

HELSECERT

Digitale trusler mot helsesektoren

Gunnar A. Johansen, HelseCERT

A person in a dark suit is shown from the chest down, typing on a laptop. The scene is overlaid with various futuristic digital elements in a glowing blue color. On the left, a shield-shaped icon contains binary code and a keyhole symbol. In the center, there are several floating panels and lines representing data and network connections. On the right, a circular icon with a blue dot is connected to lines. The overall aesthetic is high-tech and professional.

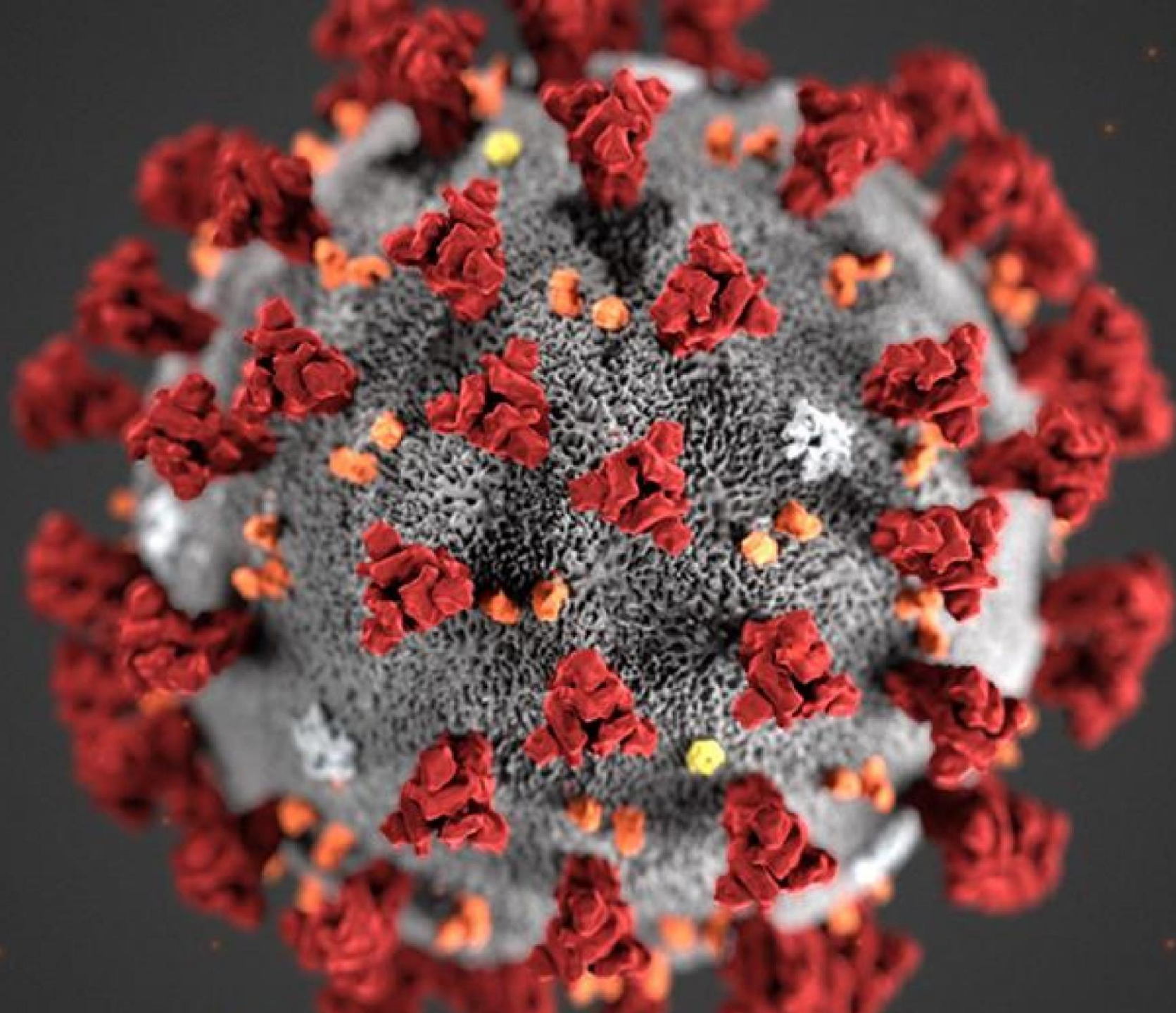
FOREBYGGE, OPPDAGE, HÅNDTERE

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

En skadevare har infisert flere små og mellomstore organisasjoner i helsesektoren.

Saksnummer: 565799

Start: 27.08.20 16.00

Slutt: Ukjent

Pressemelding fra Hedmark IKT vedrørende data-angrep.

Kvelden 1. september fanget vi opp et angrep rettet mot våre e-postservere, som potensielt kan være skadelig for våre datasystemer.

Varsel om pågående Emotet-kampanje

Publisert: 04.09.2020

NCSC ønsker å varsle om en pågående Emotet-kampanje observert i Norge.

COBALT STRIKE

cobaltstrike.com



COBALT STRIKE

ADVANCED THREAT TACTICS FOR PENETRATION TESTERS

DOWNLOAD

[FEATURES](#) [SCREENSHOTS](#) [TRAINING](#) [SUPPORT](#)

Event Log	Screenshots	Beacon 10.10.10.4@1008	Script Console
USER	computer	pid	when
SYSTEM	DC	4016	09/11 14:16:00
SYSTEM	DC	4016	09/11 13:54:00
SYSTEM	FILESERVER	1008	09/11 13:54:00
what's hagg	WS2	3952	09/11 13:54:00
SYSTEM	DC	4016	09/11 13:53:21
SYSTEM	FILESERVER	1008	09/11 13:53:21
what's hagg	WS2	3952	09/11 13:53:21

What is Cobalt Strike?

Cobalt Strike is software for Adversary Simulations and Red Team Operations.



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



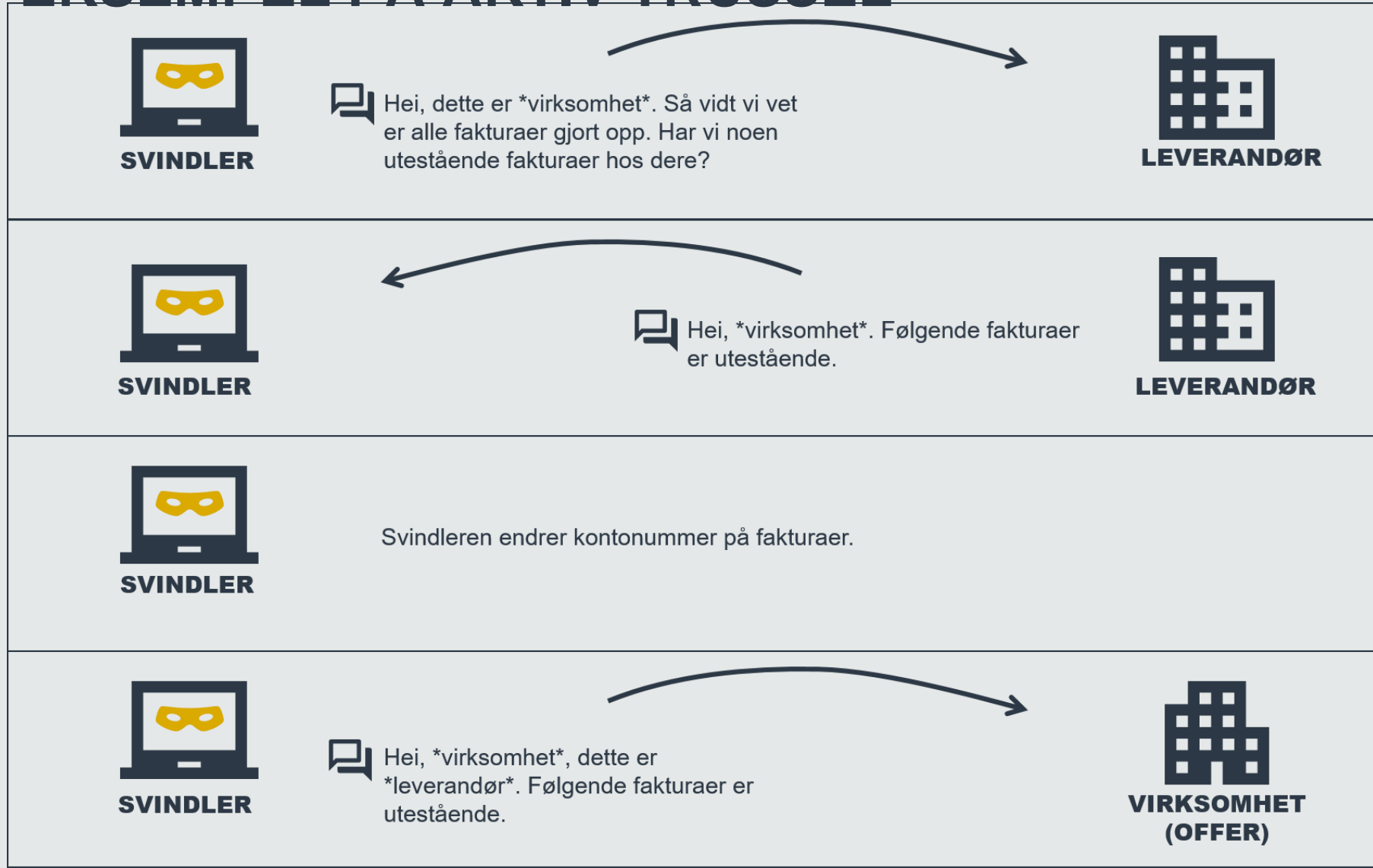
INNBRUDD: Det har blitt utført et omfattende datainnbrudd hos den psykiatriske helseinstitusjonen Vastaamo i Helsinki. Foto: Heikki Saukkomaa / Lehtikuva

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.

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 Kripas 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?

NASJONAL SIKKERHETSMYNDIGHET



Hvordan forebygge, oppdage og håndtere dataangrep

HÅNTERING AV DIGITAL SPIONASJE

NASJONAL SIKKERHETSMYNDIGHET

NSMs Grunnprinsipper for IKT-sikkerhet
versjon 2.0



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.



Passord

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



Oppdatering

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



Administratorkontoer

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



To-faktor

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



Applikasjonshvitelisting

Applikasjonshvitelisting vil hindre kjøring av uautorisert programvare.



DMARC

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



Segmentering

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



Sårbarhetsskanning

Gjennomfør sårbarhetsskanning for å oppdage sårbare maskiner i eget nettverk.



post@helsecert.no