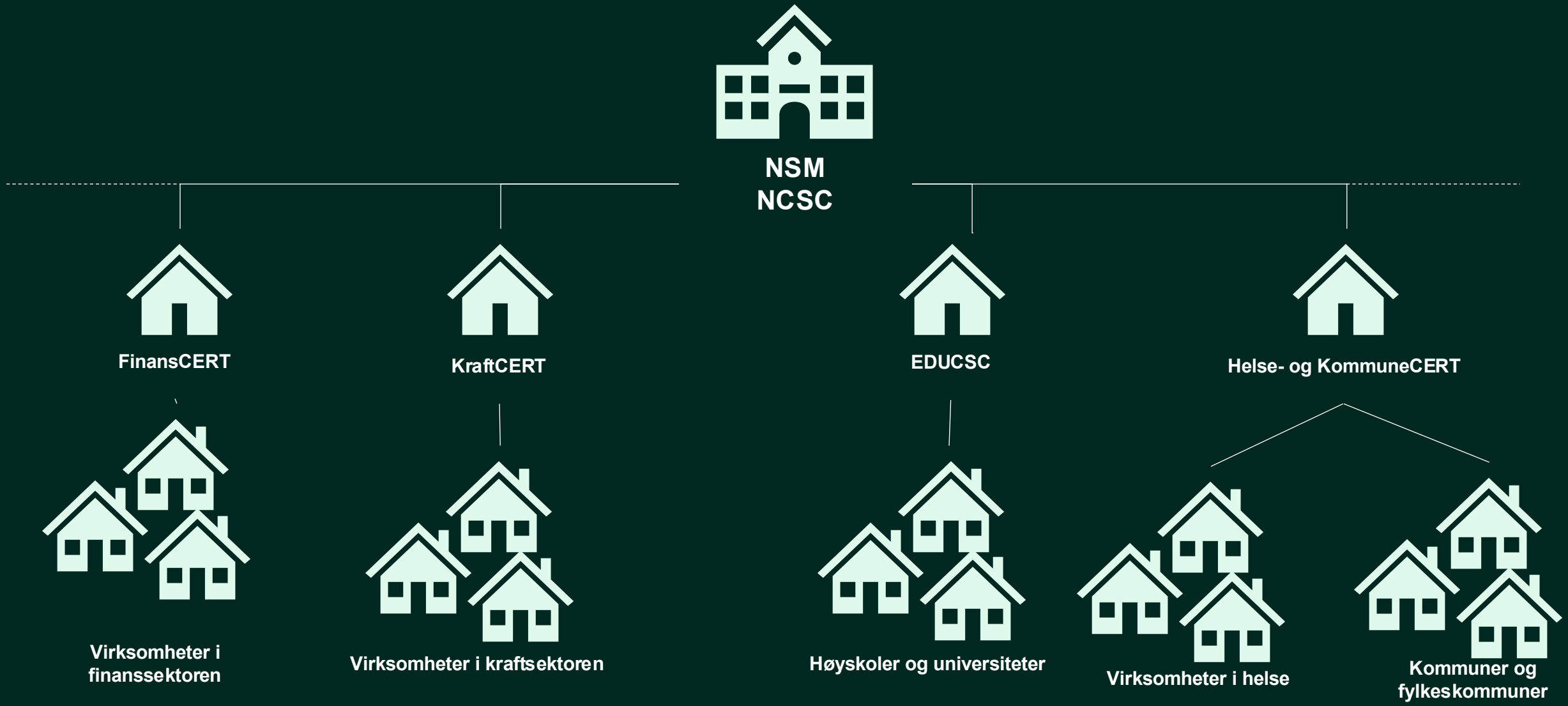
TLP:GREEN

Helse- og KommuneCERT

- Sektorvis responsmiljø (SRM) for helse- og kommunesektoren

TLP:GREEN

Sektorvis responsmiljøer



TLP:GREEN

Helse- og KommuneCERT

- Sektorvis responsmiljø (SRM) for helse- og kommunesektoren
- En avdeling i Norsk helsenett SF
- HelseCERT etablert i 2011
- KommuneCERT fra 1.12.2023
- 35 ansatte

- Helse- og KommuneCERT er en felles enhet.

Norsk helsenett

← hans.kristian.stromme@nhn.no

Enter password

Password

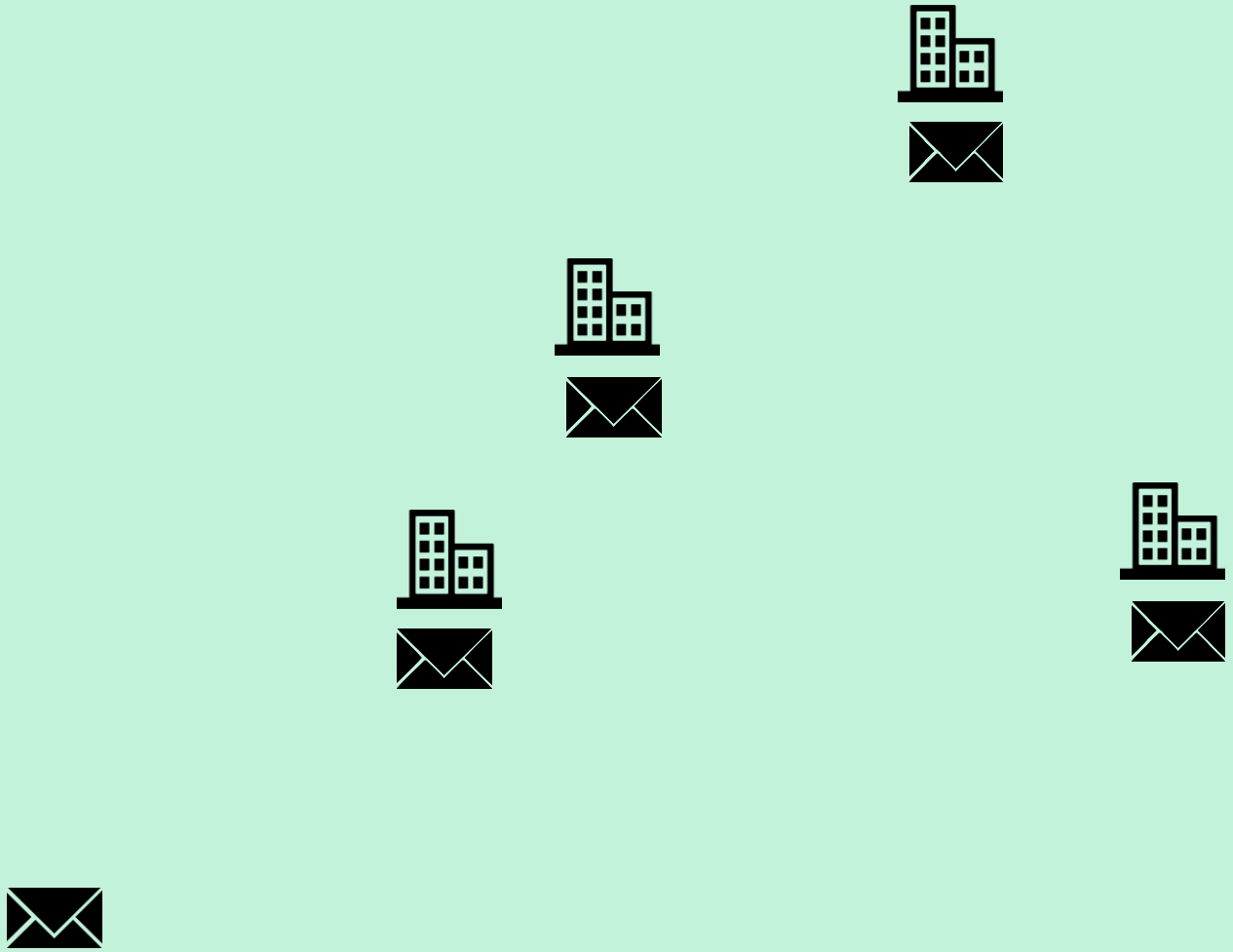
Forgot my password

Use your face, fingerprint, PIN, or security key instead

Sign in

TLP:GREEN

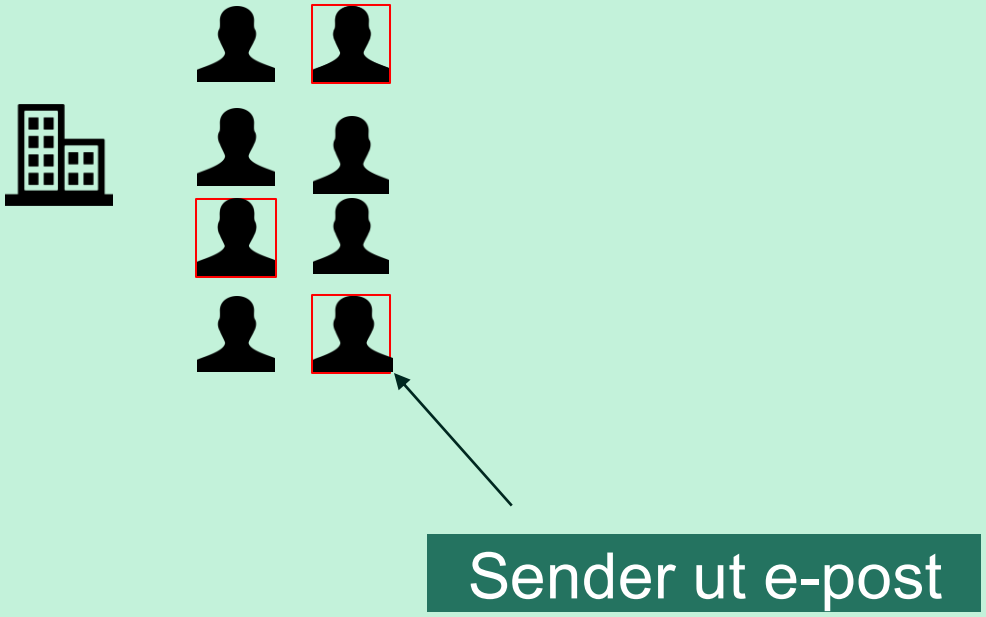
AitM-phishing



Går til adresser i kontaktliste og adresser man har sendt e-post med før.

TLP:GREEN

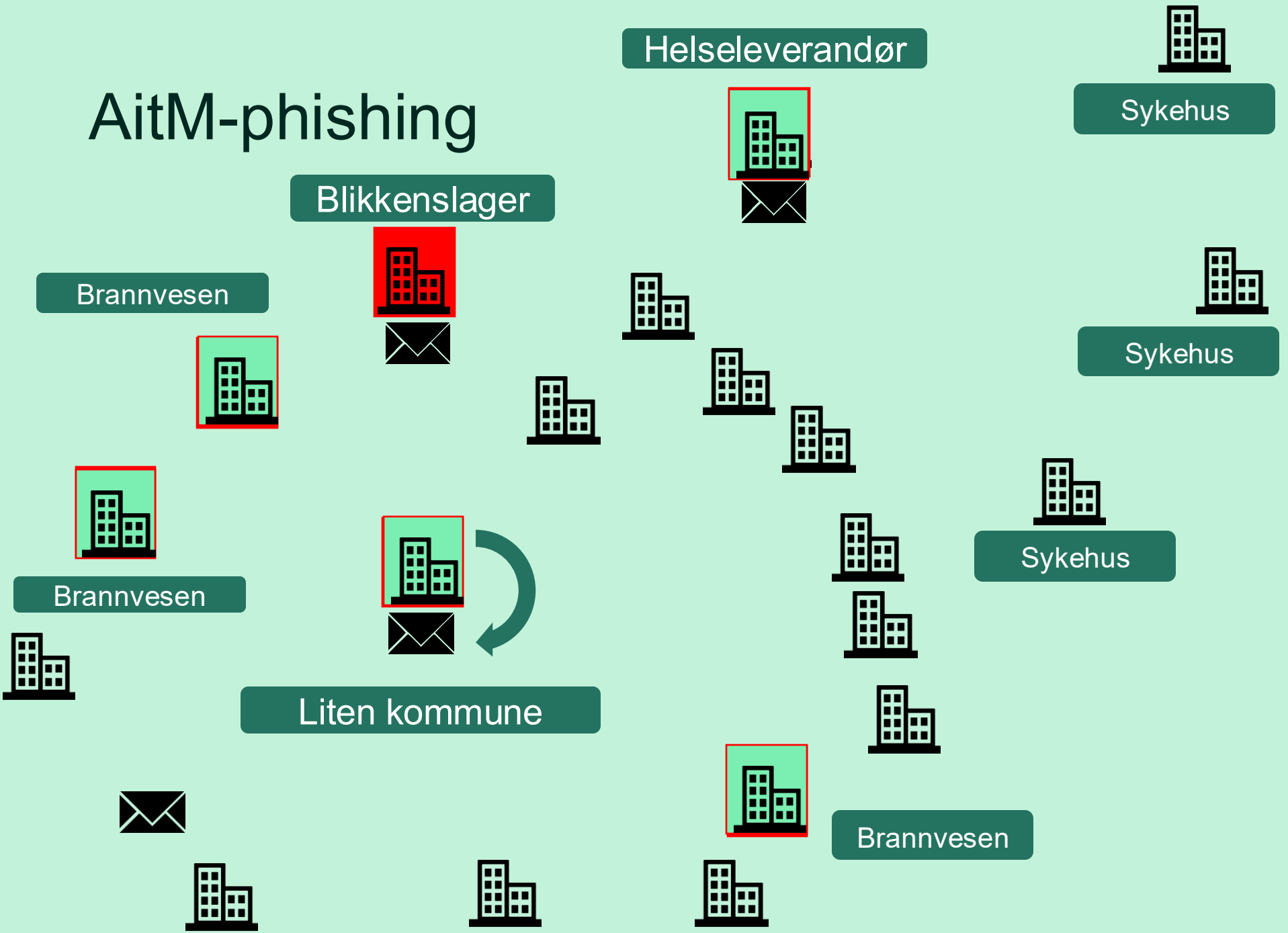
Konsekvens?



OneDrive

TLP:GREEN

AitM-phishing



TLP:GREEN

Hva betyr dette for dere?

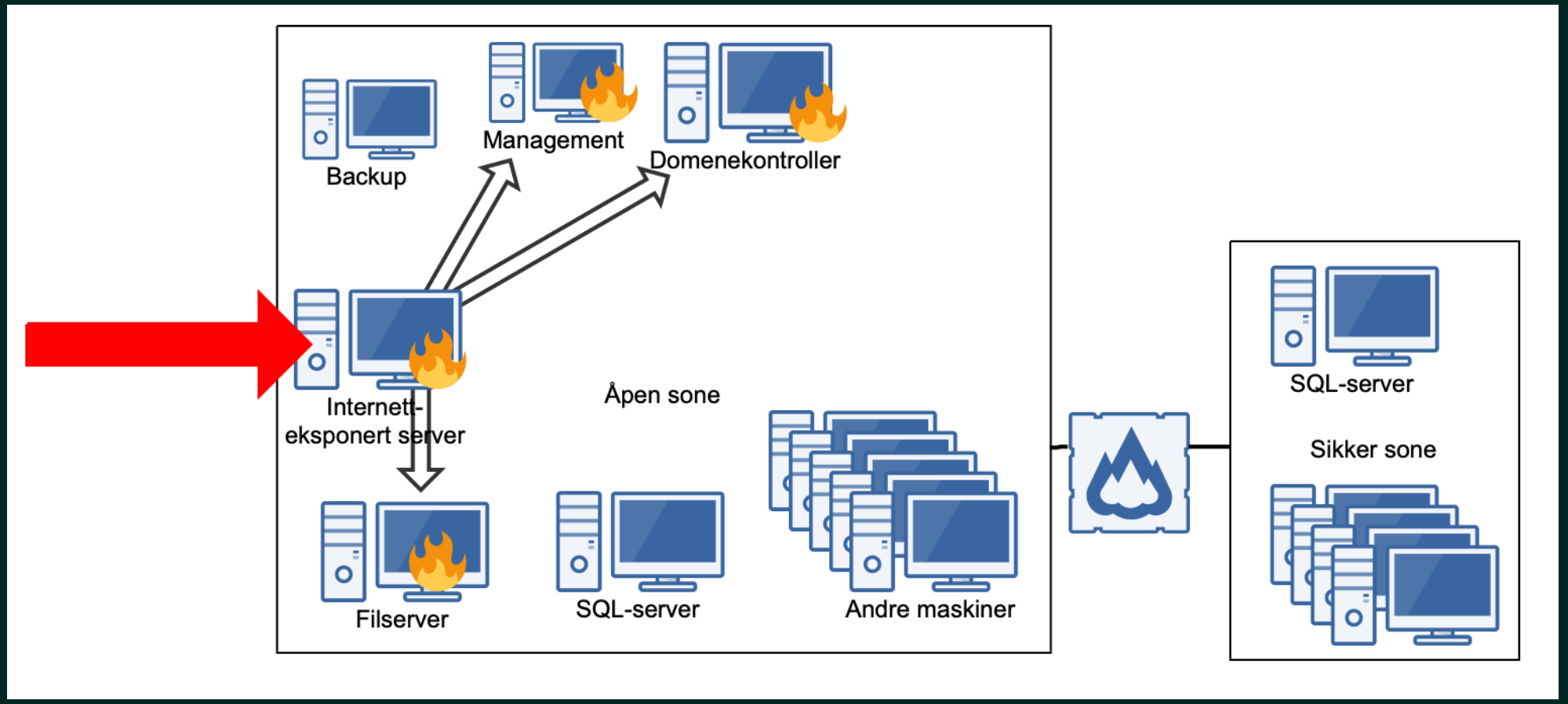
- Veldig effektivt angrep
  - “Jeg fikk en e-post fra noen jeg trodde jeg kunne stole på”
- Uvisst konsekvensomfang
  - Du vet ikke hvilken/om info som går tapt
  - Kan enkelt brukes i svindel
  - Brukes for angripe andre
- Krever sikring
  - Blokkeringslister hos oss --> plaster
  - Phishingresistent autentisering --> løsning

TLP:GREEN

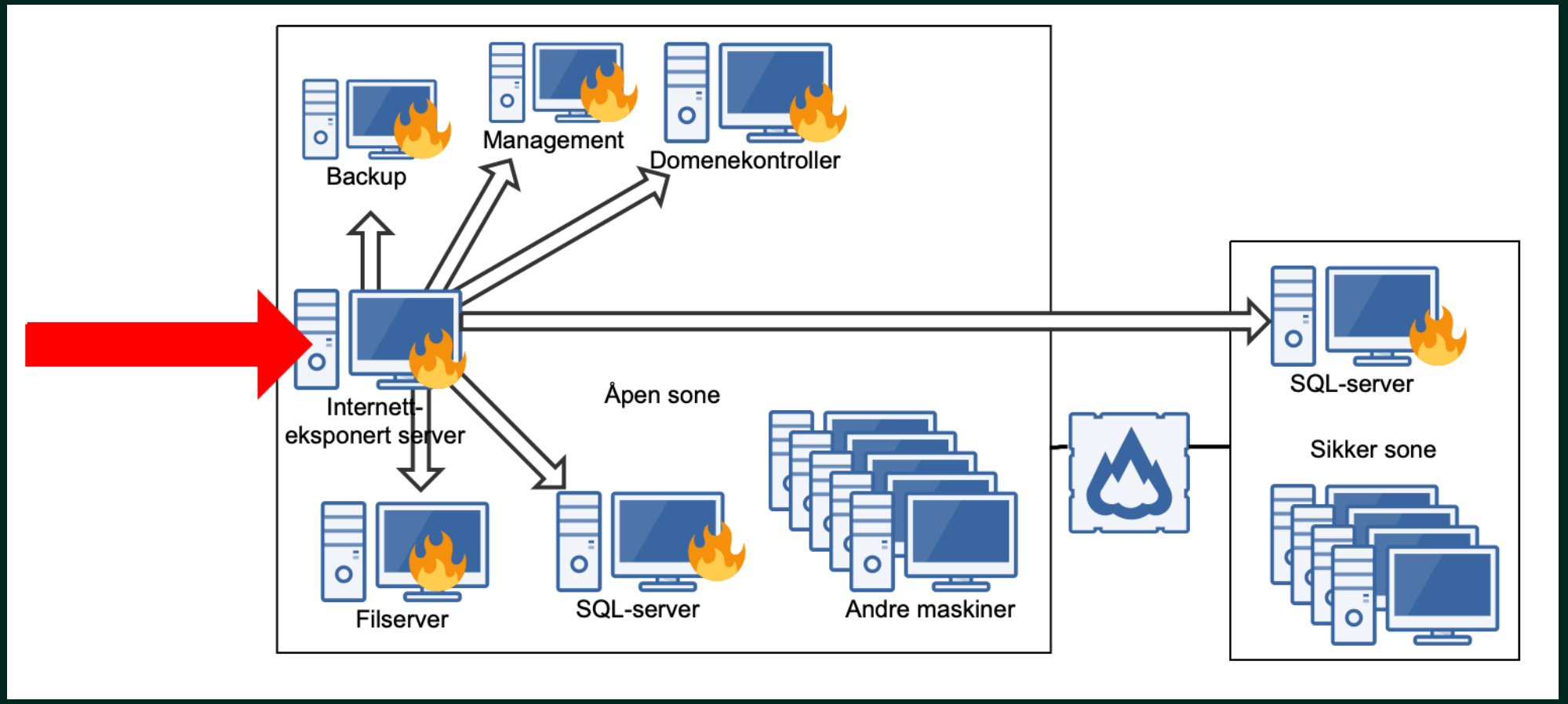
"Ukjent" virksomhet – Hvor mange???

- "[DATO] mottar vi en henvendelse fra [REDACTED] som melder at de er utsatt for et datainnbrudd."
- "Den sannsynlige veien inn er en sårbarhet i [SYSTEM]."
- "[REDACTED] føler de har kontroll på hendelsen."
- "Omfanget av fotfestet er uklart."
- "Angriper skal ha vært inne i systemet i litt over to timer."

TLP:GREEN


Backup
Management
Domenekontroller
Internett-
eksponert server
Åpen sone
Filserver
SQL-server
Andre maskiner
SQL-server
Sikker sone

TLP:GREEN


Backup
Management
Domenekontroller
Internett-
eksponert server
Åpen sone
Filserver
SQL-server
Andre maskiner
SQL-server
Sikker sone

TLP:GREEN

Attribusjon

- En angriper?
- To angripere?
- Tre angripere!

TLP:GREEN

Attribusjon - TA3

- Dag 0, dag 1, dag 19
- Utnyttelse av sårbarhet
- Antas å ha samarbeid med TA1
- TA3 er en statlig iransk aktør
  - Mint Sandstorm / TunnelVision

TLP:GREEN

Attribusjon - TA2

TA3

TA2

TA1

- Dag 6, dag 9
- Utnyttelse av sårbarhet
- Cobalt Strike
- Tydelige knytninger til ransomware
- Ryddet bort av AV
- Samme aktør krypterte systemer hos andre en til to dager senere
  - Ikke helsesektor
  - Ikke Norge

TLP:GREEN

Attribusjon - TA1

- Aktivitet dag 19 og dag 20
- Antatt samarbeid med TA3
- Attribusjon av bakdør (BADHATCH) i åpne kilder
- All informasjon vi besitter peker mot en utpressingsaktør
- Ingen indikasjon på statlig aktør

TLP:GREEN

Vår ressursbruk

- Jobbet med hendelsen i 6 uker
- Fra 1 til 10 ansatte som jobbet helt eller delvis med hendelsen
- Estimert over et halvt årsverk

TLP:GREEN

Hva betyr dette for meg?

- “Små” hendelser blir fort store
  - Oppdag tidlig
  - Håndter ferdig
- Viktig med AV eller EDR , og oppfølging
- AD-tiering --> Se eget webinar

HelseCERT |

Sykeh

TLP:GREEN

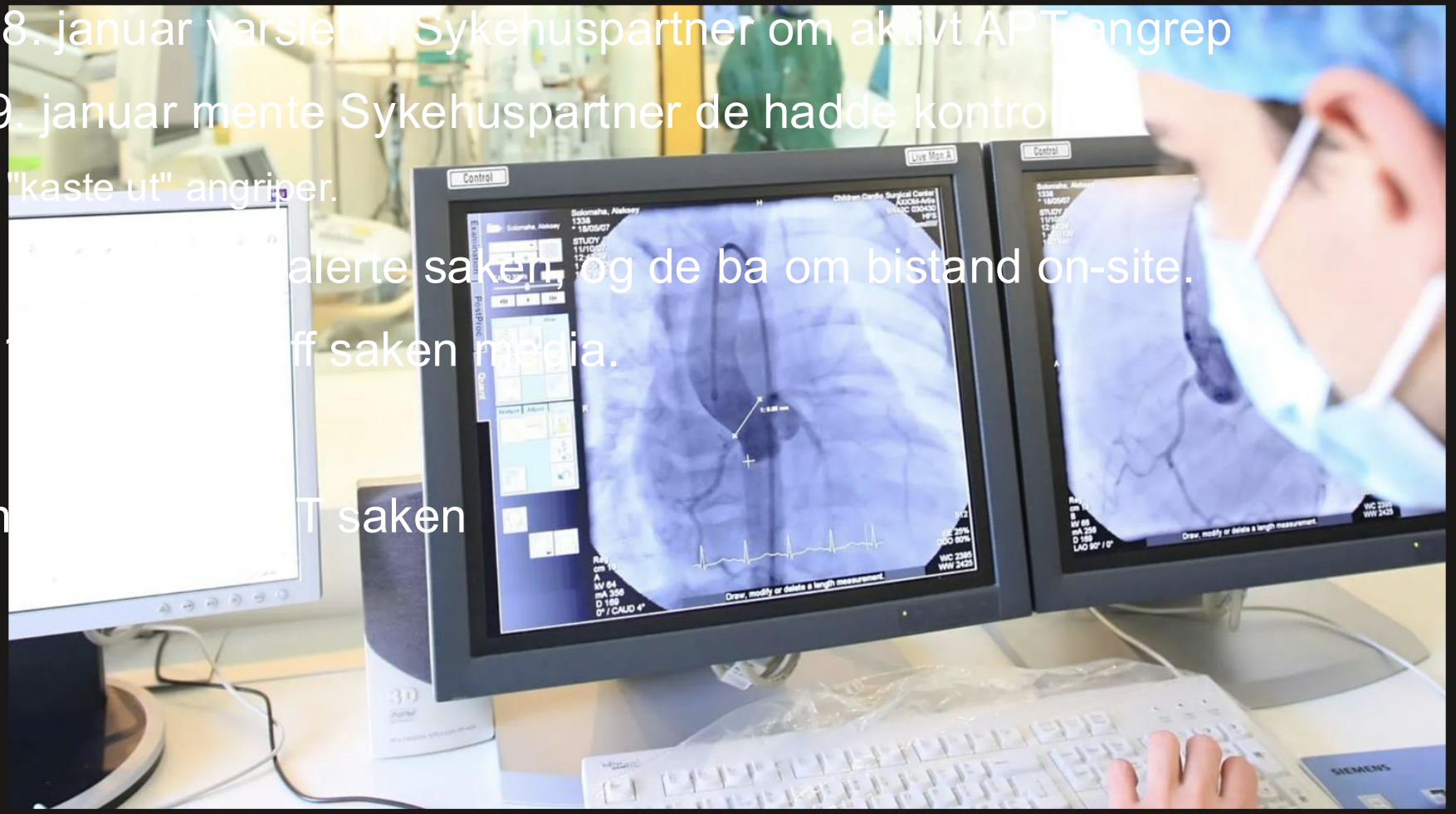
SIKKERHET

PST og Kripos etterforsker innbrudd i datasystemene i Helse Sør-Øst

Mistenker en avansert og profesjonell aktør.

- Mandag 8. januar varslet vi Sykehuspartner om aktivt APT angrep
- Tirsdag 9. januar mente Sykehuspartner de hadde kontroll
  - Valgte å "kaste ut" angriper.
- Lørdag 1 alerte saken, og de ba om bistand on-site.
- Mandag ff saken media.

- 5. desem T saken



Illustrasjonsbilde: Helse-IT Foto: Colourbox

Norsk helsene

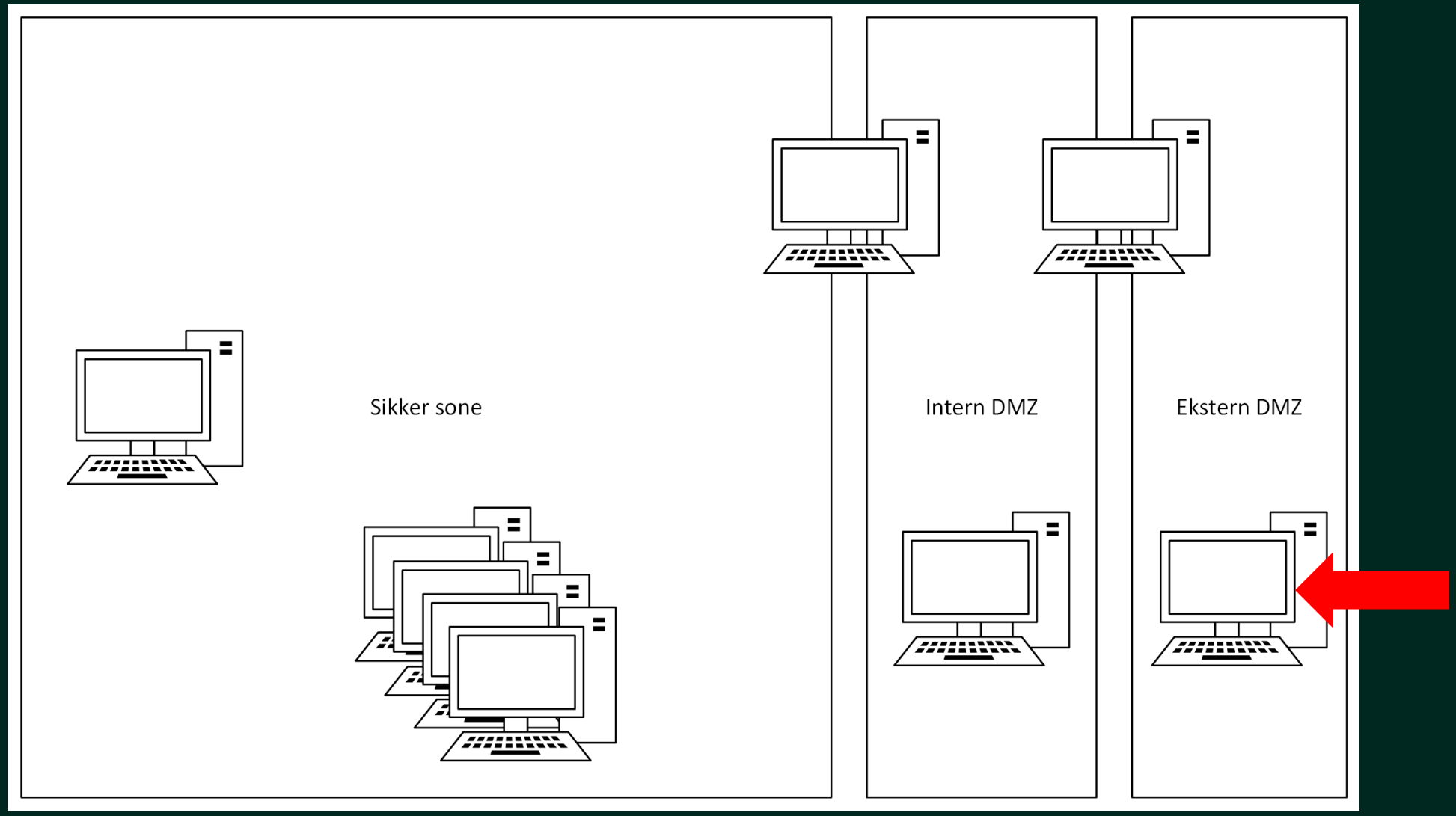
TLP:GREEN

Sykehuspartner

- Kompromittert 18. Desember.
- Angriper brøt seg inn på en gammel server som var flyttet fra et annet miljø.
- Angriper viste umiddelbart interesse for et elæringssystem.
- Hentet ut kildekoden til dette systemet.

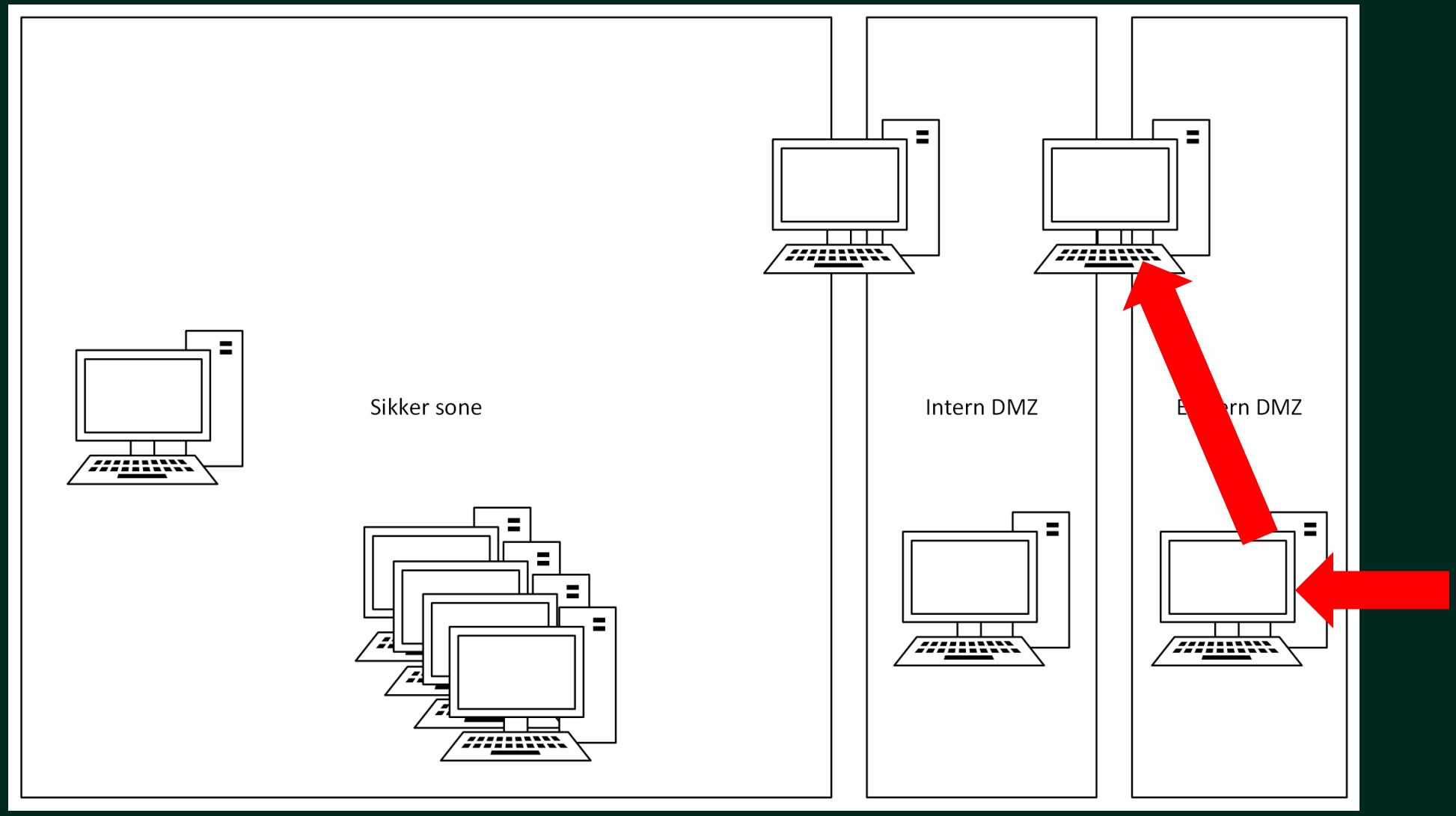
TLP:GREEN

Sykehuspartner



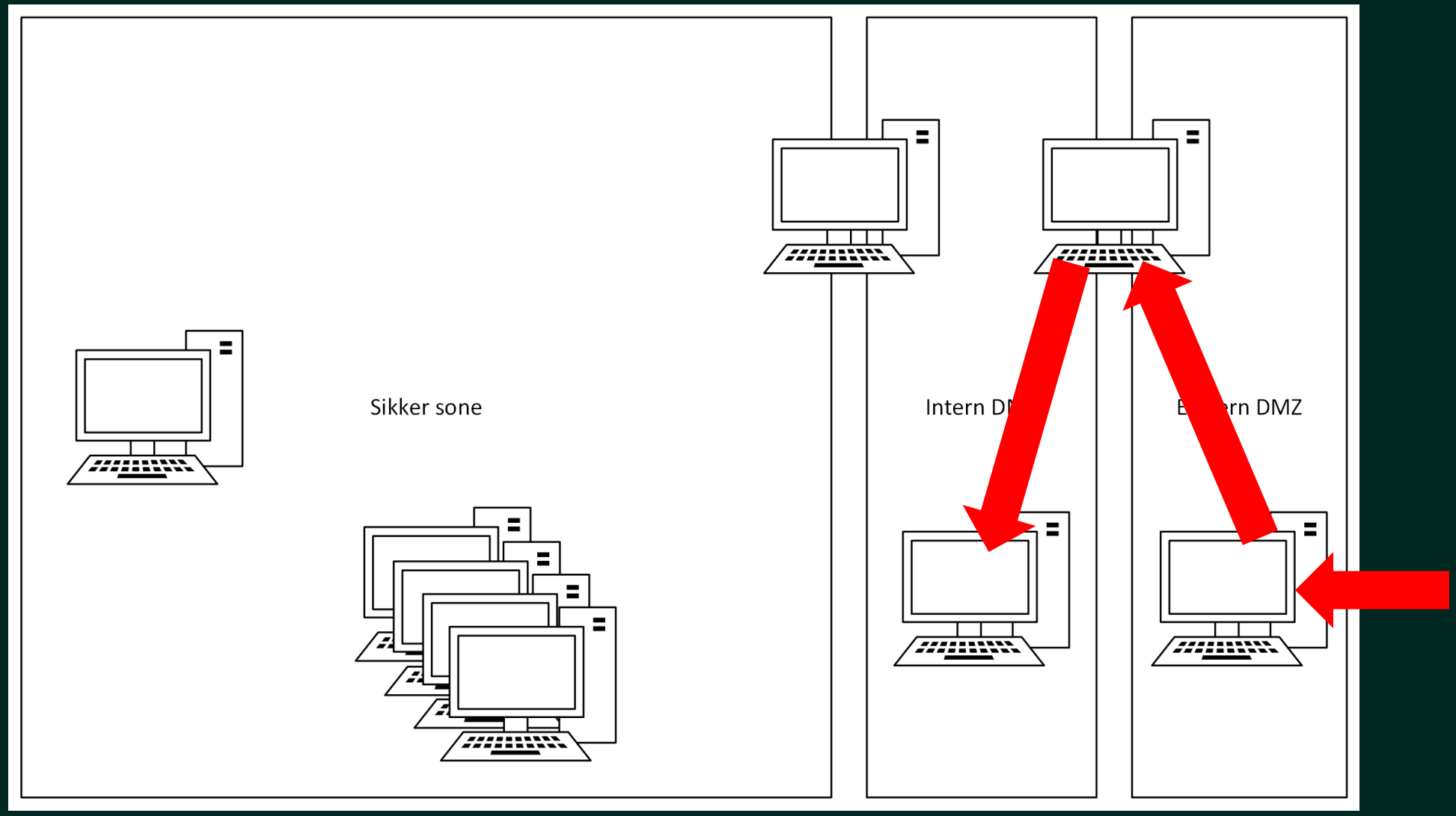
TLP:GREEN

Sykehuspartner



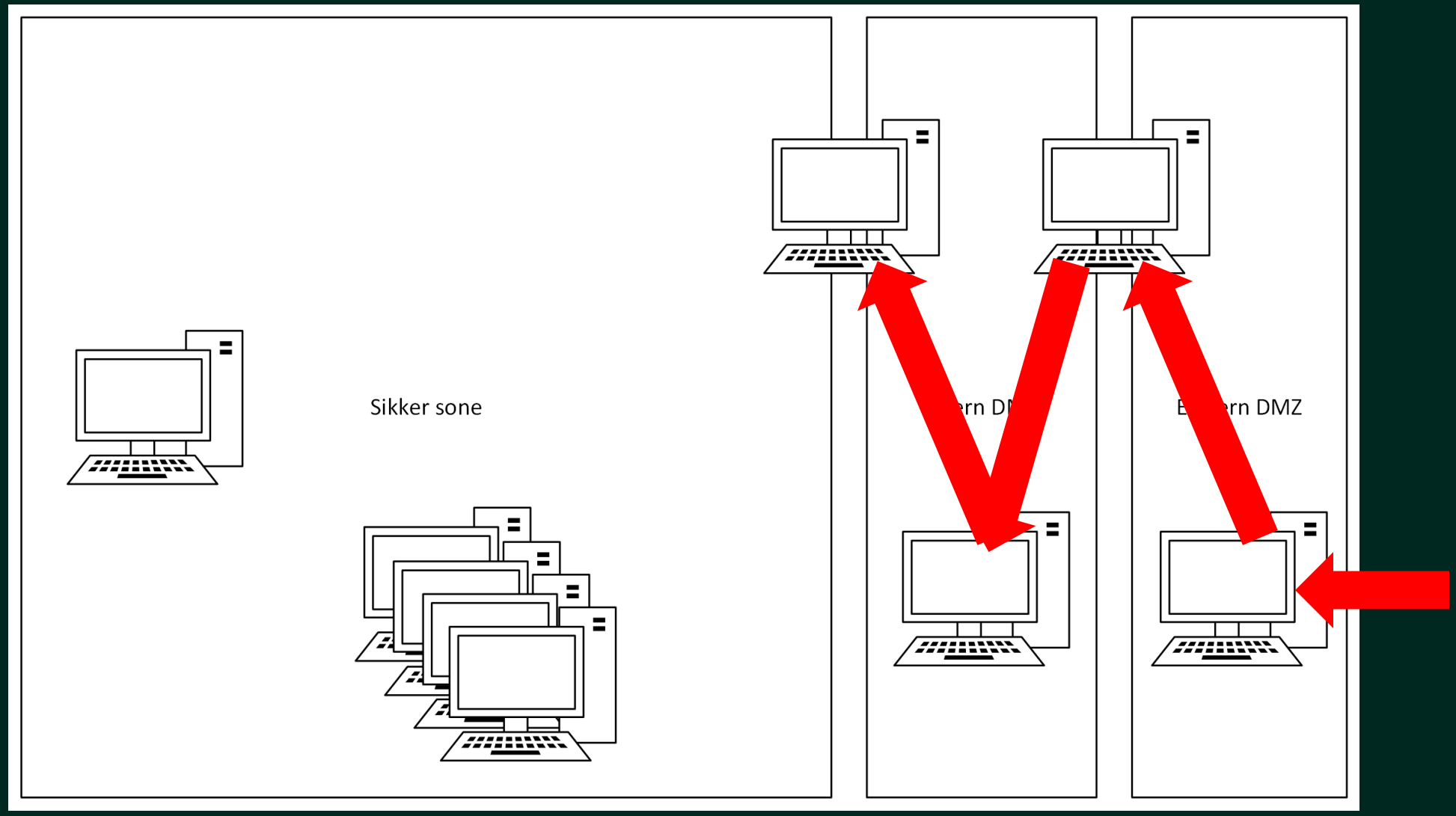
TLP:GREEN

Sykehuspartner



TLP:GREEN

Sykehuspartner



TLP:GREEN

Sykehus

- Statlig kinesi
- APT40
  - Hainan Xiand
  - Chinese Mini
- Vår vurderin

TLP:GREEN

Hva betyr dette for meg?

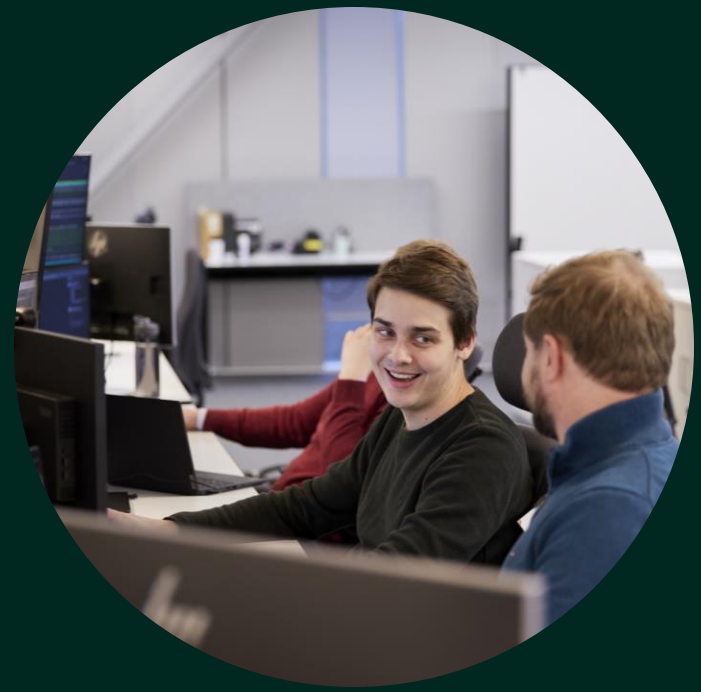
- Server på internet? Fiks sårbarheten i dag
- Viktig med AV/EDR , og oppfølging

Norsk helsenett

TLP:GREEN

Helse- og KommuneCERT

for helse- og kommunesektoren



post@helsecert.no