

OPPLÆRING CYBERSIKKERHET

Trusselbildet, status i sektoren, og hva vi gjør
Erfaringer fra penetrasjonstester og hendelser

Hans Kristian Strømme
Sikkerhetsanalytiker HelseCERT

**KAN DIGITALE ANGREP SETTE
HELSE- OG OMSORGSSEKTOREN
SJAKKMATT?**



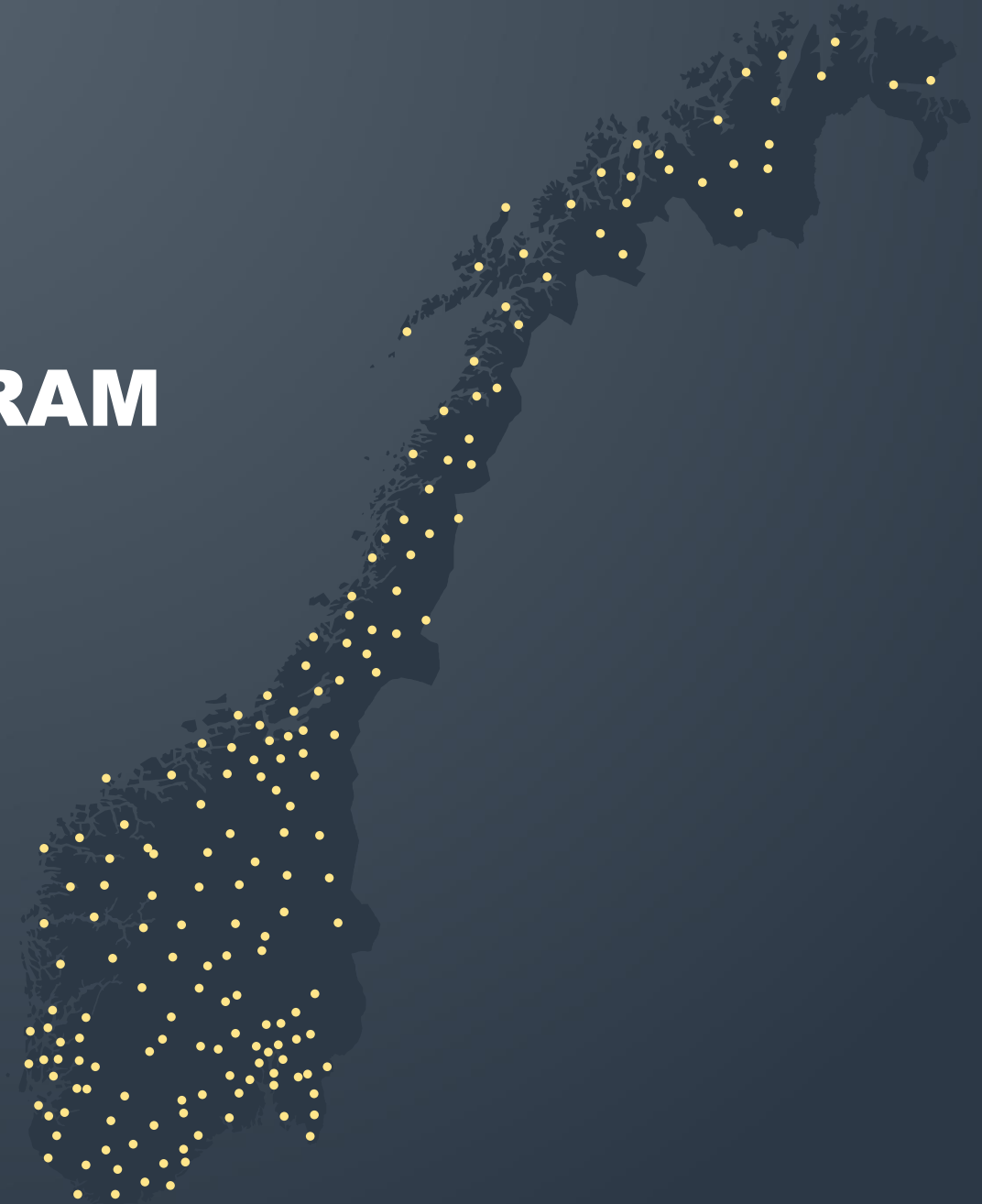


FOREBYGGE, OPPDAGE, HÅNDTERE
HELSECERT

NBP - TJENESTER TIL HELE SEKTOREN

NASJONALT BESKYTTELSESPROGRAM

- Hele spesialisthelsetjenesten
- 380 kommuner*
- Alle sentrale etater
- Opp mot 150 private leverandører



NBP - TJENESTER TIL HELE SEKTOREN

NASJONALT BESKYTTELSESPROGRAM

- Sensorplattform
- Sårbarhetsskanning
- Inntrengingstesting
- Internasjonalt nettverk
- Trussel- og sårbarhetsinformasjon
- Råd, veiledning og bistand



DBD – Digital Beskyttelse i Dybden på innsiden.

DIGITAL BESKYTTELSE I DYBDEN

- Sikkerhetsmonitorering – oppdage og respondere på innsiden
- Intern sårbarhetsskanning
- Sårbarhetsanalyse
- Inntrengingstesting
- Cyber threat hunting



Digitaliseringstrender

Primærhelsetjenesten **E-KONSULTASJON**



Omsorg for eldre og pleietrengende
VELFERDSTEKNOLOGI



Spesialisthelsetjenesten

ØKT DIGITALISERING



AiR





NASJONALE VURDERINGER

NASJONALT TRUSSELBILDE

- Statlige aktører
- Organiserte kriminelle
- Politisk motiverte hacktivist


```
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
```

TRUSSELVURDERING I HELSESEKTOREN

SPIONASJE OG VINNING

- Økonomisk kriminalitet
 - Løsepengevirus
 - Direktørsvindel
- Digital spionasje
- Sabotasje



Dagens trusselaktør er

AVANSERT

MÅLRETTET

PROFESJONELL

RESSURSSTERKE

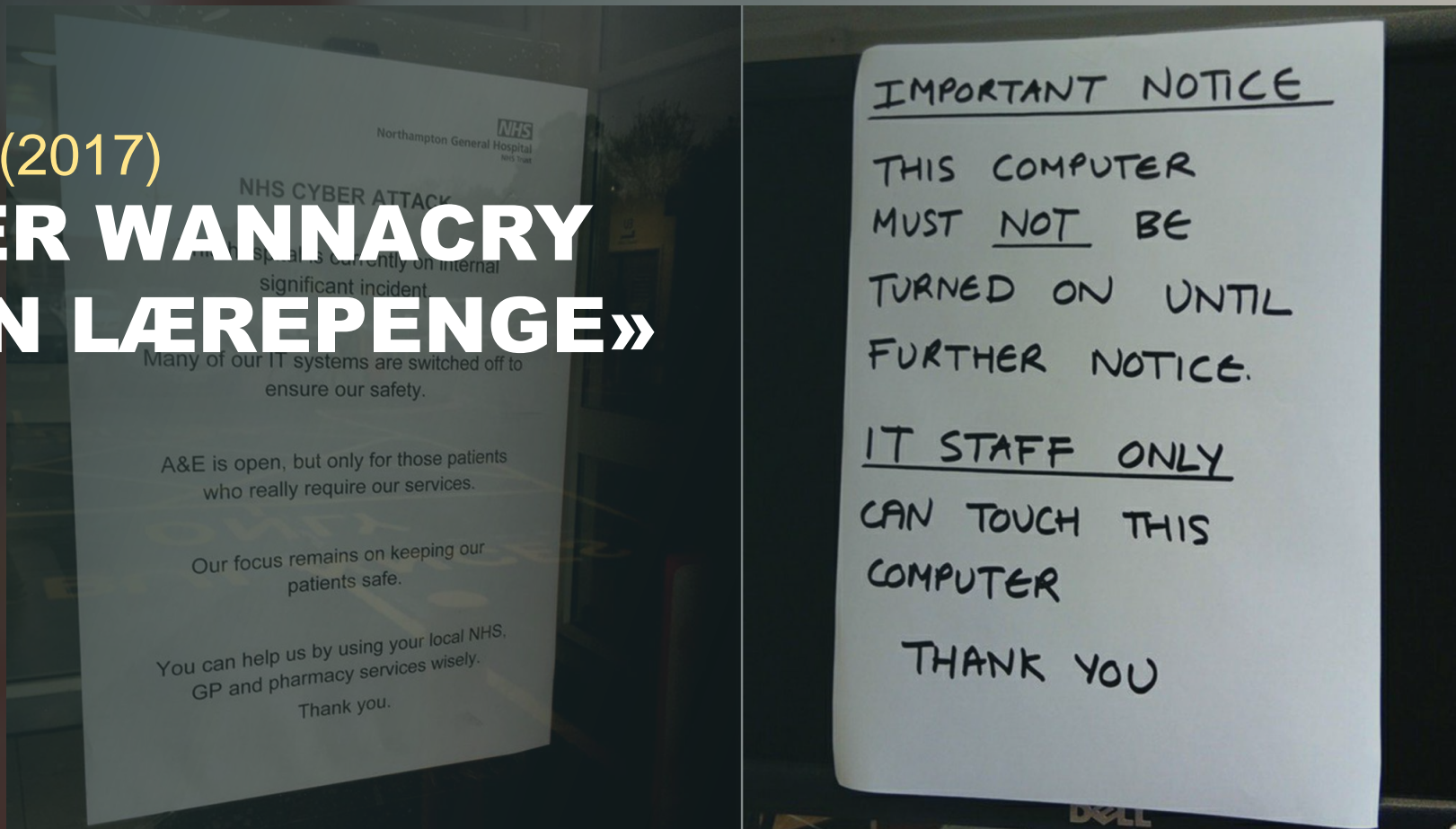
TAKTISK & STRATEGISK

Stavanger kommune mistet 500 000 i «direktørsvindel»

Stavanger kommune har ved en feil betalt en halv million kroner til nettsvindlere. Svindlerne ble avslørt da de prøvde å få utbetalt samme sum en gang til.

Wannacry (2017)

«HÅPER WANNACRY VAR EN LÆREPENGE»



Northampton General Hospital
NHS

NHS CYBER ATTACK

Many of our IT systems are currently on internal
significant incident

Many of our IT systems are switched off to
ensure our safety.

A&E is open, but only for those patients
who really require our services.

Our focus remains on keeping our
patients safe.

You can help us by using your local NHS,
GP and pharmacy services wisely.
Thank you.

IMPORTANT NOTICE

THIS COMPUTER
MUST NOT BE
TURNED ON UNTIL
FURTHER NOTICE.

IT STAFF ONLY
CAN TOUCH THIS
COMPUTER

THANK YOU

HSØ-angrepet (2018)

**«AVANSERT, MÅLRETTET
DATAINNBRUDD HOS
HELSE SØR-ØST»**



19.03.2019

Warning:

Cyber Attack Against the Hydro Network.

Hydro-angrepet (2019)

«**DATAANGREPET**

KOSTET 300-350

MILLIONER»

-Security

ORBS
HYDRO ER

UNDER CYBER-
ANGREP.

IKKE KOBLE
PC TIL NETTVEKK
INNTIL NY

BESKJED

ORBS



TRE VANLIGE METODER

HVORDAN BLIR VI ANGREPET?

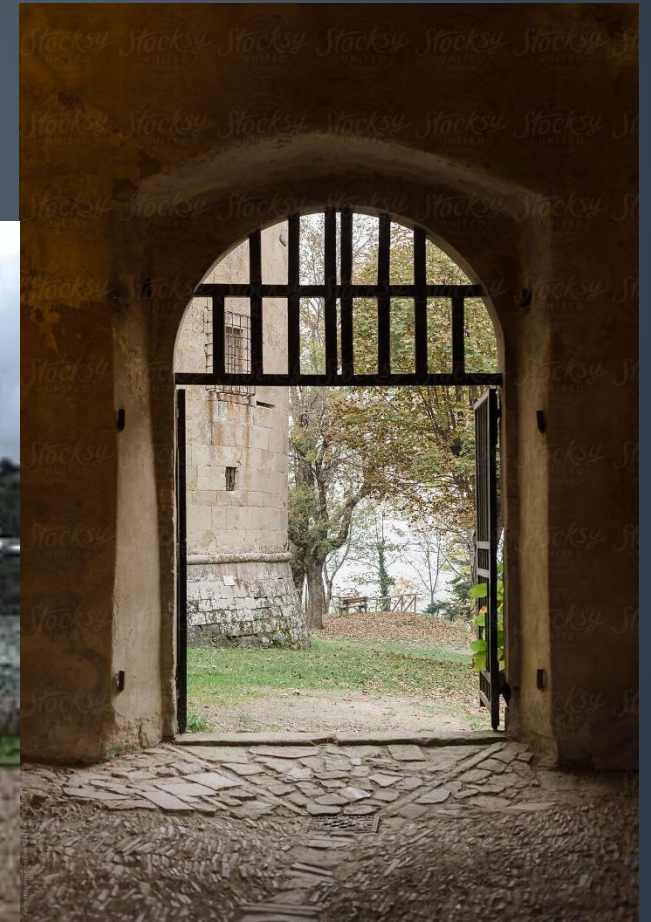
- Utdaterte / sårbare systemer
- Phishing og skadevare på epost
- Passordgjetting / passord på avveie



Hva med
medisinsk utstyr?

Medisinsk utstyr

- Opprinnelig laget for definerte oppgaver uten behov for nettverksforbindelse.
- I dag skal de gjerne snakke med:
 - Journalsystemer
 - Interne nett
 - eksterne nett



Ny teknologi gir nye angrepsvektorer

Sofie Nystrom Retweeted



MIT Technology Review @techreview · Feb 6, 2018

Hovering computers will make it increasingly possible to hack equipment that doesn't connect directly to the internet.



Cyberwarfare is taking to the skies, aboard drones

Hovering computers will make it increasingly possible to hack equipment that doesn't connect directly to the internet.The ...

technologyreview.com



Retweets 43

Likes 29



- Sertifisering vs oppdatering



stolav.no/avdelinger/divisjon-st-olavs-driftsservice/medisinsk-teknikk#medisinsk-... ☆

Det stilles svært strenge krav til kvaliteten på selve utstyret og til vedlikehold og reparasjoner i og med at det medisinske tekniske utstyret ofte er koblet direkte på- eller i pasientene.

Hvordan kan vi «digitalisere»
medisinsk utstyr på en sikker
måte?

Asset management



Tilgangskontroll

- Trengs det tilgangskontroll (passord / annet)
- Har plassering og tilgjengelighet noe å si?
 - Internett
 - Lokalt nett
 - Fysisk tilgang



Segmentering





Skanning



Oppsummert

- Asset management
 - Tilgangskontroll
 - Segmentering
 - Kontroll på USB
-

Spørsmål?

Påmelding til sårbarhetsvarsel for medisinsk utstyr kontakt:

post@helsecert.no

norsk**helsenett**

HelseCERT