HELSECERT

Digitale trusler mot helsesektoren

Gunnar A. Johansen, HelseCERT

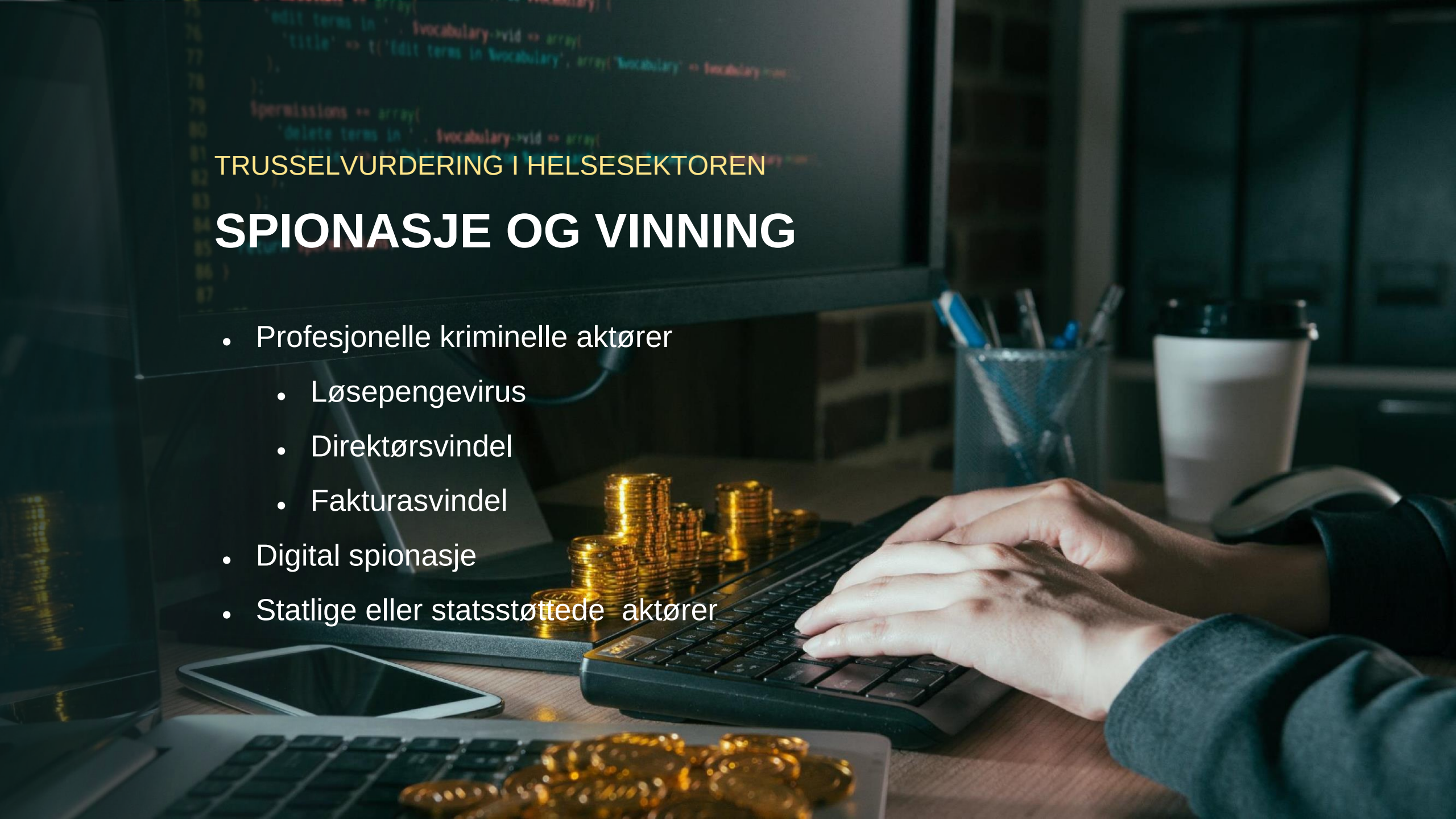
norskhelsenett

FOREBYGGE, OPPDAGE, HÅNDTERE

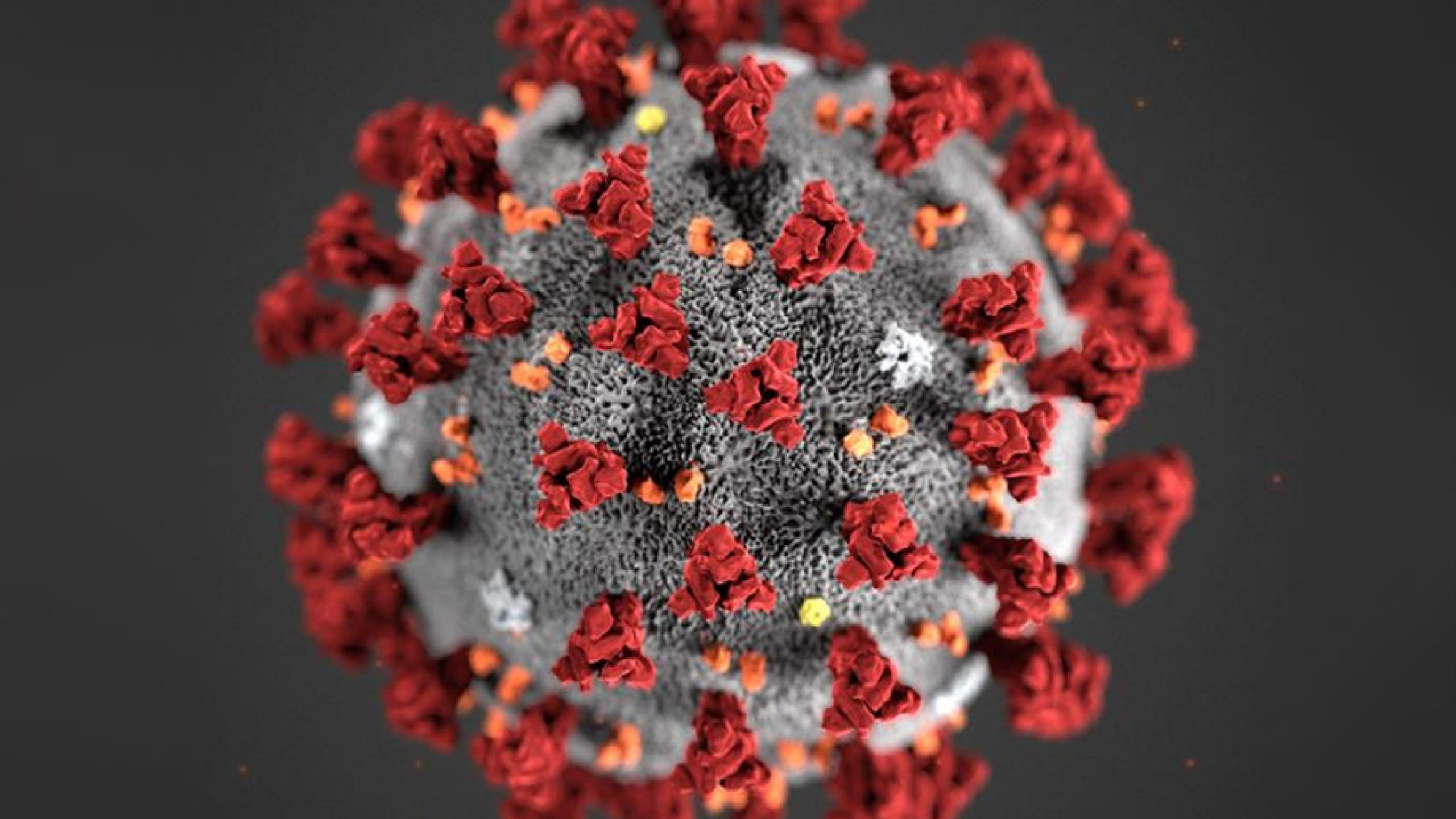
HELSECERT

TRUSSELVURDERING I HELSESEKTOREN

SPIONASJE OG VINNING



- Profesjonelle kriminelle aktører
  - Løsepengevirus
  - Direktørsvindel
  - Fakturasvindel
- Digital spionasje
- Statlige eller statsstøttede aktører



VANLIGE METODER

HVORDAN BLIR VI ANGREPET?

- E-post
- Sårbare tjenester på Internett

EMOTET TREFFER NORGE

COBALT STRIKE

Dataangrepet: Kan skade korona-beredskapen

10.000 ansatte i sju kommuner i Innlandet ble tirsdag kveld utsatt for et alvorlig e-postangrep. – En alvorlig situasjon midt i en pandemi, sier fylkesmannen.

ALVORLIG: Justisminister Monica Mæland og fylkesmann i Innlandet Knut Storberget diskuterte angrepet på sikkerhetskonferansen i Lillehammer.
FOTO: OLE MARTIN SPONBERG

Andreas Krantz
Journalist

Mette Finborud Børresen
Journalist

Trond Ivan Hagen
Journalist

Ann-Kristin Mo
Journalist

Kilde: **NRK / NTB**

Publisert 2. sep. kl. 00:17
Oppdatert 2. sep. kl. 14:37

INNBRUDD: Det har blitt utført et omfattende datainnbrudd hos den psykiatriske helseinstitusjonen Vastaamo i Helsinki. Foto: Heikki Saukkomaa / Lehtikuva

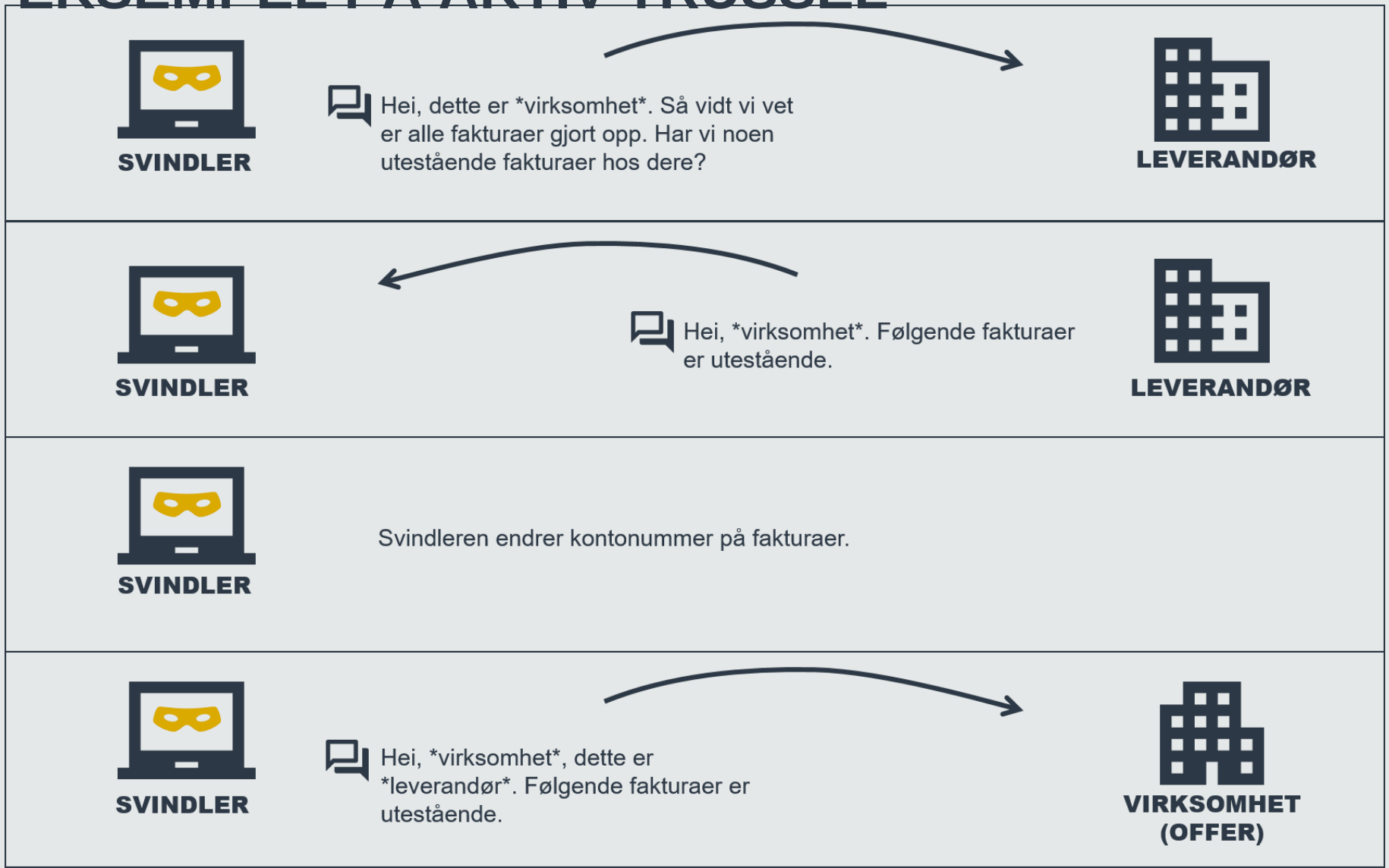
Hacker-skandale i Finland: Sensitiv informasjon om 40.000 psykiatriske pasienter på avveie

Personnumre, adresser og journalnotater til flere titalls tusen pasienter er stjålet. Nå presses pasientene for penger for å unngå publisering av opplysningene.

Faksimile: vg.no

Modus operandi

EKSEMPEL PÅ AKTIV TRUSSEL



SVINDELAKTØR

- Aktiv i Norge siden høst 2019
- Aktiv i Norge og Norden
- Forsøk i helsesektor på opptil 1.7 millioner EUR
- Forsøk mot utdanningssektor i Norge i både 2019 og 2020

UiT svindlet for 12 millioner

UiT betalte ut 12 millioner kroner til det som viste seg å være svindel. Pengene gikk til det som så ut som en faktura for en røntgenmaskin.

Verken politiet eller Kripos har så langt klart å identifisere gjerningspersonene i saken. Ingen av de ansatte ved UiT er mistenkt i saken.

FOTO: STIG BRØNDBO/UIT - NORGES ARKTISKE UNIVERSITET

Fra:

nrk.no,

Publisert:

19. desember 2019

Vaksinasjon – tiltak og forebyggende aktivitet

HVORDAN ØKE VÅR MOTSTANDSDYKTIGHET?


NSM
NASJONAL SIKKERHETSMYNDIGHET
Hvordan forebygge, oppdage og håndtere dataangrep
HÅNDTERING AV
DIGITAL SPIONASJE
NASJONAL SIKKERHETSMYNDIGHET
NSMs
Grunnprinsipper
for IKT-sikkerhet
versjon 2.0
NSM
NASJONAL SIKKERHETSMYNDIGHET
Anbefalinger for å øke evnen til å oppdage og håndtere uønskede hendelser og digitale angrep mot IKT-systemer
LOGGING
T SIKKERHET I IKT-SYSTEMER

TAKK FOR MEG

Sikkerhetskultur

Jobb med å bygge en god sikkerhetskultur i virksomheten. Gjennomfør opplæring og bevisstgjør ansatte.

Oppdatering

Oppgrader program- og maskinvare for å ta i bruk ny sikkerhetsfunksjonalitet og lukke sikkhetshull.

To-faktor

Innfør to-faktor-autentisering for tjenester tilgjengelig på internett for å hindre misbruk av kompromitterte eller dårlige passord.

DMARC

Beskytt e-post-domener med DMARC, som blokkerer uautorisert e-post og hindrer misbruk av domene.

Sårbarhetsskanning

Gjennomfør sårbarhetsskanning for å oppdage sårbare maskiner i eget nettverk.

Passord

Etabler en god passordpolicy og gi opplæring i hvordan å lage gode passord. Unngå gjenbruk.

Administratorkontoer

Beskytt administratorkontoer. Unngå at brukere har administratorrettigheter. Bruk LAPS for lokal admin.

Applikasjonshvitelisting

Applikasjonshvitelisting vil hindre kjøring av uautorisert programvare.

Segmentering

Benytt klientbrannmur for å unngå intern spredning. Segmenter nettverket ditt, ikke glem servere.

post@helsecert.no