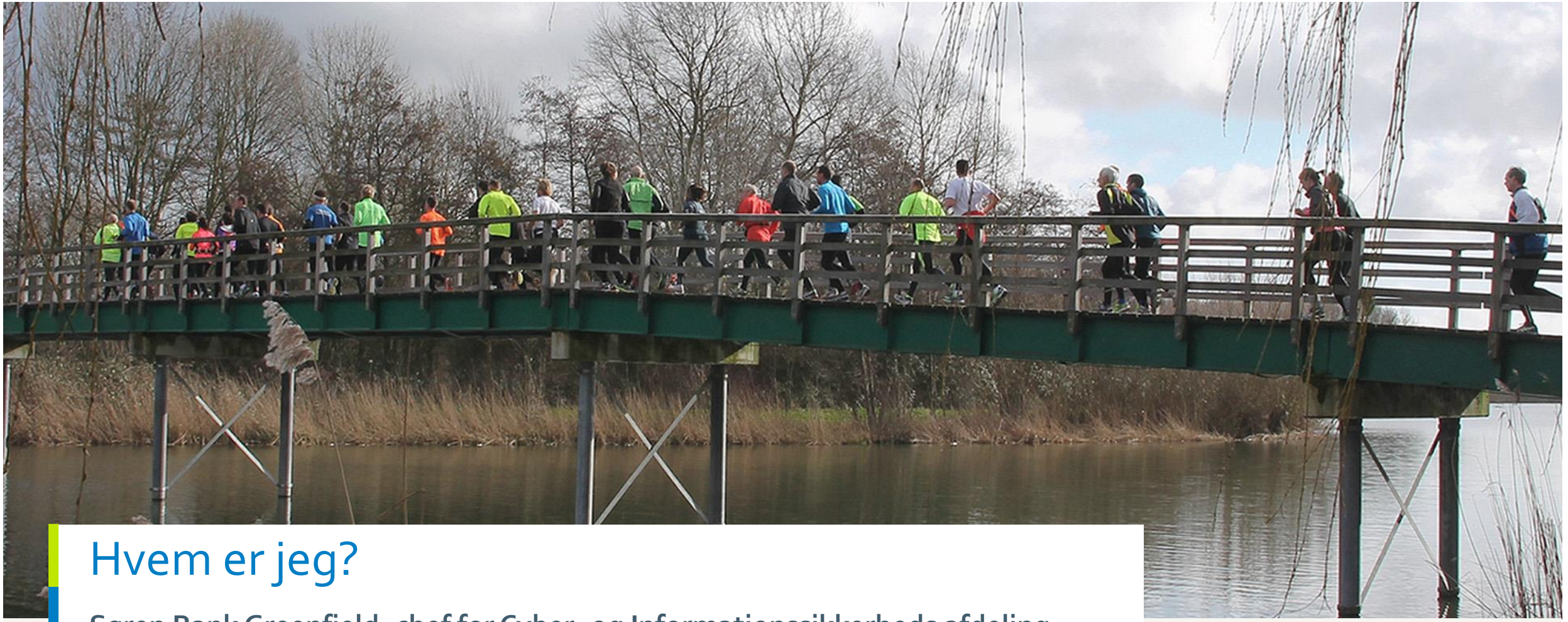
Fremtidens model for bedre cybersikkerhed i det digitale behandlingsparadigme

E sundhedsobservatorium – Session E3 – Oplæg 1

SUNDHEDSDATA-
STYRELSEN



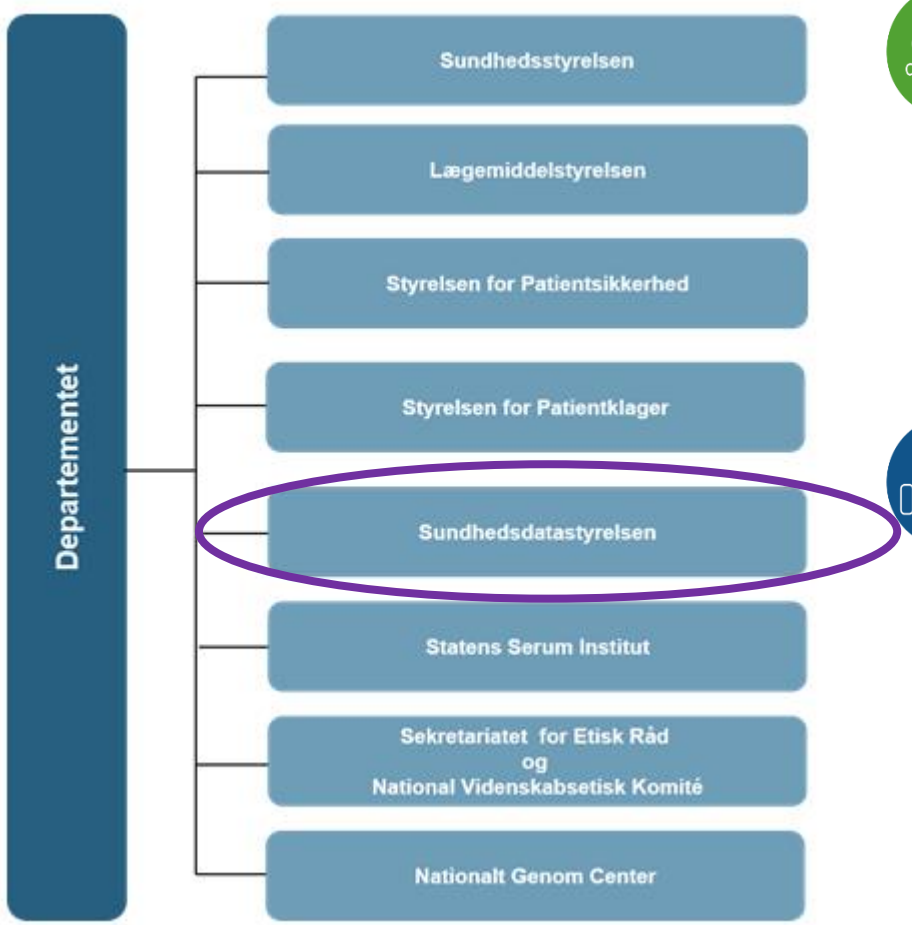
Hvem er jeg?

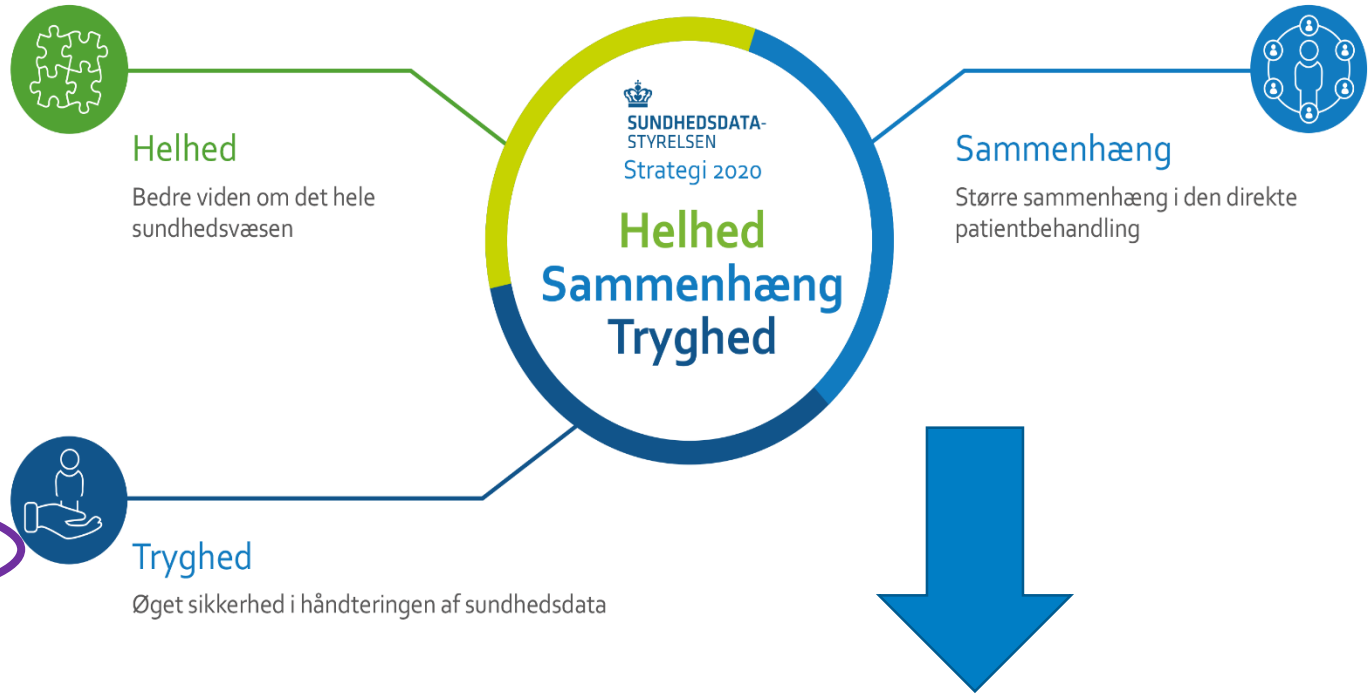
Søren Bank Greenfield, chef for Cyber- og Informationssikkerheds afdeling.

- Faglig baggrund som operationel sikkerhedschef, CISO og med viden indenfor brugervendt infrastruktur, identitetsstyring og cybersikkerhed. Har før været i KBH amt, Glostrup hospital og Regionh (CIMT).

SUNDHEDSDATA-
STYRELSEN

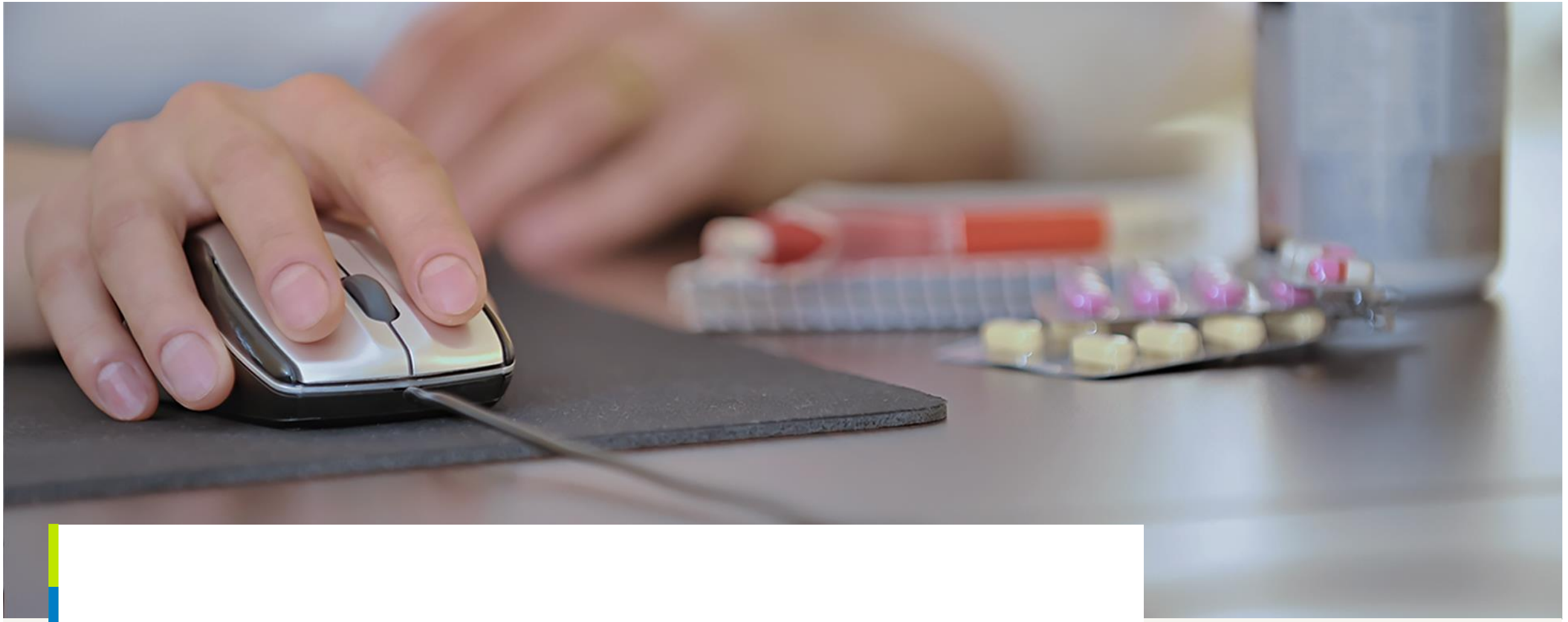
Sundhedsministeriet





Afdelingen har til opgave at facilitere og koordinere den fælles indsat for at **styrke og øge** kapabiliteten og kapaciteten indenfor Cyber- og Informationssikkerhed i Sundhedsdatastyrelsen, Sundhed- og Ældre ministeriet og **på tværs af sundhedsvæsenet**

SUNDHEDSDATA-STYRELSEN



Det digitale behandlingsparadigme

Hvad er det lige? Hvad er nyt i det? Hvad ser vi ind i?

SUNDHEDSDATA-
STYRELSEN

E-sundhedsobservatorium 2021

Dag 1

COVID-19 har åbnet en digital informationsvej mellem primær og sekundærsektor

Kunstig intelligens til billeddiagnostik af brystkræft - hurtigere diagnostik til bedre behandling

Datadeling – if you can't beat them, join them

Kunstig intelligens (AI) på danske hospitaler – Kan AI hjælpe med at mindske uligheden?

To know before you know!

Digitale kompetencer – hvordan rammer man et "moving target"?

COVID-19 – en gamechanger for datadrevet ledelse

VDX under Corona

Kan man anvende videokonsultation i Psykiatrien?

ReMoTe: Fra skepsis til sikker brug af videokonsultation i almen praksis

Dag 2

Er min digitale løsning medicinsk udstyr?

Effekten af apps til patienter – hvad viser studierne i TELEMED databasen?

MinSundhed-appen – når lillesøster bliver stor

"Spørg en læge om Coronavirus" – nem og direkte adgang til læger på sociale medier kan skabe tryghed

Intelligent teknologi skal styrke omsorg og nærvær i ældreplejen

D3: Wearables og PRO

Dine data – Vores Sundhed: Borgeres selvskabte data er en guldgrube for fremtidens patient og sundhedsvæsen

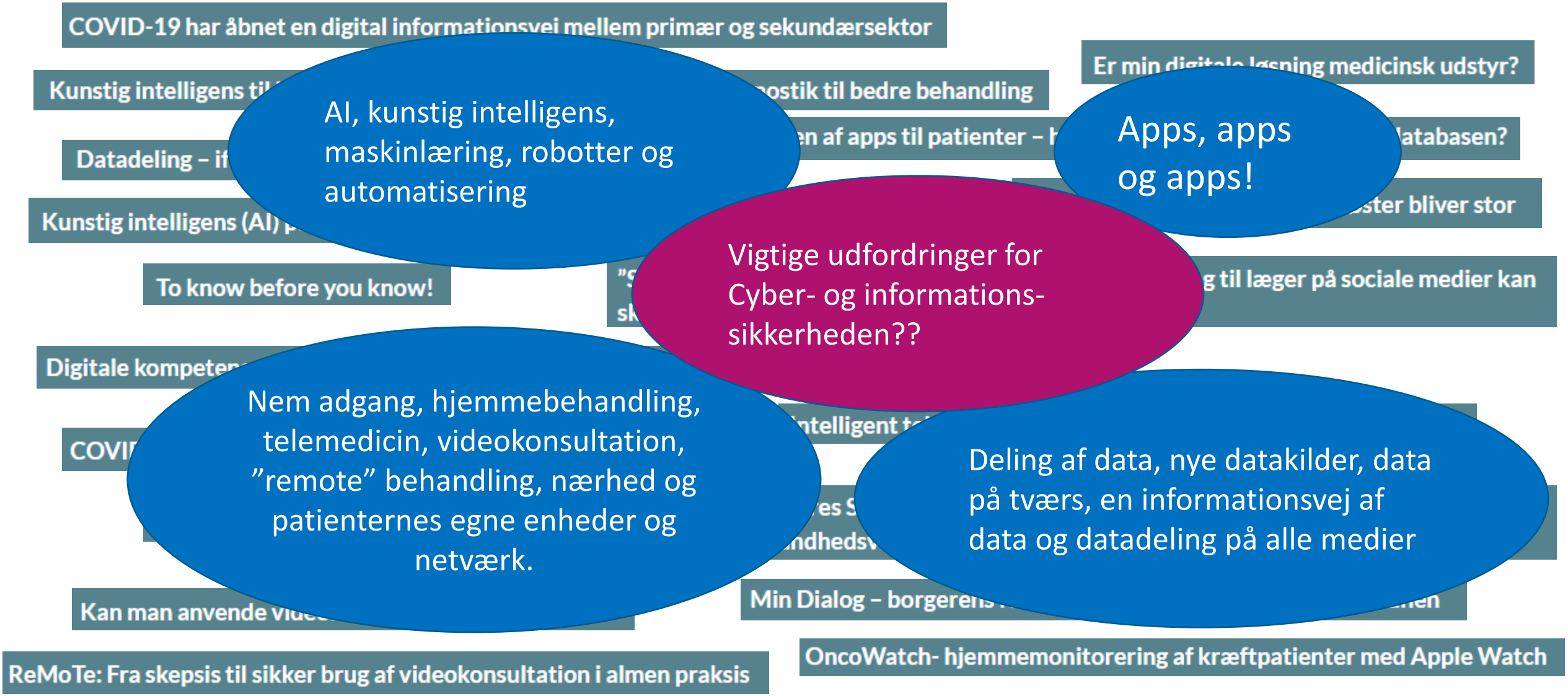
Min Dialog – borgerens foretrukne dialogværktøj med kommunen

OncoWatch- hjemmemonitorering af kræftpatienter med Apple Watch

E-sundhedsobservatorium 2021

Dag 1

Dag 2



SUNDHEDSDATA-STYRELSEN

Nyt paradigme og så Cyber- og informationssikkerheden?

- **Udfordring 2: Vi er endnu mere afhængige af**
  - Dataforbindelser
  - Tech giganters HW
  - Tech giganters software

- **Udfordring 1: Vi bestemmer ikke mere**
  - Enheder og deres opsætning
  - Hjemmenetværket, HW og opsætning

- **Udfordring 3. Vi står overfor cyberkriminelle der**
  - Har udviklet effektive og agile forretningsmodeller
  - Har større omsætning end det 10 største land
  - Har investeret voldsomt i automatisering og AI

- **Udfordring 4: Brugerne er vigtige for forsvaret**
  - Brugerne og deres viden er også vores forsvar

Udfordring 1: Vi er ikke i herre over enheder og netværk

Report: Working from home jeopardizes network security

According to the survey, 77% of employees working from home are accessing corporate systems via insecure "BYOD"—or "bring your own device." Additionally, two-thirds of respondents (66%) report the use of collaborative software such as Zoom and Microsoft Teams, which have been criticized recently for security flaws—in the case of Zoom, this included uninvited users "Zoom bombing" graphic images, and the leaking of private material.

The habits of work-from-home employees may arise from the different attitudes arou workers have while at the office versus at home. It could also result from the increase facing remote workers who, during COVID-19, are dealing with a range of other respo like home-schooling children or taking care of parents—and the study found that wor were particularly lax with security measures. Nearly all respondents, 93%, report reus passwords for application logins and for devices. Nearly a third (29%) have given acc applications or devices to family members. And more tha third (37%) save passwo browsers of their corporate devices.

Philips Hue White LED pære - E27 - 2-PACK - BT

Udfordring 2: Vi er afhængige af andre sektorer!

Bil og enheder indeholder samlet 23 simkort!

Udfordring 3: Vores modstandere - Hvordan ser en hacker ud?

Udfordring 3: Vores modstandere - CaaS

Feature

Cybercrime as a service: a very modern business

Derek Manky

Show more

+ Add to Mendeley Share Cite

https://doi.org/10.1016/S1361-3723(13)70053-8

Cybercrime has continued to evolve and today it exists in a
has itself become big business, and as with all emerging ma
vendors that serve the cybercrime market have expanded th
range of activities.

Cybercrime has evolved into a complex, highly organised h
leaders, engineers, infantry, and hired money mules and a
entered the lexicon of cybercrime – Crime as a Service (Caa
FortiGuard Labs examines how the cybercrime world has n
business.

https://www.sciencedirect.com/science/article/abs/pii/S1361372313700538

Yet for 17% of those, paying the ransom did not guarantee the return of stolen data. However, as public awareness of potential cyberthreats grows there is reason for optimism in the fight against ransomware.

https://www.kaspersky.com/about/press-releases/2021_over-half-of-ransomware-victims-pay-the-ransom-but-only-a-quarter-see-their-full-data-returned

Udfordring 3: AI hos modstanderne

June 9, 2021

This is how fast a password leaked on the web will be tested out by hackers

"About half of of the accounts were accessed within 12 hours of us actually seeding the sites. 20% are accessed within an hour and 40% are accessed within six hours. That really shows you how quickly a compromised account is exploited," Crane Hassold, senior director of threat research at Agari, told ZDNet.

Cybersecurity researchers planted phoney passwords on the web. They found that attackers were extremely quick to test if usernames and passwords worked.

READ FULL STORY

https://www.zdnet.com/article/this-is-how-fast-a-password-leaked-on-the-web-will-be-tested-out-by-hackers/

Cybercriminals scanned for vulnerable Microsoft Exchange servers within five minutes of news going public

Research suggests the cheap hire of cloud services has allowed cyberattackers to quickly pick out targets.

By Charlie Osborne for Zero Day | May 19, 2021 -- 10:00 GMT (11:00 BST) | Topic: Security

Cybercriminals began searching the web for vulnerable Exchange Servers within five minutes of Microsoft's security advisory going public, researchers say.

According to a review of threat data from enterprise companies gathered between January and March this year, compiled in Palo Alto Networks' 2021 Cortex Xpanse Attack Surface threat report and published on Wednesday, threat actors were quick-off-the-mark to scan for servers ripe to exploit.

When critical vulnerabilities in widely adopted software are made public, this may trigger a race between attackers and IT admins: one to find suitable targets -- especially when proof-of-concept (PoC) code is available or a bug is trivial to exploit -- and IT staff to perform risk assessments and implement necessary patches.

The report says that in particular, zero-day vulnerabilities can prompt attacker scans within as little as 15 minutes following public disclosure.

SECURITY

LastPass password manager fine-tunes its multi-factor authentication options

Cyber security 101: Protect your privacy from hackers, spies, and the government

The best antivirus software and apps

The best VPNs for business and home use

The best security keys for two-factor authentication

Colonial Pipeline attack: What happened (ZDNet YouTube)

MORE FROM CHARLIE OSBORNE

Security
Bizarro banking Trojan surges across Europe

https://www.zdnet.com/article/cybercriminals-scanned-for-vulnerable-microsoft-exchange-servers-within-five-minutes-of-news-going-public

Udfordring 4: Brugerne og deres viden er også vores forsvar

citibank.com

citibank.com

The "a" in the later url is a cyrillic alphabet.

An average internet user can easily fall for this. Be careful for every mail requiring you to click on a link.

Please Stay Alert

Fremtidens model for bedre cybersikkerhed i det digitale behandlingsparadigme – kræver derfor

- at vi samarbejder, både i sektoren men også på tværs af sektorerne!
- at sikkerheden flytter med hele vejen ud til enheder, henover netværk - Zero trust hele vejen.
- at ALLE! Skal kunne agere i forhold til cybersikkerhed.
- at vi kan opdage, analysere og reagere lynhurtigt – AI og automatisering er nøglen.

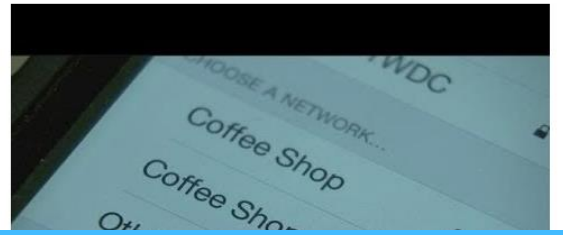
Ekstra slides hvis Ole er "go" ☺

SUNDHEDSDATA-
STYRELSEN

Offentlige Wifi set fra en hacker

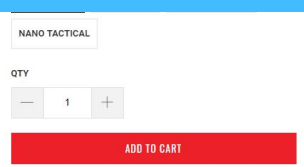
Liste ☺

Hacking



Sluk for din wifi!

Brug kabel eller indbygget modem i stedet ☺!



https://e-channelnews.com/top-5-most-dangerous-public-wifi-attacks/

Hackernes værktøjer – Wi-fi Pineapple

NEXT

SALE

WIFI PINEAPPLE

$199.99

The leading rogue access point and WiFi pentest toolkit for close access operations. Passive and active attacks analyze vulnerable and misconfigured devices.

The WiFi Pineapple® NANO and TETRA are the 6th generation pentest platforms from Hak5. Thoughtfully developed for mobile and persistent deployments, they build on over 10 years of WiFi attack expertise.

WIFI PINEAPPLE

TETRA BASIC | NANO BASIC | TETRA TACTICAL | NANO TACTICAL

QTY

— 1 +

ADD TO CART

NEXT

SALE

WIFI PINEAPPLE

$239.99 ~~$299.99~~

You Save 20% ($60.00)

The leading rogue access point and WiFi pentest toolkit for close access operations. Passive and active attacks analyze vulnerable and misconfigured devices.

The WiFi Pineapple® NANO and TETRA are the 6th generation pentest platforms from Hak5. Thoughtfully developed for mobile and persistent deployments, they build on over 10 years of WiFi attack expertise.

WIFI PINEAPPLE

TETRA BASIC | NANO BASIC | TETRA TACTICAL | NANO TACTICAL

QTY

— 1 +

ADD TO CART

https://shop.hak5.org/collections/sale/products/wifi-pineapple

Bruges til at lave avancerede ”man-in-the-middle” angreb ved at efterligne foretrukne netværk. Man lades som om man er brugerens hjemmenetværk og så skifter mobil/ipad/pc’er automatisk over til denne dims.
Kan målrettes så det ikke er alle der påvirkes.

https://www.youtube.com/watch?v=CV39QzFpJx4

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 på Twitter
@dcissund

DCISSund information
www.sundhedsdata.dk/informationssikkerhed