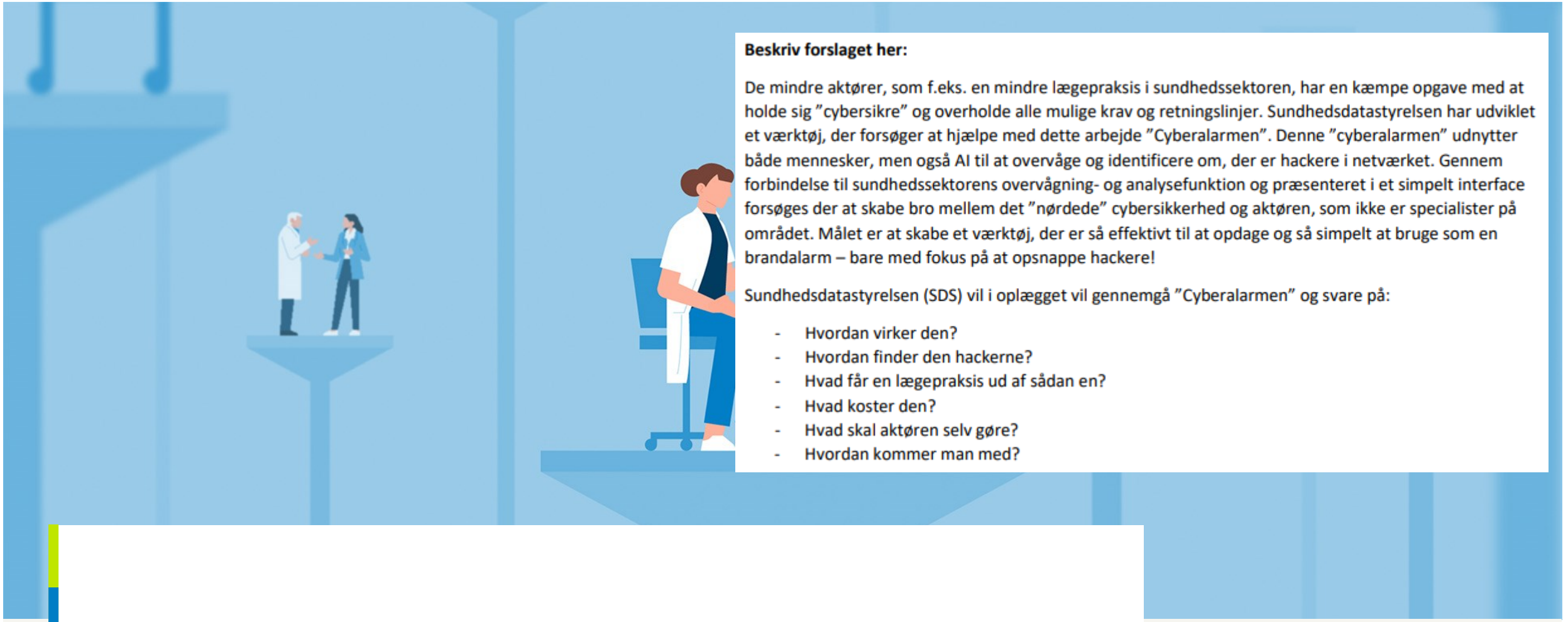


Beskriv forslaget her:

De mindre aktører, som f.eks. en mindre lægepraksis i sundhedssektoren, har en kæmpe opgave med at holde sig "cybersikre" og overholde alle mulige krav og retningslinjer. Sundhedsdatastyrelsen har udviklet et værktøj, der forsøger at hjælpe med dette arbejde "Cyberalarmen". Denne "cyberalarmen" udnytter både mennesker, men også AI til at overvåge og identificere om, der er hackere i netværket. Gennem forbindelse til sundhedssektorens overvågning- og analysefunktion og præsenteret i et simpelt interface forsøges der at skabe bro mellem det "nørdede" cybersikkerhed og aktøren, som ikke er specialister på området. Målet er at skabe et værktøj, der er så effektivt til at opdage og så simpelt at bruge som en brandalarm – bare med fokus på at opsnappe hackere!

Sundhedsdatastyrelsen (SDS) vil i oplægget vil gennemgå "Cyberalarmen" og svare på:

- Hvordan virker den?
- Hvordan finder den hackerne?
- Hvad får en lægepraksis ud af sådan en?
- Hvad koster den?
- Hvad skal aktøren selv gøre?
- Hvordan kommer man med?

Cyberalarmen – en hjælp til de små lægepraksis!

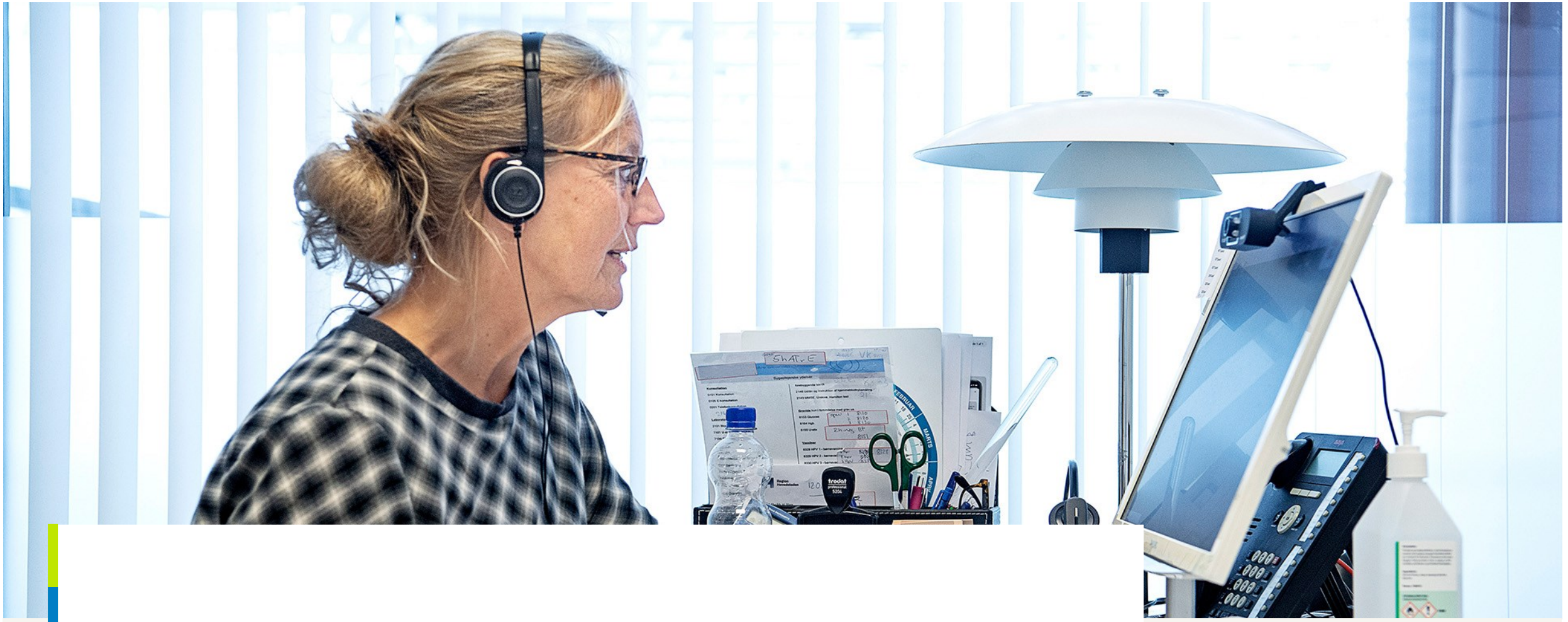
17 min

SUNDHEDSDATA-
STYRELSEN

Budskaber, postulater og agenda

- Det er ikke nok med analyser, vejledninger og rådgivning – der skal også noget ”faktisk sikkerhed” på bordet!
- Håndgribelige initiativer er nemmere at forklare og implementere end ”meta” initiativer
- Det er tid til at komme ud af ”specialist-kommunikationen” og skifte til forståelighed og aflæselighed.

- ~~Del 1: Tog vi under **Cyber, AI og alt det her – mulighed eller trussel?!**~~
- Del 2: Hvad er problemet?
- Del 3: Hvad gør vi så ved det?



Del 2: Hvad er problemet?

SUNDHEDSDATA-
STYRELSEN

Analyser

DIGITALISERINGSSTYRELSEN

Hovedkonklusioner

Fremgang i SMV'ernes digitale sikkerhedsniveau

- SMV'erne øger fortsat deres investeringer i digital sikkerhed. I 2021 har **37 pct.** af SMV'erne øget deres investeringer i digital sikkerhed sammenlignet med 2020, hvilket er den relativt største stigning siden 2018.
- **16 pct.** af SMV'erne gennemførte *ikke* de to helt basale it-sikkerhedstiltag i 2022; opdatering af software og backup af data. Dette er en markant forbedring sammenlignet med 2021, hvor **24 pct.** af SMV'erne *ikke* gennemførte de to basale tiltag. Det er især andelen af virksomheder, der anvender backup af data, som er steget fra 2021 til 2022.
- **35 pct.** af SMV'erne har et for lavt digitalt sikkerhedsniveau set i forhold til deres risikoprofil. Igen ses der dog fremgang i forhold til **44 pct.** i det forgange år.

De helt små virksomheder (5-9 ansatte) halter fortsat efter

- Blandt de helt små virksomheder (mikrovirksomheder) med 5-9 ansatte er det blot **71 pct.** af virksomhederne, som anvender de to basale sikkerhedstiltag i 2022. Dermed er der hele **29 pct.**, som *ikke* anvender de to basale tiltag som en del af deres digitale sikkerhed. Dette gælder til sammenligning **16 pct.** blandt de øvrige SMV'er med 10-249 ansatte.
- Blandt mikrovirksomhederne findes desuden *ikke* en positiv udvikling i brug af it-sikkerhedstiltag siden den seneste undersøgelse blandt mikrovirksomhedernes digitale sikkerhed, som blev gennemført i 2019.

SMV'ernes brug af organisatoriske sikkerhedstiltag

- Blot **54 pct.** af SMV'erne gennemfører dokumentation om forholdsregler, aktiviteter og procedurer vedr. it-sikkerhed. Blandt de virksomheder, som gennemfører dokumentation af deres it-sikkerhed er det kun **36 pct.**, som har opdateret denne dokumentation indenfor de seneste 12 måneder.
- Der er også plads til forbedring hvad angår ledelsen involvering i virksomhedernes digitale sikkerhed, da blot **36 pct.** af de adspurgte SMV'er svarer, at virksomhedens ledelse *i høj grad* er involveret i beslutninger om virksomhedens arbejde med digital sikkerhed (hvilket er på niveau med det forgange år).

Varetagelse af it-sikkerhedsmæssige opgaver og mangel på it-specialister

- **17 pct.** af SMV'erne har eller har forsøgt at rekruttere it-specialister i 2021. Heraf har **60 pct.** haft svært ved at besætte stillingen. Mange SMV'er har ikke en decideret it-sikkerhedsmedarbejder ansat, men anvender netop generelle it-specialister til også at varetage virksomhedens it-sikkerhedsmæssige opgaver. Derfor kan en mangel på it-specialister få negative konsekvenser for virksomhedernes digitale forsvar.
- I 2022 har hele **77 pct.** af SMV'erne (i et vist omfang) benyttet sig af ekstern hjælp til at løfte virksomhedens digitale sikkerhed (dette tal er steget fra **68 pct.** i 2020). Men **25 pct.** af de SMV'er, som anvender en ekstern leverandør, stiller *ikke* krav til leverandøren om fx behandling af data, it-sikkerhedsforanstaltninger og/eller løbende dokumentation om it-sikkerhed.

It-sikkerhedshændelser

- Samlet set har **28 pct.** af SMV'erne og **57 pct.** af de store virksomheder oplevet en it-sikkerhedshændelse i 2021 (dette tæller både utilsigtede hændelser såsom fx softwarefejl og ondsindede, forsætlige hændelser såsom fx ransomware-, phising eller Denial of Service angreb). Ses alene på de ondsindede/forsætlige hændelser har **9 pct.** af SMV'erne og **20 pct.** af de store virksomheder oplevet en it-sikkerhedshændelse i 2021.

https://digst.dk/media/29043/digital-sikkerhed-i-danske-smver-2023_endelig0310-a.pdf

ERHVERVSSTYRELSEN

Analysens hovedresultater er:

It-sikkerhedsforanstaltninger og SMV'ernes sikkerhedsniveau

- 25 pct. af de danske SMV'er anvendte *ikke* de to basale it-sikkerhedsforanstaltninger i 2020: opdatering af styresystemer og backup af data. Det er omtrent på samme niveau som i 2018 og 2019.
- 44 pct. af SMV'erne har et for lavt sikkerhedsniveau i forhold til deres sikkerhedsprofil.
- Andelen af SMV'erne som benytter mange it-sikkerhedsforanstaltninger (mellem 8-9) er steget med fire procentpoint siden 2018. Til sammenligning har andelen som benytter få it-sikkerhedsforanstaltninger (mellem 0-4) været nogenlunde stabil over samme periode.

It-sikkerhed og digitalisering i et covid-år

- Som følge af covid-19 har 68 pct. af SMV'erne et øget brug af remote løsninger. SMV'erne der har forøget sit brug af remote løsninger, er også mere digitalt sikre.
- 55 pct. af SMV'erne som har øget forbruget af to eller flere remote løsninger har implementeret mange it-sikkerhedsforanstaltninger (mellem 8-9).
- Til sammenligning har 54 pct. af SMV'erne, som ikke har et forøget brug af nogen remote løsninger, implementeret få it-sikkerhedsforanstaltninger (mellem 0-4).

Udfordringer og begrænsninger ved at øge it-sikkerhedsniveauet

- Mangel på viden og kompetencer til at håndtere it-sikkerhedsløsninger er SMV'ernes største udfordring med at hæve it-sikkerhedsniveauet, mens den største udfordring for virksomhederne med over 250 ansatte er manglende tilslutning fra medarbejderne.
- Således svarer 12 pct. af SMV'erne, at de ikke har viden og kompetencer, til at øge deres it-sikkerhed. Til sammenligning svarer kun 3 pct., at det er mangel på specifikke løsninger på markedet, der udgør en begrænsning.

It-sikkerhedshændelser

- I 2020 oplevede 17 pct. af de danske SMV'er mindst en af følgende fire it-sikkerhedshændelser: 1. blokeret adgang til it-services, 2. sletning, ødelæggelse, misbrug eller videregivelse af data (forsætligt eller utilsigtet), 3. it-relateret økonomisk svindel og 4. andre it-sikkerhedshændelser.
- Den mest udbredte it-sikkerhedshændelse er blokeret adgang til it-services (hvis man ser bort fra kategorien "andre it-sikkerhedshændelser").
- Således har 7 pct. af SMV'erne oplevet denne it-sikkerhedshændelse, mens det til sammenligning er 19 pct. af virksomhederne med over 250 ansatte.

Dataetik og it-sikkerhed

- De SMV'er som arbejder aktivt med dataetik, har implementeret flere it-sikkerhedsforanstaltninger, end de SMV'er som ikke arbejder aktivt med dataetik.

https://digst.dk/media/28897/digital-sikkerhed-i-danske-smver_erhvervsstyrelsen_sep2022_wa-1.pdf

SUNDHEDSDATA-STYRELSEN

Cyber- og informationssikkerhed hos lægen

D

to 25-04-2024 08:44

DCISvarsel

DCISSUND, TLP: WHITE, KRITIKALITET: Orange, To zero-day-sårbarheder i Cisco ASA/FTD 25 april 2024 - 08:43

Til Søren Bank Greenfield

TLP: WHITE/CLEAR (Informationerne anses ikke som særligt følsomme og kan frit deles)

Kære aktør

DCIS Sund er blevet bekendt med to nyligt opdaterede zero-day-sårbarheder i Cisco Adaptive Security Appliance (ASA) og Firepower Threat Defense (FTD).

Situationsoverblik:

De to sårbarheder er, ifølge Cisco, blevet udnyttet siden november 2023 mod statslige netværk til at deployere malware. Denne malware består af to dele, Line Dancer og Line Runner. Line Dancer er en hukommelsesbaseret shellcode-loader, der hjælper med at levere og udføre vilkårlig shellcode for at deaktivere logning, give fjernadgang og eksfiltrere opsnappede pakker. Line Runner er en persistent bagdør, der har flere forsvarsmekanismer til undvigelse af opdagelse og tillader ondsindede aktører at køre vilkårlig Lua-kode på de udnyttede systemer.

Sårbarheden / sårbarheder med tildelt CVSS:

- CVE-2024-20353 CVSS: 8.6
- CVE-2024-20359 CVSS: 6.0

Berørte produkter:

- Cisco ASA
- Cisco FTD

Anbefalinger:

Aktører kan med fordel opdatere deres Cisco ASA/FTD-produkter til en fikset version.

Konsekvens ved ikke at handle:

En ondsindet aktør kan udnytte disse sårbarheder til at deployere malware.

Læs mere på:

https://www.bleepingcomputer.com/news/security/arcanedoor-hackers-exploit-cisco-zero-days-to-breach-govt-networks/
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h#fs
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2

For sundhedssektorens aktører:

Dialog om varslinger kan fortages på chat-kanalen Sektorforum.
Tilmelding til Sektorforum kan ske gennem:
https://mattermost.energicert.dk/signup_user_complete/?id=w7hh8wmxj3b3dm415tfig19pfc&md=link&sbr=su

---

"Image created by OpenAI's DALL-E."

Cyber- og informationssikkerhed hos lægen

SUMMA

Over the week, severa
impacted by security ev
Hospital in Cannes, the It
Italia and the Irish game d
Further afield, FIN7 wa
manufacturing sector, U
allegedly breached by Inte
the Russia-nexus Sandv
impacting French, Polish,
warned that MFA messag
subsidiary Duo were stol
nation-state adversary re
research non-profit MIT
vulnerabilities in Ivanti Co
In terms of hacktivist-relat
marginal de-escalation in
last week has precipitatec
in the EU, though Moroc
targeted a Spanish cor
similarly targeted by pro-
reporting period, albeit on
certainly in response t
announcement of a bilater

CENTER FOR CYBERSIKKERHED

TLP:GREEN
Situationsbillede
26. april 2024, kl. 12:16
Nationalt

2 Fremhævede nyheder 26. apr, kl. 12:15

Nedenstående er en samling af historier, som medierne rapporterer om, og som situationscenteret ønsker at fremhæve.

2.1 Ondsindede aktører anvender i større grad sårbarheder til at opnå adgang til netværk

Mandiant har udgivet deres årlige trend rapport. De beskriver f.eks. hvordan aktører i større grad er begyndt at anvende zero-days til at opnå adgang, hvor de tidligere anvendte phishing i højere grad. Mandiant har observeret at 38% af kompromitteringer opstår grundet udnyttelse af sårbarheder. Yderligere er dwell-time, altså tiden som aktører har adgang til ens netværk før de opdages, faldet til 10 dage. I forrige rapport var medianen 16 dage før aktørerne blev opdaget. Bemærk at fundet også kan betyde, at aktøren bevidst har gjort sig bemærket ved eksempelvis at deployere ransomware. Situationscenteret observerer dagligt mange forsøg på at scanne virksomheders netværk for potentielle sårbarheder gennem sensornetværket. Situationscenteret anbefaler derfor, at man prioriterer at opdatere sine systemer hurtigst muligt, samt har et robust sårbarhedshåndterings program.

23.04.24 Mandiant - M-Trends 2024: Our View from the Frontlines

Attackers are taking greater strides to evade detection. This is one of the running themes in our latest release: M-Trends 2024. This edition of our annual report continues our tradition of providing relevant attacker and defender metrics, and insights into the latest attacker tactics, techniques and procedures, along with guidance and best practices on how organizations and defenders should be responding to threats.

23.04.24 Mandiant - M-Trends 2024 Special Report

In this 15th edition, M-Trends provides an inside look at the evolving cyber threat landscape, with data drawn directly from frontline incident response investigations and threat intelligence findings of high-impact attacks and remediations around the globe.

Image created by OpenAI's DALL·E.

to 25-04-2024 08:44

DCISvarsel

DCISSUND, TLP: WHITE, KRITIKALITET: Orange, To zero-day-sårbarheder i Cisco ASA/FTD 25 april 2024 - 08:43

Til Søren Bank Greenfield

TLP: WHITE/CLEAR (Informationerne anses ikke som særligt følsomme og kan frit deles)

TLP:GREEN
Situationsbillede
26. april 2024, kl. 12:16
Nationalt

ce (ASA) og

e malware.
le-loader, der
snappede
llader

mary

vet deres cybertrend rapport, M-trends 2024. Rapporten peger bl.a.
nytter zero-days til at opnå initial adgang til ofres systemer, hvor
rede.
på flere sårbarheder, som udnyttes aktivt: En ny sårbarhed i CrushFTP
læse og skrive filer og opnå fjerneksekvering af kode på serveren.
t tre sårbarheder i Cisco ASA og Cisco FTD-programmet, som tillader
g autentificeret Local Code Execution. CFCS anbefaler at opdatere

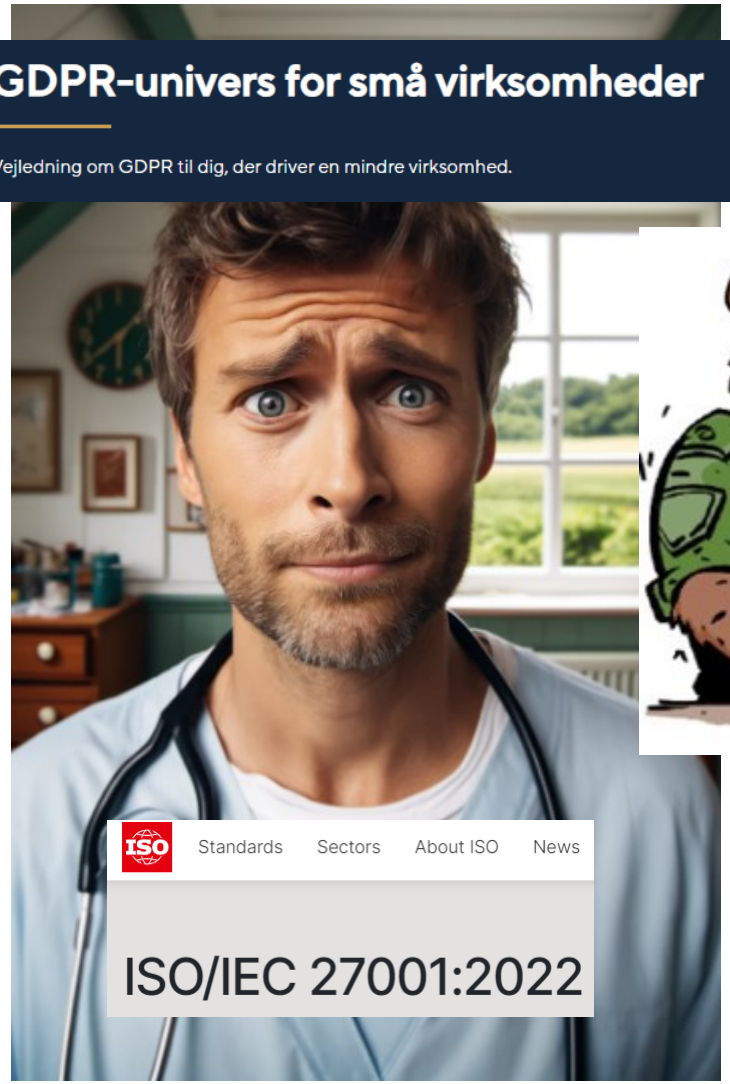
rdel opdatere deres Cisco ASA/FTD-produkter til en fikset version.

e at handle:
kan udnytte disse sårbarheder til at deployere malware.

ingcomputer.com/news/security/arcanedoor-hackers-exploit-cisco-zero-days-to-breach-govt-networks/
ps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h#fs
ps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2

rens aktører:
er kan fortages på chat-kanalen Sektorforum.
rforum kan ske gennem:
t.energicert.dk/signup_user_complete/?id=w7hh8wmxj3b3dm415tfig19pfc&md=link&sbr=su
---

Cyber- og informationssikkerhed hos lægen



to 25-04-2024 08:44

DCISvarsel

DCISSUND, TLP: WHITE, KRITIKALITET: Orange, To zero-day-sårbarheder i Cisco ASA/FTD 25 april 2024 - 08:43

Til Søren Bank Greenfield

TLP: WHITE/CLEAR (Informationerne anses ikke som særligt følsomme og kan frit deles)

Kære aktør

DCIS Sund er blevet bekendt med to nyligt opdaterede zero-day-sårbarheder i Cisco Adaptive Security Appliance (ASA) og Firepower Threat Defense (FTD).

Situationsoverblik:

De to sårbarheder er, ifølge Cisco, blevet udnyttet siden november 2023 mod statslige netværk til at deployere malware. Denne malware består af to dele, Line Dancer og Line Runner. Line Dancer er en hukommelsesbaseret shellcode-loader, der hjælper med at levere og udføre vilkårlig shellcode for at deaktivere logning, give fjernadgang og eksfiltrere opsnappede pakker. Line Runner er en persistent bagdør, der har flere forsvarsmekanismer til undvigelse af opdagelse og tillader ondsindede aktører at køre vilkårlig Lua-kode på de udnyttede systemer.

Sårbarheden / sårbarheder med tildelt CVSS:

- CVE-2024-20353 CVSS: 8.6
- CVE-2024-20359 CVSS: 6.0

Berørte produkter:

- Cisco ASA
- Cisco FTD

Anbefalinger:

Aktører kan med fordel opdatere deres Cisco ASA/FTD-produkter til en fikset version.

Konsekvens ved ikke at handle:

En ondsindet aktør kan udnytte disse sårbarheder til at deployere malware.

Læs mere på:

https://www.bleepingcomputer.com/news/security/arcanedoor-hackers-exploit-cisco-zero-days-to-breach-govt-networks/
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h#fs
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2

For sundhedssektorens aktører:

Dialog om varslinger kan fortages på chat-kanalen Sektorforum.
Tilmelding til Sektorforum kan ske gennem:
https://mattermost.energicert.dk/signup_user_complete/?id=w7hh8wmxj3b3dm415tfig19pfc&md=link&sbr=su

---

https://www.iso.org/standard/27001

https://www.datatilsynet.dk/hvad-siger-reglerne/vejledning/gdpr-univers-for-smaa-virksomheder

"Image created by OpenAI's DALL-E."

SUNDHEDSDATA-STYRELSEN

Del 3: Hvad gør vi så ved det?

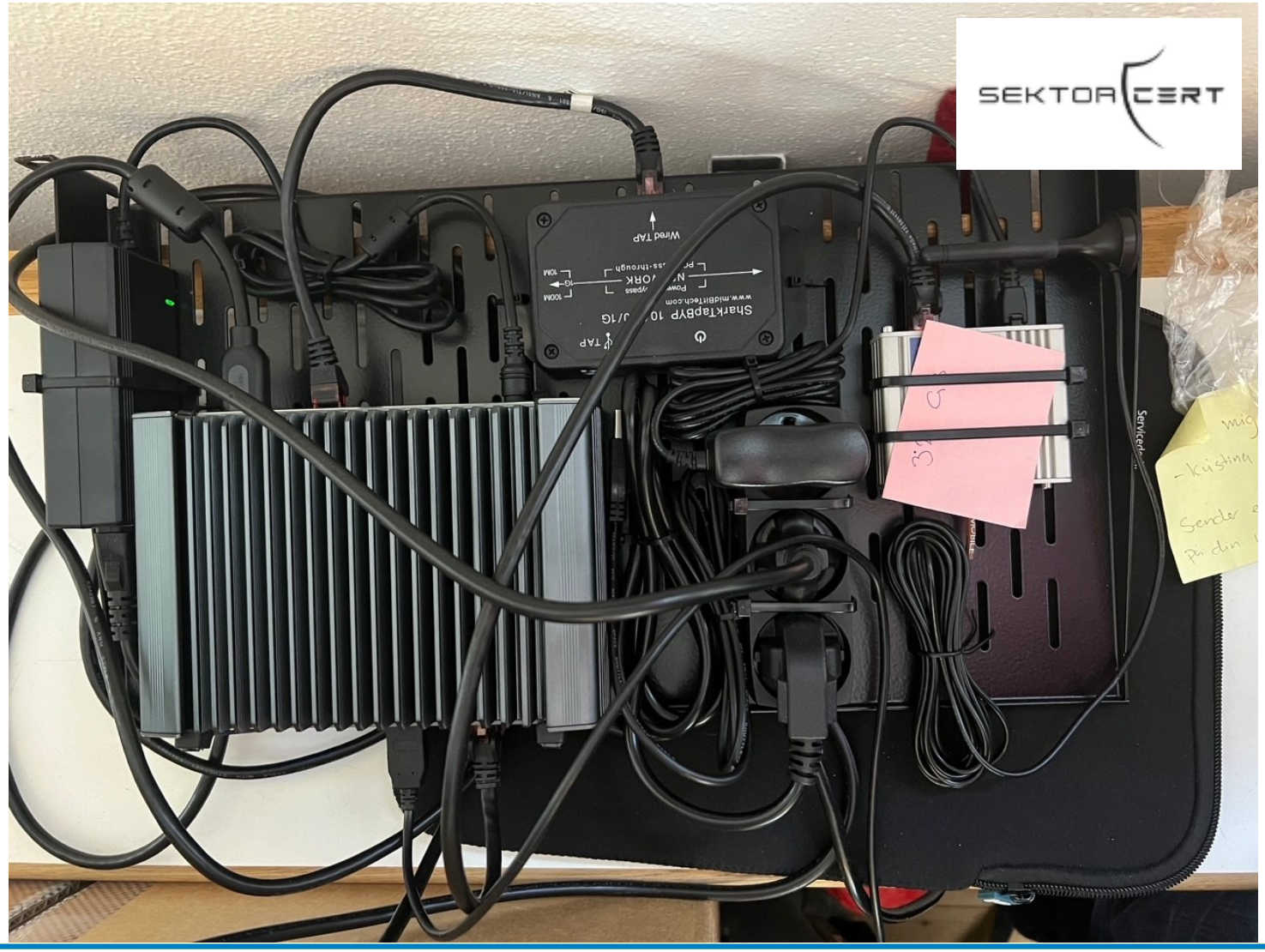
SUNDHEDSDATA-
STYRELSEN

Ok, hvad så?


Fødevarekontrol
Dato
16-08-2023
Tidligere kontrol
09-03-2023
31-03-2022
Scan og læs kontrolrapporten på findsmiley.dk
Ministeriet for Fødevarer, Landbrug og Fiskeri
Fødevarestyrelsen

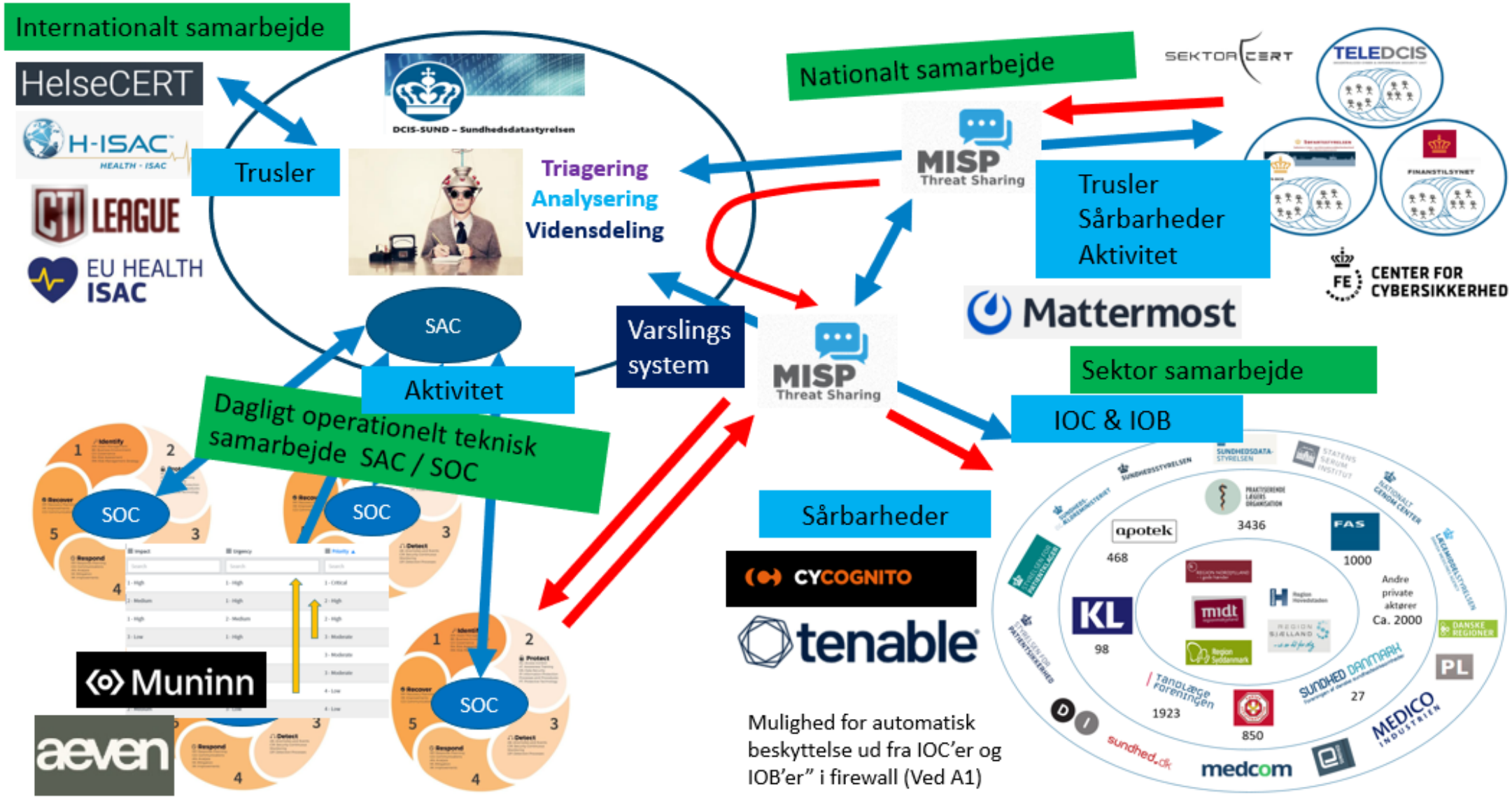

FIRE

Ned i en boks!



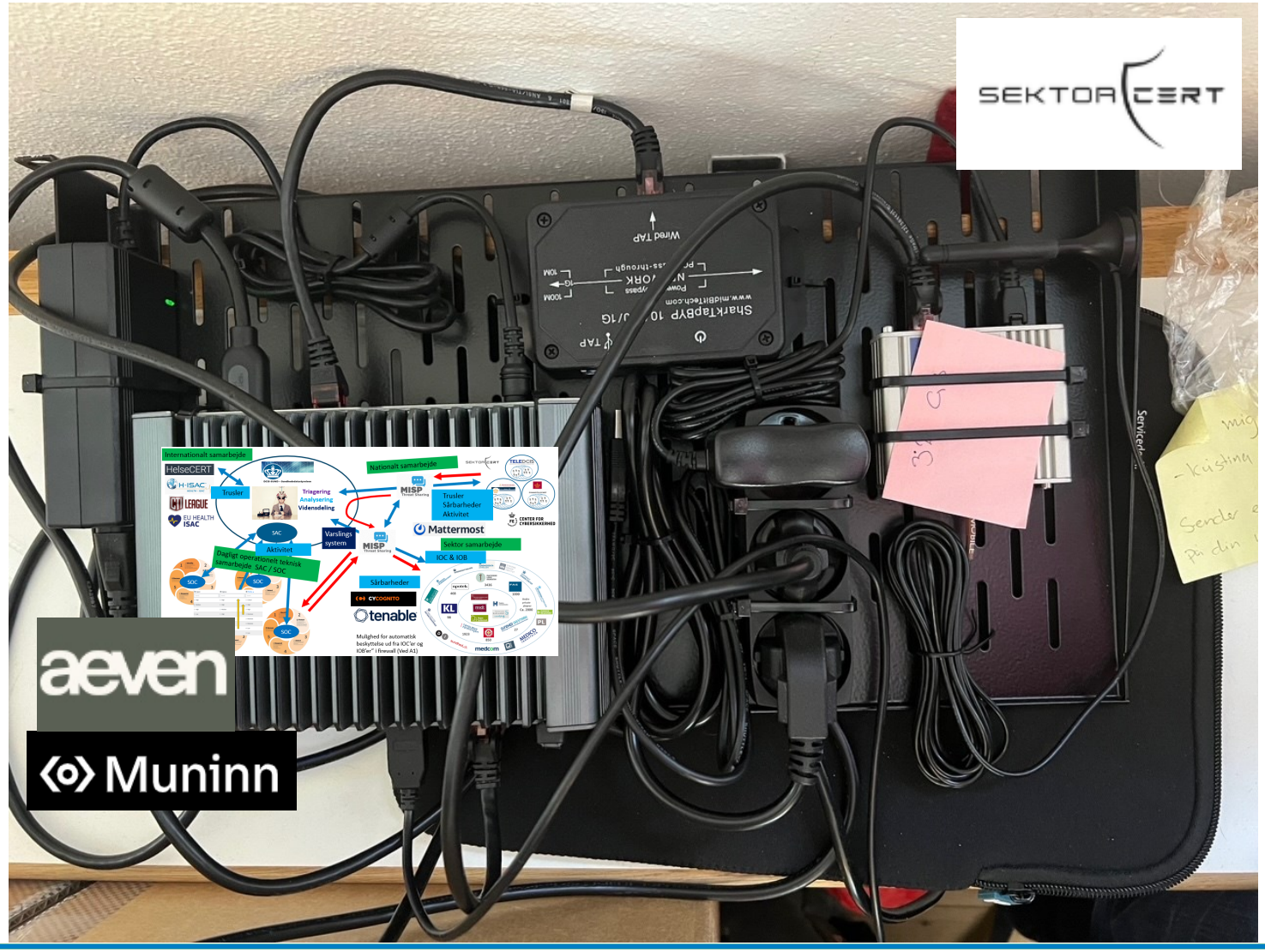
SUNDHEDSDATA-
STYRELSEN

Ned i en boks!



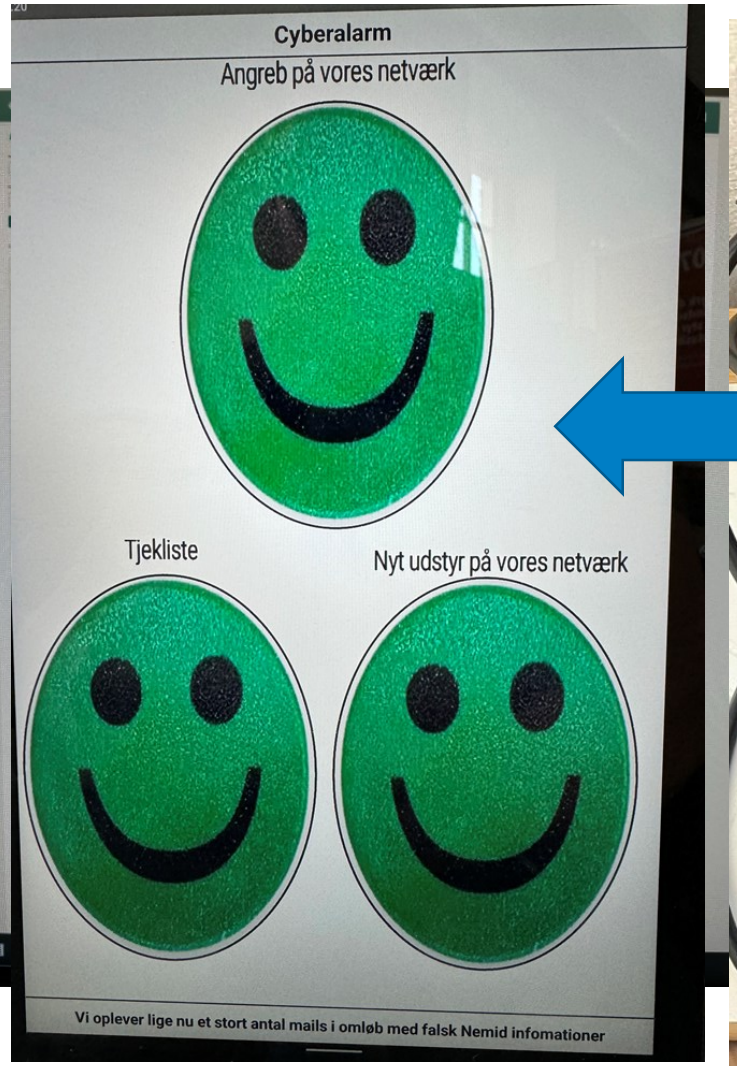
SUNDHEDSDATA-STYRELSEN

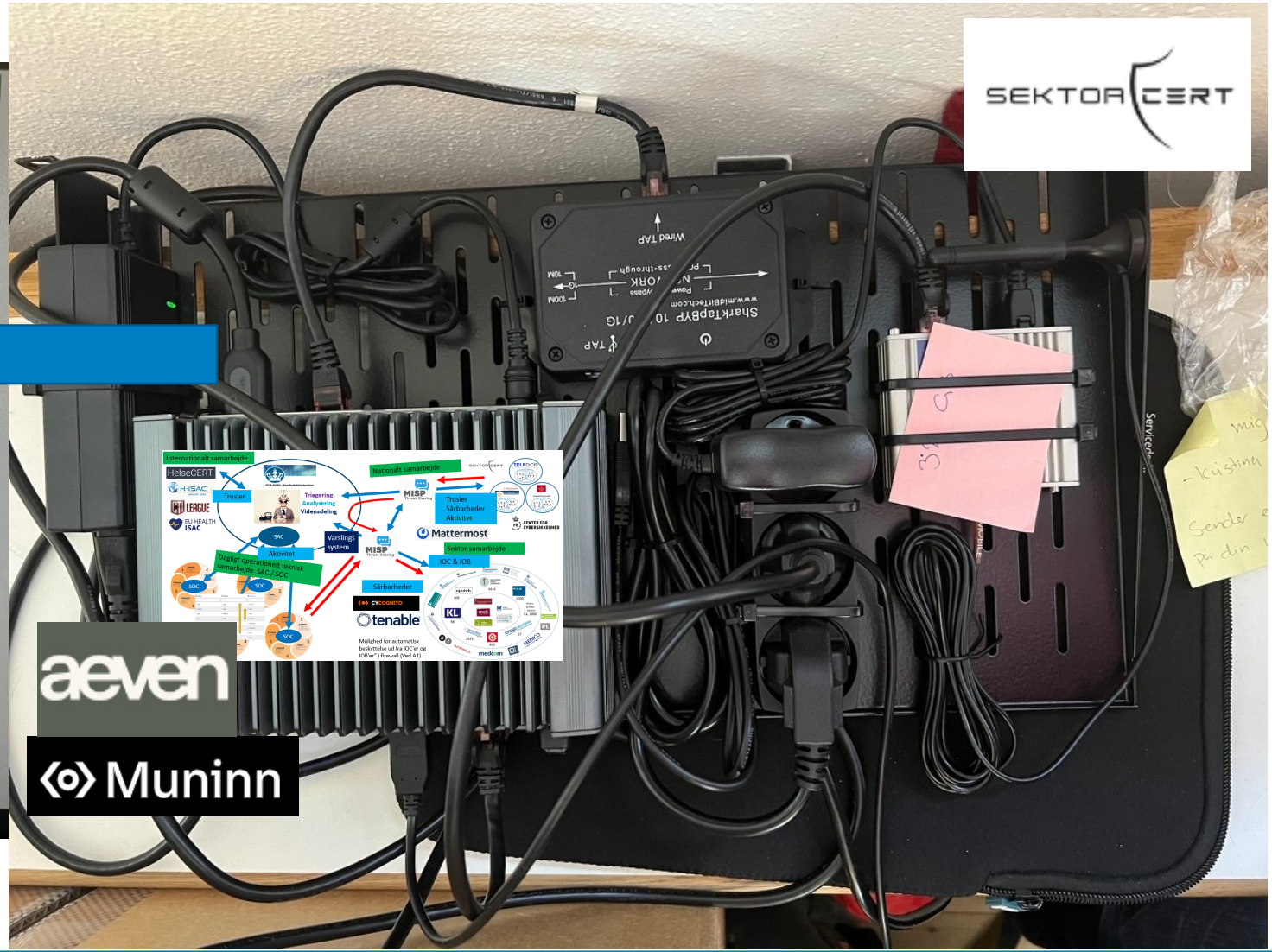
Ned i en boks!



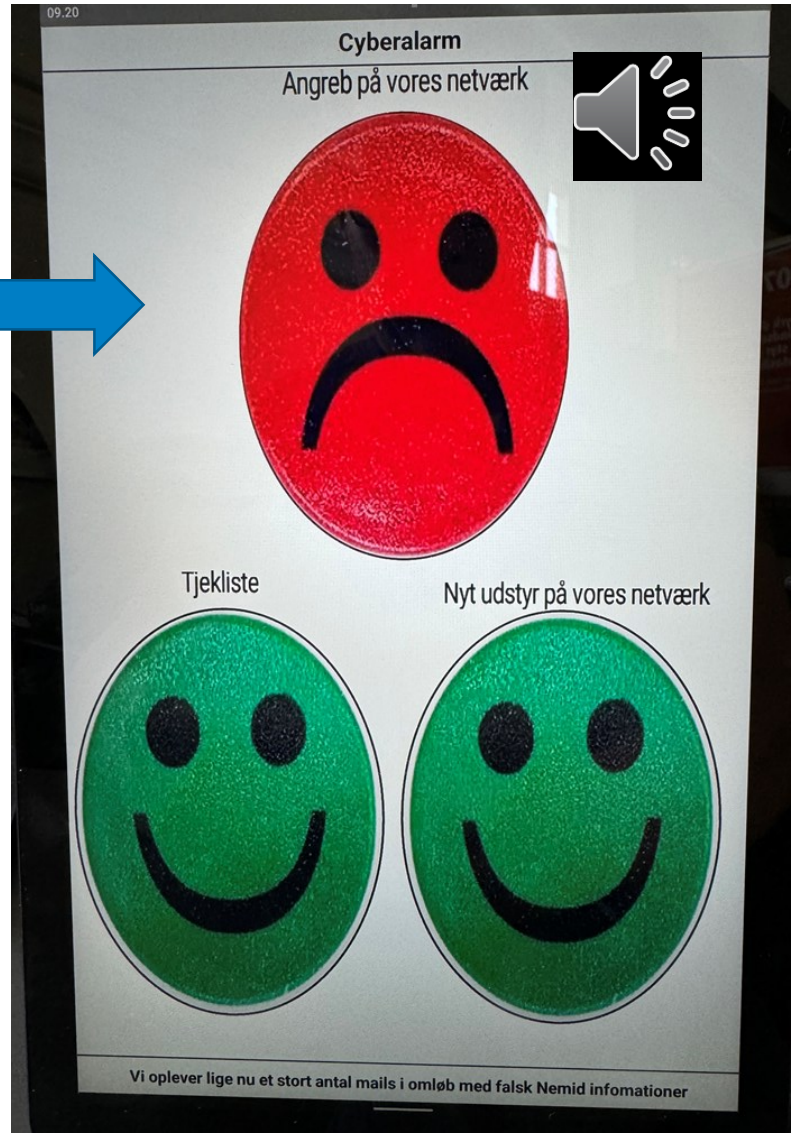
SUNDHEDSDATA-STYRELSEN

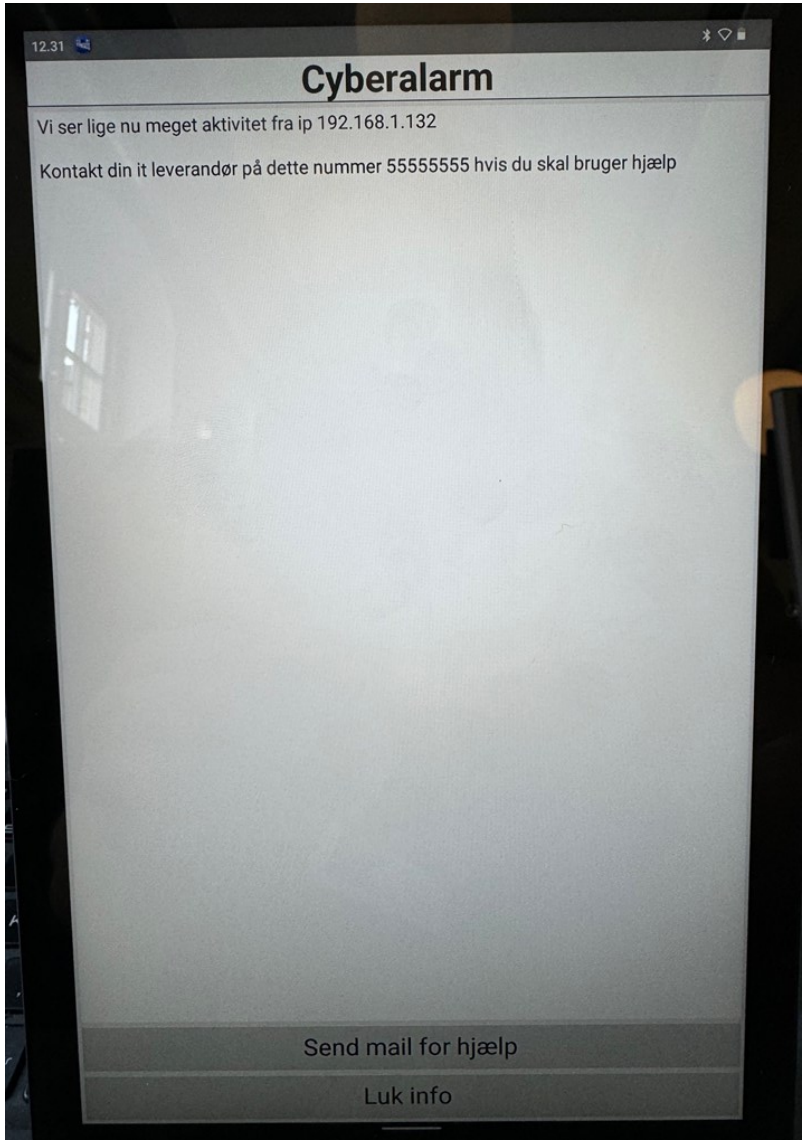
Ned i en boks!



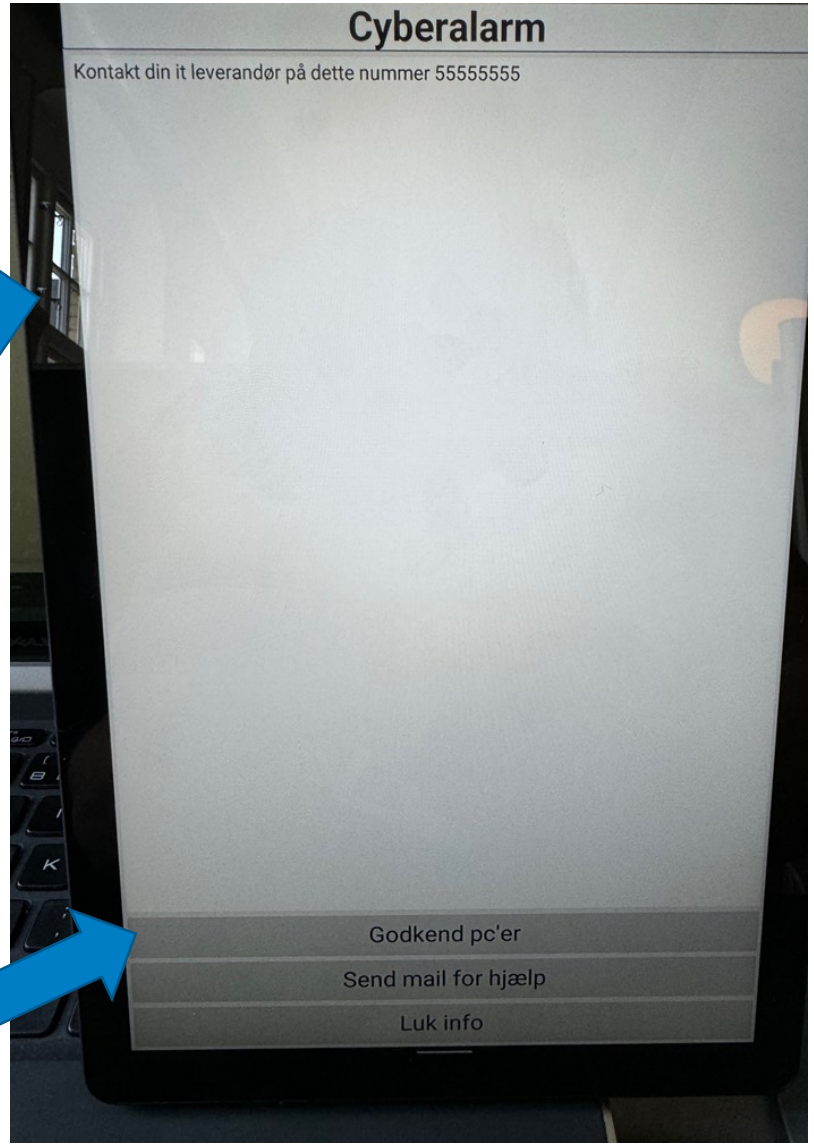


SUNDHEDSDATA-STYRELSEN

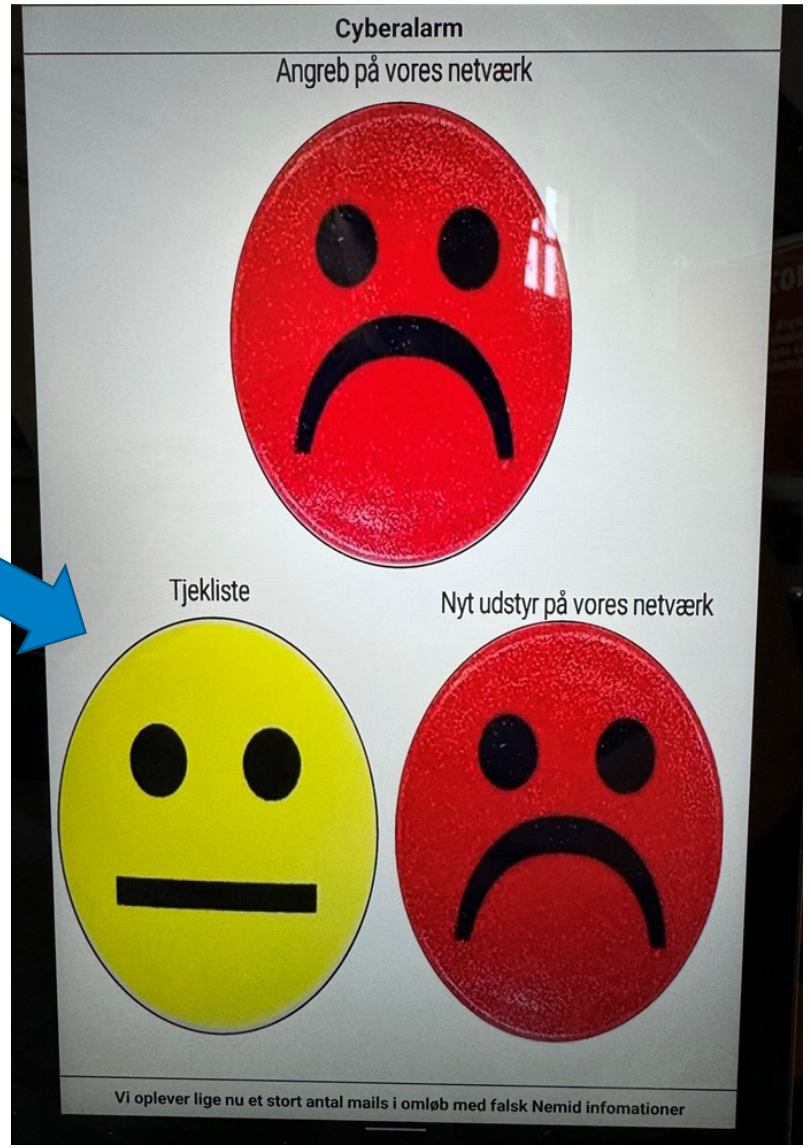




SUNDHEDSDATA-STYRELSEN



SUNDHEDSDATA-STYRELSEN



- 24 awareness spørgsmål om året:
  - Hvornår har du sidst nulstillet klinikkens passwords?
  - Hvornår har du sidst talt med din leverandør og kontrolleret at backupen er gennemført?
- Giver en "temperatur" på cyberrobustheden i klinikken.

Status

- Cyberalarmen skal pilottestes hos en række klinikker i Kalundborg og Korsør-området
- Vi har indgået en aftale med PLO omkring en udvidelse af pilloten og idriftsættelse i 2025
- Pilottesten skal bidrage til at afklare,
  - om lægerne vil anvende boksene,
  - om de kan finde ud af at aflæse interfacet, og
  - om boksene får dem til at føle sig mere trygge eller utrygge?

SUNDHEDSDATA-STYRELSEN

Opsummering og budskaber!

- Giv lægen noget håndgribeligt!
  - også ved meta tiltag som awareness (tjeklisten)
- Kommunikér på en forståelig og nem måde!
  - Det skal være nemt og hurtigt at afkode, hvad man skal gøre!
- Fokusér på også at hjælpe med faktisk sikkerhed!
  - Vejledning er godt, aktion er bedre ☺

"Images created by OpenAI's DALL-E."

Spørgsmål?

Søren Bank Greenfield

SBGR@sundhedsdata.dk

SUNDHEDSDATA-
STYRELSEN

Sundhedsdatastyrelsen
Ørestads Boulevard 5
2300 København S

T: +45 7221 6800
E: kontakt@sundshedsdata.dk
W: sundhedsdata.dk

Kontakt

DCIS Sund

DCISSUND@sundhedsdata.dk

DCISSund information

https://sundhedsdatastyrelsen.dk/informationssikkerhed