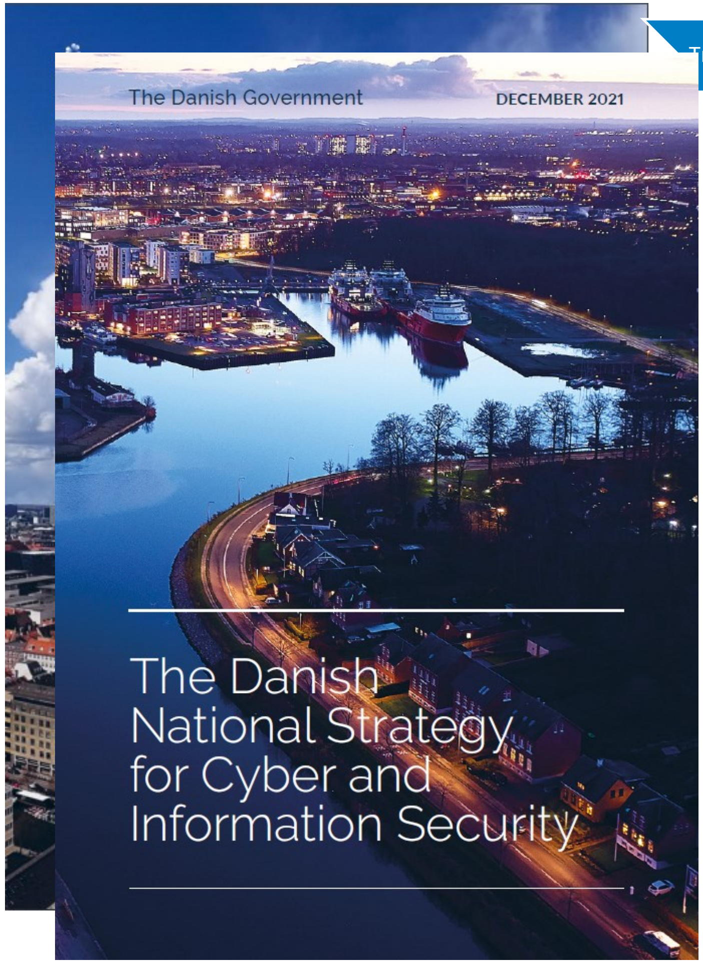
What’s new in policy?

Danish Health National Cybersecurity Strategy (NCSS)

DANISH HEALTH
DATA AUTHORITY

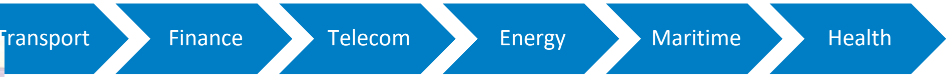
Danish Cyber Security Strategies

The cross-sectoral national strategy 2018-2021 → 2022-2024

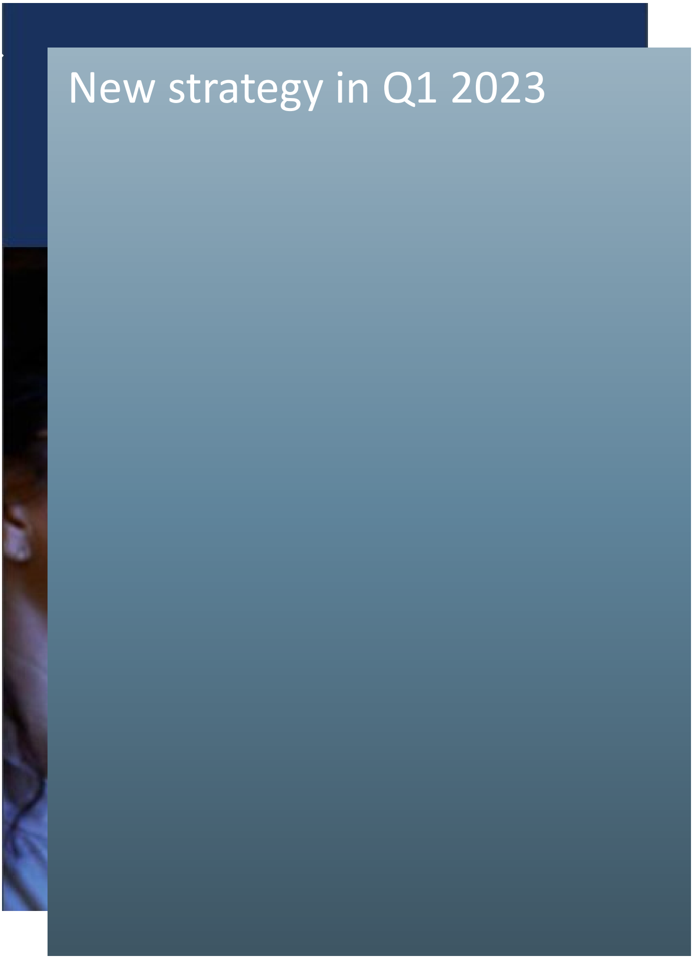

The Danish Government

DECEMBER 2021

The Danish National Strategy for Cyber and Information Security



The health sector strategy 2019-2022 → 2023-2025


New strategy in Q1 2023

An ambitious effort targeting government and vital societal functions.

The new national strategy will

- Cover more sectors
- Cover more critical systems
- Strengthen technical minimum requirements.

The health sector strategy focus

- Operational capacities
- Collaboration across the sector
- Stricter cyber security requirements.

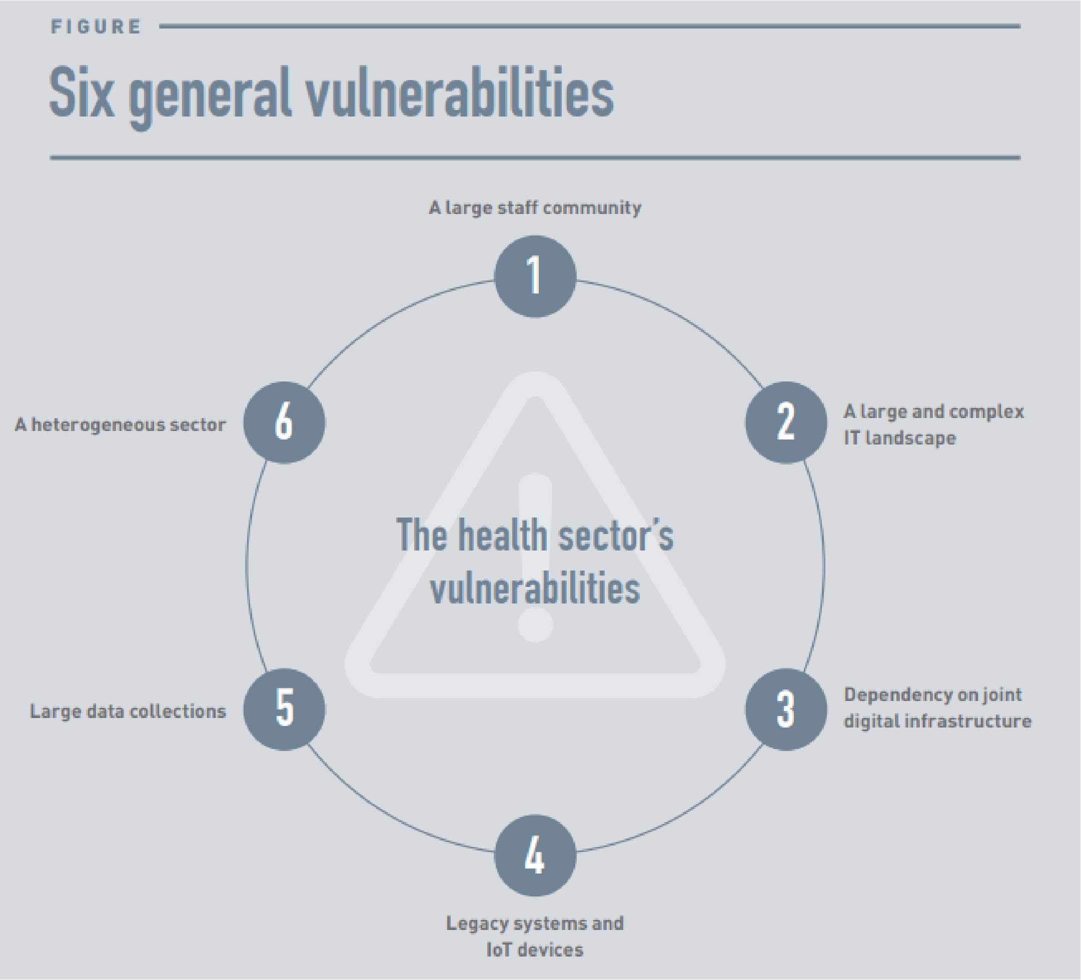
The new health sector strategy 2023-2025

- Continue the good work
- More focus on the smaller actors
- Identify and utilise potential in the best possible way**.**

https://en.digst.dk/strategy/the-danish-national-strategy-for-cyber-and-information-security/

https://sundhedsdatastyrelsen.dk/da/strategier-og-projekter/cyberstrategi

Current strategy



FIGURE

Six general vulnerabilities

The health sector's vulnerabilities

1 A large staff community

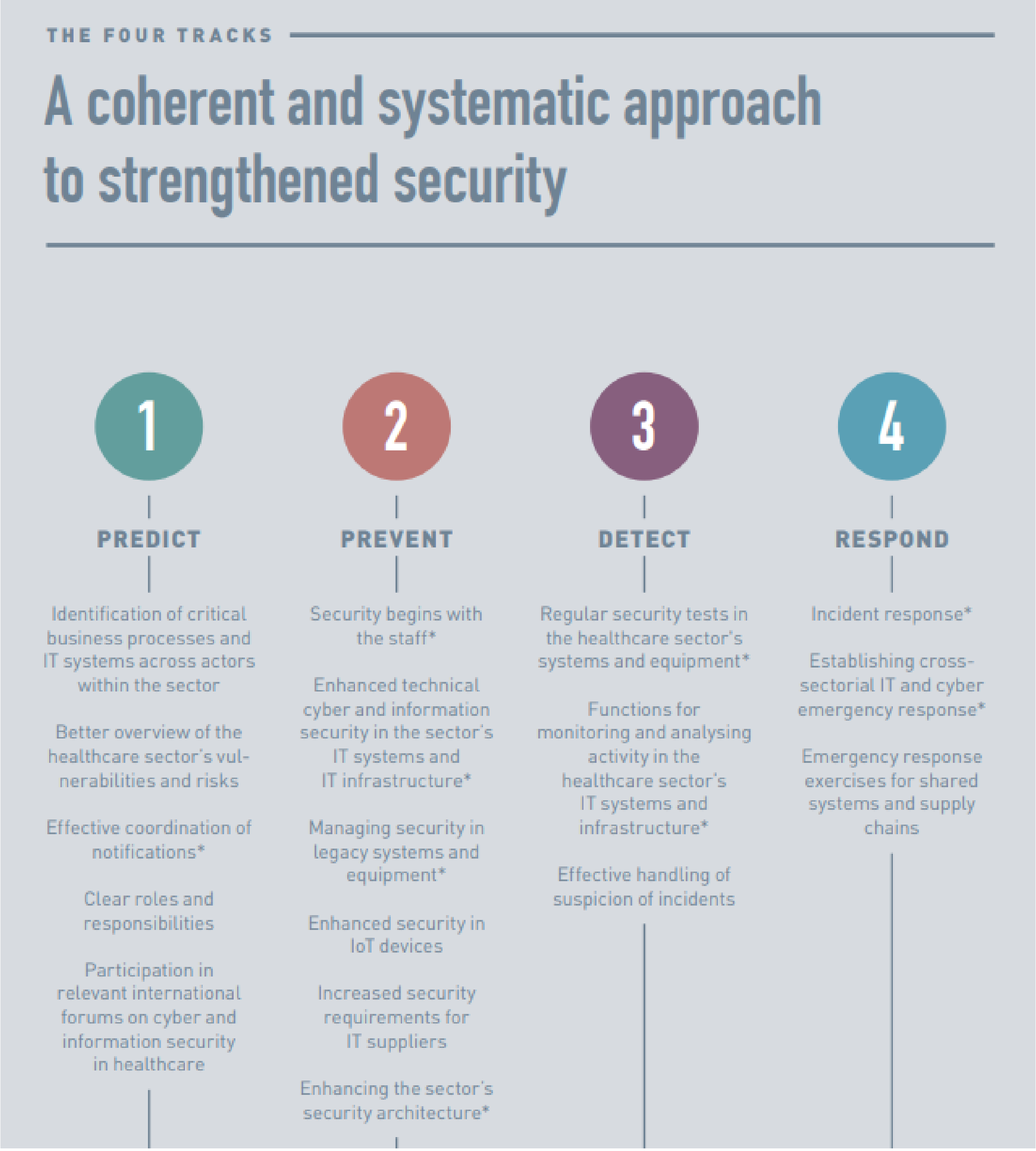
2 A large and complex IT landscape

3 Dependency on joint digital infrastructure

4 Legacy systems and IoT devices

5 Large data collections

6 A heterogeneous sector



THE FOUR TRACKS

A coherent and systematic approach to strengthened security

1 PREDICT

- Identification of critical business processes and IT systems across actors within the sector
- Better overview of the healthcare sector's vulnerabilities and risks
- Effective coordination of notifications*
- Clear roles and responsibilities
- Participation in relevant international forums on cyber and information security in healthcare

2 PREVENT

- Security begins with the staff*
- Enhanced technical cyber and information security in the sector's IT systems and IT infrastructure*
- Managing security in legacy systems and equipment*
- Enhanced security in IoT devices
- Increased security requirements for IT suppliers
- Enhancing the sector's security architecture*

3 DETECT

- Regular security tests in the healthcare sector's systems and equipment*
- Functions for monitoring and analysing activity in the healthcare sector's IT systems and infrastructure*
- Effective handling of suspicion of incidents

4 RESPOND

- Incident response*
- Establishing cross-sectorial IT and cyber emergency response*
- Emergency response exercises for shared systems and supply chains

New strategy – keep in focus

- Operational collaboration, emergency preparedness and exercising it
- Cybersecurity demands for the suppliers
- Keep expanding the technical tools to detect and predict
- Quick and targeted warnings and operational and usable guidelines
- Collaboration between the operators in the sector and cross sectors
- Keep the riskbased approach!

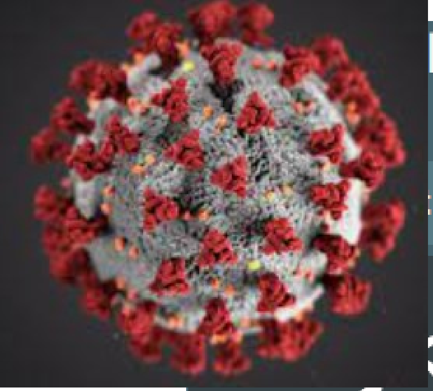
New strategy – New focus areas

- Cybersecurity for SMWs
- Cybersecurity at home, near or inside the patients
- Even more collaboration between the operators in the sector and cross sectors
- Mapping of the important systems in the sector, their suppliers and their suppliers and what open source products they use
- Vulnerability scanning and management
- Education of both healthcare- and cybersecurity-professionals in the sector

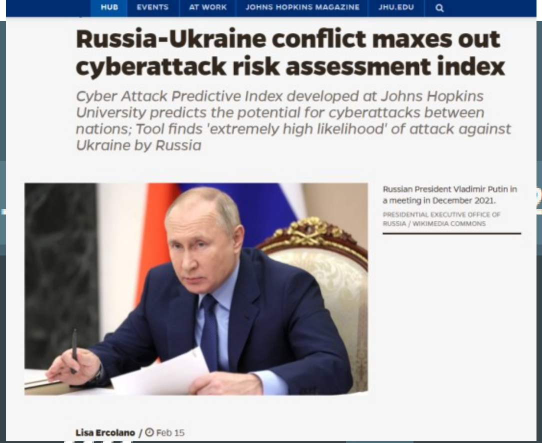
Above all else – It has to be dynamic and react to change!

What shall a cybersecyrity policy cope with in 2022??

DANISH HEALTH
DATA AUTHORITY



hændelser i sundhedssektoren



HUB EVENTS AT WORK JOHNS HOPKINS MAGAZINE JHU.EDU

Russia-Ukraine conflict maxes out cyberattack risk assessment index

Cyber Attack Predictive Index developed at Johns Hopkins University predicts the potential for cyberattacks between nations; Tool finds 'extremely high likelihood' of attack against Ukraine by Russia

Russian President Vladimir Putin in a meeting in December 2021.

PRESIDENTIAL EXECUTIVE OFFICE OF RUSSIA / WIKIMEDIA COMMONS

Lisa Ercolano / Feb 15

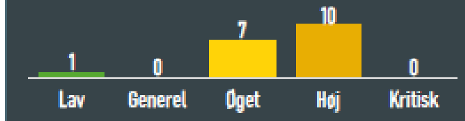
tal 2021

Generel

Udvalgte varsler

- Kritisk sårbarhed i FortiWeb OS
- Aktiv udnyttelse af ProxyShell sårbarheder
- Sårbarheder i Atlassain Confluence
- Sårbarheder i Palo Alto produkter

Antal udsendte varsler



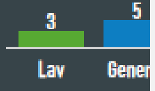
4. Kvartal 2021

Øget

Udvalgte varsler

- Kritisk sårbarhed i Apache Log4j kodebibliotek
- Citrix ADC, Citrix Gateway og Citrix SD-WAN WANOP
- Zero-day i Windows installer (MSI)
- Multiple Vulnerabilities in Apache HTTP Server Affecting Cisco Products

Antal udsendte varsler



Apache LOG4J ™

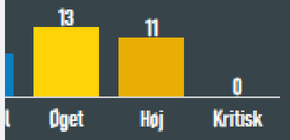
1.

Øget

Udvalgte varsler

- Destruktive cyberangreb observeret mod ukrainske organisationer
- Zero-day fix til apple enheder
- Zero-day i Google Chrome browser
- Øget fokus på kritisk infrastruktur
- 2 Zero-days i Mozilla Firefox
- Sårbarhed i Infusionspumper

Antal udsendte varsler



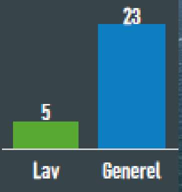
2. Kvartal 2022

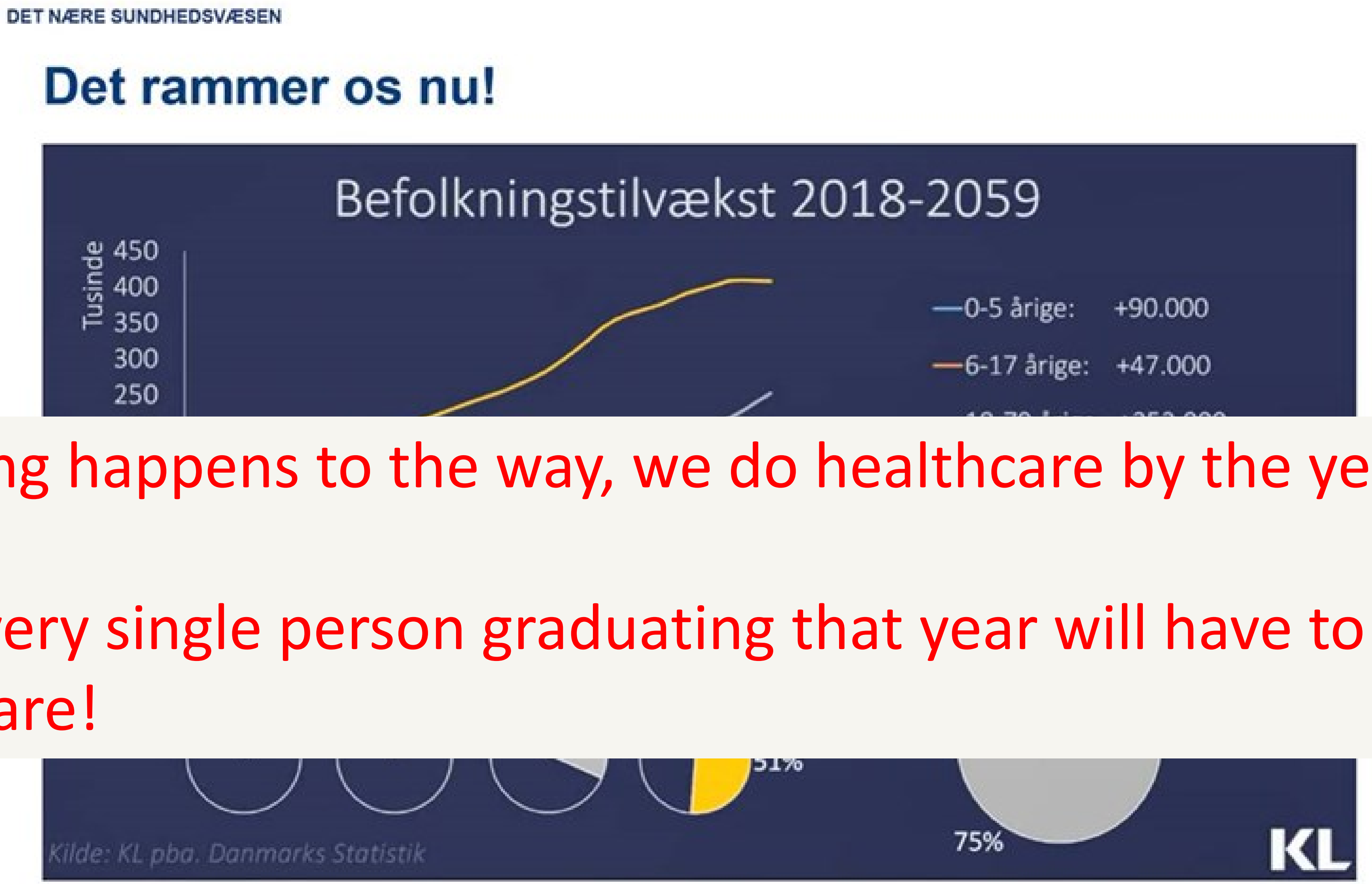
Generel

Udvalgte varsler

- Kritiske sårbarheder i VMware
- Kritisk opdatering til Zyxel firewlls og VPN
- TLSstorm sårbarhed i Avaya og Aruba
- Hackere udnytter kritisk fejl i Zyxel firewalls og VPN'er
- Alvorlige sårbarheder i SonicWall SSLVPN SMA 1000-serien

Antal udsendte varsler





DET NÆRE SUNDHEDSVÆSEN

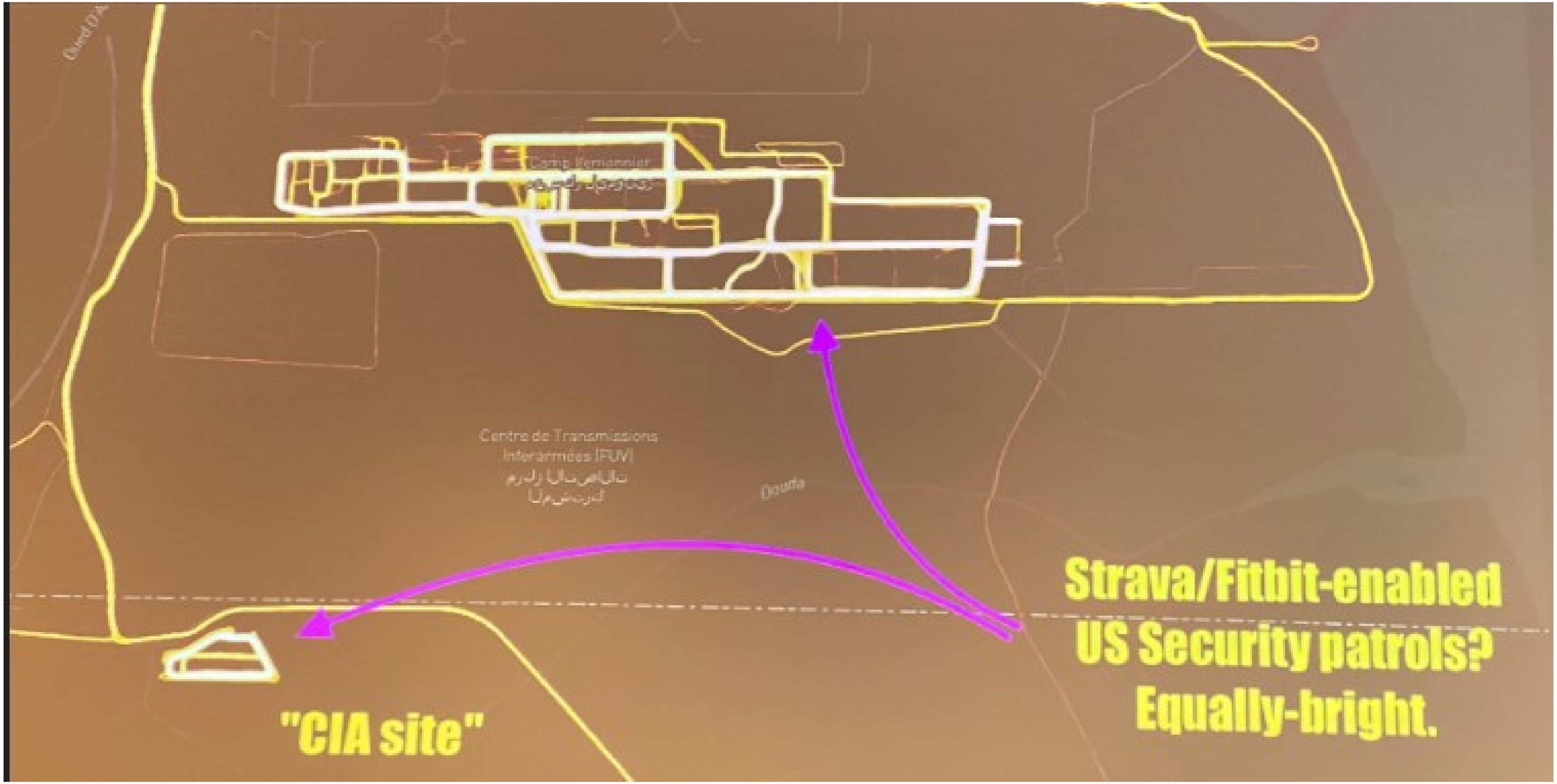
Det rammer os nu!

Kilde: KL pba. Danmarks Statistik

If nothing happens to the way, we do healthcare by the year 2030

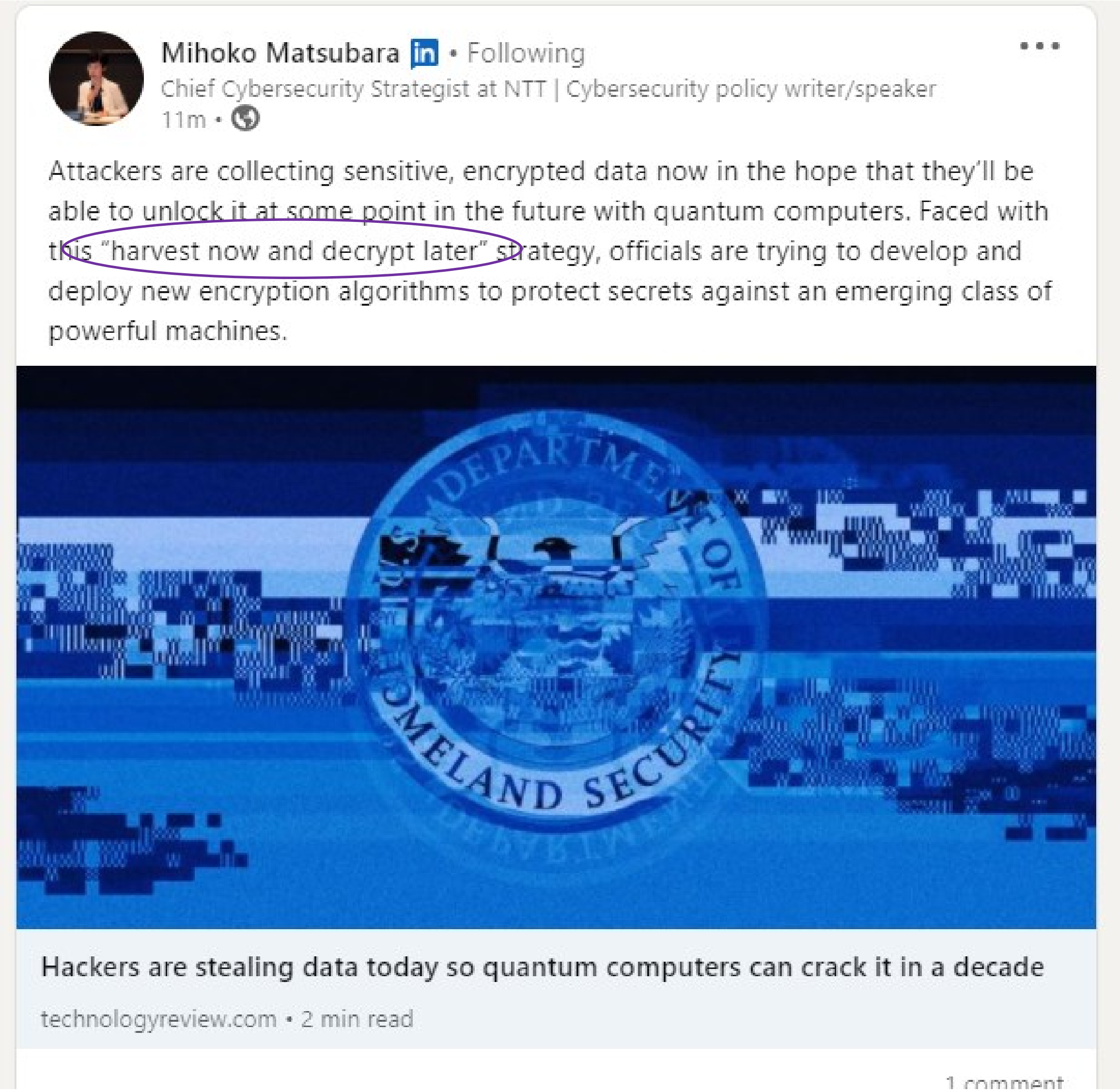
Then every single person graduating that year will have to work in healthcare!

http://2019.e-sundhedsobservatoriet.dk/program/



Strava/Fitbit-enabled US Security patrols? Equally-bright.

"CIA site"



Mihoko Matsubara in • Following

Chief Cybersecurity Strategist at NTT | Cybersecurity policy writer/speaker

11m •

Attackers are collecting sensitive, encrypted data now in the hope that they'll be able to unlock it at some point in the future with quantum computers. Faced with this "harvest now and decrypt later" strategy, officials are trying to develop and deploy new encryption algorithms to protect secrets against an emerging class of powerful machines.

Hackers are stealing data today so quantum computers can crack it in a decade

technologyreview.com • 2 min read

1 comment

https://www.technologyreview.com/2021/11/03/1039171/hackers-quantum-computers-us-homeland-security-cryptography/

Paradigmeshift

You need a policy that is also resilient to change and keeps it viability also when facing

- Outside forces and megatrends
- Hackers at AI speed
- Data explosion
- Encryptions and quantum
- Interconnection, reliability and distribution

Søren Bank Greenfield

SBGR@sundhedsdata.dk

DANISH HEALTH
DATA AUTHORITY

The Danish Health Data Authority
Ørestads Boulevard 5
DK-2300 Copenhagen S

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

Contact

DCIS SUND

DCISSUND@sundhedsdata.dk

DCISSund on Twitter
@dcissund

DCISSund information and news
www.sundhedsdata.dk/informationssikkerhed