

Cyberalarmen – at opdage eller ikke at opdage hackerne!

Ole Fisker, Søren Bank Greenfield

It og digitalisering

Cyber- og informationssikkerhedsafdeling.

Digital Sundhed Danmark





Cyberalarmen – at opdage eller ikke at opdage hackerne!

Kan du finde en hacker?

Håndgribeligt initiativ til den lille klinik, apotek, Fys/ergo, tandlæge...



Bevare tilliden



Når cybertruslerne står for døren, sårbarhederne er "uendelige" og de geopolitiske vinde blæser kraftigere og kraftigere
– hvad gør den lille sundhedsaktør så?

Sundhedssektorens strategi for cyber- og informationssikkerhed 2023- **2027**



Sundhedssektoren samarbejde om cybersikkerhed

https://sundhedsdatastyrelsen.dk/Media/638641645405294664/strategi_cyber_informationssikkerhed_2023_2025.pdf

Internationalt samarbejde



Trusler
Sårbarheder
IOC/IOA & IOB



SundCERT
24/7/365

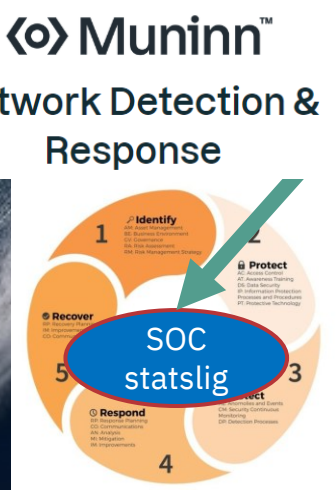
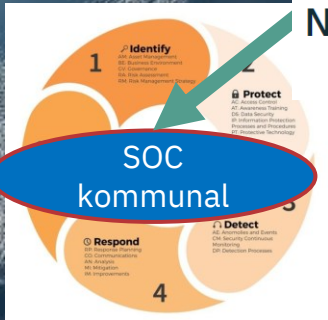
Trusler
Sårbarheder
IOC/IOA & IOB



Nationalt samarbejde



Dagligt operationelt
samarbejde SAC / SOC



"Real time" aktivitet



Cyberalarmen



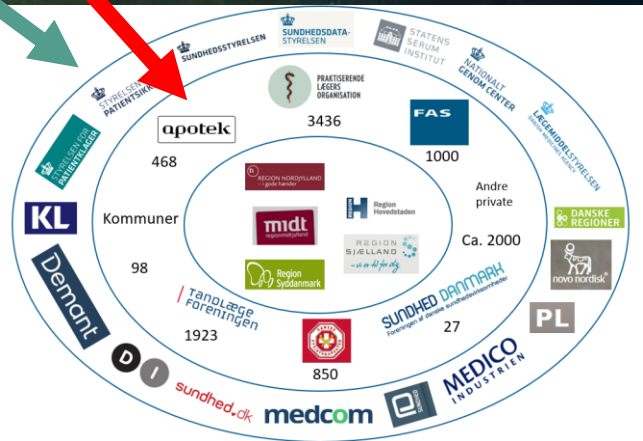
A3 -> A1



E-mail
Varslings
System



Sektor samarbejde



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

Cyberalarmen

Håndgribeligt initiativ til den lille klinik, apotek, Fys/ergo, tandlæge...



EU AI Act: first regulation on artificial intelligence

The use of artificial intelligence in the EU will be regulated by the AI Act, the world's first comprehensive AI law. Find out how it will protect you.

Digital sikkerhed i danske SMV'er, 2024



Digital sikkerhed i danske SMV'er, 2023



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.

Ideen!







Muninn

Notification Details

Cyberalarm

Kommunikations hierarki:

Vi oplever lige nu et stort antal mails i omløb med falsk Nemid infomationer

Nyt udstyr	PC'er med Sårbarheder
	
Checklist	Angreb på vores netværk

Cyberalarm

"Breaking news" fra SundCERT

- Der er en phishing kampagne
- Et af de større systemer er nede

Tablet

Kontakt din it leverandør på dette nummer
55555555

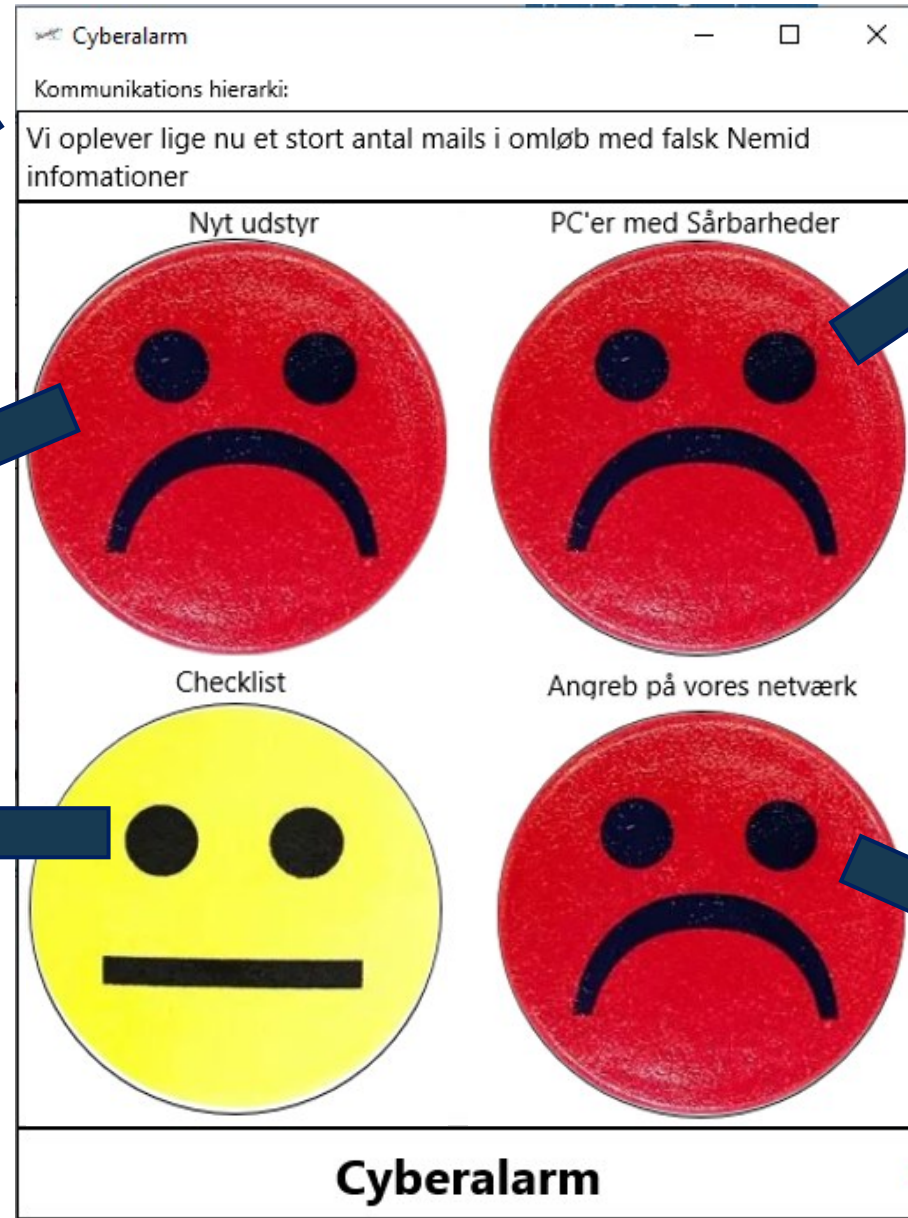
Luk

Godkend Udstyr

Send mail for hjælp

Et "awareness" spørgsmål pr. 14 dage:

- Hvornår har du sidst resat jeres passwords i klinikken?
- Hvornår har du ringet til din leverandør og kontrolleret om backuppen er i orden?



Maskine Navn PC34342 mangler patch .

hvis du skal bruge hjælp til dette ring til
(55555555)

Luk

Send mail for hjælp

Vi ser lige nu meget aktivitet fra ip
192.168.1.132

Kontakt din it leverandør på dette nummer
55555555 hvis du skal bruger hjælp

Luk

Send mail for hjælp

Status for Cyberalarmen

- Cyberalarmen er i pilotdrift hos en række klinikker i DK (**80+2 fys/ergo**).
- Der er gjort klar til yderligere **100** cyberalarmer og vi er i dialog med Tandlæger, speciallæger og apoteker omkring, hvem der skal på i næste runde (**vil du være med? ☺**).
- Vi har indgået aftale om at hjælpe Portugal, Holland og så Estland til at få "Cyberalarmen" på deres "setup".
- Målet er at lave et "toolkit" så andre lande i EU også selv kan gøre det.





Tak for ordet



Følg med på LinkedIn for seneste nyt

Vil I være med??

Sundcert@sundhedsdata.dk eller OLEF@sundhedsdata.dk