



## From Covid-19 to War

*Is our risk perception ready for an emerging threat landscape?*

Søren Bank Greenfield - Head of Department *Cyber and Information security*

Tanja Kaufmann - Head of Section *The decentralized cyber and information security unit*



**DANISH HEALTH  
DATA AUTHORITY**

# The art of making the right decisions



# The missing piece of the puzzle



# Risk perception

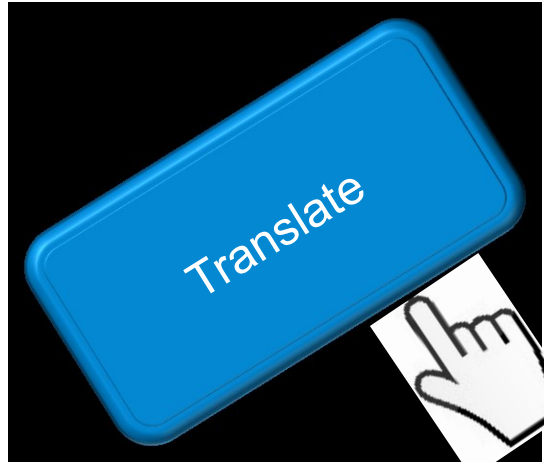


*Overall, risk perception can be explained as a subjective understanding, of which the individual's preconditions, context and intuition determine how a risk is experienced and assessed (Slovic, 2000: 220).*

The big unknown factor

# THE PERCEPTION GAP!





## So what's next?

*By translating our expert knowledge, we create a foundation for qualified decisions about risk and mitigation.*

# And now we add the emerging threats!!

First we had Covid-19  
*"Let's go more digital"*



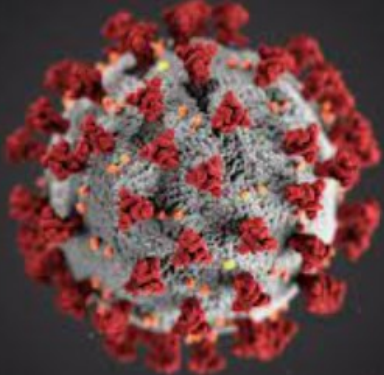
Then came the war  
*"Let's go redundant!"*



# What to expect in the future ?

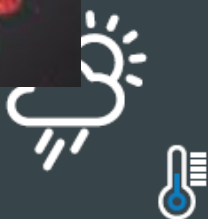






# hændelser i sundhedssektoren

1. Kvartal 2021

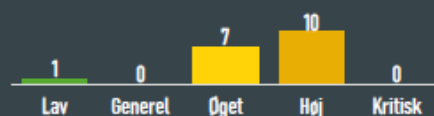


Generel

## Udvalgte varslar

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

## Antal udsendte varslar



4. Kvartal 2021

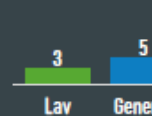


Øget

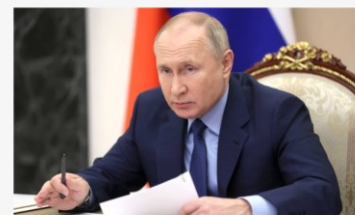
## Udvalgte varslar

- › 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 varslar



1. Kvartal 2022



Lisa Ercolano / © Feb 15

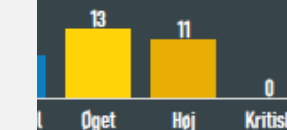


Øget

## Udvalgte varslar

- › 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 varslar



## 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 / WIMEDIA COMMONS

2. Kvartal 2022

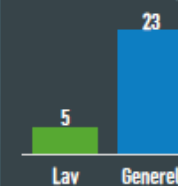


Generel

## Udvalgte varslar

- › Kritiske sårbarheder i VMware
- › Kritisk opdatering til Zyxel firewalls 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 varslar





# Cybercrime as a service (CaaS) and the main cashcow - Ransomware attacks are booming

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

[Get rights and content](#)

Cybercrime has continued to evolve and today it exists in a highly organised form. It has itself become big business, and as with all emerging markets, the suppliers and vendors that serve the cybercrime market have expanded their offer to encompass a range of activities.

Cybercrime has evolved into a complex, highly organised hierarchy involving leaders, engineers, infantry, and hired money mules and a worrying new phrase has entered the lexicon of cybercrime – Crime as a Service (CaaS). Derek Manky of FortiGuard Labs examines how the cybercrime world has matured into big business.

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

March 30, 2021

## Over half of ransomware victims pay the ransom, but only a quarter see their full data returned

More than half (56%) of ransomware victims paid the ransom to restore access to their data last year, according to a global study of 15,000 consumers conducted by global security company Kaspersky.

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](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)

# The hackers are ahead!

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 \(ZDNet YouTube\)](#)




**SAMSUNG**

### Introducing Galaxy Book Series

[BUY NOW](#)

\* Screen images simulated for illustrative purpose.

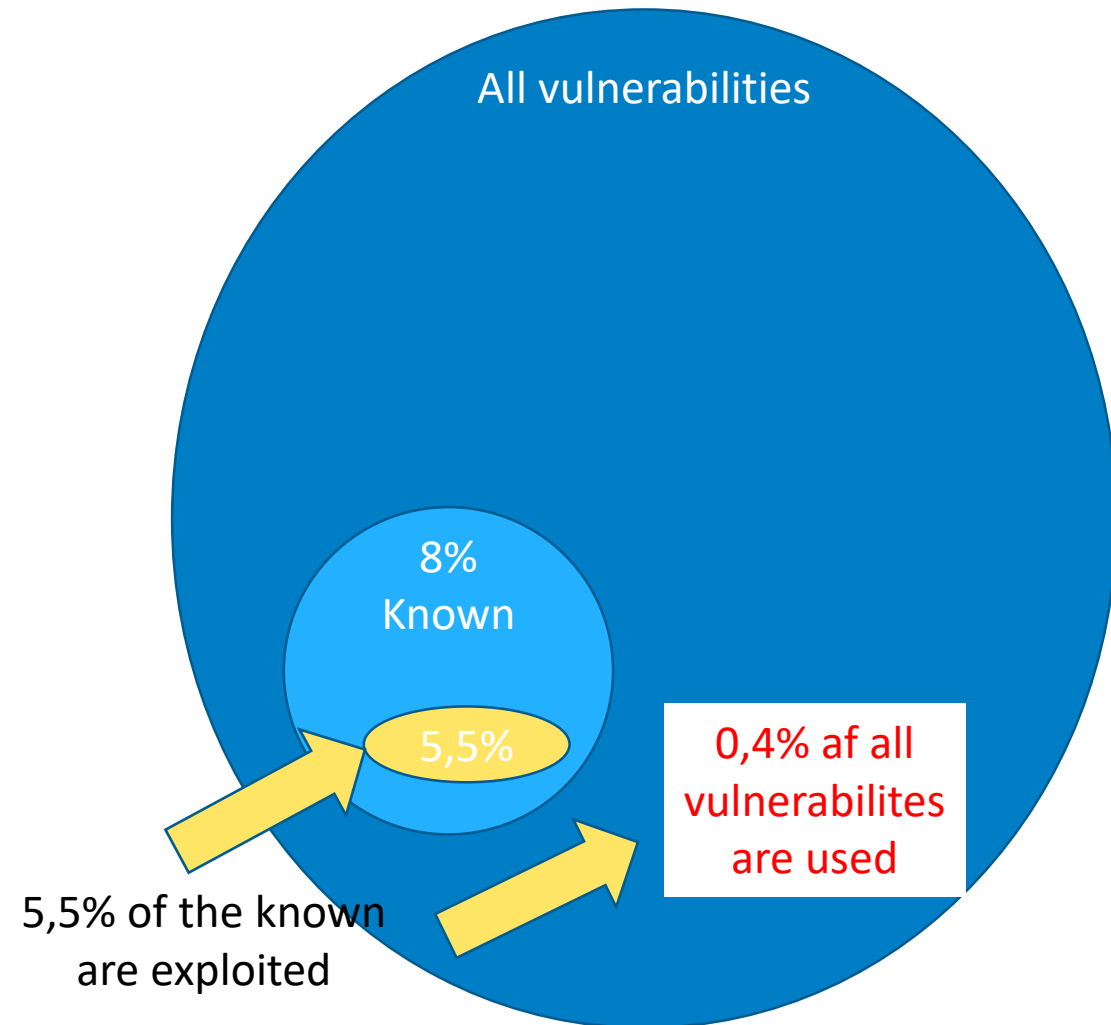
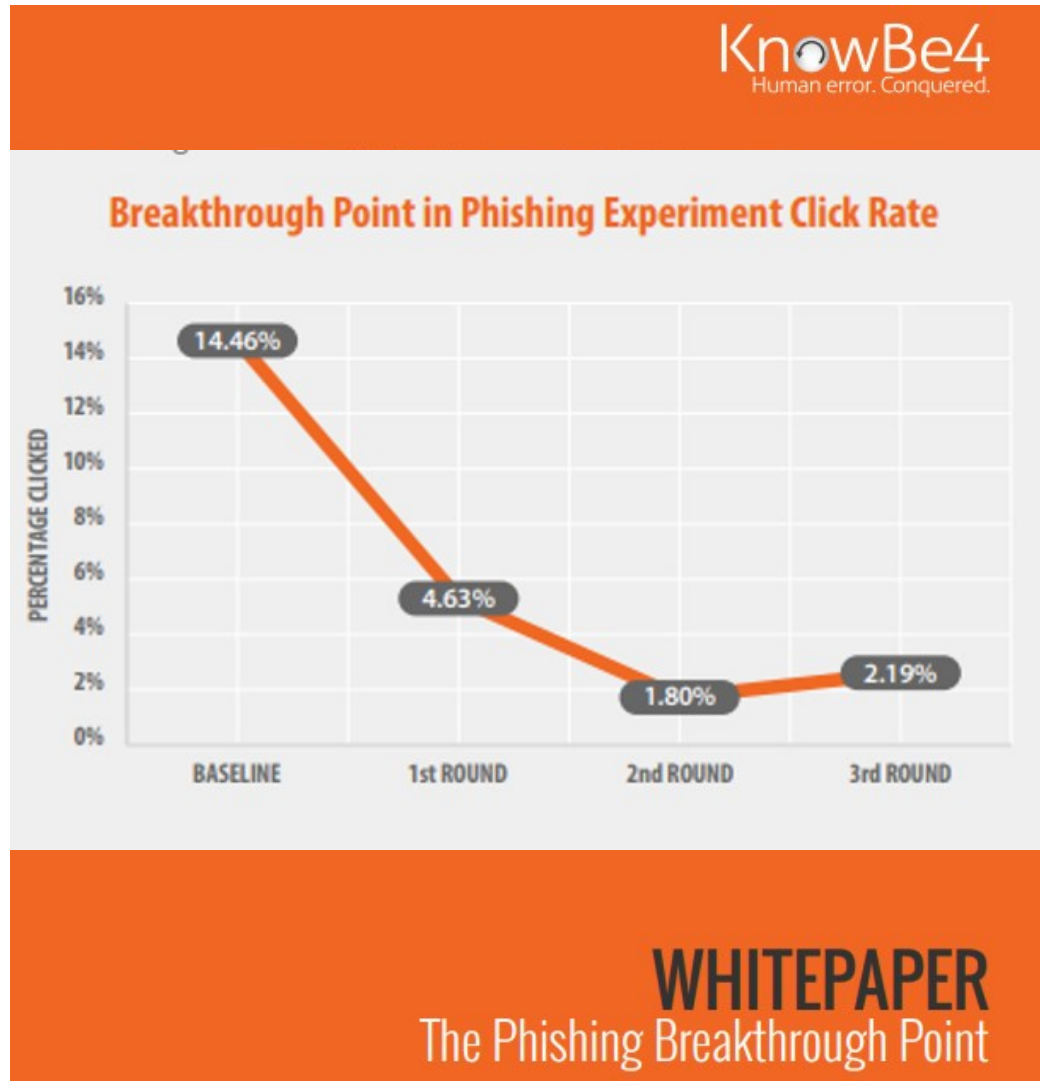
**MORE FROM CHARLIE OSBORNE**



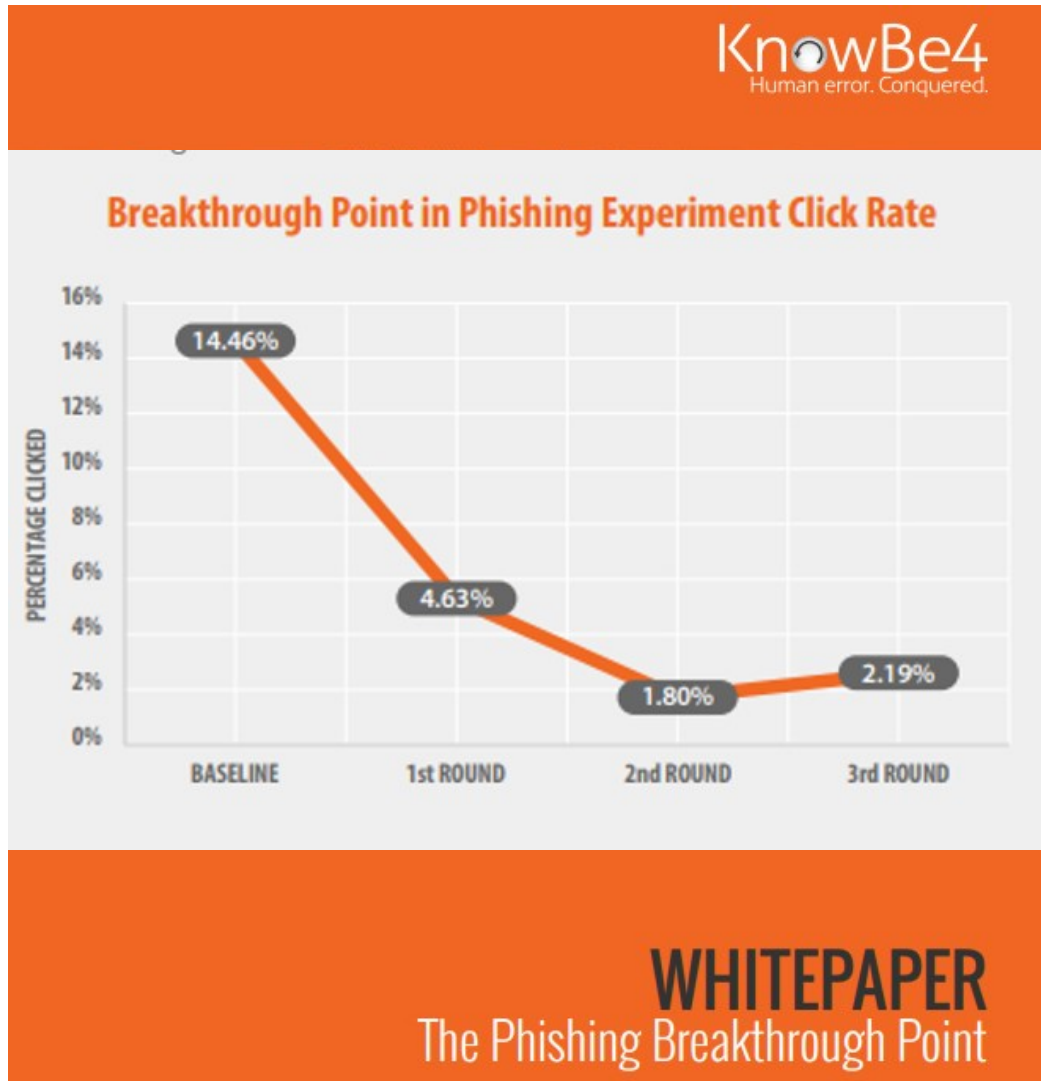
[Security Bizarro banking Trojan surges across Europe](#)

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

# There will always be vulnerabilities – human and technical



# There will always be vulnerabilities – human and technical



## Only 5.5% of all vulnerabilities exploited in the wild

Most vulnerabilities that are exploited in the wild have a score of 9 or 10.



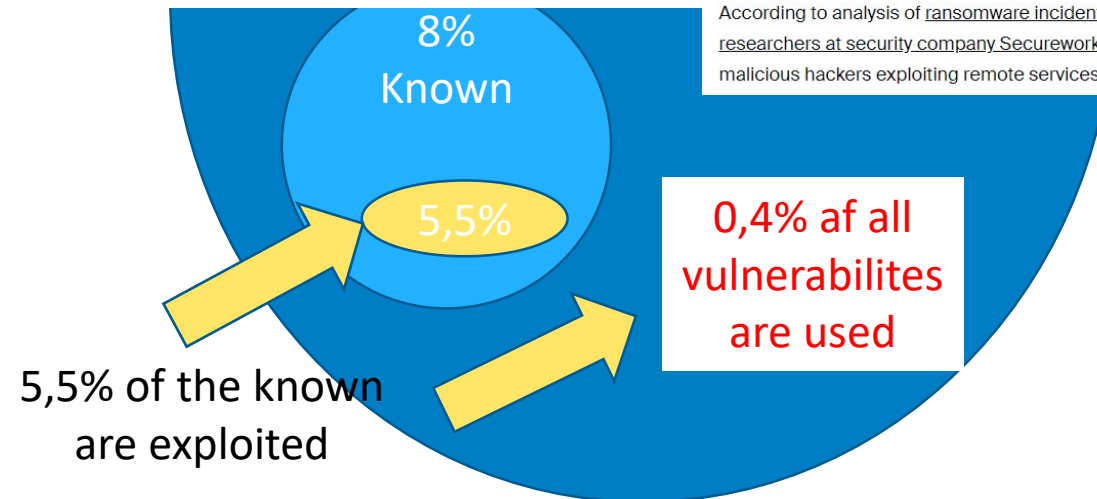
By Catalin Cimpanu for Zero Day | June 4, 2019 -- 19:30 GMT (20:30 BST) | Top



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.



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

# We are dependent on each other across sectors – collaboration is key!



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



Ambulancer skal den kommende tid køre rundt med en netværksscanner og kortlægge mobilnet 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>

Announce

**PLUS.**

Bluebeam gør det nemt at standardisere byggeprocesser.

Vis mig hvordan

BLUEBEAM

Job fra **JOBFINDER**

**NEXEL** Einstallatør til teknisk sagsbehandling

**ORGANIS** Dygtige IT-ingeniører til beskyttelse af Danmarks klassificerede...

**TEKNOLOGISK INSTITUT** VVS-tekniker, VVS-installatør eller ingeniør til inspektion og...

# Data explosion and hiring people – We have to think differently

## 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**

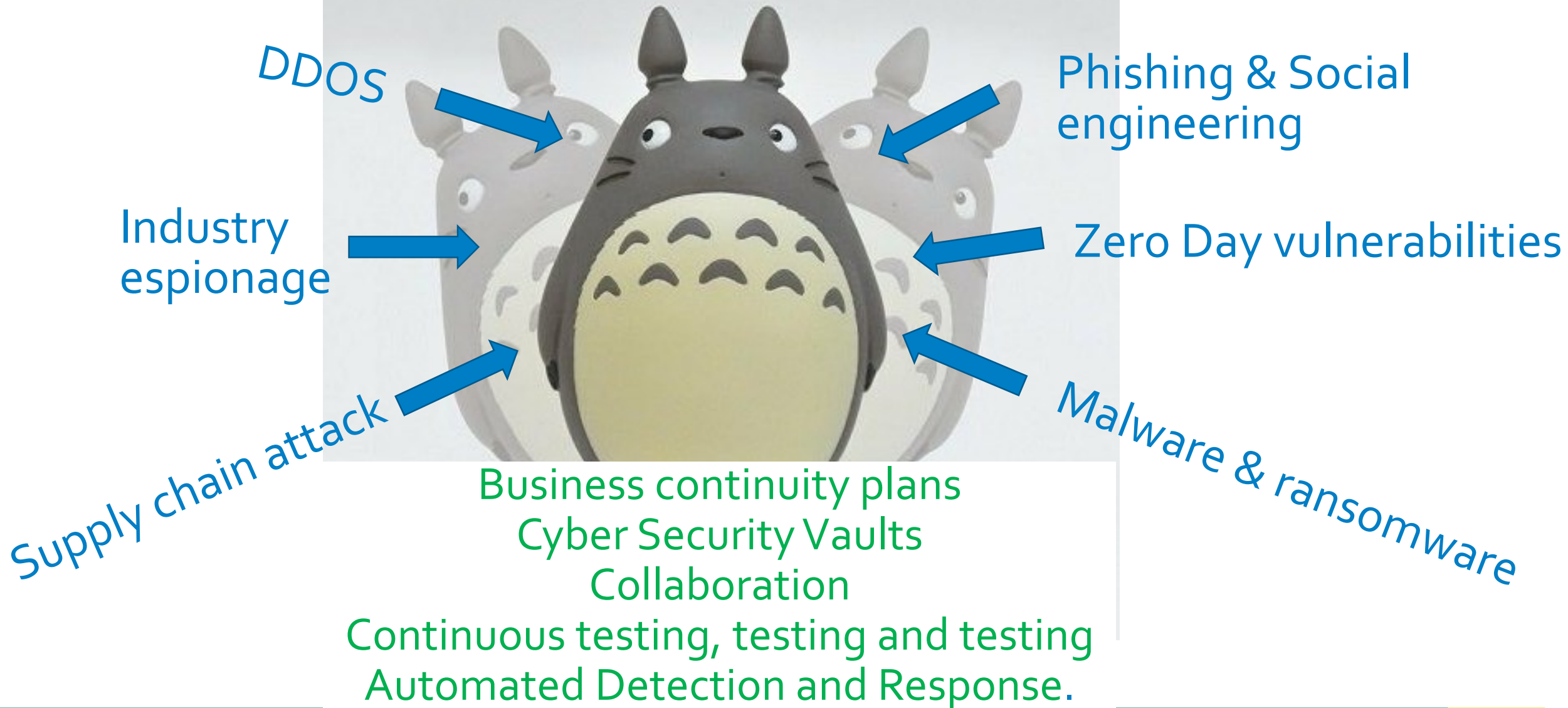
<https://www.information-age.com/overcoming-biggest-cyber-security-staff-challenges-12349922>

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/>

# Cybersecurity is no longer enough – we need **Cyber Resilience**





# How to mitigate??

Key challenge	Mitigation
<p><b>The hackers are ahead!</b> – they have agile business models, make tons of money and invest in AI and ML to recon and attack</p>	<p>Collaborations is key - create communities of trust and <b>share vulnerabilities and solutions</b> for the common good.</p> <p>Think differently and <b>invest in automation of tasks (AI and ML)</b> wherever possible.</p>
<p><b>There will always be vulnerabilities – technical and human.</b> No matter what we do.</p>	
<p>No firm or sector is independent, digitization makes collaboration key!</p>	
<p><b>Staffing shortage and massive amounts of data in cyber security</b></p>	<p>You cant predict or protect - you have to be able to be <b>Cyber resilient</b></p> <p>Emphasize on initiatives that make you recover quickly:  <b>Business continuity plans</b> (from offline)  <b>Cyber Security Vaults</b> (air gapped offline backup)  <b>Collaboration</b> with other (trusted circles and <b>MISP</b>)  <b>Continuous testing</b>, testing and testing of the emergency team  Invest in automated <b>Network Detection and Response</b></p>
<p><b>Cyber security is not enough anymore</b></p>	
<p>Hackers are copying encrypted data - <b>Harvest now and decrypt later</b> strategy</p>	<p>No real solutions yet –  Begin planning and implementing the use of <b>quantum encryptions</b> where really needed!  Begin mapping <b>where are you using encryption</b> and when the “new” ones will be “old”.</p>



## DANISH HEALTH DATA AUTHORITY

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

T: +45 7221 6800  
E: [kontakt@sundshedsdata.dk](mailto:kontakt@sundshedsdata.dk)  
W: [sundhedsdata.dk](http://sundhedsdata.dk)

Søren Bank Greenfield

[SBGR@sundhedsdata.dk](mailto:SBGR@sundhedsdata.dk)

## Contact

DCIS SUND

[DCISSUND@sundhedsdata.dk](mailto:DCISSUND@sundhedsdata.dk)



DCISSund on Twitter  
[@dcissund](https://twitter.com/dcissund)

DCISSund information and news

[www.sundhedsdata.dk/informationssikkerhed](http://www.sundhedsdata.dk/informationssikkerhed)