Cybertruslen i 3 perspektiver - Siscon/LIGA/Dubex

Cybertruslen i et ledelsesperspektiv

Jacob Herbst

København

Den 15. marts 2022

Dubex:

Dubex A/S

Konsulent- og sikkerhedsydelser lokalt og globalt

Højt specialiserede it-sikkerheds-eksperter

Kvalitet
Service
Kompetence

Managing risk – Enabling growth

First mover

CERTIFICERING AF INFORMATIONSSIKKERHED
DNV·GL
ISO/IEC 27001

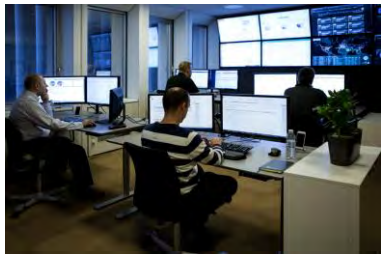
EY
ISAE
3000

digital tryghed

Eftertragtet arbejdsplads

Motiverede medarbejdere

Største it-sikkerhedspartner i Danmark



Selvfinansierende og privatejet siden 1997

Egen 7x24 onsite fuldt bemandede Security Analytic Center

Dubex Incident Response Team

Dubex:

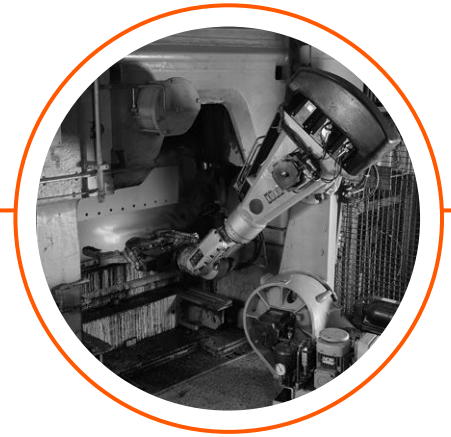
The industrial revolutions - the short story

”Industry 0.0” – crafts	Industry 1.0	Industry 2.0	Industry 3.0	Industry 4.0

Manually
Production was manual - all products were unique

Steam Engines
Mechanical production and railways powered by steam engines

Electricity
Mass production and assembly line

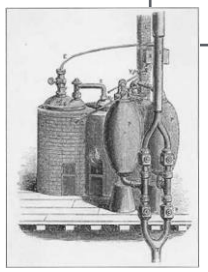


Computers
Automation using electronics and simple computers (PLCs)

Digitization
Information and communication technology

untill ~1800 | 1800 ~ 1900 | 1900 ~ 1970 | 1970 ~ 2010 | 2010 ~ future

Steam Engine (1784)



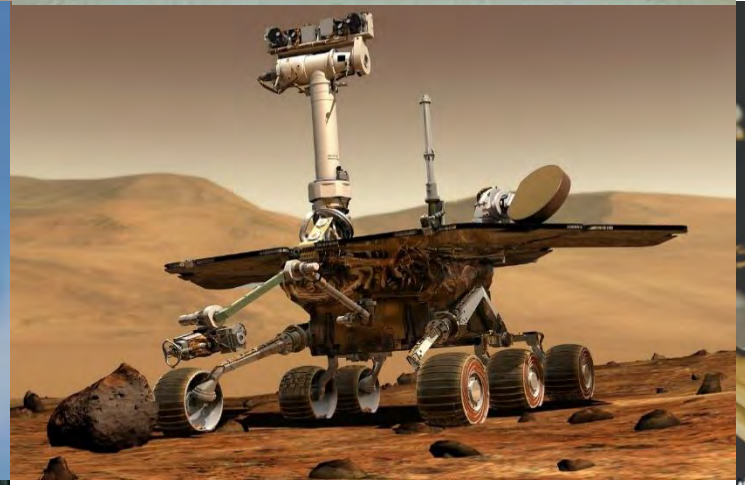
First assembly line Cincinnatic Slaughterhouse (1870)

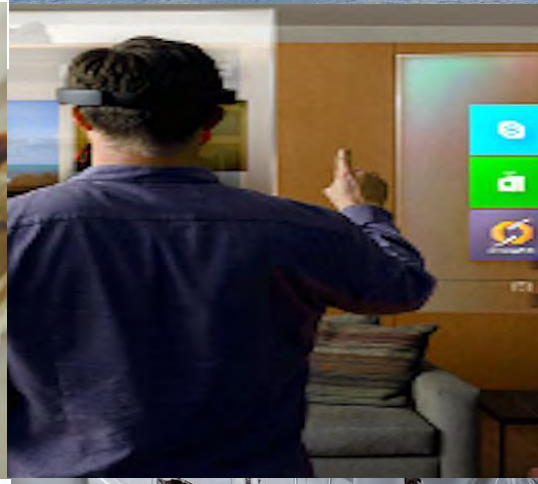
First modern PLC - Modicon 084 (1969)

Dubex:


HYUNDAI DRIVE


amazon

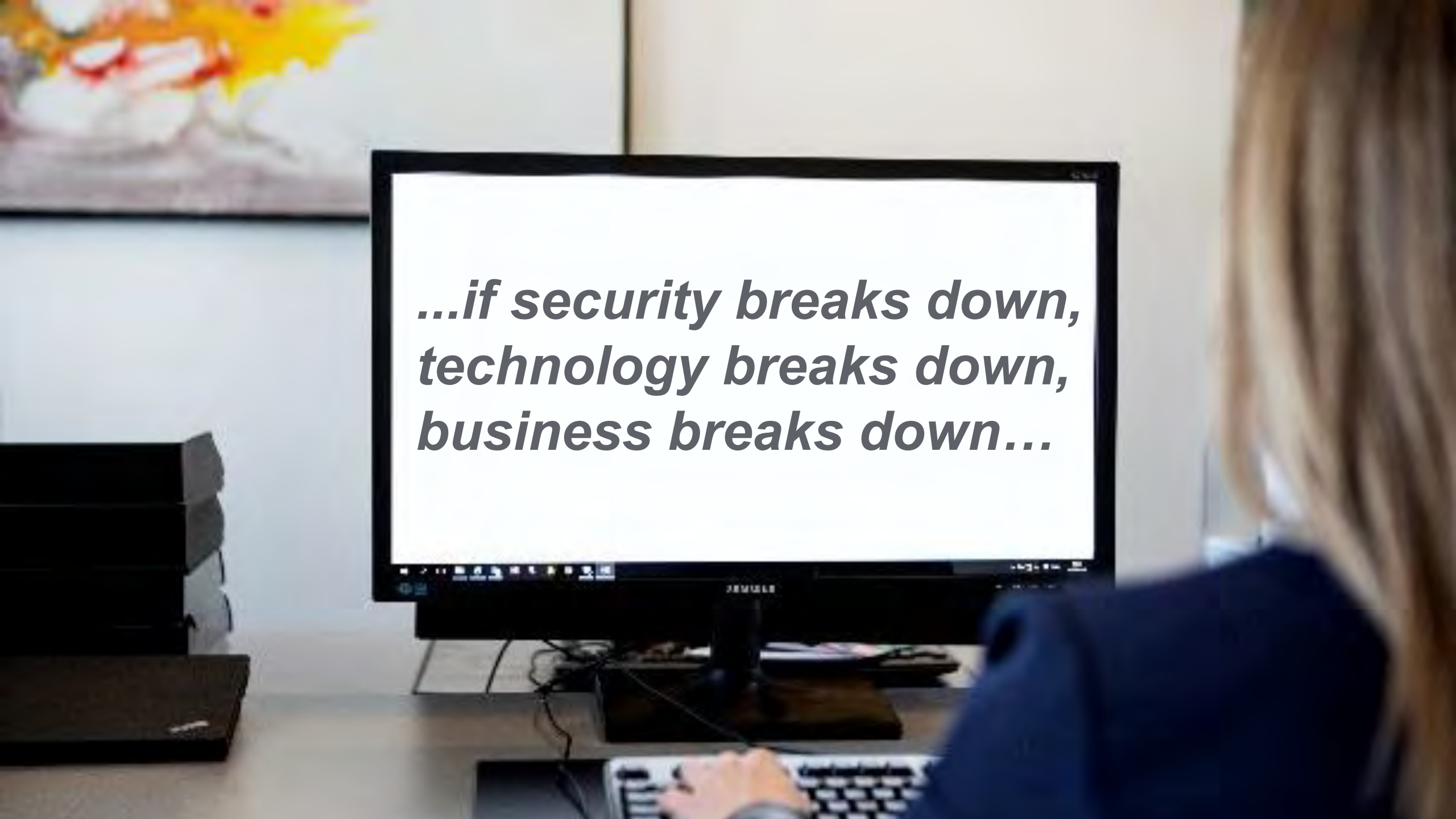




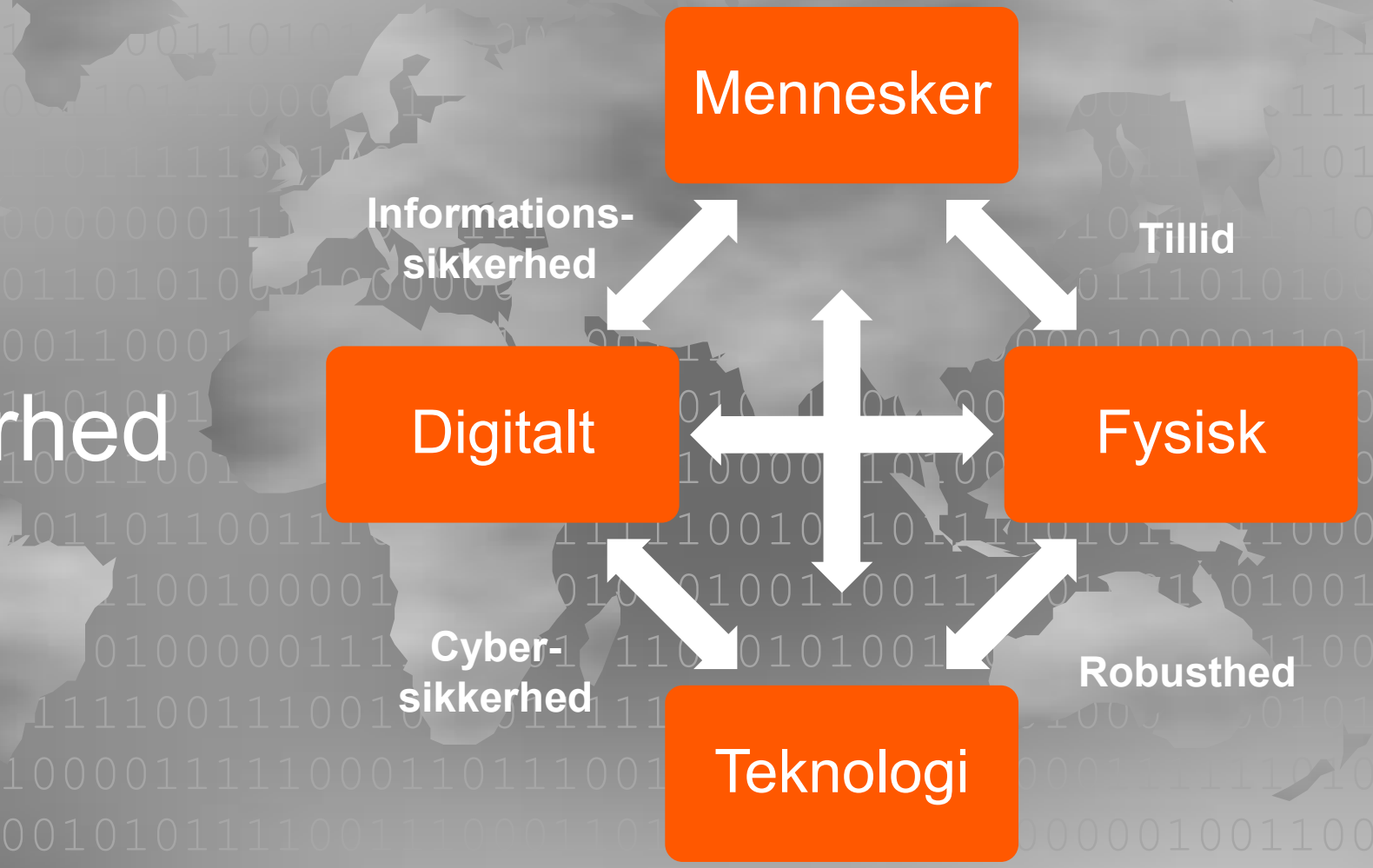

ST. JUDE MEDICAL
ASSURITY MRI™
PM2272 DDDR
S/N1234567

ALL COMPANIES ARE DIGITAL COMPANIES

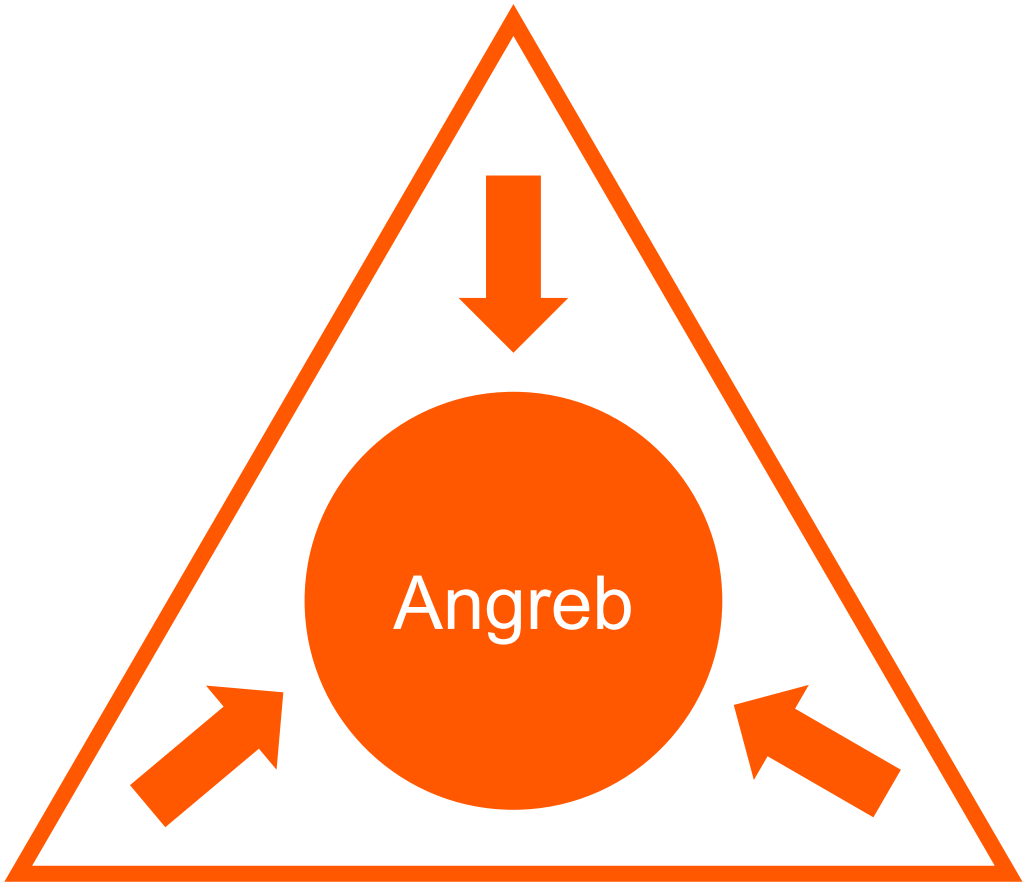
– Some Just Don’t Know It


...if security breaks down,
technology breaks down,
business breaks down…

Digital sikkerhed



Aktør & motiv



Evner & metoder

Mulighed

Cybertruslen mod Danmark 2021

Formålet med denne trusselsvurdering er at informere danske beslutningstagere, myndigheder og virksomheder om cybertruslen mod Danmark. Viden om truslen skal bl.a. kunne bruges til at prioritere tiltag hos den enkelte myndighed og virksomhed. Dette produkt vurderer trusselsniveauerne for forskellige typer af cybertrusler, men trusselsvurderingen indeholder ikke konkrete råd og vejledninger til at imødegå disse trusler.

Hovedvurdering

- Truslen fra cyberkriminalitet er **MEGET HØJ**. Alle danske myndigheder, virksomheder og borgere er udsat for en vedvarende og aktiv trussel fra cyberkriminelle. Truslen underbygges af de cyberkriminelles evne til at udvikle og omstille sig til nye virkeligheder samt det specialiserede samarbejde, der foregår på lukkede internetfora.
- Truslen fra cyberspionage er **MEGET HØJ**. CFCS vurderer, at fremmede stater kan og vil forsøge på at stjæle værdifuld information fra Danmark. Særligt interessante mål på det udenrigs- og sikkerhedspolitiske område er udsat for en vedvarende interesse fra statslige aktører. Konkrete hændelser og løbende angrebsforsøg understreger gang på gang denne vurdering.
- CFCS vurderer, at truslen fra destruktive cyberangreb mod danske myndigheder og virksomheder er **LAV**. Flere stater har kapaciteten til at udføre destruktive angreb, men det er mindre sandsynligt, at de aktuelt har intention om at udføre den type angreb mod danske mål.
- Truslen fra cyberaktivisme er **LAV**. De mange protester, der har præget 2020, har ikke ført til en stigning i antallet af cyberaktivistiske angreb på verdensplan. Antallet af angreb ligger således på niveau med de seneste år.
- Truslen fra cyberterror er **INGEN**. Alvorlige cyberangreb, hvor hensigten er at skabe samme effekt som mere konventionel terror, forudsætter tekniske evner og organisatoriske ressourcer, som militante ekstremister aktuelt ikke har. Hensigten er samtidigt begrænset.

CENTER FOR CYBERSIKKERHED

Trusselsniveauer

Forsvarets Efterretningstjeneste bruger følgende trusselsniveauer.

INGEN	Der er ingen indikationer på en trussel. Der er ikke erkendt kapacitet eller hensigt. Angreb/skadevoldende aktivitet er usandsynlig.
LAV	Der er en potentiel trussel. Der er en begrænset kapacitet og/eller hensigt. Angreb/skadevoldende aktivitet er mindre sandsynlig.
MIDDEL	Der er en generel trussel. Der er kapacitet og/eller hensigt og mulig planlægning. Angreb/skadevoldende aktivitet er mulig.
HØJ	Der er en erkendt trussel. Der er kapacitet, hensigt og planlægning. Angreb/skadevoldende aktivitet er sandsynlig.
MEGET HØJ	Der er en specifik trussel. Der er kapacitet, hensigt, planlægning og mulig iværksættelse. Angreb/skadevoldende aktivitet er meget sandsynlig.

- Truslen fra cyberkriminalitet er **MEGET HØJ**. Alle danske myndigheder, virksomheder og borgere er udsat for en vedvarende og aktiv trussel fra cyberkriminelle. Truslen underbygges af de cyberkriminelles evne til at udvikle og omstille sig til nye virkeligheder samt det specialiserede samarbejde, der foregår på lukkede internetfora.
- Truslen fra cyberspionage er **MEGET HØJ**. CFCS vurderer, at fremmede stater kan og vil forsøge på at stjæle værdifuld information fra Danmark. Særligt interessante mål på det udenrigs- og sikkerhedspolitiske område er udsat for en vedvarende interesse fra statslige aktører. Konkrete hændelser og løbende angrebsforsøg understreger gang på gang denne vurdering.


Demant


AK TECHOTEL


coop


ISS


BAUHAUS


Colonial Pipeline Company


Vestas


KALUNDBORG
FORSYNING


JBS


BY APPOINTMENT TO THE ROYAL DANISH COURT
Royal Greenland

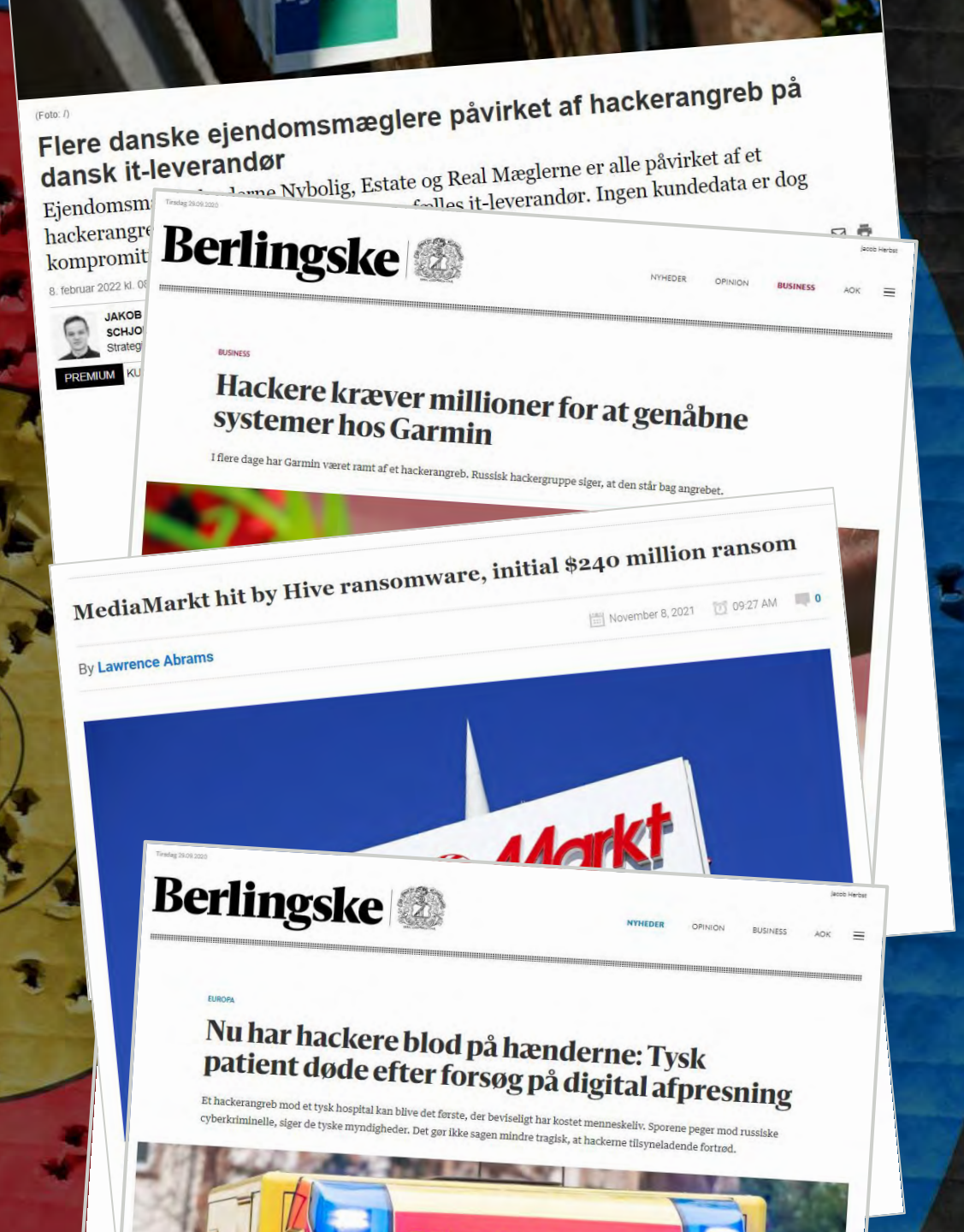

WÜRTH


accenture

Big game hunting – målrettet ransomware

…. Digitale gidseltagere på storvildtjagt

- Fokus for krypto-ransomware ændret fra private til målrettet mod virksomheder
- Ransomware spedes via målrettet hacking og funktioner der tillader spedning internt i virksomhedens netværk og systemer
- Flere ransomware-as-a-service (RaaS) aktører
- Krav om markant højere løsesummer
- Tyveri af data med trusler om offentliggørelse ved manglende betaling
- Påvirkning af aktiekurser med mulighed for spekulation



Angrebet af DarkSide med ransomware den 7. maj 2021

Medførte mangel på brændstof på den amerikanske østkyst

Præsident Biden erklærede nødretstilstand den 9. maj

Driften begyndte igen den 12. maj 2021

Betalte løsesum på
75 bitcoins ~ $4.4 million
få timer efter angrebet…

Hackere bag angreb på Coop kræver halv milliard kroner

800 svenske Coop-butikker har i weekenden måttet holde lukket efter hackerangreb i USA. Russiske hackere ser ud til at stå bag.

Coop-butikkerne i Sverige er fortsat ramt af hackeres hærgen, og kæden opfordrer svenskerne til at holde sig orienteret på nettet, om deres lokale butik er åbnet igen.
Foto: Coop Sverige

THOMAS BREINSTRUP
journalist

Lyt til artiklen

Hackerne bag det angreb, som hen over weekenden betød lukning af 800 Coop-butikker i Sverige, har nu krævet næsten en halv milliard kroner for at slippe deres kvælertag.

Søndag krævede hackerne i et opslag på den såkaldte mørke del af internettet 70 millioner dollar (439 millioner kroner) for låse de data op, som de har taget som gidsler, og som har ramt hundredvis af virksomheder verden over.

Opslaget ligger på en blog, som normalt bruges af den berygtede, **russiske** hackergruppe REvil. It-sikkerhedseksperter anser det for sandsynligt, at det er REvil, der står bag angrebet.

Fredag aften begyndte kassesystemerne at drille

Det ramte fredag det amerikanske it-firma Kaseya i Miami, hvis it-system bruges af it-leverandøren Visma Esscom, som står for systemerne hos Coop i Sverige.

Her begyndte personalet fredag aften omkring klokken 18.30 at melde om problemer.

Berlingske

Hackere bag angreb på Coop kræver halv milliard kroner

800 svenske Coop-butikker har i weekenden måttet holde lukket efter hackerangreb i USA. Russiske hackere ser ud til at stå bag.

Coop-butikkerne i Sverige er fortsat ramt af hackeres hærgen, og kæden opfordrer svenskerne til at holde sig orienteret på nettet, om deres lokale butik er åbnet igen.
Foto: Coop Sverige

THOMAS BREINSTRUP
jobnalist

Opdateret d. 05. juli 2021 kl. 19:00
Del denne artikel

Lyt til artiklen

Hackerne bag det angreb, som hen over weekenden betød lukning af 800 Coop-butikker i Sverige, har nu krævet næsten en halv milliard kroner for at slippe deres kvælertag.

Søndag krævede hackerne i et opslag på den såkaldte mørke del af internettet 70 millioner dollar (439 millioner kroner) for låse de data op, som de har taget som gidsler, og som har ramt hundredvis af virksomheder verden over.

Opslaget ligger på en blog, som normalt bruges af den berygtede, russiske hackergruppe REvil. It-sikkerhedseksperter anser det for sandsynligt, at det er REvil, der står bag angrebet.

Fredag aften begyndte kassesystemerne at drille

Det ramte fredag det amerikanske it-firma Kaseya i Miami, hvis it-system bruges af it-leverandøren Visma Esscom, som står for systemerne hos Coop i Sverige.

Her begyndte personalet fredag aften omkring klokken 18.30 at melde om problemer.

18 augusti, 2021 • Pressmeddelande

Nu är alla Coops butiker öppna

Alla butiker runt om i landet har nu kunnat öppnas igen, efter IT-störningarna som påverkade Coops kassasystem i nästan hela landet. IT-störningen är en del av en större global cyberattack som riktats mot det amerikanska mjukvarubolaget Kaseya. Flera andra svenska och internationella företag har drabbats av samma händelse.

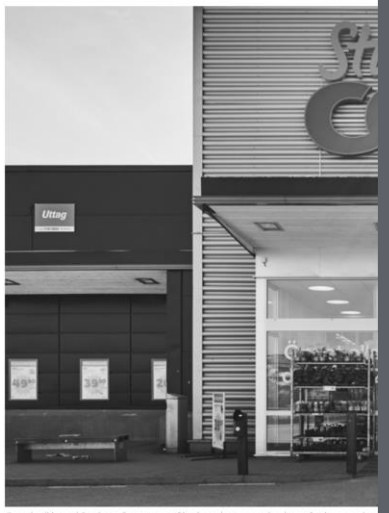
Läs mer

Berlingske

NYHEDER OPINION BUSINESS AOK

Hackere bag angreb på Coop kræver halv milliard kroner

800 svenske Coop-butikker har i weekenden måttet holde lukket efter hackerangreb i USA. Russiske hackere ser ud til at stå bag.



Coop-butikkerne i Sverige er fortsat ramt af hackeres hærgen, og kæden opfordrer svenskere
Foto: Coop Sverige

THOMAS BREINSTRUP
journalist

Lyt til artiklen

Hackerne bag det angreb, som hen over weekenden betød
i Sverige, har nu krævet næsten en halv milliard kroner for

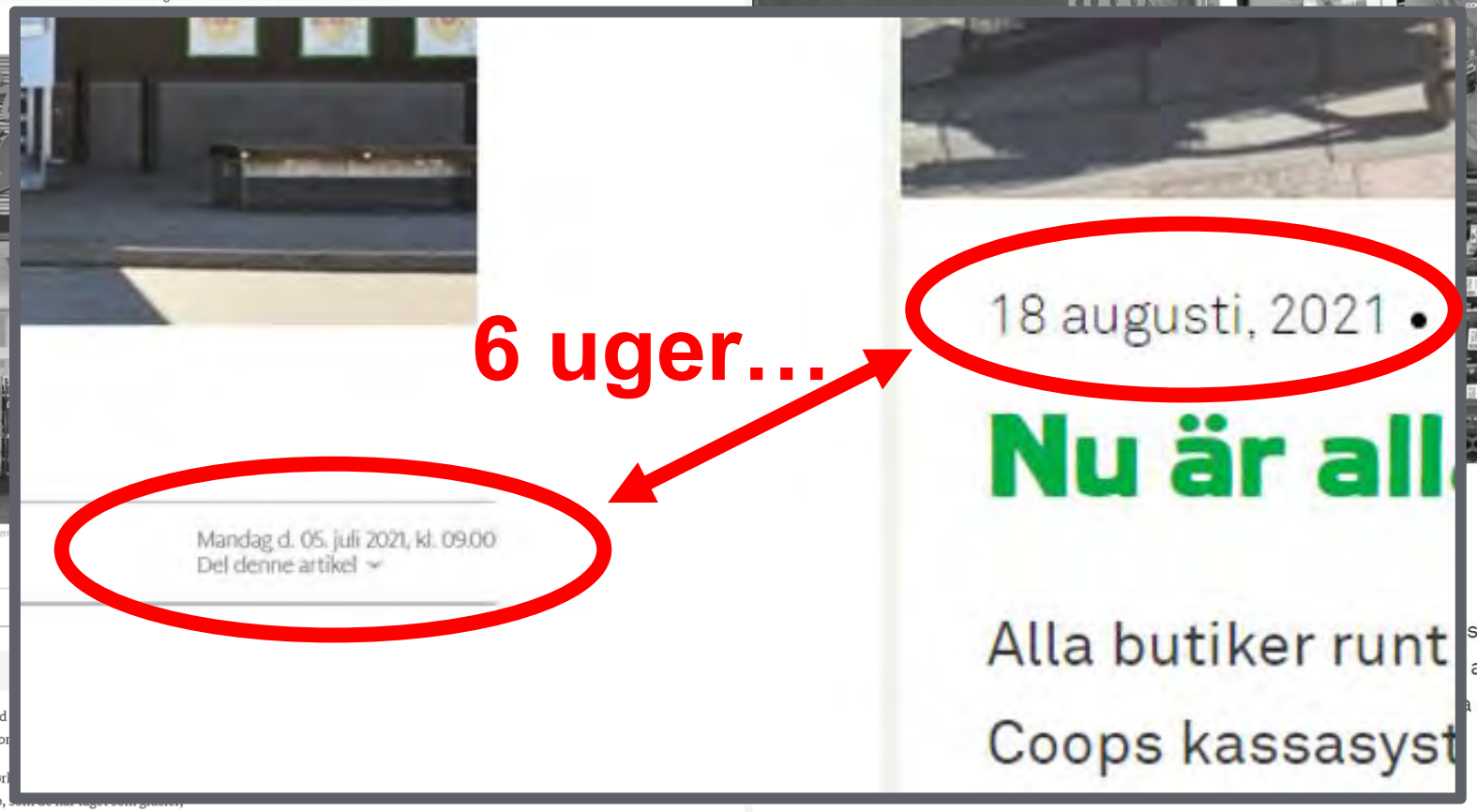
Søndag krævede hackerne i et opslag på den såkaldte mørk
millioner dollar (439 millioner kroner) for låse de data op,
og som har ramt hundredvis af virksomheder verden over.

Opslaget ligger på en blog, som normalt bruges af den berygtede, russiske hackergruppe REvil. It-sikkerhedseksperter anser det for sandsynligt, at det er REvil, der står bag angrebet.

Fredag aften begyndte kassesystemerne at drille

Det ramte fredag det amerikanske it-firma Kaseya i Miami, hvis it-system bruges af it-leverandøren Visma Esscom, som står for systemerne hos Coop i Sverige.

Her begyndte personalet fredag aften omkring klokken 18.30 at melde om problemer.



störningarna som påverkade
av en större global cyberattack
andra svenska och

Läs mer

Hackerangreb koster høreapparatgigant over en halv milliard kroner

Af Louise Kastberg loka@berlingske.dk

Høreapparatkæmpen Demant har nedjusteret sine forventninger til driftsresultatet for 2019 med over 550 mio. kr. som konsekvens af cyberkriminalitet. Investeringsøkonom kalder det en »choknedjustering«.

Den 3. september 2019 blev høreapparatselskabet Demant ramt af et hackerangreb. Som følge af »den kritiske hændelse« meddelte Demant torsdag i en fondsbørsmeddelelse, at selskabet nedjusterer forventningerne til driftsresultatet for 2019.

»Vi har nu været i stand til at vurdere hændelsens finansielle effekt for helåret 2019, selvom vores vurdering fortsat er usikker på dette tidspunkt i genetableringsprocessen. Vores nuværende foreløbige vurdering indikerer en samlet negativ finansiel effekt på EBIT (driftsresultatet, red.) i 2019 i intervallet 550-650 mio. kr., hvilket inkluderer en forventet fratrukket forsikringsdækning på ca. 100 mio. kr.,« står der i meddelelsen.

»Effekten er i altovervejende grad relateret til et estimeret tabt salg samt en svækkelse af vækstmomentum. Vi forventer at afholde omkostninger direkte forbundet med hændelsen på 50 mio. kr., hvilket er inkluderet i den finansielle effekt,« skriver Demant.

»Choknedjustering«

Per Hansen, investeringsøkonom i Nordnet, kalder det en »choknedjustering«.

»Investorerne er ikke overraskede over nedjusteringen, men størrelsen gør meget stort indtryk. Det, som afgør, hvor meget aktien falder, er, om angrebet er blevet inddæmmet. Om sikkerheden nu er så stærk og god, at det ikke kan gentages, og om de økonomiske konsekvenser af nedjusteringen er så stor, at ledelsen har meldt risikoen »godt og vel ud«,« lyder det i en kommentar fra Per Hansen.


Demant A/S (DEMANT)
Senest 212,50
I dag % -2,52%
I dag +/- -5,50
Køb 212,50
Sælg 212,50
Højest 221,50
Lavest 211,70
Omsætning (Antal) 401.670
Oversigt
Om virksomheden
Udvikling
Minimer
Graf
TA
OMX Copenhagen 25
1 år +8,97%
Ransomware
Tuesday 3. September 2019
Monday 2. September 2019
Stock price: 208.40
Monday 10. oktober 2019
Stock price: 161.70
260,00
250,00
240,00
220,00
210,00
200,00
190,00
180,00
170,00
160,00
mar '19
apr '19
maj '19
jun '19
jul '19
aug '19
sep '19
okt '19
nov '19
dec '19
jan '20
feb '20
1d
1u
1m
3m
i år
1 år
3 år
5 år
10 år

GN Store Nord A/S (GN)

Senest	I dag %	I dag +/-	Køb	Sælg	Højest	Lavest	Omsætning (Antal)
384,80	-0,72%	-2,80	384,80	384,80	393,50	381,20	561.863

Oversigt | Om virksomheden

Nordnet

Udvikling

Minimer

Graf

TA | OMX Copenhagen 25

1 år +36,65%

1d | 1u | 1m | 3m | i år | 1 år | 3 år | 5 år | 10 år

Dubex:

BØRSEN.
LEDELSE
torsdag 29. oktober 2020


Foto: Steven Achiam

Topchef: Vi er et andet selskab efter hackerangreb

Søren Nielsen, topchef for Demant, lærte at tage cybertruslen seriøst, da virksomheden blev ramt af et hackerangreb, der kostede over en halv milliard. Eksperter er enige: Med en stigende trussel er der øget behov for, at dansk erhvervsliv sætter fokus på sikkerheden i de øverste lag af organisationen.

Stort tema om datasikkerhed.

Det er den største realtrussel nu om dage for et samlet kollaps af en global virksomhed

Søren Nielsen, topchef i Demant

"Now a days, it is the largest real threat for a total collapse of a global corporation"

We are sorry, but your files have been encrypted!

Don't worry, we can help you to return all of your files!

Files decryptor's price is [redacted] USD

If payment isn't made until [redacted] UTC the cost of decrypting files will be doubled

Time left to double price:

00 days 12h:30m:15s

What the matter? | Buy GandCrab Decryptor | Support is 24/7 | Test decrypt | English

What the matter?

Your computer has been infected with **GandCrab Ransomware**. Your files have been encrypted and you can't decrypt it by yourself.
In the network, you can probably find decryptors and third-party software, but it won't help you and **it only can make your files undecryptable**

What can I do to get my files back?

You should buy **GandCrab Decryptor**. This software will help you to decrypt all of your encrypted files and remove GandCrab Ransomware from your PC.
Current price: [redacted]. As payment, you need cryptocurrency DASH or Bitcoin

What guarantees can you give to me?

You can use test decryption and decrypt **1 file for free**

What is *cryptocurrency* and how can I purchase GandCrab Decryptor?

You can read more details about cryptocurrency at Google or here.
As payment, you have to buy DASH or Bitcoin using a credit card, and send coins to our address.

How can I pay to you?

You have to buy Bitcoin or DASH using a credit card. Links to services where you can do it: Dash exchanges list, Bitcoin exchanges list
After it, go to our payment page Buy GandCrab Decryptor, choose your payment method and follow the instructions

How to recovery your files

Your network targeted by **RobbinHood** ransomware.
We've been watching you for days and we've worked on your systems to gain full access to your company and bypass all of your protections.
You must pay us in **4 days**, if you don't pay in the speficied duration, the price increases **$10,000** each day after the period. After 10 days your keys and your panel will be removed automatically and you won't be able to get your data back. We're watching you, if you want to know who we are, just ask google, don't upload your files to virustotal or services like that, don't call FBI or other security organizations. For security reasons **don't shutdown your systems**, don't recover your computer, don't rename your files, it will damage your files. All procedures are automated so don't ask for more times or somthings like that we won't talk more, all we know is MONEY. If you don't care about yourself we won't too. So do not waste your time and **hurry up!** Tik Tak, Tik Tak, Tik Tak!

What happened to your files?

All of your files locked and protected by a strong encryption with RSA-4096 ciphers.
More information about the RSA can be found here:
https://en.wikipedia.org/wiki/RSA_(cryptosystem)

In summery you can't read or work with your files, But with our help you can recover them.
It's **impossible** to recover your files without private key and our unlocking software (You can google: Baltimore city, Greenville city and RobbinHood ransomware)

Just pay the ransomware and end the suffering then get better cybersecurity

How to get private key or unlocking software?

How to recovery your files

Your network targeted by RobbinHood ransomware.
We've been watching you for days and we've worked on your systems to gain full access to your company and bypass all of your protections.
You must pay us in 4 days, if you don't pay in the speficied duration, the price increases $10,000 each day after the period. After 10 days your keys and your panel will be removed automatically and you won't be able to get your data back. We're watching you, if you want to know who we are, just ask google, don't upload your files to virustotal or services like that, don't call FBI or other security organizations. For security reasons **don't shutdown your systems**, don't recover your computer, don't rename your files, it will damage your files. All procedures are automated so don't ask for more times or somthings like that we won't talk more, all we know is MONEY. If you don't care about yourself we won't too. So do not waste your time and hurry up! Tik Tak, Tik Tak, Tik Tak!

What happened to your files?

In summery you can't read or work with your files, But with our help you can recover them.
It's **impossible** to recover your files without private key and our unlocking software (You can google: Baltimore city, Greenville city and RobbinHood ransomware)

Just pay the ransomware and end the suffering then get better cybersecurity

Just pay the ransomware and end the suffering then get better cybersecurity

How to get private key or unlocking software?

DoppelPaymer

[redacted] Your network has been penetrated.

This link and your decryption key will expire in 21 days after your systems were infected.
Sharing this link or email will lead to the irreversible removal of the decryption keys.

NO TIME remains for special price.

All files on each host in your network have been encrypted with flawless algorythm.

Backups were either encrypted or deleted and backup disks were formatted.

There is no working decryption software that may solve this.

Do not rename the encryted or informational text files. Do not move the encrypted or informational text files.

This may lead to the impossibility of recovery of the certain files.

Also, we have gathered all your private sensitive data.
So if you decide not to pay, we would share it.
It may harm your business reputation.

Online chat

Kilde: COVEWARE Blog -DopplePaymer TOR site as of December 2019

Your network has been breached and all data were encrypted.
Personal data, financial reports and important documents are ready to disclose.

To decrypt all the data and to prevent exfiltrated files to be disclosed at http://hiveleakdbtnp76ulyhi52eag6c6tyc3xw7ez7iqy6wc34gd2nekazyd.onion/
you will need to purchase our decryption software.

Please contact our sales department at:

http://hivecust6vhekztbqgdnkks64ucehqacge3dij3gyrrpdp57zoq3ooqd.onion/

Login: xUvZHAXDfpoW
Password: xvsX47VFucuDKUw4i77C

To get an access to .onion websites download and install Tor Browser at:
https://www.torproject.org/ (Tor Browser is not related to us)

Follow the guidelines below to avoid losing your data:

- Do not modify, rename or delete *.key.21k5p files. Your data will be undecryptable.
- Do not modify or rename encrypted files. You will lose them.
- Do not report to the Police, FBI, etc. They don't care about your business. They simply won't allow you to pay. As a result you will lose everything.
- Do not hire a recovery company. They can't decrypt without the key. They also don't care about your business. They believe that they are good negotiators, but it is not. They usually fail. So speak for yourself.
- Do not reject to purchase. Exfiltrated files will be publicly disclosed.

REvil ransomware gang – Quanta Computer (April 2021)

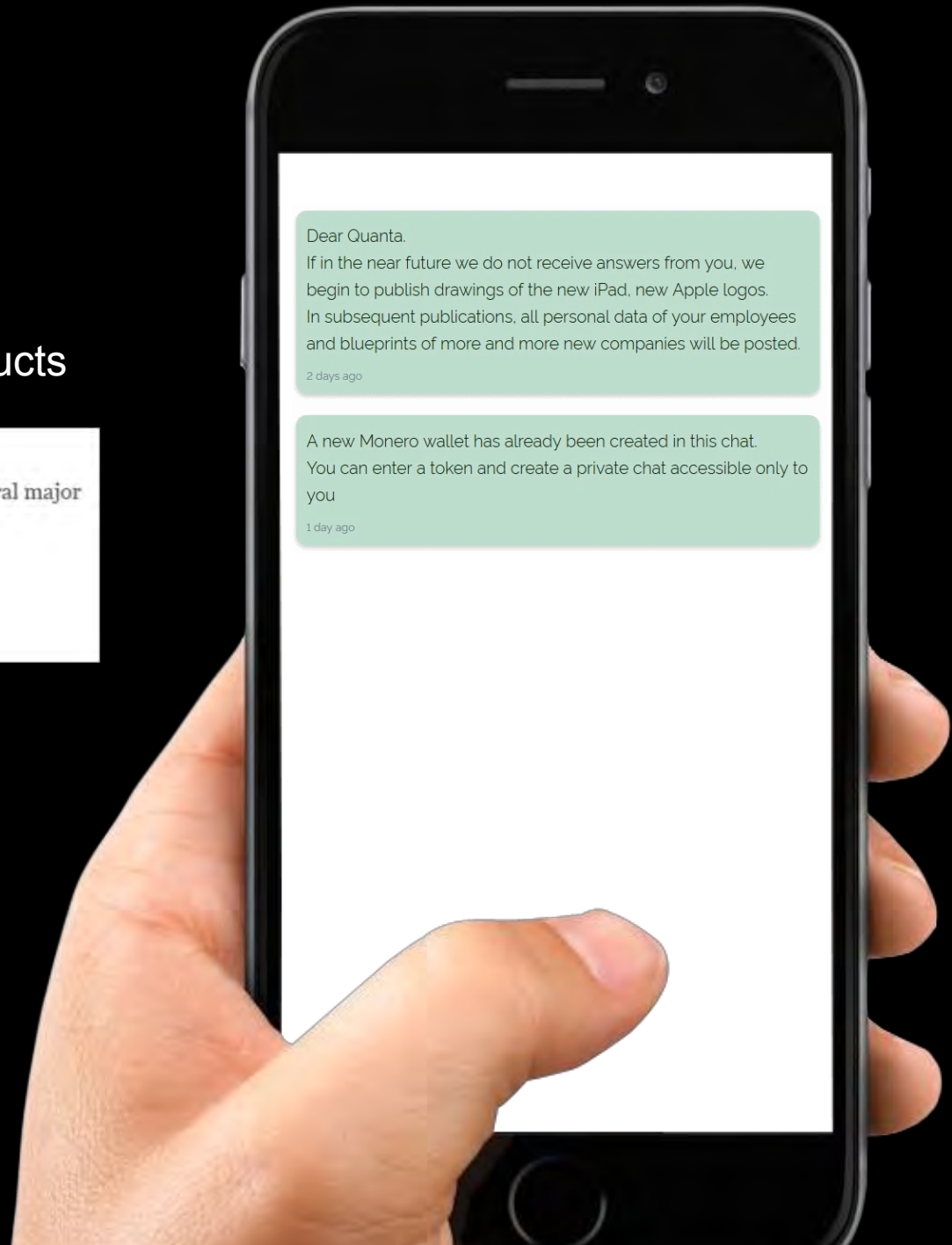
Quanta, a Taiwan-based original design manufacturer (ODM) manufacting Apple Watch, Macbook Air, and Macbook Pro

Revil stole data belonging, including drawings for Apple products

P.S.
Our team is negotiating the sale of large quantities of confidential drawings and gigabytes of personal data with several major brands.
We recommend that Apple buy back the available data by May 1.

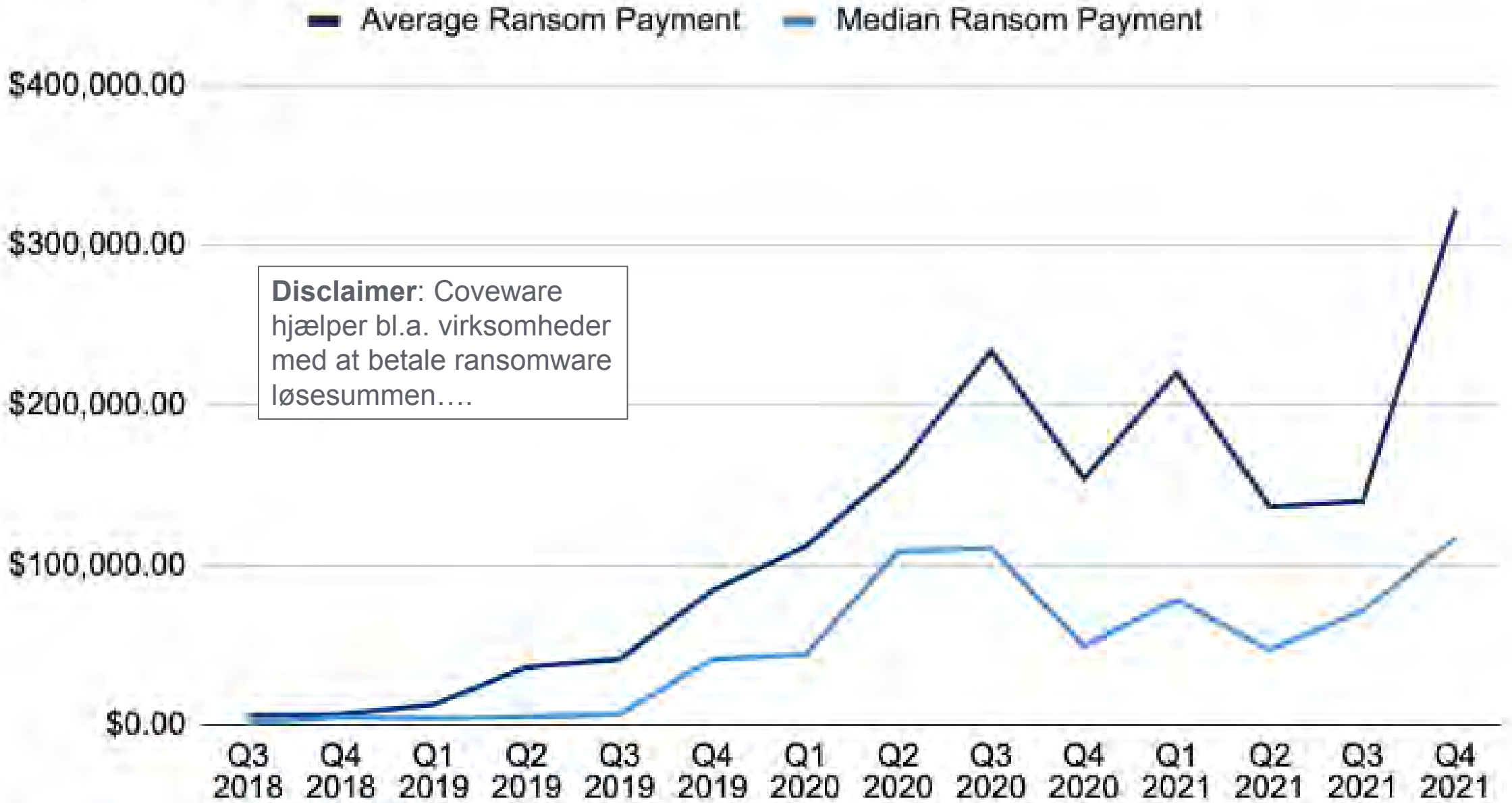
More and more files will be added every day.
The same is in pdf format

Quanta Computer



Dubex:

Ransom Payments By Quarter

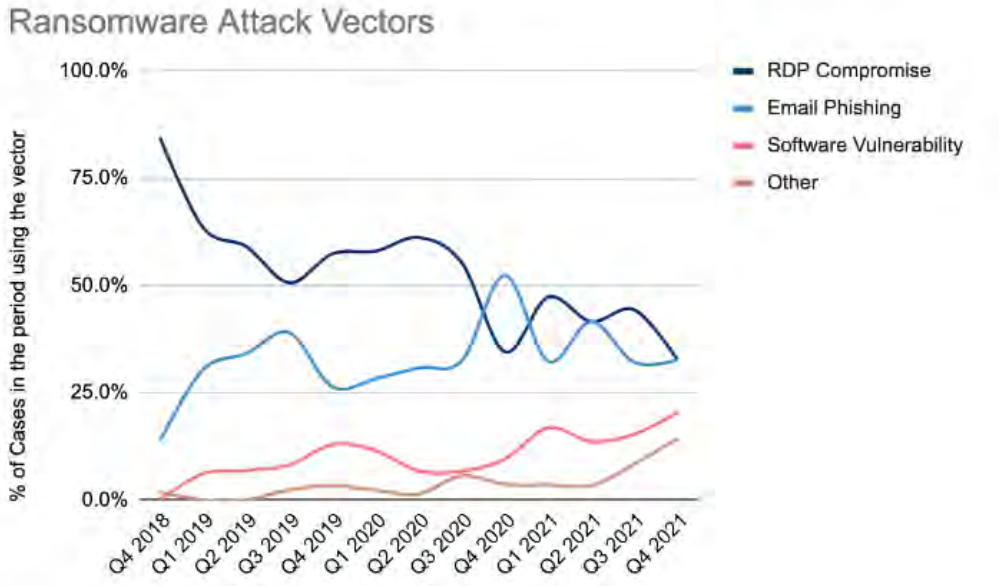


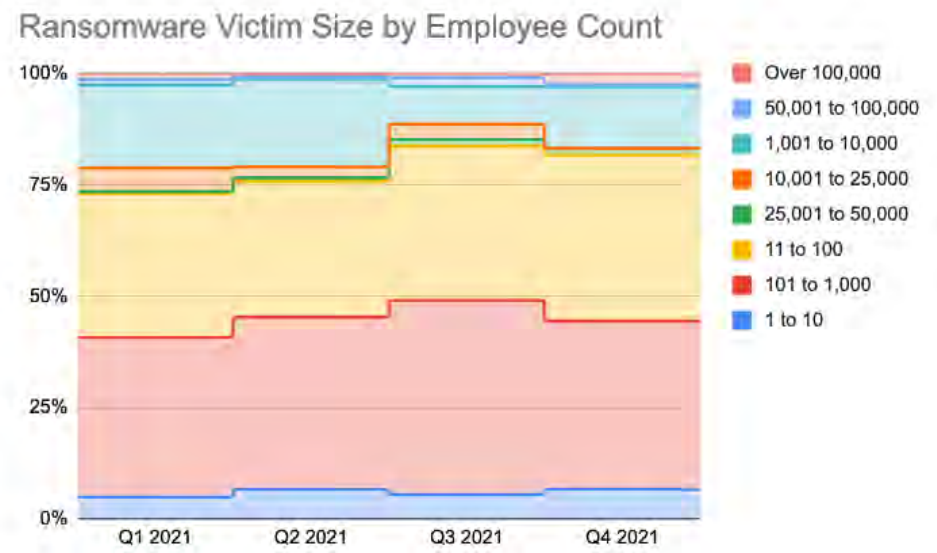
Disclaimer: Coveware hjælper bl.a. virksomheder med at betale ransomware løsesummen….

https://www.coveware.com/blog/2022/2/2/law-enforcement-pressure-forces-ransomware-groups-to-refine-tactics-in-q4-2021

Ransomware Inital Attack Vectors

Remote Access | **E-mail Phishing** | **Vulnerabilities** | **USB** | **Insider attacks**

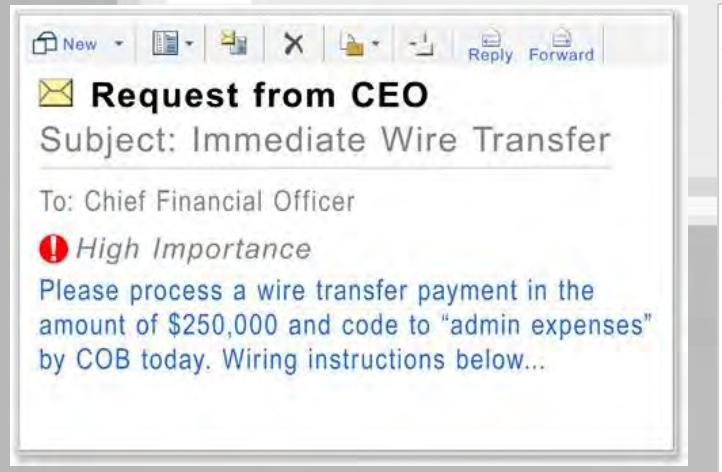


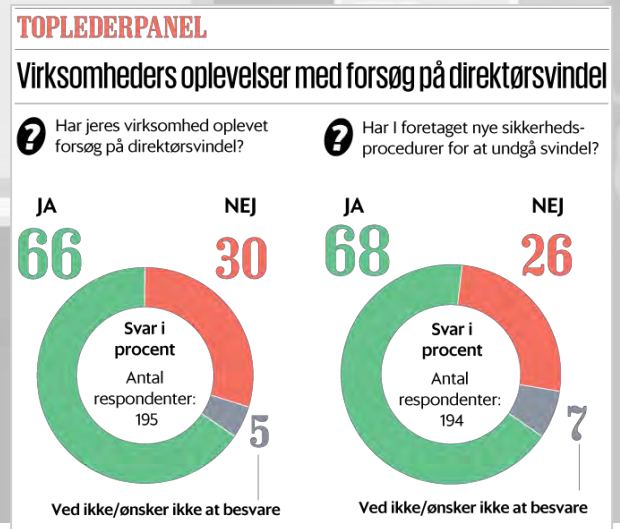


https://www.coveware.com/blog/2022/2/2/law-enforcement-pressure-forces-ransomware-groups-to-refine-tactics-in-q4-2021

Business E-Mail Compromise - CEO/CFO Svindel

- Svindel rettet mod de ansatte der må overføre penge
- Rammer ofte i ferieperioder eller ved fravær
- Målrettet med stor indsats for at få kendskab til virksomhedens ansatte, processer og procedurer
- Hacking af mailsystem anvendes for at kunne sende mails med rigtig afsender og modificere kommunikationen
- Går efter manipulation af eksisterende betalinger og aftaler
- Deep-fake som metode til at udføre svindel





Social medier - hacked

- Hackere overtager adgangen til sociale medier

- Ejeren (virksomheden / personen) kan hereafter "købe" adgang til kontoen tilbage

VIRKSOMHEDSCASE

› Fra lav it-sikkerhed til styrket tillid

Hackere overtog Facel
Stofbanditten genvanc
tilmed tilliden blandt
hackerangrebet, der s
endte med at styrke fo

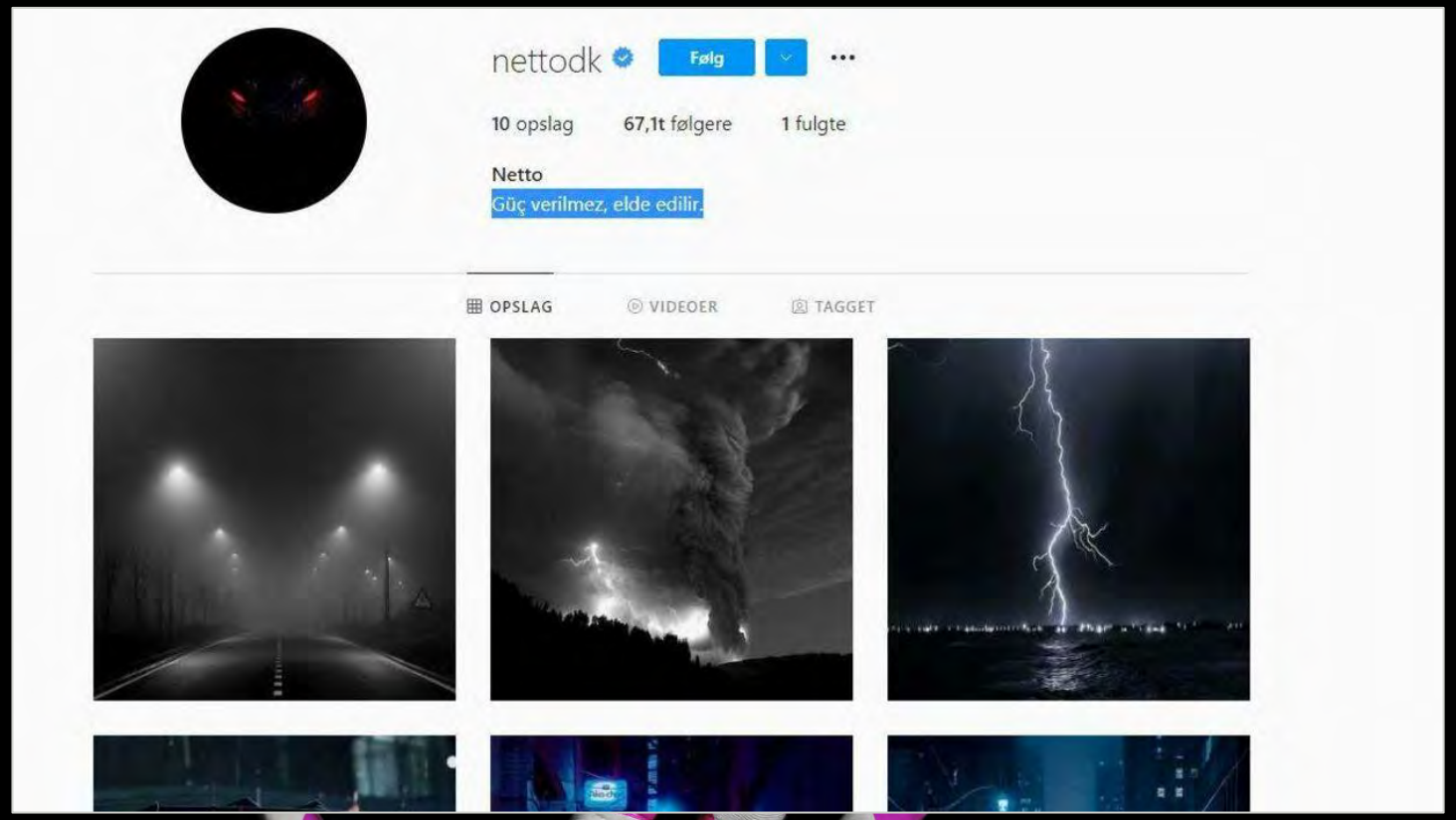
› Se video og læs me

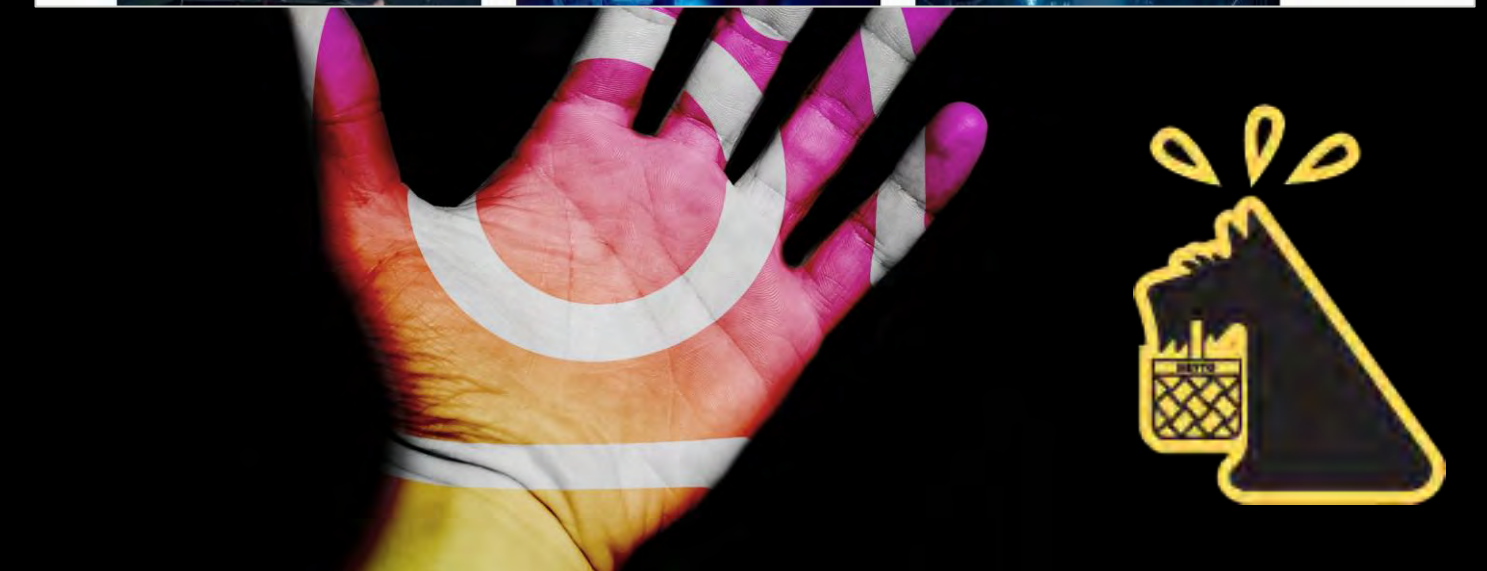
sikker digital DK

VIRKSOMHEDSCASE

› Stærkere sikkerhed - og en ren 'love storm'

https://www.dr.dk/nyheder/indland/marie-louise-og-thomas-stod-uden-hjaelp-da-de-fik-hacket-instagram-kontoen-det-er





Michael Løve • 2nd
Direktør, Netto
1d •

+ Follow

Netto, Salling Groups Instagram profil er kommet i karantæne efter at den blev hacket for en uge siden.

Vi har ca. 70k følgere og i den seneste uge har de kunne se billeder, som har undret mange. Billederne er selvfølgelig lagt op af hackerne og helt efter drejebogen har de også krævet penge for at give Netto kontrol over sin Instagram profil igen.

Der er ikke andet i Netto, som er hacket, og der er ingen risiko for vores Instagram følgere. Vi samarbejder tæt med Instagram om at få kontrollen tilbage og vi beklager selvfølgelig situationen meget. Men vi har også besluttet at vi hellere vil leve med forvirringen end betale hackerne.

Til alle jer der bruger sociale medier skal også her lyde en opfordring til at sikrer jer mod hacking. Skift password jævnligt, brug 2-faktor godkendelse og log alle enheder af engang imellem.

See translation

Der er ikke andet i Netto, som er hacket, og der er ingen risiko for vores Instagram følgere. Vi samarbejder tæt med Instagram om at få kontrollen tilbage og vi beklager selvfølgelig situationen meget. Men vi har også besluttet at vi hellere vil leve med forvirringen end betale hackerne.

Til alle jer der bruger sociale medier skal også her lyde en opfordring til at sikrer jer mod hacking. Skift password jævnligt, brug 2-faktor godkendelse og log alle enheder af engang imellem.

Michael Løve • 2nd
Direktør, Netto
1d •

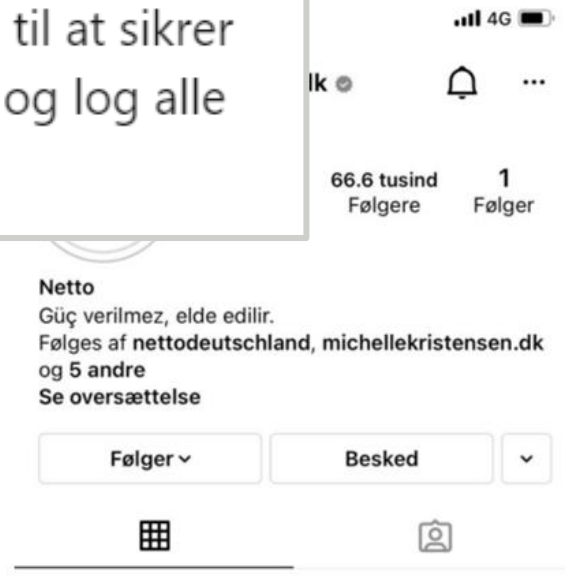
+ Follow •••

Netto, Salling Groups Instagram profil er kommet i karantæne efter at den blev hacket for en uge siden.

Vi har ca. 70k følgere og i den seneste uge har de kunne se billeder, som har undret mange. Billederne er selvfølgelig lagt op af hackerne og helt efter drejebogen har de også krævet penge for at give Netto kontrol over sin Instagram profil igen.

g der er ingen risiko for vores
l Instagram om at få kontrollen tilbage
get. Men vi har også besluttet at vi
hackerne.

gså her lyde en opfordring til at sikrer
rug 2-faktor godkendelse og log alle



Supplychain angreb

- Angreb mod virksomhedens leverandører
- Angreb på virksomheden via deres leverandør

Equipment: routers, servers, tablets, phones, storage, devices etc.

Services: data processing, IaaS, PaaS, SaaS, data feeds, cloud and managed service etc.

Software: common-off-the-shelf (COTS) and proprietary etc.

Connectivity: Different kinds of communication, Internet, 4G/5G etc.

AK TECHOTEL

Natten til torsdag begyndte et regulært mareridt for AK Techotel, der står bag it-systemet Picasso.

Systemet er brugt af cirka 900 hoteller verden over, men siden onsdag klokken 02, har det været nede.

Det er ondsindede hackere, der står bag nedbruddet, og de har ikke villet 'løslade' booking-systemet, før de har fået en stor løsesum betalt i kryptovalutaen Bitcoin.

Et af de berørte hoteller er Helnan Marselis Hotel i Aarhus, hvor hotelreceptionist Kamilla Rasmu
på sit bord.

TIP OS

Kender du til sagen? Så tip os
her.

papirarbejde, samtidig med vi s
lovgivningen,« siger hun til B.T. t

Men det er håb forude, om end c
driftsinformation, hvor man kan
har AK Techotel meget udførligt

Her lyder det, at de er ramt af ra
hvor man tager et system eller d
Hvis man vil åbne dataen eller p
program til at låse krypteringen

Den nøgle sælger hackerne, til d

VIRKSOMHEDSCASE

› Vores leverandør blev hacket

Selv et internationalt hacker-angreb kunne ikke lægge Hotel Bredehus ned. De tog slagene, men står nu stærkere end nogensinde før. Få historien om, hvordan man kan rejse sig igen, når ens leverandør rammes af et hackerangreb.

› Se video og læs mere om Bredehus Hotel

Hacking Inc.

"Traditional" Organized Cybercriminals	Money Mules
Malware Writer	Inject Writer
Exploit Kit Load Vendor	Network and System Admin
Data Processing Specialists	Network Exploitation Specialists
Service Providers	Cyber-criminal Recruitment

BITCOIN MAKES THE WORLD GO ROUND…

Cybercrime To Cost The World $10.5 Trillion Annually By 2025

https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

Stater og efterretningstjenester

Cyberangreb er billige, nemme, effektive og risikofri

- Cyber-spionage
- Propaganda og indblanding - påvirkning på bl.a. sociale medier
- Samarbejde mellem stater og kriminelle

Alle lande kan udføre angreb med små midler

- Risiko for angreb mod fysiske mål fx olieproduktion
- Målrettede angreb på virksomheder og personer
- Risiko for ”følgeskader” hos virksomheder

Politisk motiveret hacking og tiltag

- Konsekvenser for cyberangreb drages politisk, socialt og økonomisk
- Opdeling eller lukning af Internettet – fx Kina, Rusland og Indien
- Lav-intensitetskrige føres allerede mellem USA, Kina, Rusland, Iran og Nord Korea

Supply-chain

- Hvem og hvilke produkter kan vi egentlige stole på

Russia's Cyber Operations Groups

Russia is a powerful cyber actor

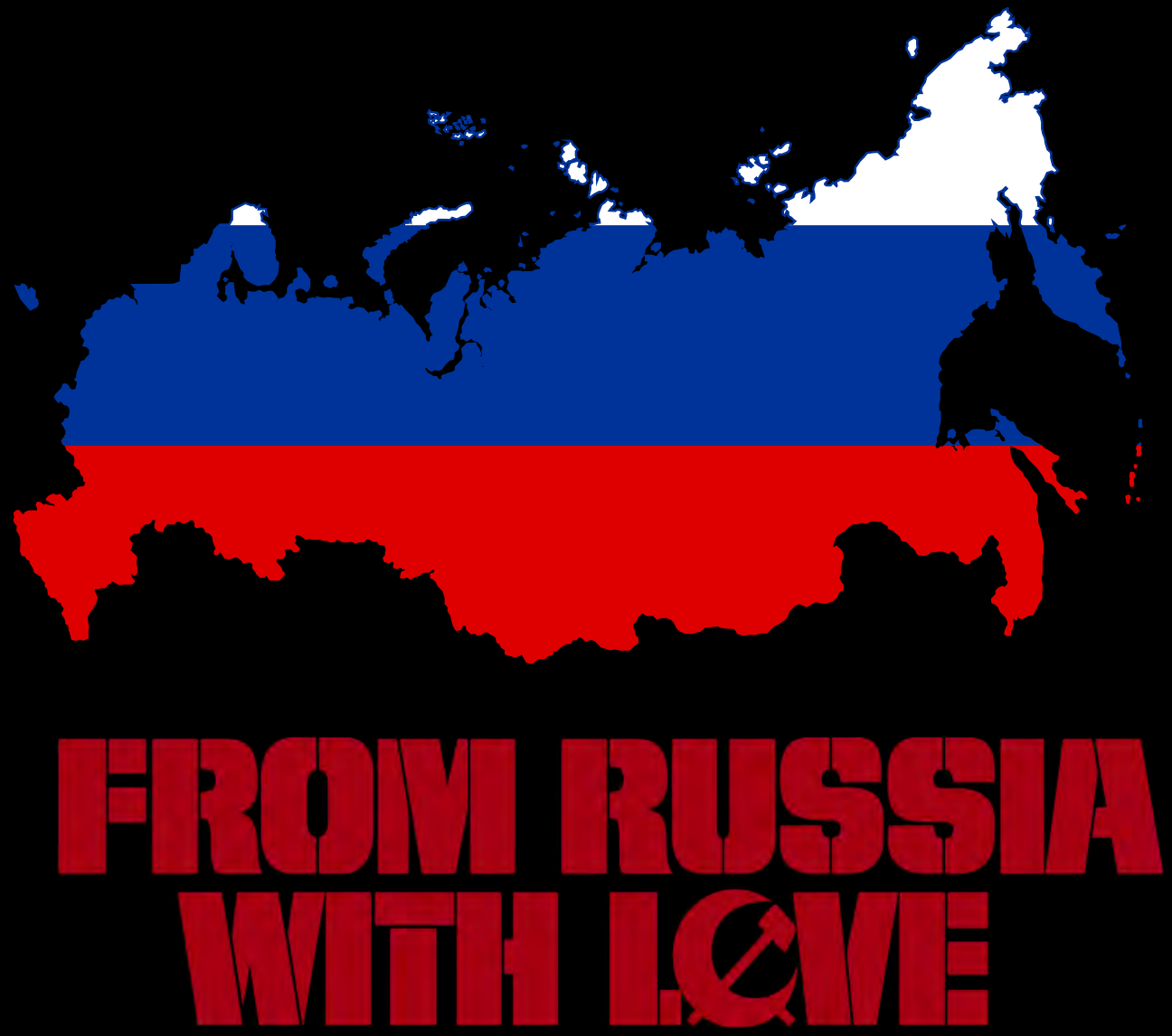
Intelligence services: FSO, FSB, SVR & GRU working with criminal actors

Not afraid to combine different coordinated attacks in cyber space and physically to meet its strategic objectives

Long-term experience and building offensive cyber capabilities since at least 1996 (Moonlight Maze)

Uses many different TTPs in their attacks

History of Russian cyberwarfare on Ukrainian
- 2013: Armageddon & Turla – spying
- 2015/16: BlackEnergy and CrashOverride
- 2017: NotPetya



Dubex:

What have happened so far in Ukraine?

DDoS on Government, Military, Financial and Telco

Destructive wipers:
- WhisperGate (13 Jan 2022)
- HermeticWiper / FoxBlade (23 Feb 2022)

Espionage: Ukraine, also internationally (CISA Alert AA22-047A)

Defacement of websites

Attacks:
- Supply chain attacks (software supplier Kitsoft)
- Vulnerability in the October CMS (CVE-2021-32648)
- Log4Shell

Influence operations / Disinformation using SMS message, social media, and other media

BEWARE of False Flag operations!!

Dubex:

Current status and other observations

Most current attacks in Ukraine are DDoS with very small risk for spillover to Danish companies

Businesses with relationships with Ukraine should be extremely cautious – attacks in Ukraine up 196% in three days

Services reconnaissance scans has been increasing since mid-January

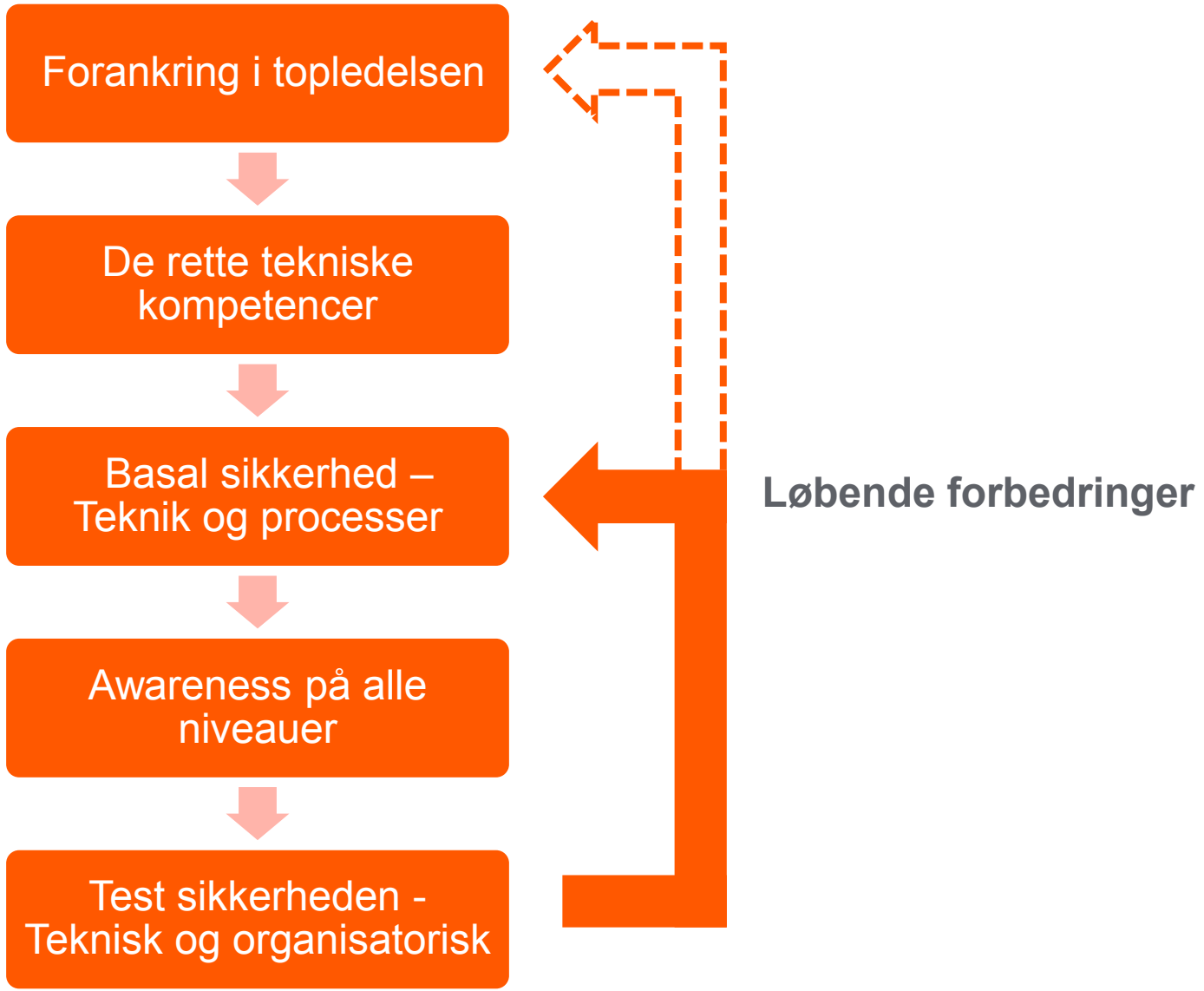
Conti (world biggest ransomware group) supporting Russia -> internal data leaked by Ukrainian worker
Conti ransomware attack on Danish company Lifa – most likely no connection to Ukraine
DDoS attack on Nordea in the Nordics – so far no indication on connection to Ukraine

Anonymous has declared cyberwar on Russia

Widespread phishing campaign from Russia attempting to compromise account credentials – targeting manufacturing and international shipping and transportation in the US/Europe

No indications of targeted attacks on Danish organizations however prepare for this can change very quickly

Dubex:


Forankring i topledelsen
De rette tekniske kompetencer
Basal sikkerhed – Teknik og processer
Awareness på alle niveauer
Test sikkerheden - Teknisk og organisatorisk
Løbende forbedringer

Dubex:

Bestyrelsesforeningens
Center for Cyberkompetencer

Vejledninger og anbefalinger for bestyrelser

Styrkelse af Strategiske Cyberkompetencer

3 årigt projekt 2019-2022 støttet af Industriens Fond

Målet er at gøre cybersikkerhed til en **konkurrencefordel** for danske virksomheder, for dansk **erhvervsliv og for samfundet som helhed**.

Dubex:

https://bestyrelsesforeningen.dk/styrkelse-af-strategiske-cyberkompetencer/

4. Temaer i en cybersikkerhedsstrategi

Virksomheders arbejde med cyber- og informationssikkerhed handler om mere end IT. Det handler i høj grad også om governance, ledelse, processer og mennesker. Sikkerhed er i sidste ende bestyrelsens ansvar, og bør være et vigtigt emne på bestyrelsens dagsorden. Cybertruslen er reel, og virksomheder er nødt til at have en strategi for at håndtere den.

De overordnede fokusområder i cybersikkerhedsstrategi er at kunne identificere, forebygge og beskytte, opdage og håndtere cyberhændelser, samt at kunne sikre genoprettelse af data, systemer, drift og omdømme efter en hændelse. Fokusområderne er inspireret fra internationale anerkendte rammeværker for håndtering af cybersikkerhed, f.eks. NIST-standarden: Identify, Protect, Detect, Respond, Recover.

Som grundprincip for sikkerhedsniveauet skal bestyrelsen arbejde ud fra, at virksomheden skal træffe *"passende og forholdsmæssige tekniske og organisatoriske foranstaltninger"* baseret på en konkret risikovurdering. Dette krav findes i nogenlunde enslydende bestemmelser i gældende regulering på sikkerhedsområdet, og anses for best practice.

Gældende regulering er sparsom med eksempler på, hvad der udgør "*passende og forholdsmæssige tekniske og organisatoriske foranstaltninger*". Det er derfor i høj grad op til den enkelte bestyrelse og virksomhed at finde den rette balance mellem risikoappetit og sikkerhedsniveau samt at fastlægge en strategi for styring af cyberrisici. Regulering og compliancekrav også til IT sikkerhed er dog aktuelt hastigt voksende, og det anbefales at inkludere udvikling i relevant regulering i den løbende rapportering.

Arbejdet med cybersikkerhedsstrategi er en ledelsesopgave på øverste niveau og omfatter alle afdelinger og funktioner i en virksomhed. Det kræver IT-forståelse, men er IKKE en IT-opgave. Arbejdet med cybersikkerhedsstrategi omfatter 6 temaer, som sammen med fokusområderne nævnt ovenfor, skal besluttes i bestyrelseslokalerne.

5 overordnede formål med en cybersikkerhedstrategi

1. **Identificer** virksomhedens risici og sårbarheder.
2. **Beskytte** virksomheden mod et cyberangreb.
3. **Opdage** hvis/når et angreb sker.
4. **Håndtere** et angreb hvis/når det sker.
5. **Genoprette** evt. ramte systemer og data.

Generelt krav til sikkerhedsniveauet

Virksomheden skal træffe passende og forholdsmæssige tekniske og organisatoriske foranstaltninger, der sikrer et sikkerhedsniveau, der passer til risikoen.

6 temaer i en cybersikkerhedsstrategi

1. Risikovurdering og sårbarheder
2. Risikoappetit og strategi
3. Planer, processer og beredskab
4. Rapportering og kontrol
5. Kultur og mennesker
6. Kompetencer og organisering

4. Temaer i en cybersikkerhedsstrategi

Virksomheders a… …rhed handler om mere end IT… processer og m… ansvar, og bør v… Cybertruslen e… for at håndtere…

De overordnede fo… og beskytte, opdag… data, systemer, dri… internationale ane… standarden: Ident…

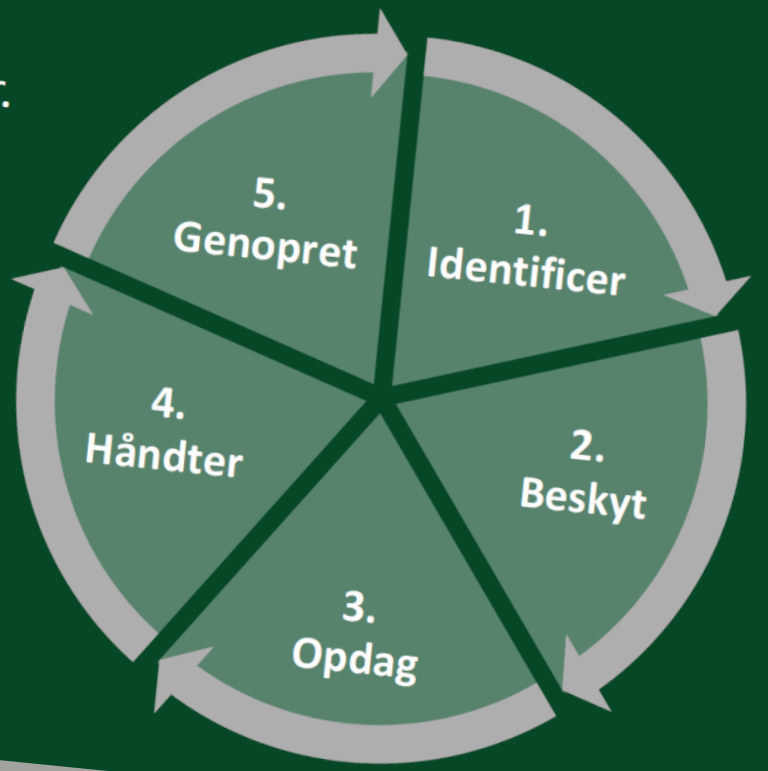
Som grundprinci… skal træffe *"pass…* baseret på en ko… bestemmelser i…

Gældende regu… *forholdsmæssig…* den enkelte be… sikkerhedsnive… compliancekrav også til IT sikkerhed… inkludere udvikling i relevant regulering i den løbende rapportering.

Arbejdet med cybersikkerhedsstrategi er en ledelsesopgave på øverste niveau og omfatter alle afdelinger og funktioner i en virksomhed. Det kræver IT-forståelse, men er IKKE en IT-opgave. Arbejdet med cybersikkerhedsstrategi omfatter 6 temaer, som sammen med fokusområderne nævnt ovenfor, skal besluttes i bestyrelseslokalerne.

5 overordnede formål med en cybersikkerhedstrategi

1. **Identificer** virksomhedens risici og sårbarheder.
2. **Beskytte** virksomheden mod et cyberangreb.
3. **Opdage** hvis/når et angreb sker.
4. **Håndtere** et angreb hvis/når det sker.
5. **Genoprette** evt. ramte systemer og data.



5 overordnede formål med en cybersikkerhedstrategi

1. **Identificer** virksomhedens risici og sårbarheder.

…kniske

…ltur og …ennesker

2. Risikoappetit og strategi

…kontrol

…ompetencer …g organisering

Identificer
(Predict & identify)

Beskyt
(Prevent & protect)

Opdag
(Detect)

Håndter
(Respond)

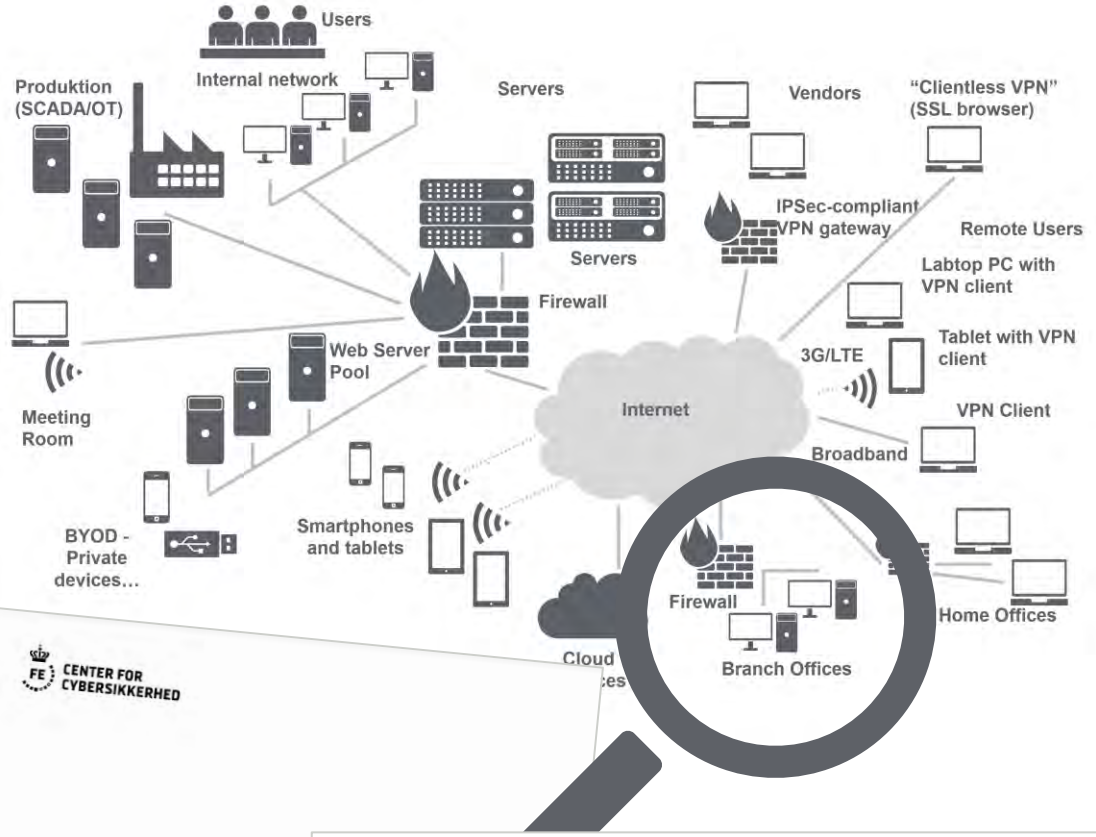
Genopret
(Recover)

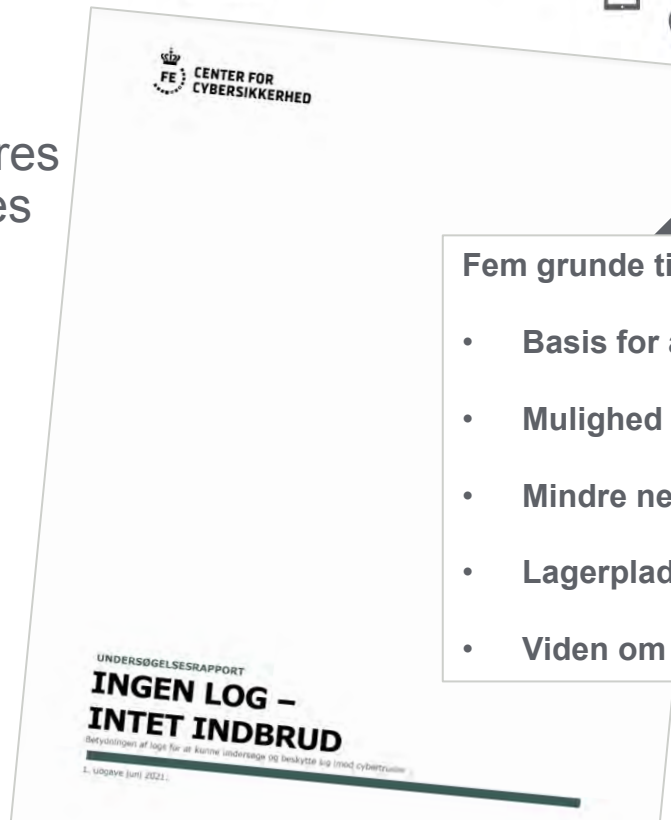
Dubex:

Hvorfor logning og overvågning?

- For at opdage en hændelse eller kompromittering skal der kikkes efter den
- Opdagelse er baseret på systematisk opsamling og analyse af alle relevante sikkerhedsdata (logdata) fra infrastrukturen
- Vigtigt med effektive use-cases så der alarmeres relevant og antallet af falske positive minimeres
- Vigtigt med processer og kompetencer
- Systematisk opsamling og analyse af logfiler tillader mere effektiv incident håndtering

Dubex:

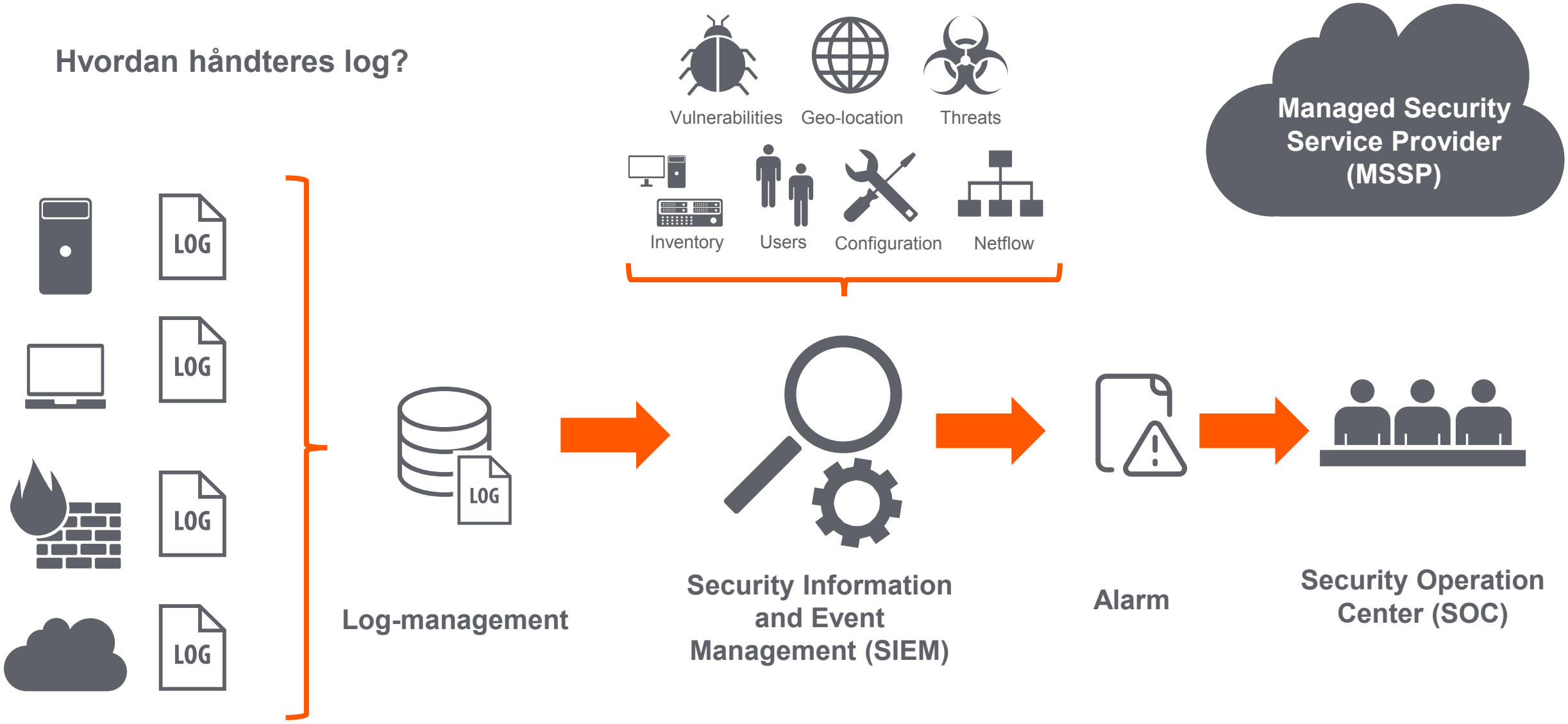




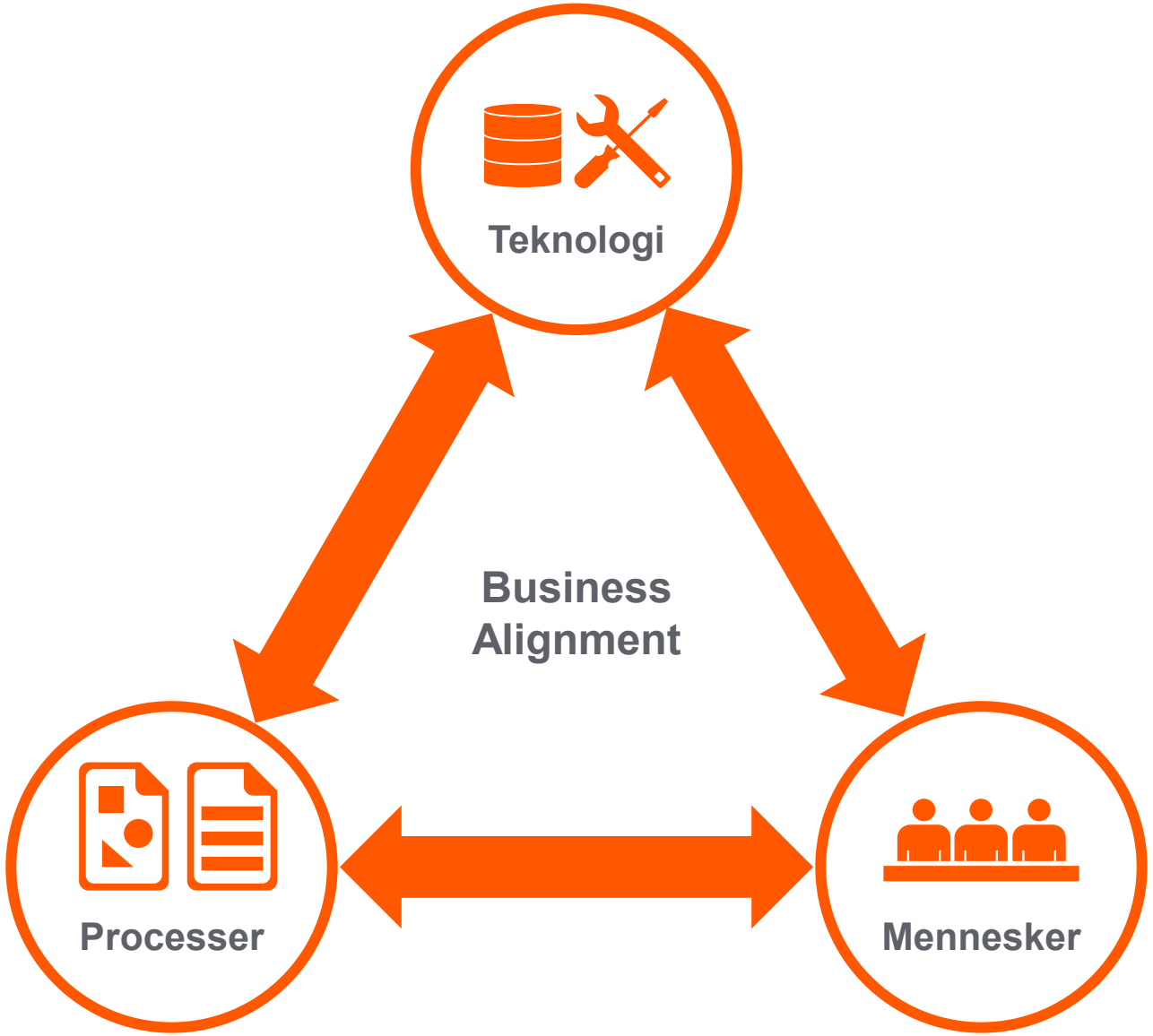
Fem grunde til at prioritere logning

- **Basis for at undersøge et cyberangreb**
- **Mulighed for at kende omfanget af cyberangreb**
- **Mindre nedetid i forbindelse med cyberangreb**
- **Lagerplads er billigt**
- **Viden om normalbilledet i netværket**

Hvordan håndteres log?



Dubex:



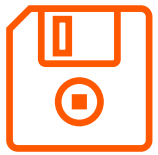
Dubex:

Top fem anbefalinger – kom i gang nu

To-faktor brugervalidering til al ekstern adgang

Overblik - se virksomheden udefra

Opdater programmer – fjern sårbarheder



Backup – og helst offline

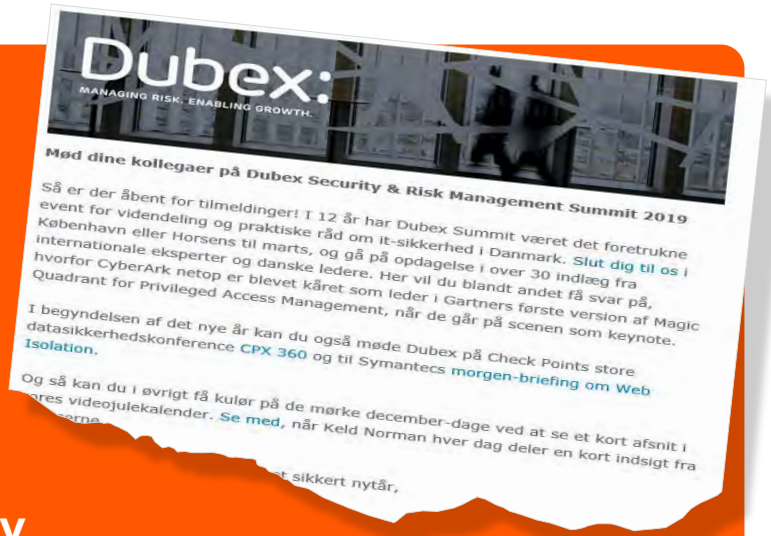
Beredskabsplan - husk at teste

… og så brug din sunde fornuft

Dubex:

Hold dig opdateret

Abonnér på Dubex' nyhedsbrev



www.dubex.dk/aktuelt/nyhedsbrev

Følg Dubex på LinkedIn & Twitter

twitter.com/Dubex

LinkedIn

www.linkedin.com/company/dubex-as

Deltag på Dubex' arrangementer

www.dubex.dk/aktuelt/events

Dubex.

Hold dig opdateret

Dubex.

TAK!

#SammenSikrerViDanmark

Jacob Herbst

jhe@dubex.dk

+45 2083 0430

Dubex A/S
Gyngemose Parkvej 50
DK-2860 Søborg

www.dubex.dk
+45 3283 0430
info@dubex.dk

Find os på Linkedin og Facebook