Resumé:

Arbejdet med informations- og cybersikkerhed har ikke tidligere befundet sig i et mere komplekst trusselslandskab end nu på bagkant af Corona og med krig i Europa. I Europa er Danmark et af de mest digitaliserede lande, hvilket er forbundet med mange muligheder, men hvordan navigerer vi i de stadigt stigende udfordringer i fremtidens digitale univers med vores nuværende viden fra Corona og situationen i Ukraine?

Blandt fremtidens udfordringer er de til stadighed større og større krav til det agile udviklingsparadigme, hvor automatiserede funktioner, stigende forretningskrav og brugen AI er med til at øge kompleksiteten i det digitale univers.

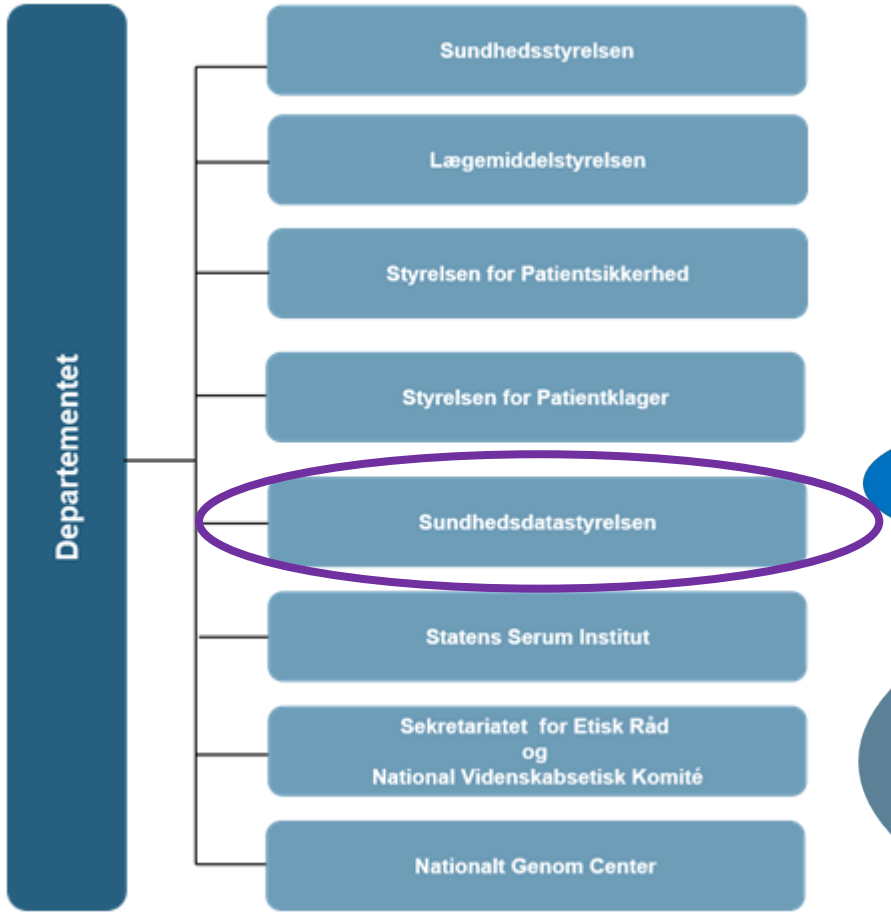
Hvordan sikrer vi borgerens behandling og datasikkerhed i en fremtid, hvor sektorens risikoscenarie udfordres, prioriteringer af sikkerheden påvirkes, og beslutninger skal træffes?

Er sundhedssektoren klar til krig i cyberspace?

Søren Bank Greenfield, chef for Cyber- og Informationssikkerheds afdeling

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, **Sundhedsministeriet** og **på tværs af sundhedsvæsenet.**

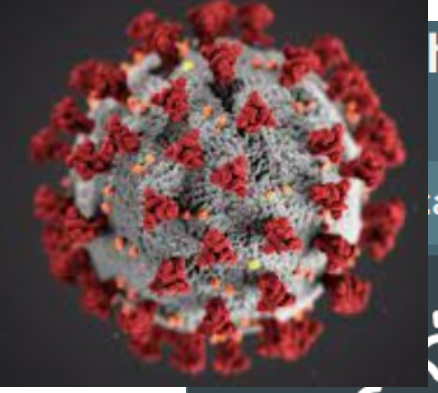
Cyber- og informationssikkerhedsafdeling (CIA)

SUNDHEDSDATA-STYRELSEN

SUNDHEDSDATA-STYRELSEN

Fra Covid-19 til krig!

SUNDHEDSDATA-
STYRELSEN



hændelser i sundhedssektoren

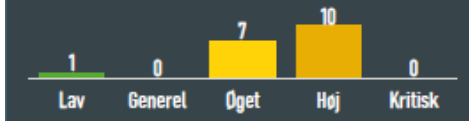
al 2021

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



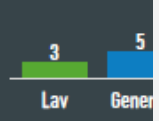
4. Kvartal 2021

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



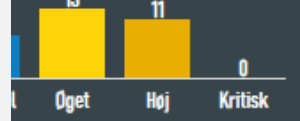
1.

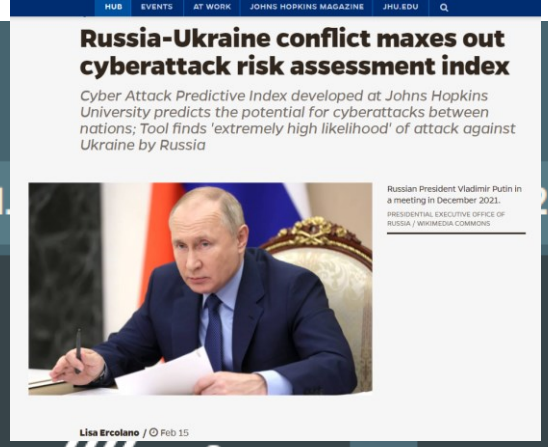
Øget

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





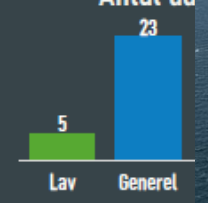
2. Kvartal 2022

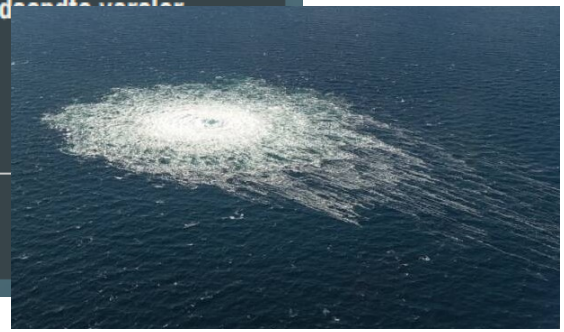
Generel

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 ud





SUNDHEDSDATA-STYRELSEN

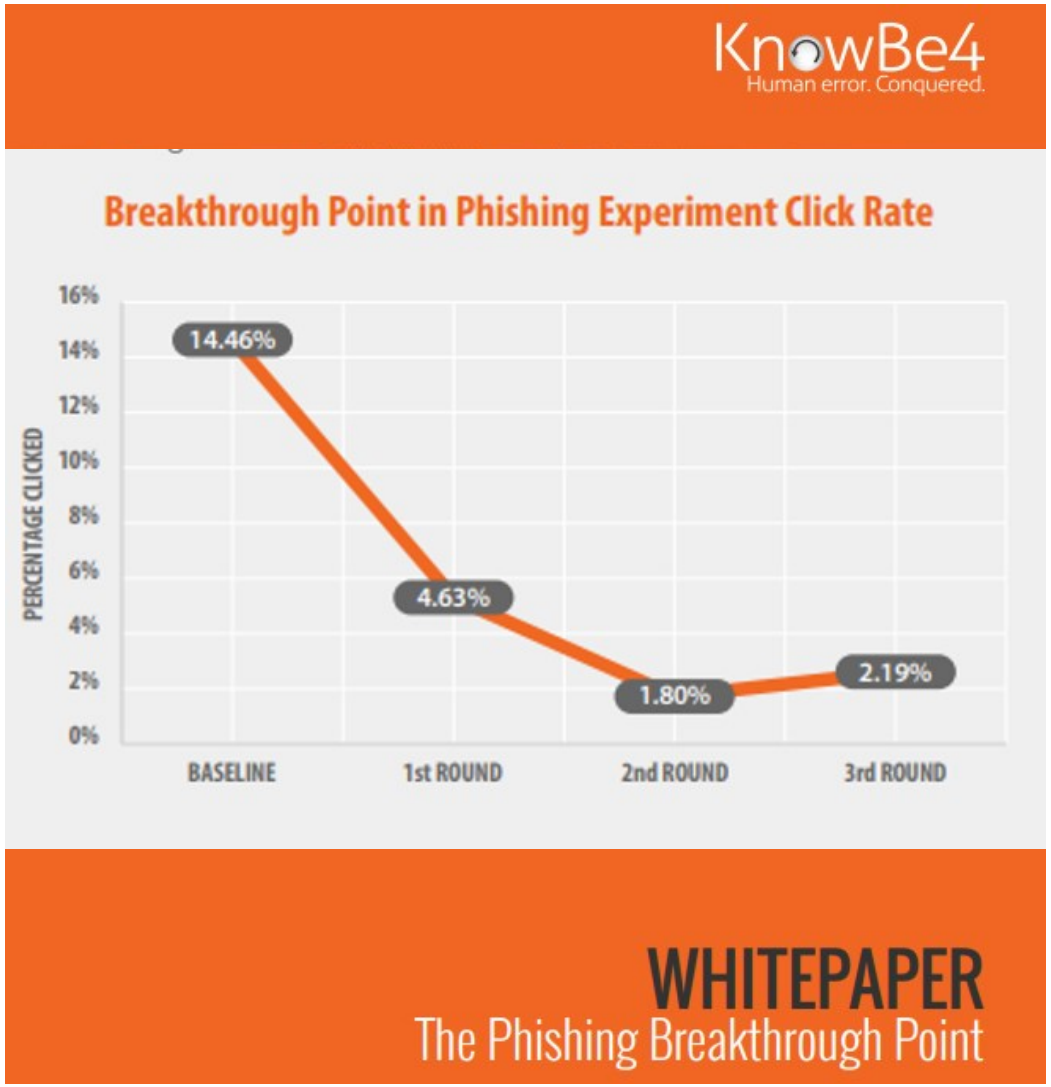
Cyberdomænet og fremtiden?

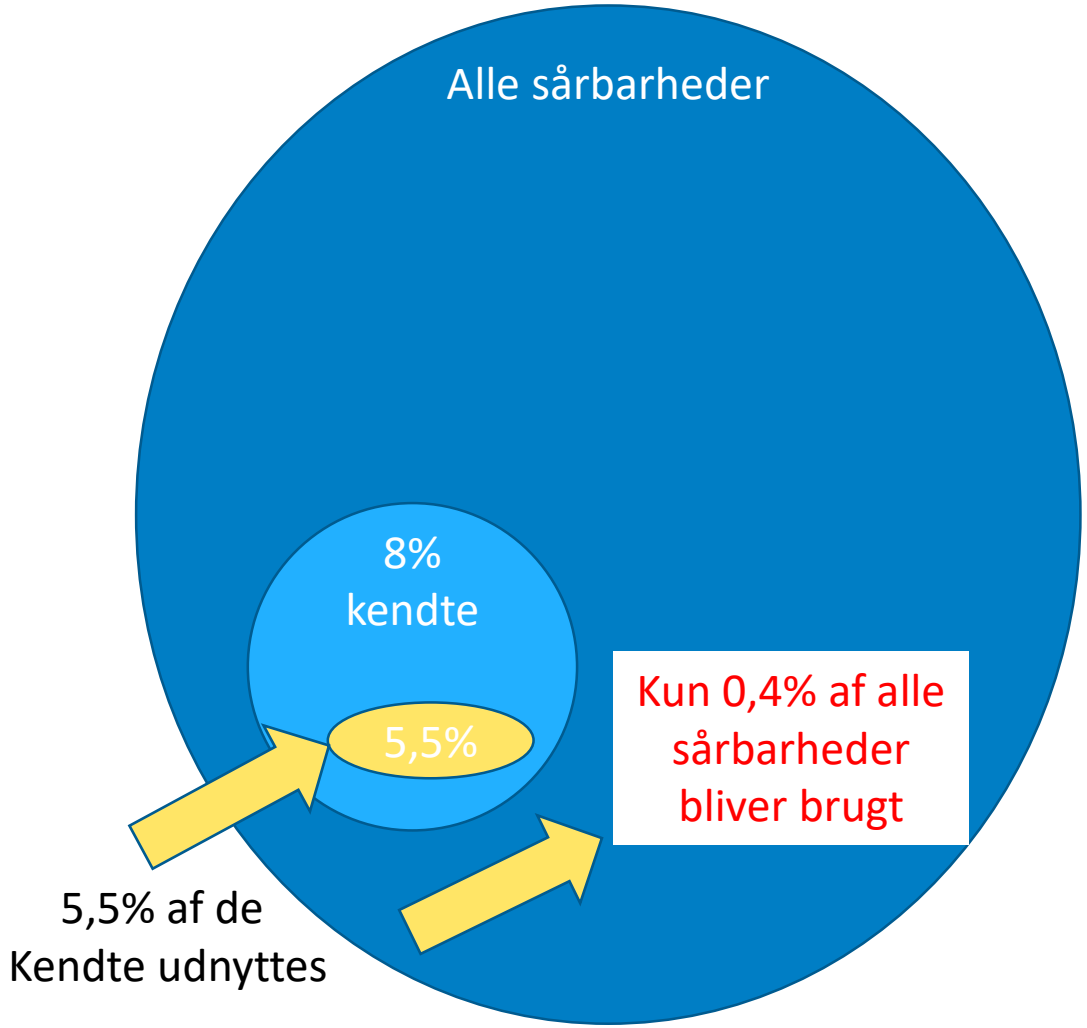
SUNDHEDSDATA-
STYRELSEN

Deepfakes

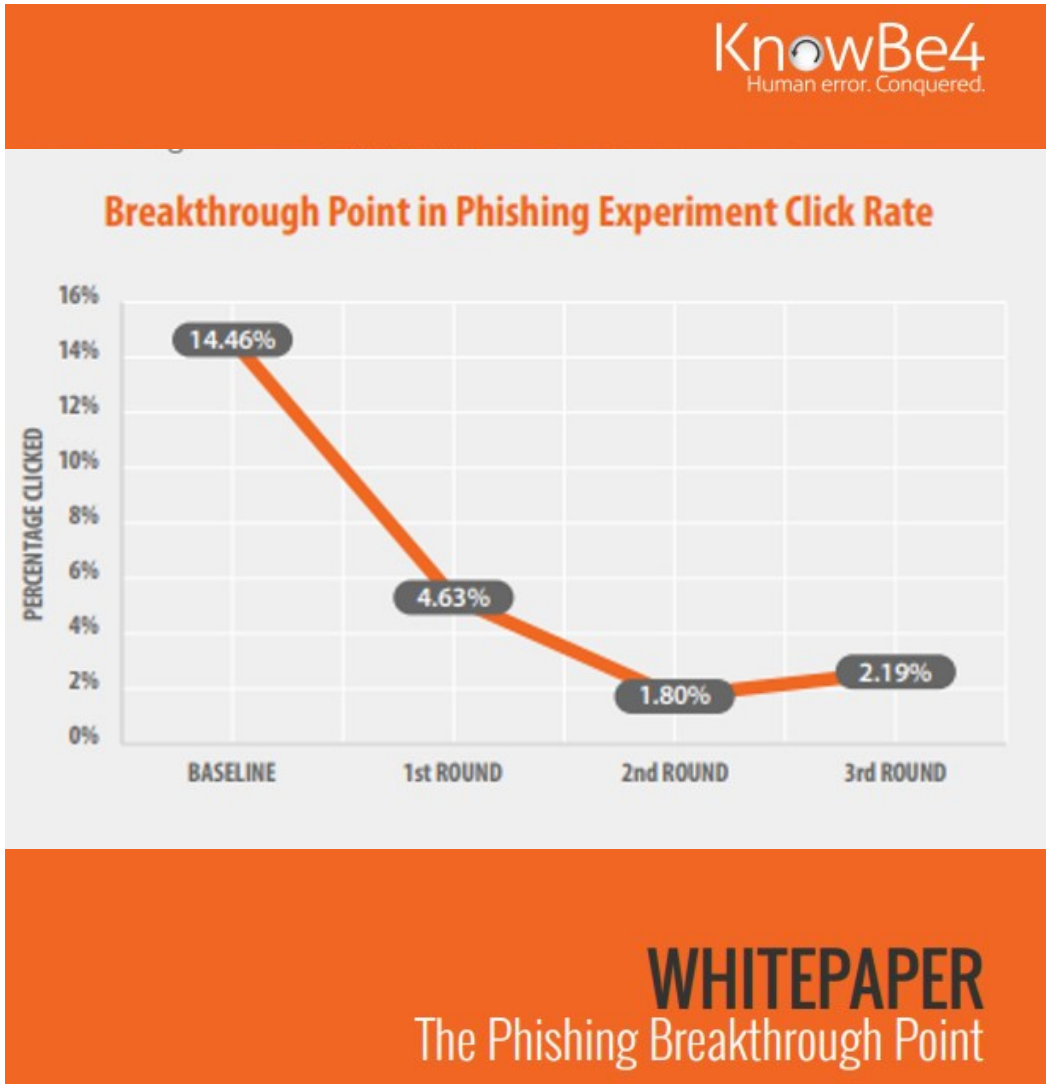
https://www.youtube.com/watch?v=oxXpB9pSETo

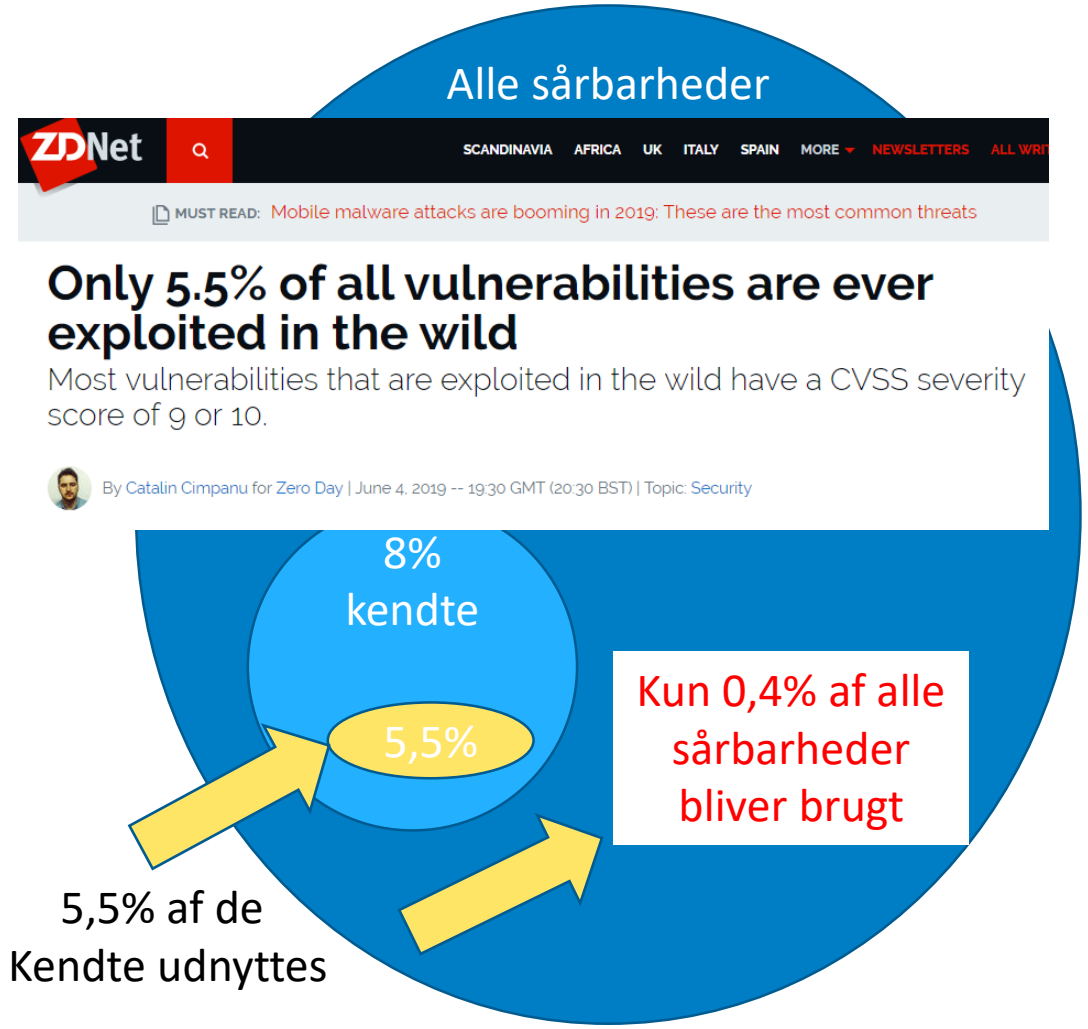
Der vil altid være sårbarheder – tekniske og menneskelige





Der vil altid være sårbarheder – tekniske og menneskelige

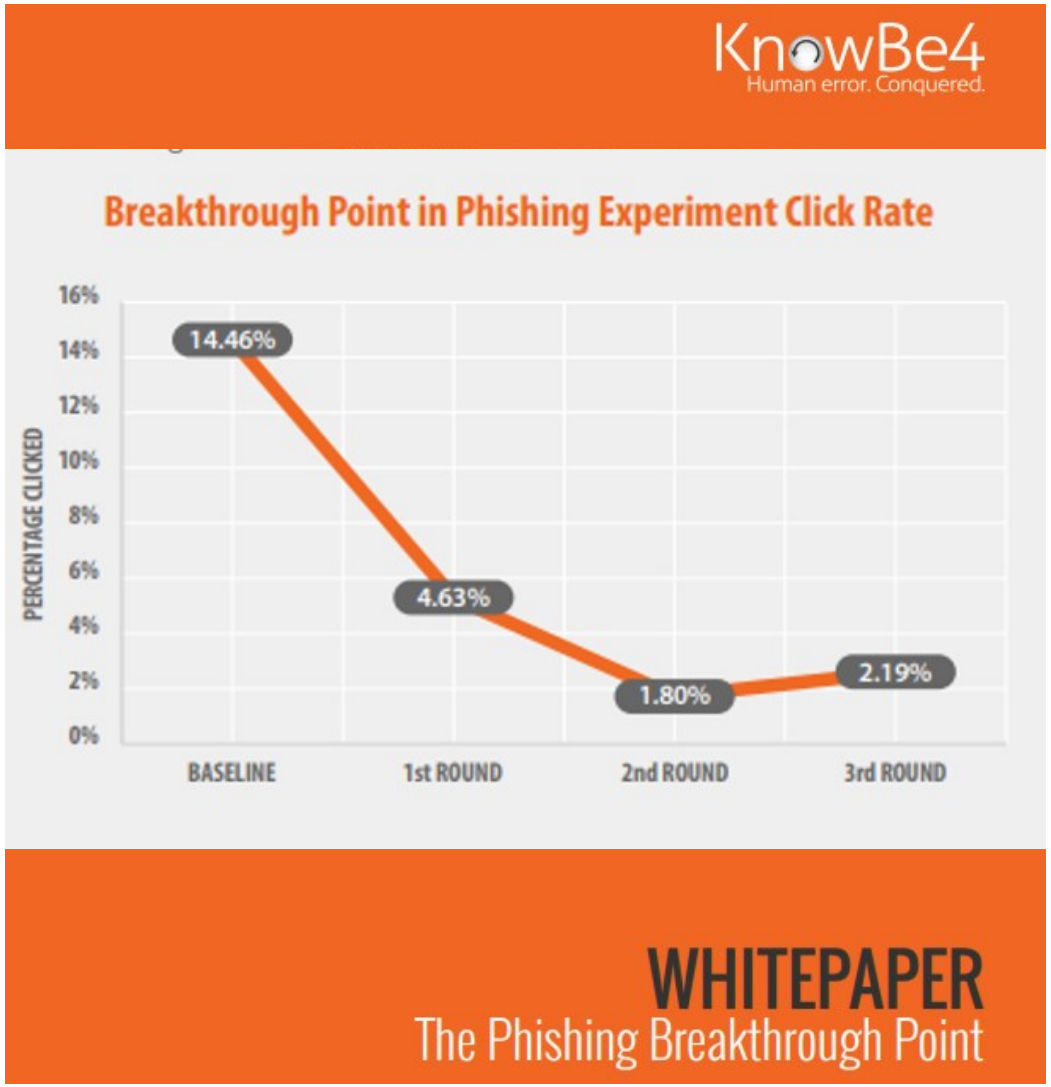


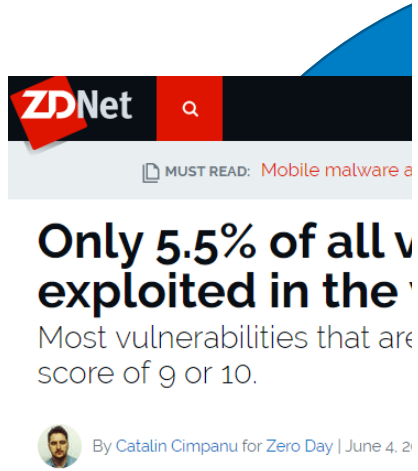


https://www.zdnet.com/article/ransomware-this-is-how-half-of-attacks-begin-and-this-is-how-you-can-stop-them

https://www.zdnet.com/article/only-5-5-of-all-vulnerabilities-are-ever-exploited-in-the-wild/

Der vil altid være sårbarheder – tekniske og menneskelige





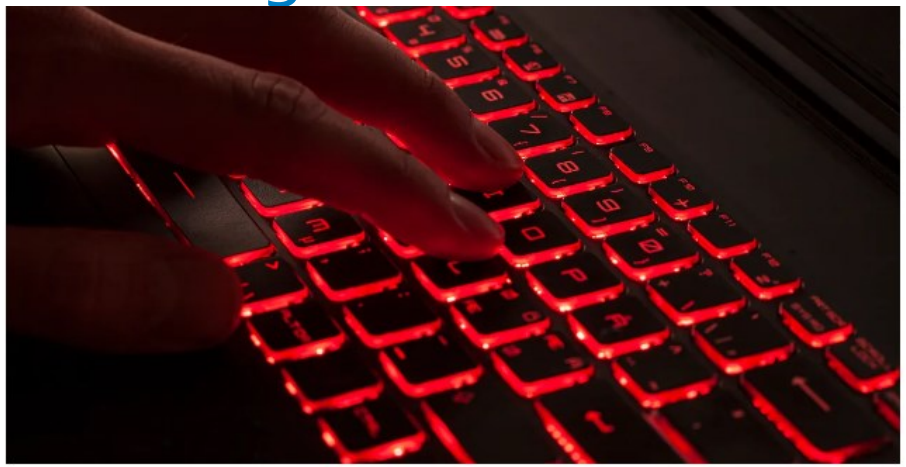
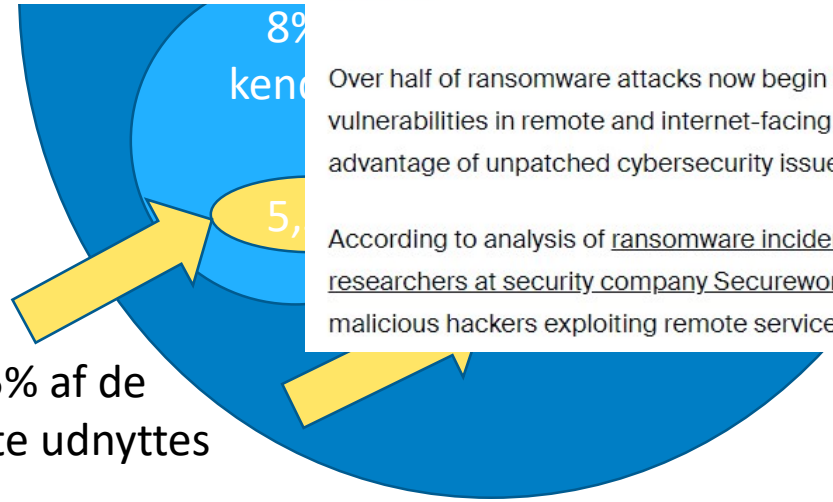


Image: Getty

Over half of ransomware attacks now begin with criminals exploiting vulnerabilities in remote and internet-facing systems as hackers look to take advantage of unpatched cybersecurity issues.

According to analysis of ransomware incidents during the past year by researchers at security company Secureworks, 52% of attacks started with malicious hackers exploiting remote services.



5,5% af de
Kendte udnyttes

https://www.zdnet.com/article/ransomware-this-is-how-half-of-attacks-begin-and-this-is-how-you-can-stop-them

https://www.zdnet.com/article/only-5-5-of-all-vulnerabilities-are-ever-exploited-in-the-wild/

Hackerne er foran!

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

Vi bliver mere og mere afhængige af hinanden på tværs!

Bil og enheder har 23 sim kort !

Når tid er afgørende for overlevelse: Ambulancer kortlægger mobilnet på Sjælland

Ambulancer skal den kommende tid køre rundt med en netværksscanner og kortlægge mobildækningen på Sjælland. (Illustration: Region Sjælland)

DTU kortlægger mobildækningen på Sjælland med en netværksscanner i en ambulance. Målet er på sigt at starte behandlingen tidligere ved slagtilfælde.

Af Laurids Hovgaard 22. sep 2022 kl. 05:10

https://ing.dk/artikel/naar-tid-afgoerende-overlevelse-ambulancer-kortlaegger-mobilnet-paa-sjaelland-261047

Data eksplosion – vi bliver nødt til at tænke på en anden måde!

Overcoming the biggest cyber security staff challenges

Organisations face resource shortages when it comes to cyber security, but there are ways to overcome this.

Andrew Rose, resident CISO EMEA at Proofpoint, discusses the biggest cyber security staff challenges facing organisations, and how to overcome them

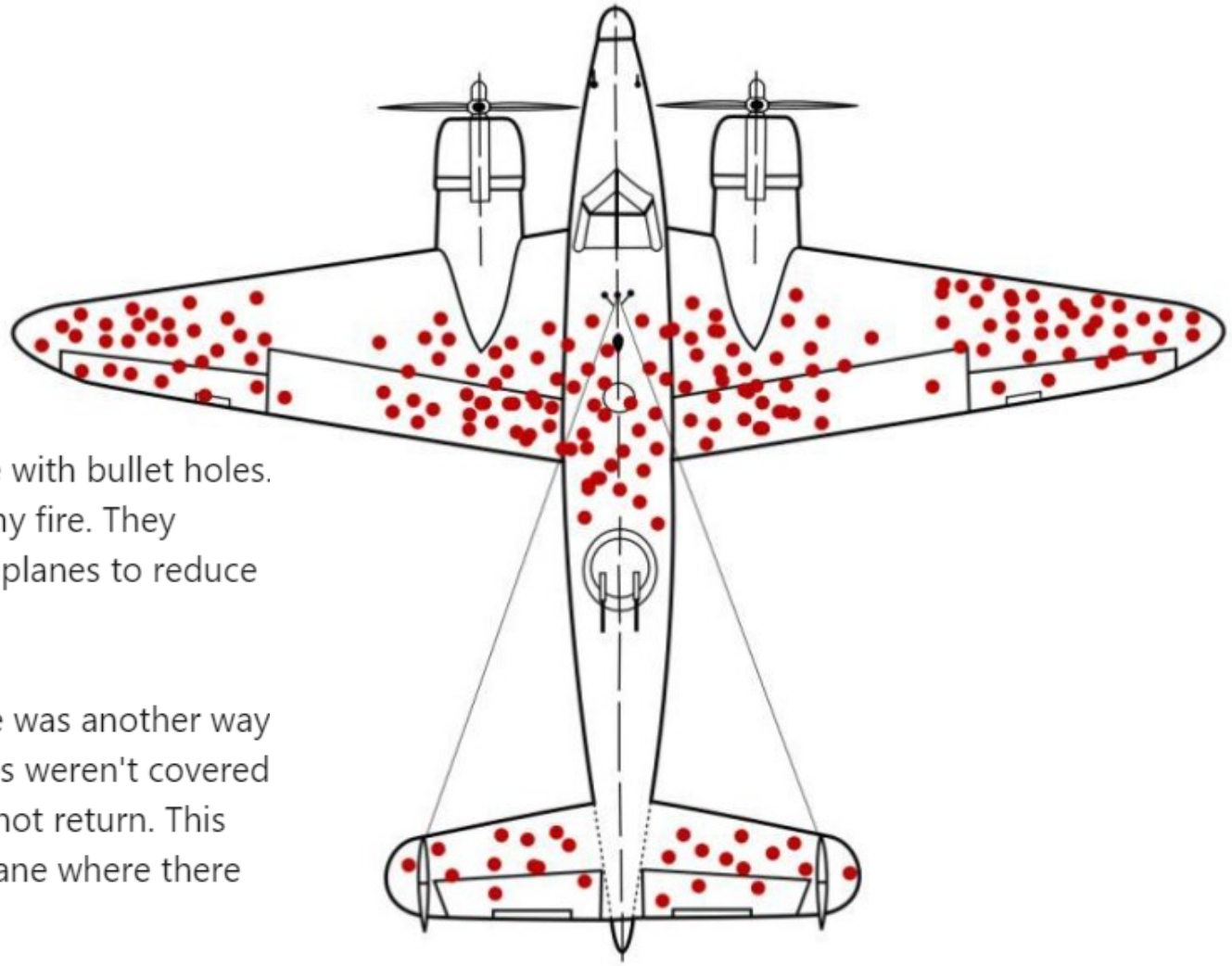
https://www.information-age.com/overcoming-biggest-cyber-security-staff-challenges-12349922

Detection of known indicators of compromise is no longer enough; security teams need tools that can detect abnormal behavior, which could signal an advanced attack before it's too late. For teams with limited resources and time, finding the budget for yet another tool is hard to justify, not to mention the complexity it adds.

In addition, the high volume of data traveling across the network makes it easy for attackers to hide their tracks and avoid detection. By blending in with normal traffic patterns, threats can hide and attackers can increase their dwell time. Attackers are patient; they may move data in small and infrequent batches to avoid being noticed. Modern attacker tactics require that security teams are prepared with NDR solutions. These can constantly monitor their networks and find strange or suspicious behavior quickly. From there, they can raise actionable alerts that help contain a cyberattack.

https://securityintelligence.com/posts/network-detection-and-response-network-security/

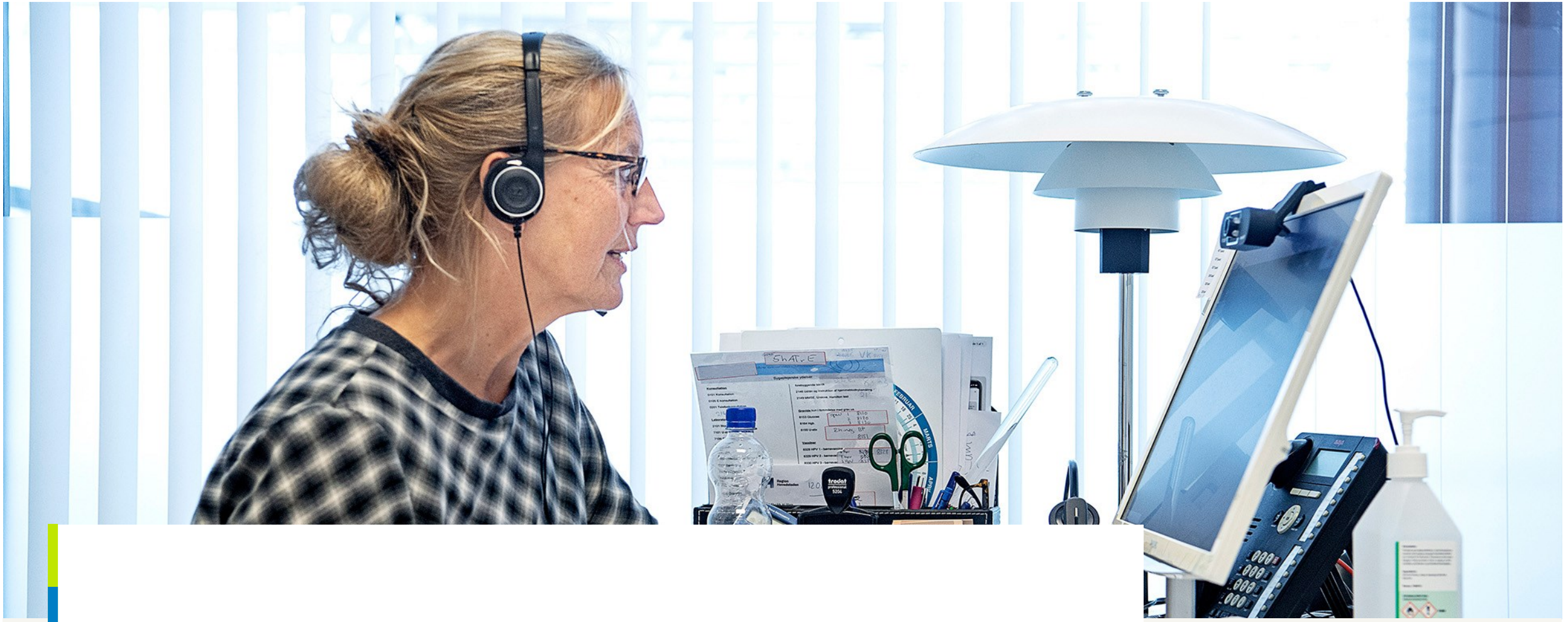
Unknown/Unknowns



During World War II, fighter planes would come back from battle with bullet holes. The Allies found the areas that were most commonly hit by enemy fire. They sought to strengthen the most commonly damaged parts of the planes to reduce the number that was shot down.

A mathematician, Abraham Wald, pointed out that perhaps there was another way to look at the data. Perhaps the reason certain areas of the planes weren't covered in bullet holes was that planes that were shot in those areas did not return. This insight led to the armor being re-enforced on the parts of the plane where there were no bullet holes.

The story behind the data is arguably more important than the data itself. Or more precisely, the reason behind why we are missing certain pieces of data may be more meaningful than the data we have.



Hvad kan man så gøre for at stå imod?

SUNDHEDSDATA-
STYRELSEN

Cybersikkerhed er ikke længere nok – Vi har brug for "Cyber Robusthed"

DDOS

Phishing & Social engineering

Industry spionage

Sårbarheder

Angreb på Supply chain

Malware & ransomware

Beredskabs- og nødplaner
Alternativ kommunikation
Løbende test af beredskab
Backup og reetableringstest

Samarbejde på tværs!
Design løsninger og systemer efter ø-drift
Automatiseret overvågning og reaktion

https://www.weforum.org/agenda/2021/11/why-move-cyber-security-to-cyber-resilience

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

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