IDA Driving IT København 2021

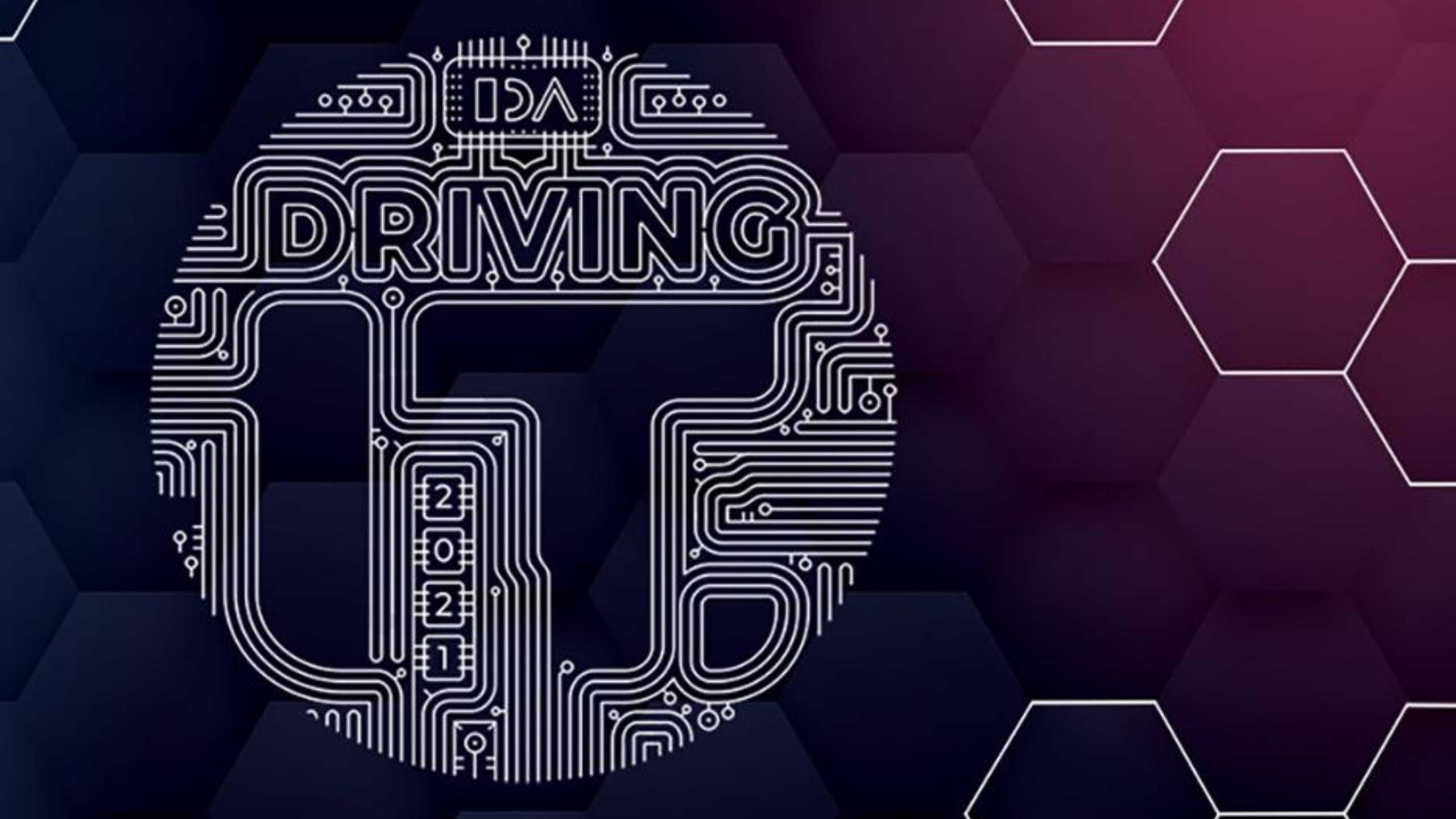
Cybersikkerhed 2022 – angreb og forsvar

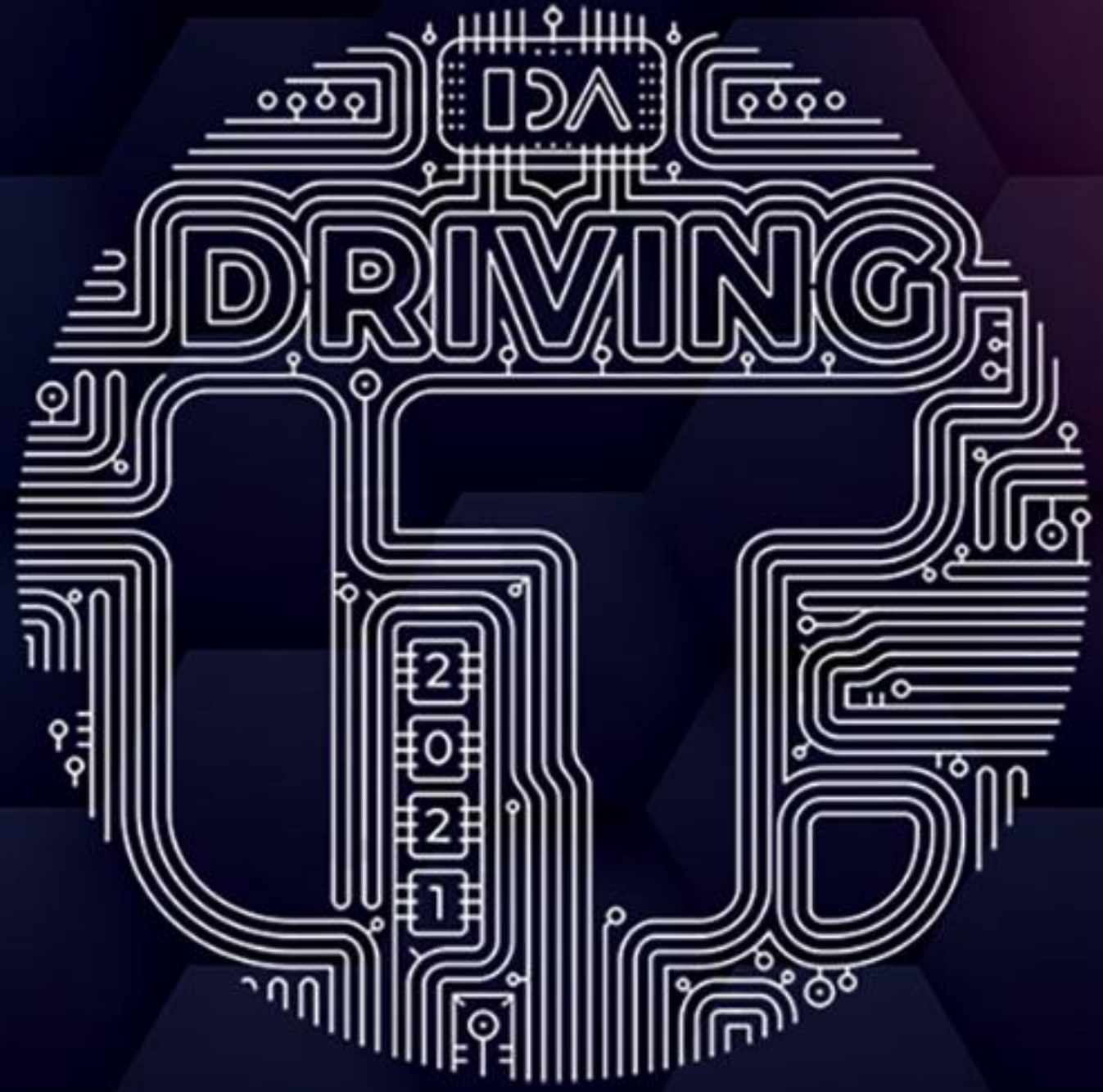
Jacob Herbst

IDA København

Den 5. november 2021

Dubex:


DRIVING
2021



IT DRIVING

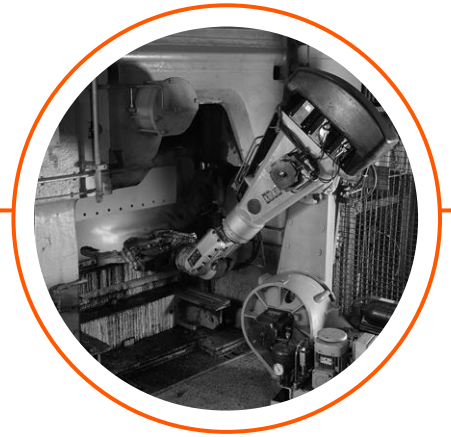
The industrial revolutions - the short story

”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

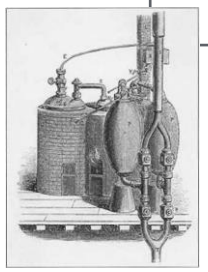


Computers
Automation using electronics and simple computers (PLCs)

Digitization
Information and communication technology

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

Steam Engine (1784)



First assembly line Cincinnatic Slaughterhouse (1870)

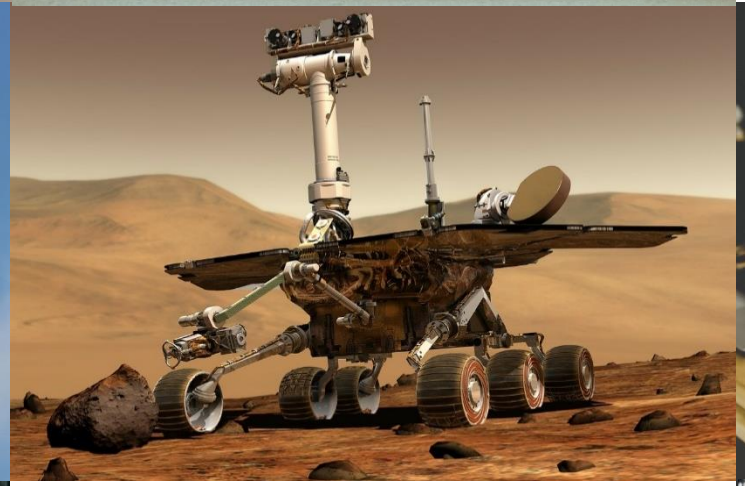
First modern PLC - Modicon 084 (1969)

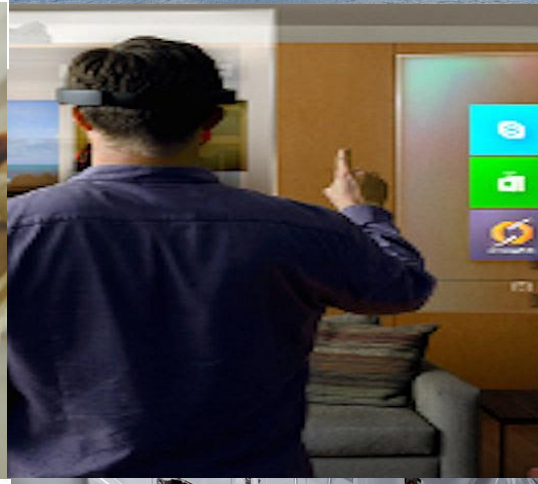
Dubex:


DIGITAL DISRUPTION
Cloud Computing
Internet of Services
Bring Your Own
Internet of Things (IoT)
Social Media
Robots
Computer Vision
Digital Twin
Mobility
Artificiel Intelligence (AI)
Machine Learning
3D Printing
Big Data Analytics
Virtual Reality
Argumented Reality
Software Defined Anything


HYUNDAI DRIVE


amazon





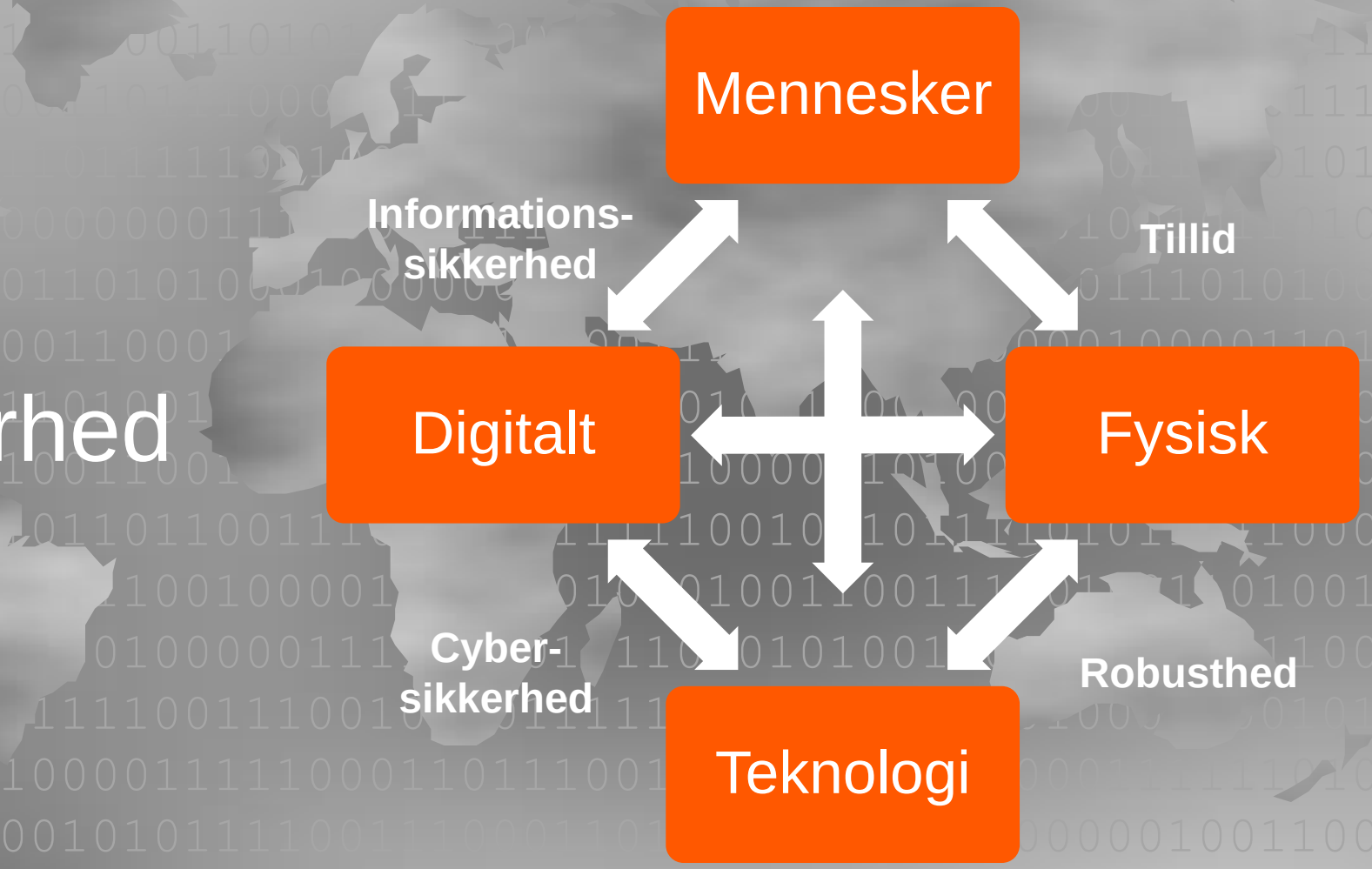

ST. JUDE MEDICAL
ASSURITY MRI™
PM1272 SSR
S/N1234567
ST. JUDE MEDICAL
ASSURITY MRI™
PM2272 DDDR
S/N1234567

ALL COMPANIES ARE DIGITAL COMPANIES

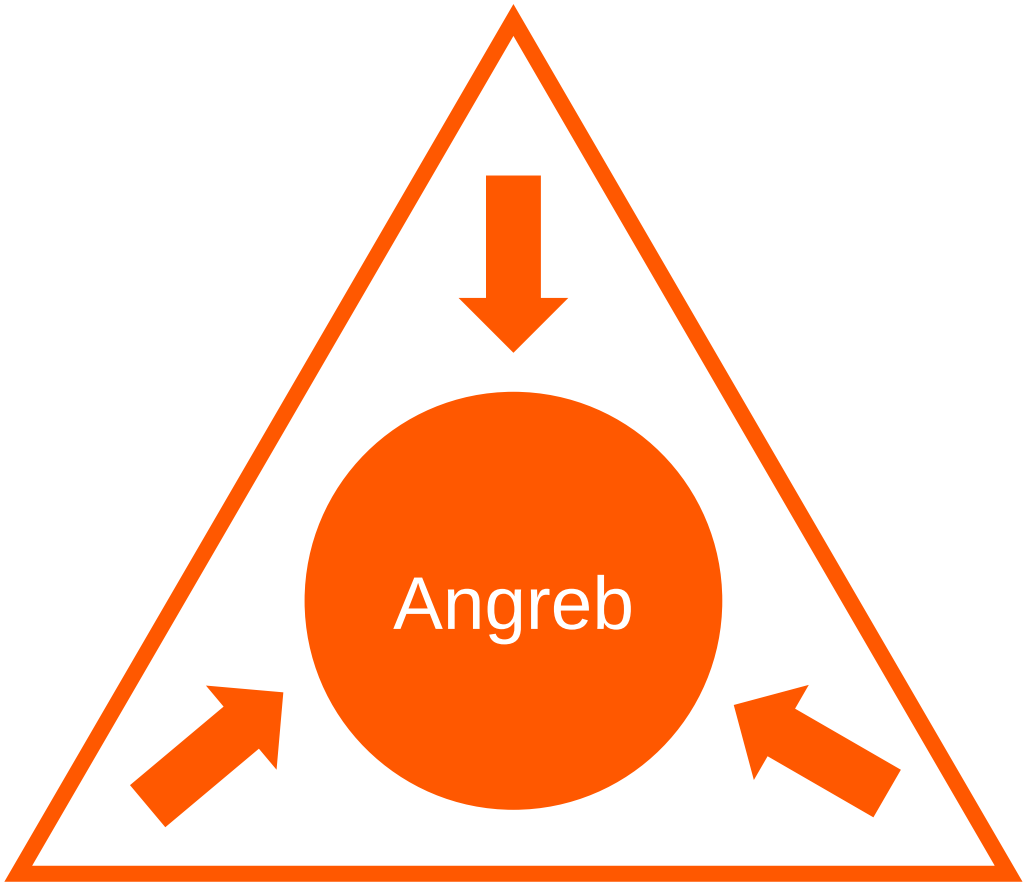
– Some Just Don’t Know It


...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


Danish Agro


KALUNDBORG
FORSYNING


JBS


DESMI

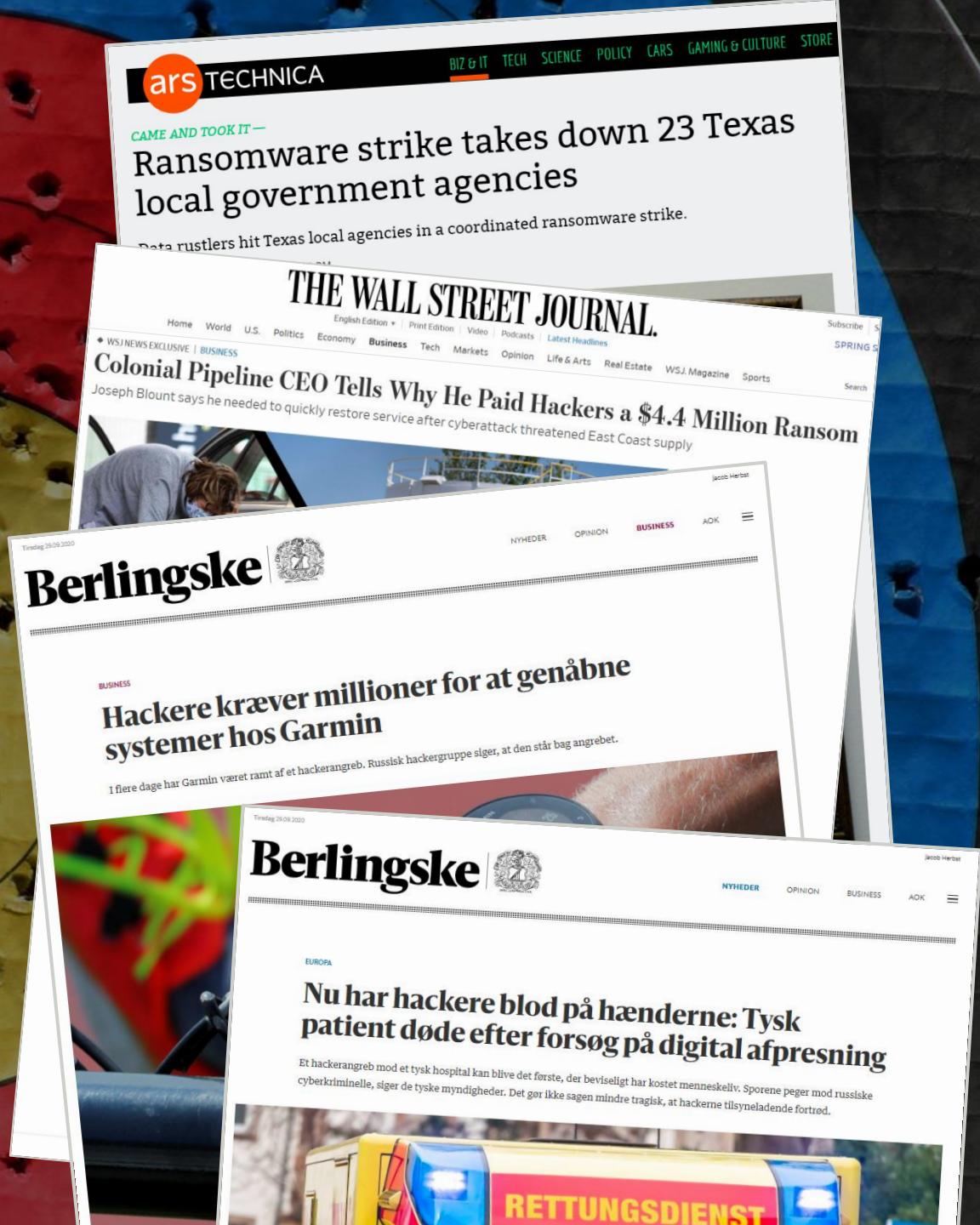

Seirbhís Sláinte
Níos Fearr
á Forbairt
Building a
Better Health
Service


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…

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
journalist

Mandag d. 05. juli 2021, kl. 09.00
Del denne artikel

Lyt til artiklen 3 min

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
journalist

Mandag d. 05. juli 2021, kl. 09.00
Del denne artikel

Lyt til artiklen 3 min

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

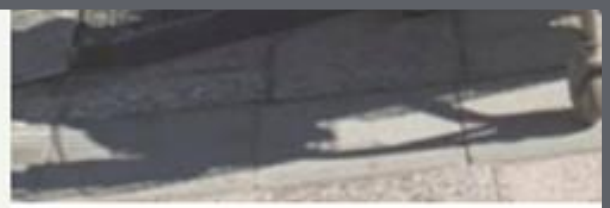
NYHEDER OPINION BUSINESS AOK

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

Mandag d. 05. juli 2021, kl. 09.00
Del denne artikel



18 augusti, 2021 •

Nu är all

Alla butiker runt

Coops kassasyst

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

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.

"We are aware of a 3rd party IT company working on your network. We continue to monitor and know that you are installing antivirus on all your computers.
But you should know that it will not help.
If you want to stop wasting your time and recover your data this week, we recommend that you discuss this situation with us in the chat ***or the problems with your network will never end****."*

Cyber Extortion Ecosystem

Motivations used by ransomware gangs

- Cold-calls to threaten victims preparing to restore data from backups
- Personal threats against the executives responsible for approving the ransom payment
- Threatened to notify business partners
- Threatened companies with DDoS attacks
- Threatened companies to notify journalists about their security breaches
- Threatened to notify privacy watchdog agencies about a breach so the company can get fined
- Sent emails to a victim's clients, asking the customers to put pressure on the company to pay its ransom demand and avoid having the customers' data leaked online
- Notify crooked market traders in advance so they can short a company's stock price

Dubex:

REvil ransomware gang – Quanta Computer (April 2021)

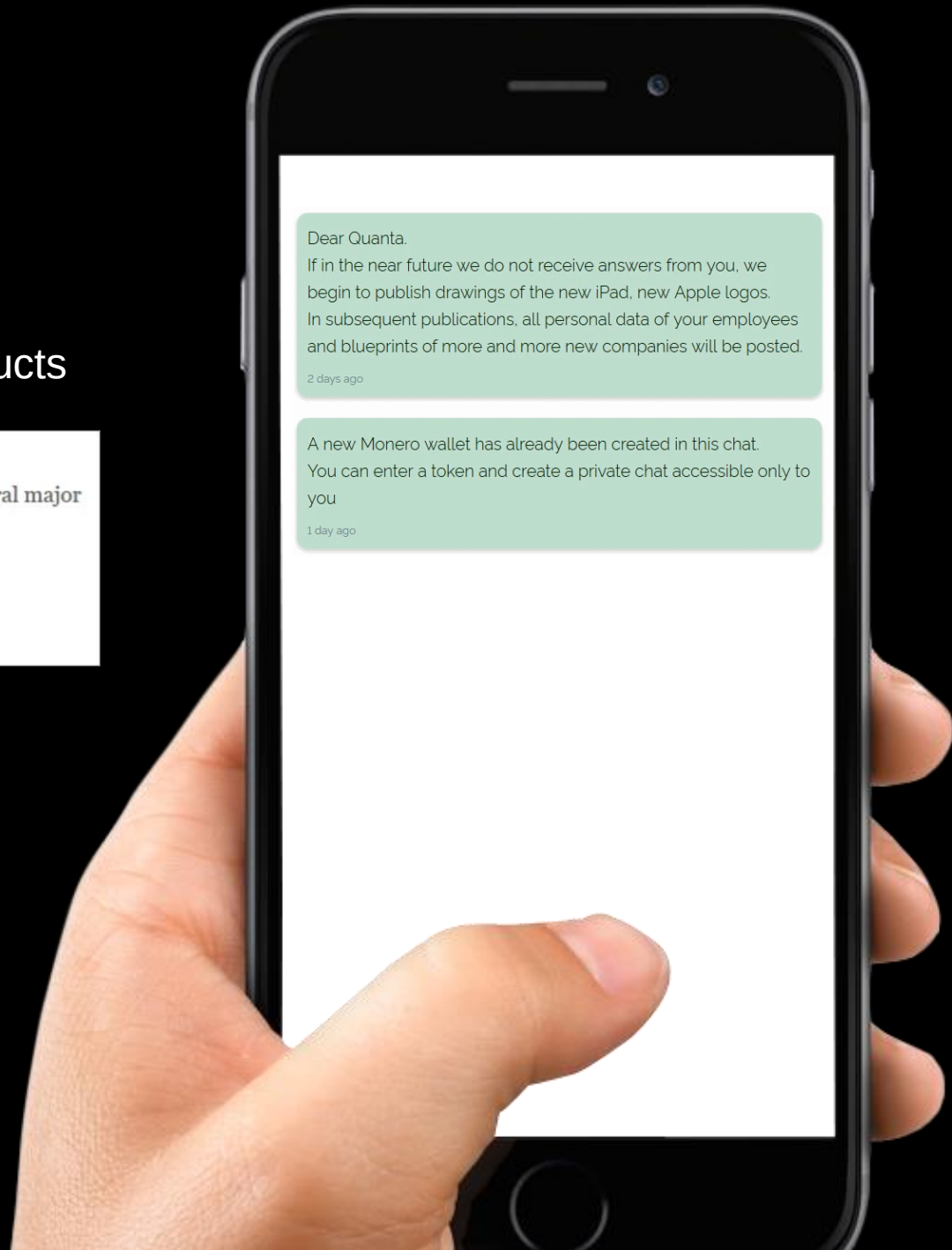
Quanta, a Taiwan-based original design manufacturer (ODM) manufacting Apple Watch, Macbook Air, and Macbook Pro

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.

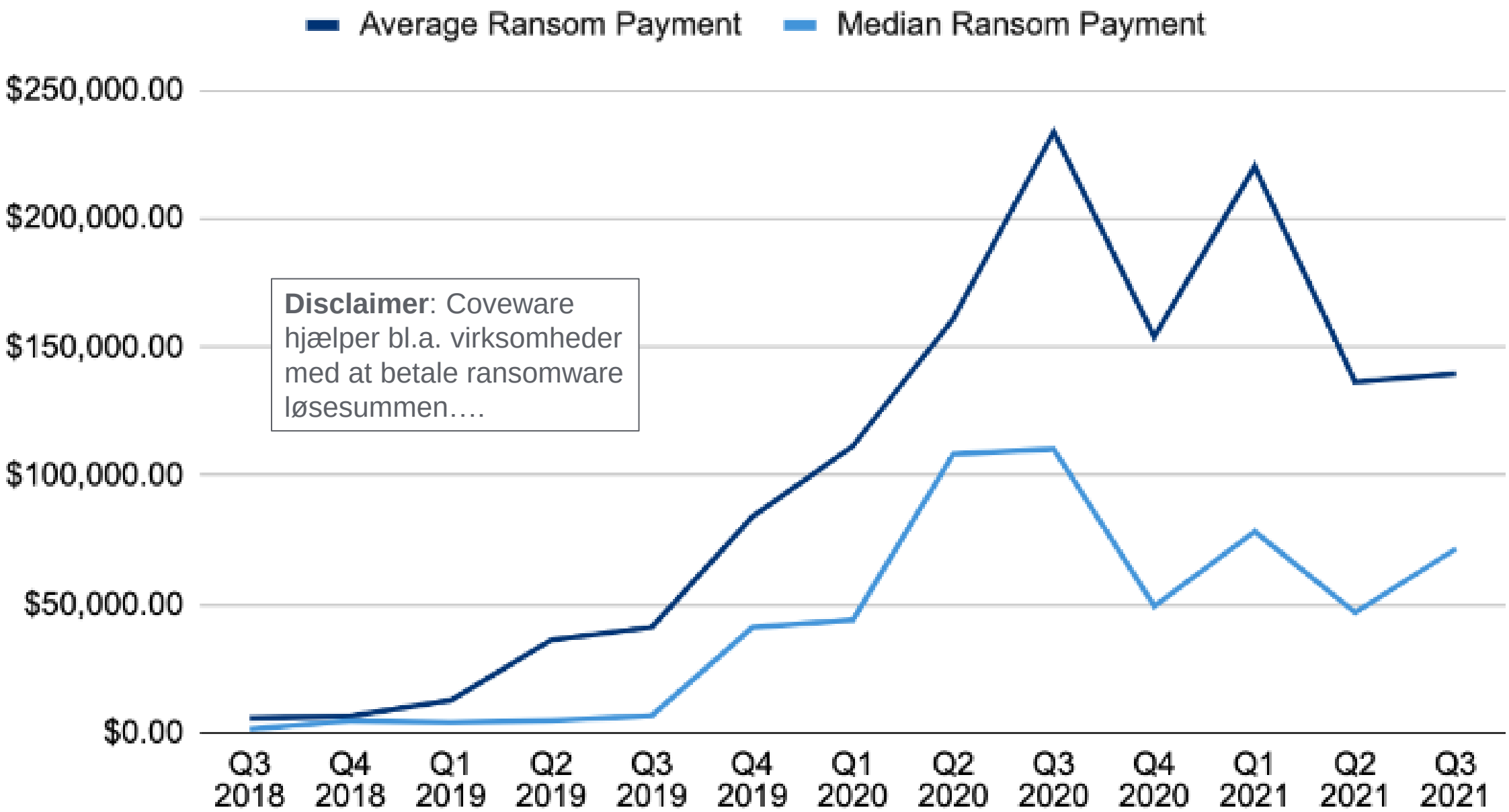
More and more files will be added every day.
The same is in pdf format

Quanta Computer



Dubex:

Ransom Payments By Quarter

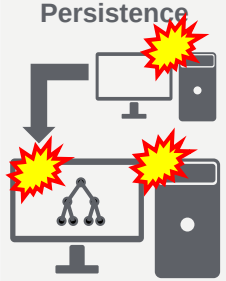


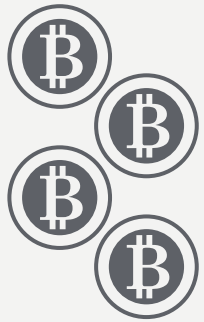
Disclaimer: Coveware hjælper bl.a. virksomheder med at betale ransomware løsesummen….

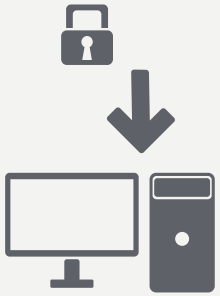
https://www.coveware.com/blog/2021/10/20/ransomware-attacks-continue-as-pressure-mounts

Ransomware Attack

Identify & Recon	Initial attack	Persistence (Download & contact)	Infiltration	Key-exchange	Payload Encryption of data	Display Blackmail note	(Payment)	(Release of files)
Identify potential victims	Phishing attack Remote Access Compromise Malware Wrapper	The network is compromised with malware Malware contacts Command & Control Server	Credential theft Lateral movement Compromise Active Directory Persistence	Disable security controls Data exfiltration Sabotage backup	Crypto ransomware downloaded Systems are being encrypted	The offer is presented with blackmail notice with a deadline	The victim pays ransom via the Tor network using Bitcoins	The victim receives a key for decrypting data



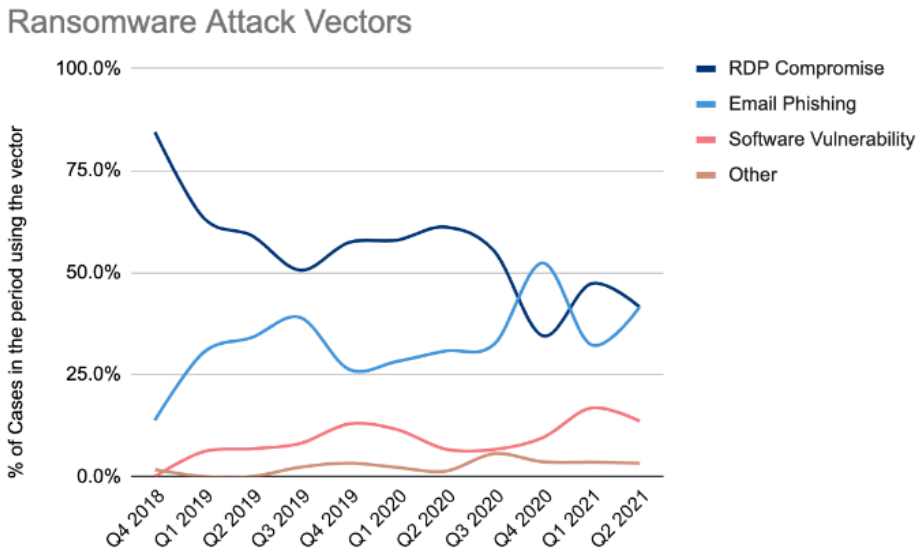


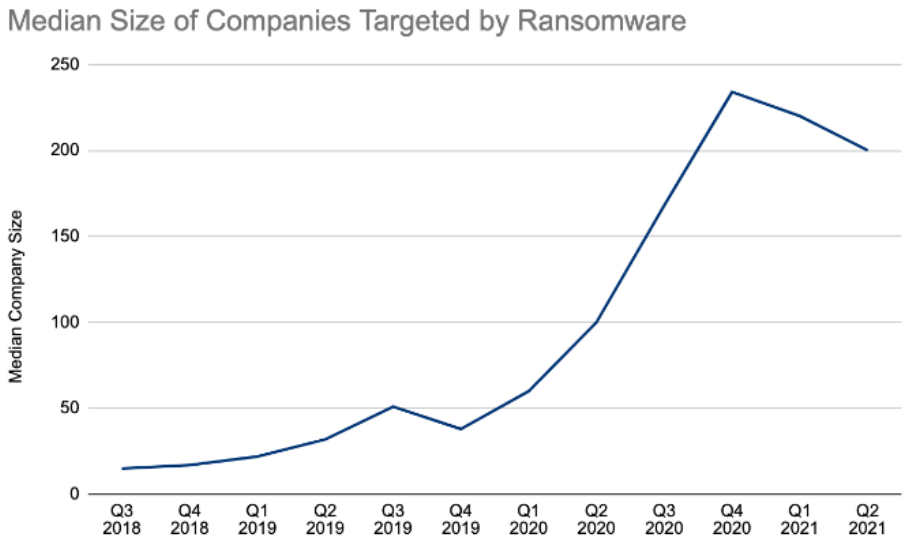


Dubex:

Ransomware Inital Attack Vectors

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

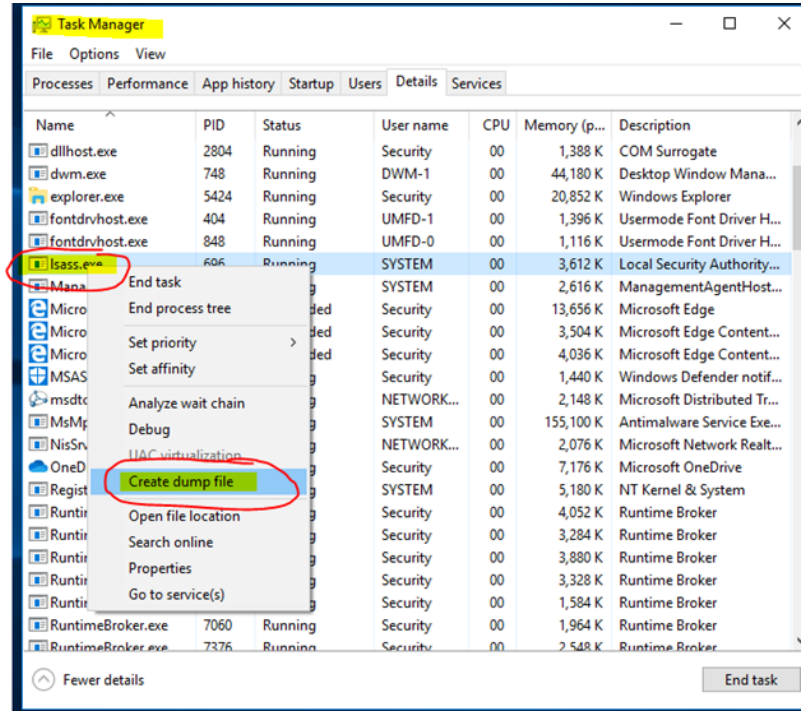




https://www.coveware.com/blog/2021/7/23/q2-ransom-payment-amounts-decline-as-ransomware-becomes-a-national-security-priority

Living of the land & Dual-Use Tools –
Fileless malware & malware less infections

- Living of the land: Existing software is used by the attacker and no additional binary executables are installed onto the system
- Dual-Use Tools: Native pre-installed with the operating system & third-party tools that are commonly installed
- Local Security Authority Subsystem Service
- Scripts are very popular, especially PowerShell
  - 77% of targeted attack incidents made use of PowerShell
  - Many script toolkits available
  - Scripts are easy to obfuscate and difficult to detect with signatures
  - Scripts are flexible and can be quickly adapted if needed



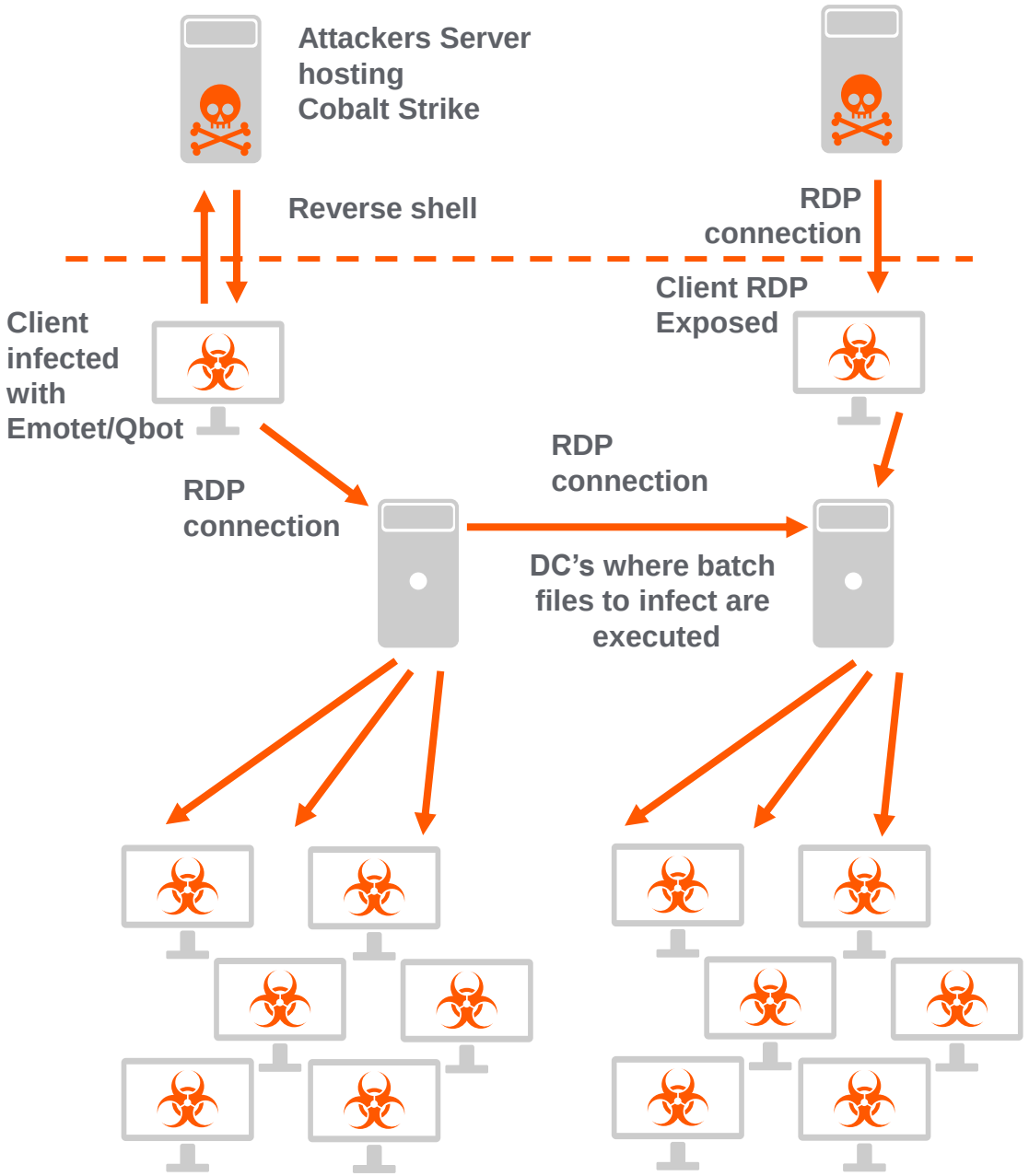
MEMORY ONLY ATTACKS	DUAL-USE TOOLS	NON-PE FILES	FILELESS LOADPOINT	NO VULNABILITIES
Remote code exploits such as EternalBlue and CodeRed	Using built in tools, such as Netsh, PsExec and service like Dropbox, Twitter to do malicious things	Documents with macros, PDFs with JavaScript and scripts (VBS, JavaScript, PowerShell,…)	Hiding scripts in the registry, WMI or GPO, e.g. Poweliks and Kotver	Finding exploitable zero-day vulnerabilities is getting more difficult
Less new files on disk	Use off-the-shelf tools & cloud services	These tools are ubiquitous	Fileless persistence loadpoint	use simple and proven methods such as email & social engineering
More difficult to detect attack	Difficult to determine actor, intent & source	Hide in plain sight and bypass whitelisting	Persistent	Cheaper and easier attack

Dubex:

Trends - Ransomware

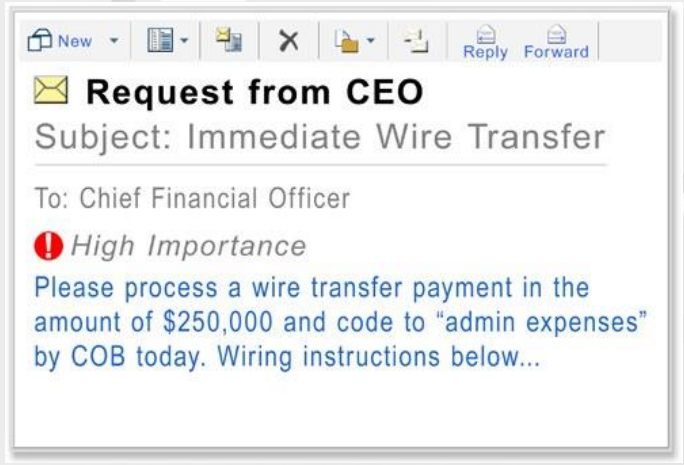
- Using MSP management tools – attacking MSP's remote support tools using hacked credentials
- Attacker code appears "trusted" while attackers elevate privileges
  - UAC bypass technics & administrative credential
  - Elevate privileges using software vulnerability
- Living off the land - PowerShell and PsExec
- Ransomware are deployed using standard software deployment tools / GPO's
- Automation-enhanced active manual attacks
- Attackers are using a combination of automated tools and humans to more effectively evade security controls
- RaaS – Ransomware as a Service
- Attacking Linux systems to compromise ESX-hosts

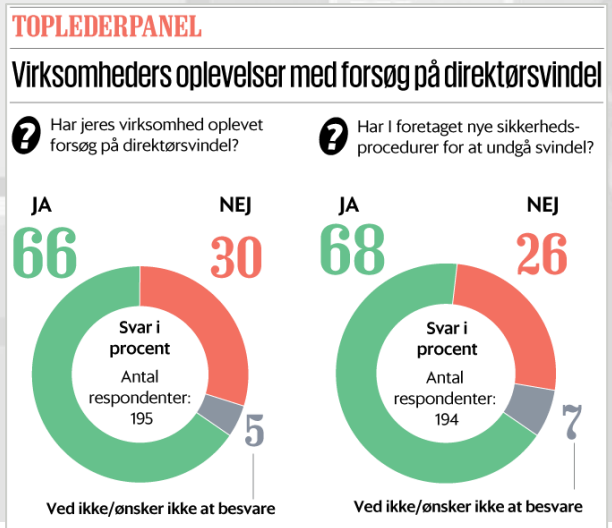
Dubex:



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

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…

$6 trillion annually by 2021

https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

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

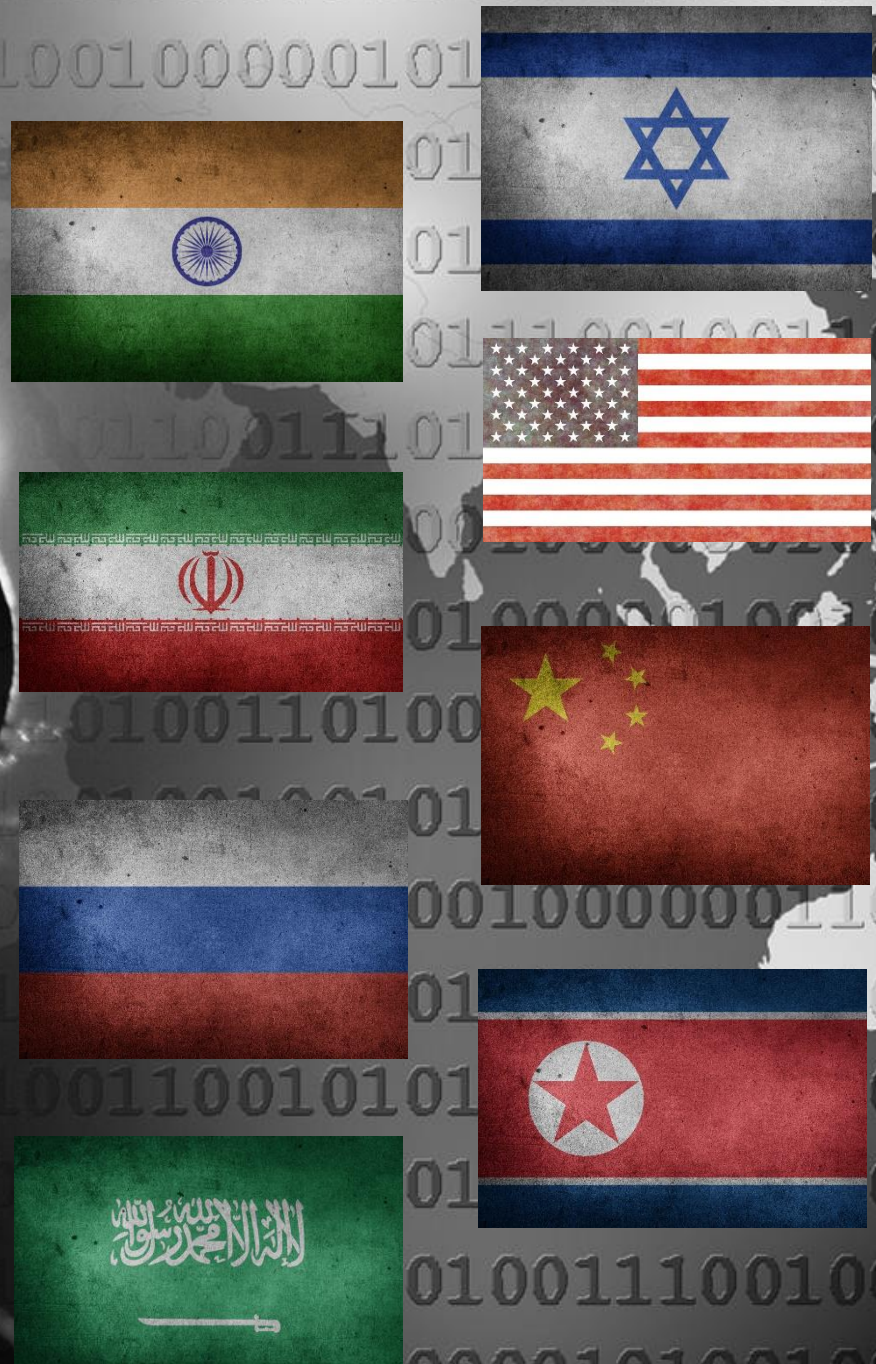
- Risiko for angreb mod fysiske mål fx olieproduktion
- Målrettede angreb på virksomheder og personer
- Risiko for ”følgeskader” hos virksomheder

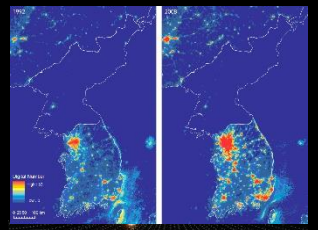
Politisk motiveret hacking og tiltag

- 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





SONY PICTURES

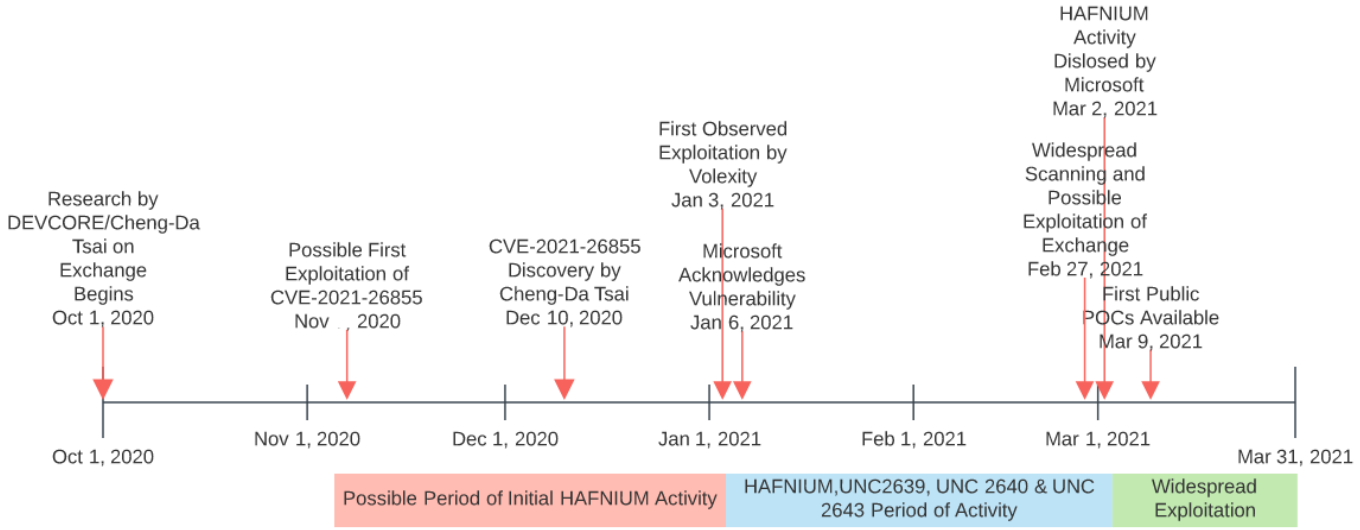
SWIFT

Society for Worldwide Interbank Financial Telecommunication

Exchange Servers under attack with 0-day exploits - Hafnium

“Please leave an exploit after the beep”

- Dubex Incident Response Team are called in to assist on Exchange Server incident in the end of January 2021
- Findings escalated to Microsoft – and found to be a zero-day exploit
- Widespread attacks from Feb. 25. 2021
- Microsoft Emergency Patch Release March 2nd, 2021
- It appears that information of how to exploit the vulnerabilities has somehow leaked
- When the exploit was disclosed by Microsoft the attacks intensified even more
- Estimates are the >30.000 Exchange systems in the U.S. alone have been hit by automated attack
- FBI did cleanup operation removing webshells

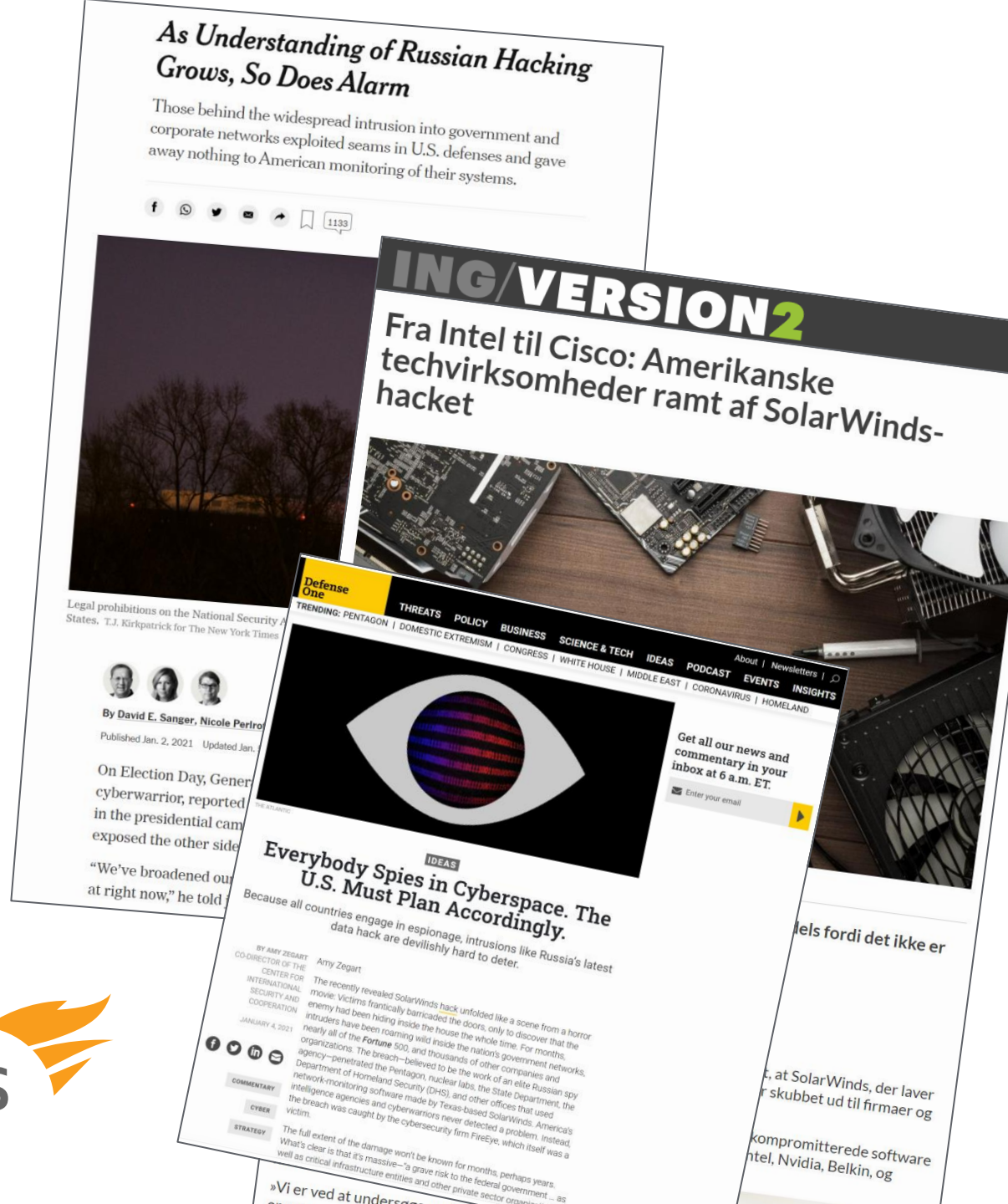


Solarwinds Supply chain attack

- Advanced Persistent Threat (APT) actor targeted the supply chain to bypass traditional enterprise perimeter and detection defenses

- The attack involved cyber actors compromising SolarWinds' build infrastructure and used that access to distribute trojanized software updates to over 18,000 SolarWinds customers

- 18.000 organizations compromised…
  - FireEye
  - Microsoft
  - Cisco
  - Palo Alto Networks
  - U.S. Treasury
  - U.S. Commerce Departments
  - U.S. Department of Energy
  - … and many more…

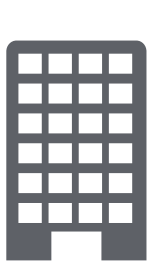


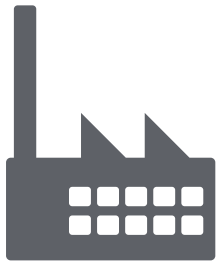
solarwinds

Dubex:

Supply chains

Sourcing materials, utilities, consultants





Refining those materials into basic parts.
Combining those basic parts to create a product.
Order fulfillment/Sales.

Product delivery.
Customer support and return services.

Dubex:

Supply chains

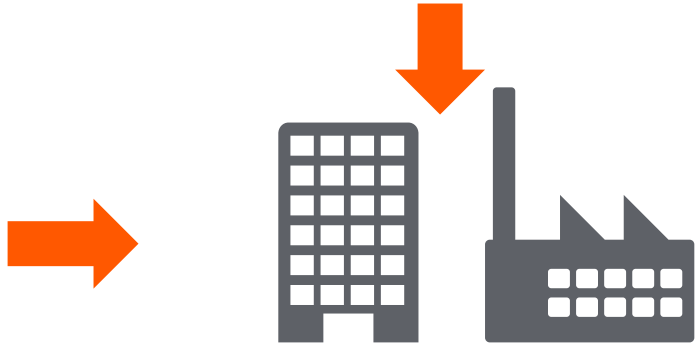
Sourcing materials, utilities, consultants

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.

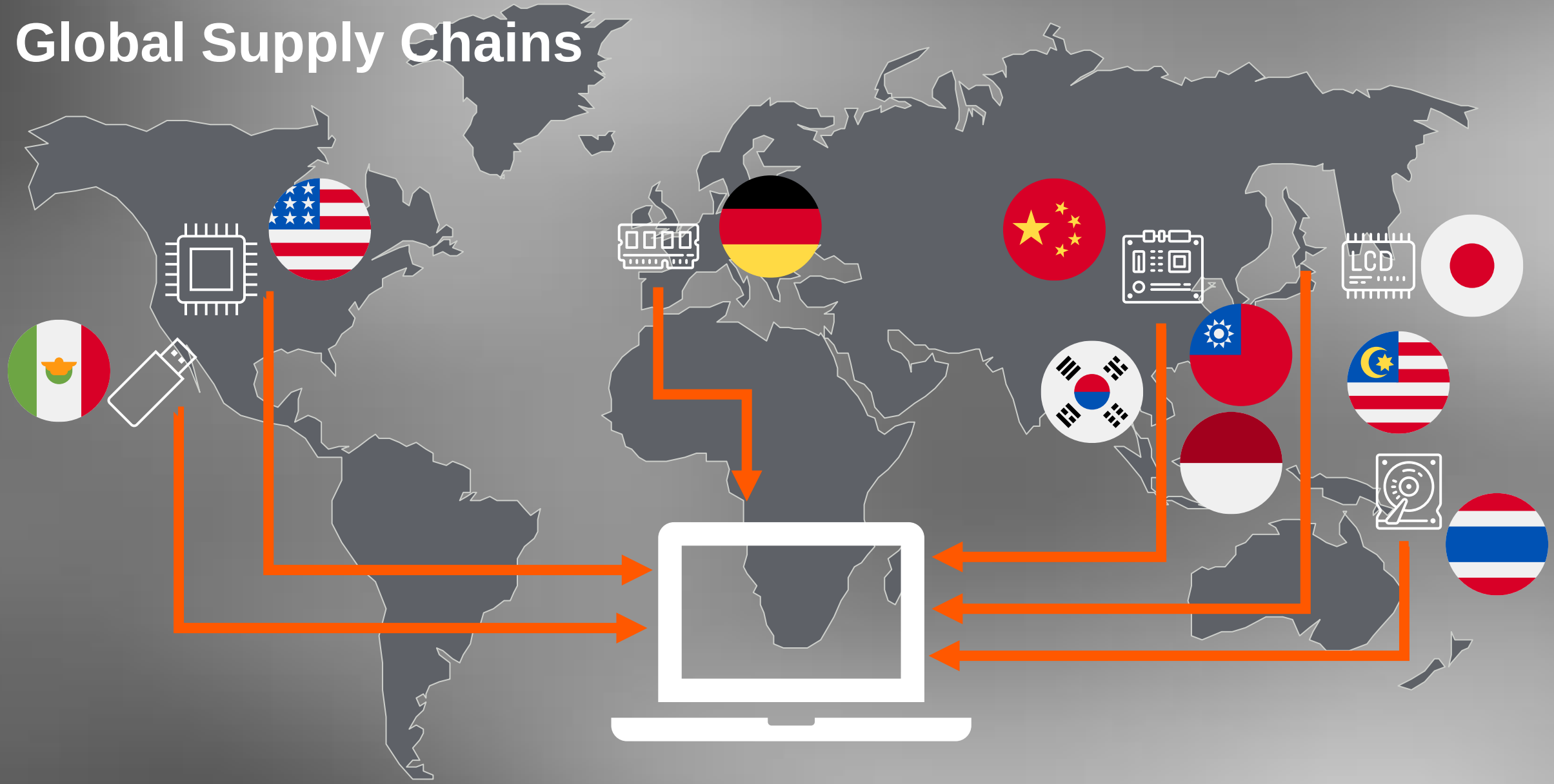


Refining those materials into basic parts.
Combining those basic parts to create a product.
Order fulfillment/Sales.

Product delivery.
Customer support and return services.

Dubex:

Global Supply Chains



Supply chains & complex products

Combines hardware & software

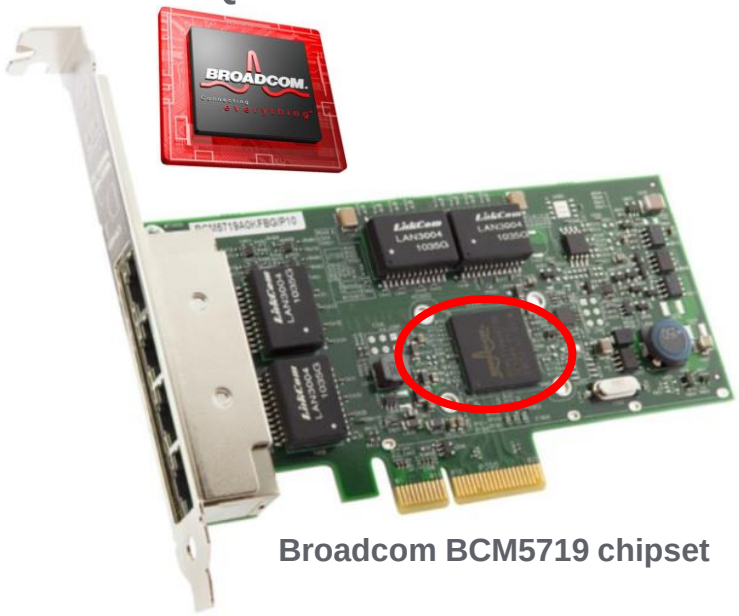
Lenovo ThinkPad X1 Carbon 6th Gen

TouchPad and
TrackPoint,
Synaptics USB device

HP Spectre x360 Convertible

HP Wide Vision FHD Camera USB device

NetXtreme Quad-Port Ethernet Controller



Broadcom BCM5719 chipset

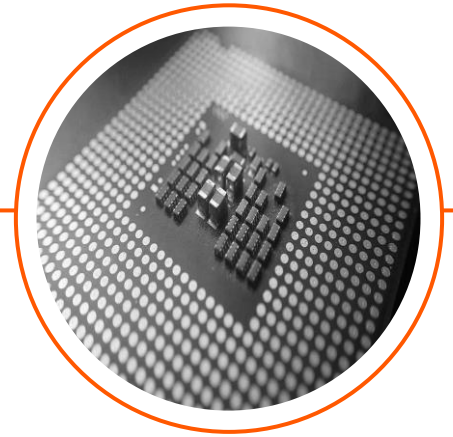
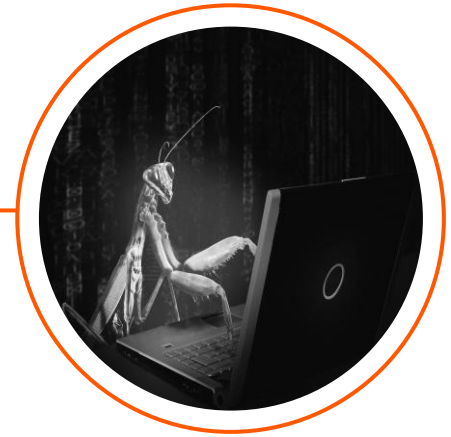
Dell XPS 15 9560

Killer Wireless-n/a/ac 1535
PCI Modul

Dubex:

https://eclypsium.com/wp-content/uploads/2020/02/Eclypsium-Unsigned-Peripheral-Firmware-Research.pdf

Types of Supply Chain Attacks in hard- and software

Software	Infrastructure	Certificates	Hardware or firmware	Pre-installed malware
				
Compromised software – source code or build process	Compromised tools or infrastructure	Stolen code-sign certificates or signed malicious apps using the identity of dev company	Compromised specialized code shipped into hardware or firmware components	Pre-installed malware (backdoors) on devices (cameras, USB, phones, etc.)

Dubex:

Targeting suppliers and software developers, the goal is to access source codes, build processes, or update mechanisms by infecting legitimate apps to distribute malware.

Supply chains & software from trusted third-party

- We trust many external third-party partner and vendors
- Companies we are working with and exchange data with
- Companies providing us with software and software updates
- Companies having vendors themself
- Companies using open-source libraries in their products
- Suppliers and software developers compromised to access source codes, build processes, or update mechanisms by infecting legitimate apps to distribute malware
- The third-parties are being used as a step-stone to attack our infrastructure

Intellect Service (MeDoc)

- Compromised April 14th 2017 by hacker group TeleBots
- MeDoc Automatic Update Servers Compromised
- Used to push XData - a stealthy backdoor
- Used to push the Petya ransomware / wiper

Handbreak

- Hacked May 2nd 2017
- Modified copy of Handbrake
- Proton RAT

Ccleaner

- Hacked August 2017
- Infected version of CCleaner distributed
- Used for highly targeted attacks against tech-companies

Google Playstore & Apple AppStore

- Tricked into serving malicious apps
- Standard software libraries compromised
- Numerous examples over the past few years

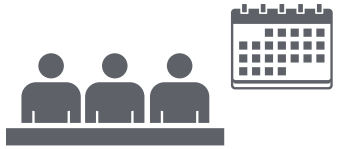
Dubex:

Konsekvenser - rammer på kort og langt sigt

Omkostninger til incident response

Mistede kunder og indtjening

Skadet omdømme & brand – mistet tillid



Mistet produktivitet

Bøder

Mistede intellektuelle værdier

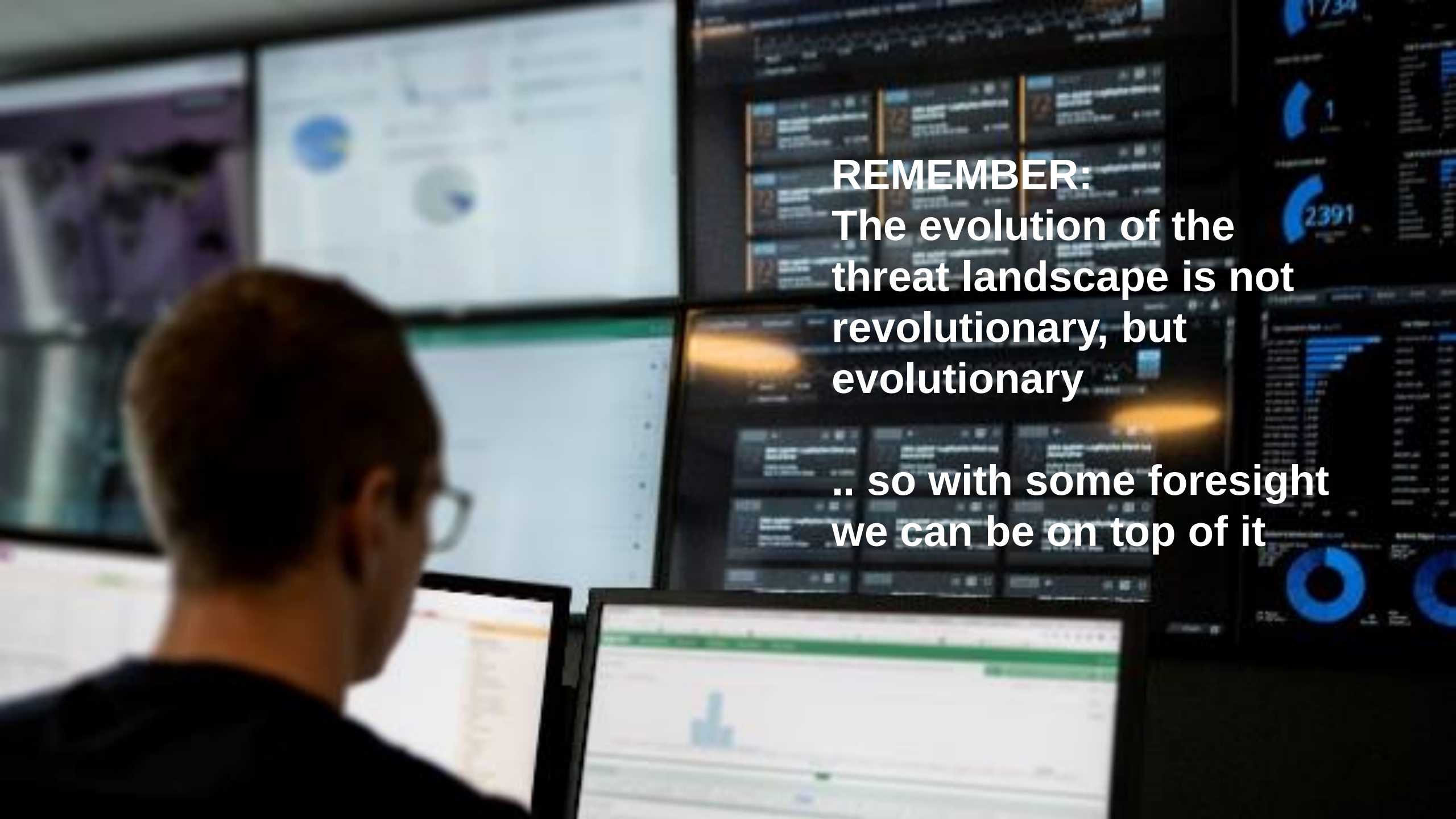
Dubex:


Threat landscape 2021 and beyond

COVID-19 & Cybersecurity – Long term effects

- A heightened dependency on digital infrastructure raises the cost of failure
- Economic crises generate more cybercriminals
- Cybercriminals changing targets
- Increased geo-political tension increases government involvement in cyber-attacks

Dubex:


REMEMBER:
The evolution of the threat landscape is not revolutionary, but evolutionary
.. so with some foresight we can be on top of it

Threats beyond 2021 - Headlines

Evolving Ransomware

Software supply chain attacks on the rise

Evasive phishing cyber attacks

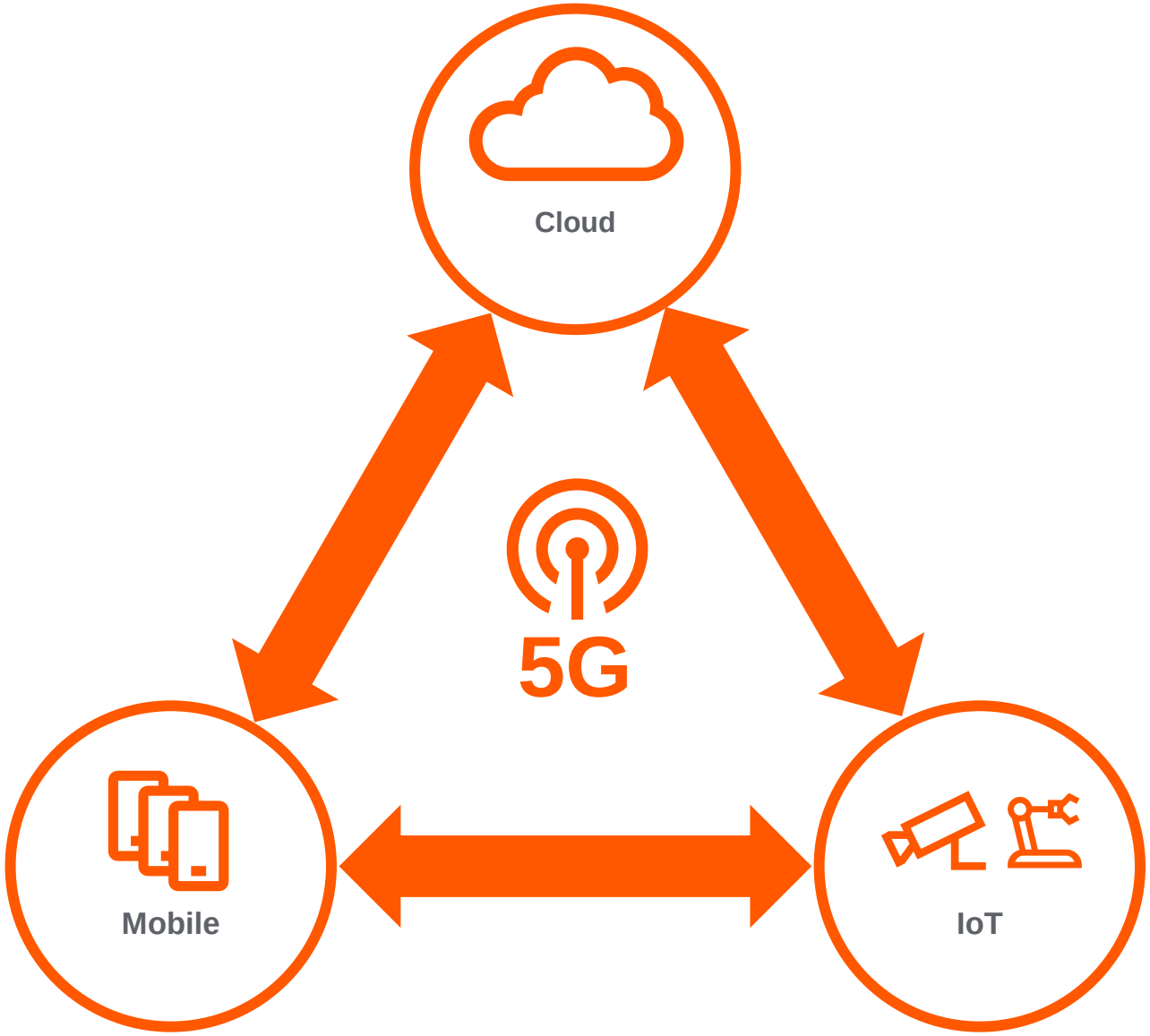
Clouds under attack

Internet of Things

Mobile device attacks

AI and Machine learning

Dubex:



- Design
- Kode sikkerhed
- API Sikkerhed
- Kryptering
- Databeskyttelse
- Adgangsstyring
- Container Sikkerhed
- Konfigurationer
- Automation

Dubex:

Cheap hardware

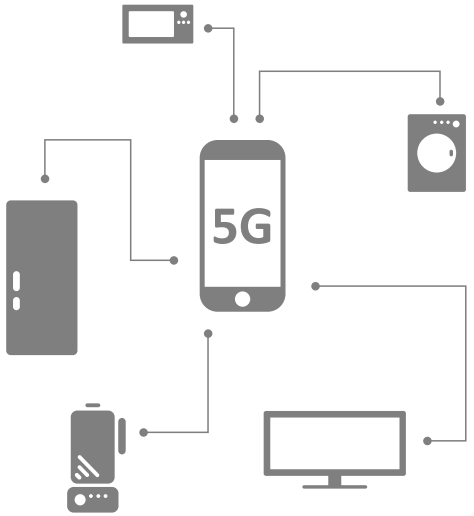
ESP32-SOLO-1

SoC: ESP32 single-core, low-power Xtensa 32-bit LX6 microprocessor
448 KB of ROM for booting and core functions
520 KB of on-chip SRAM for data and instructions
16 KB of SRAM in RTC
QSPI flash/SRAM up to 4 × 16 MB
Power supply: 2.3V to 3.6V
SPI, I2S, I2C, SDIO, UART, IR, PWM
Temperature sensor, touch sensor, ADC, DA
Connectivity: Bluetooth and Wi-Fi b/g/n dual mode

Pricing (EUR)

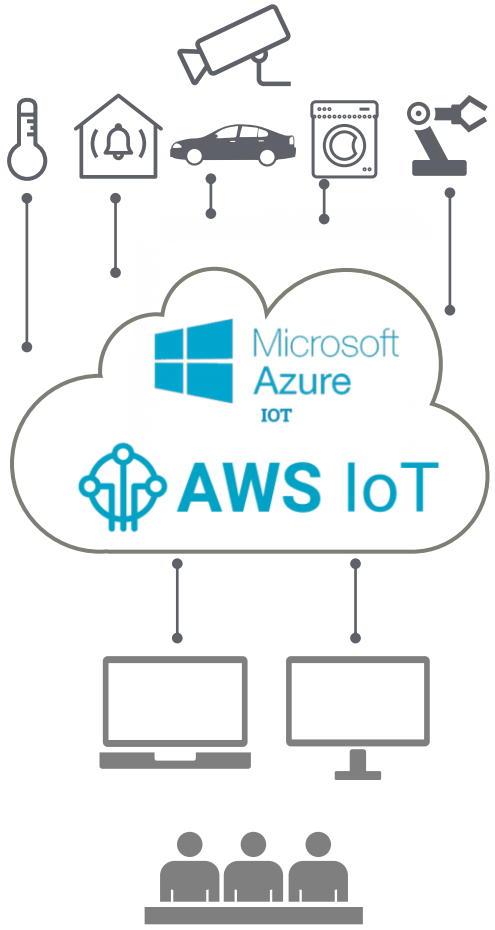
Qty.	Unit Price	Ext. Price
1	2,21 €	2,21 €

Cheap connectivity



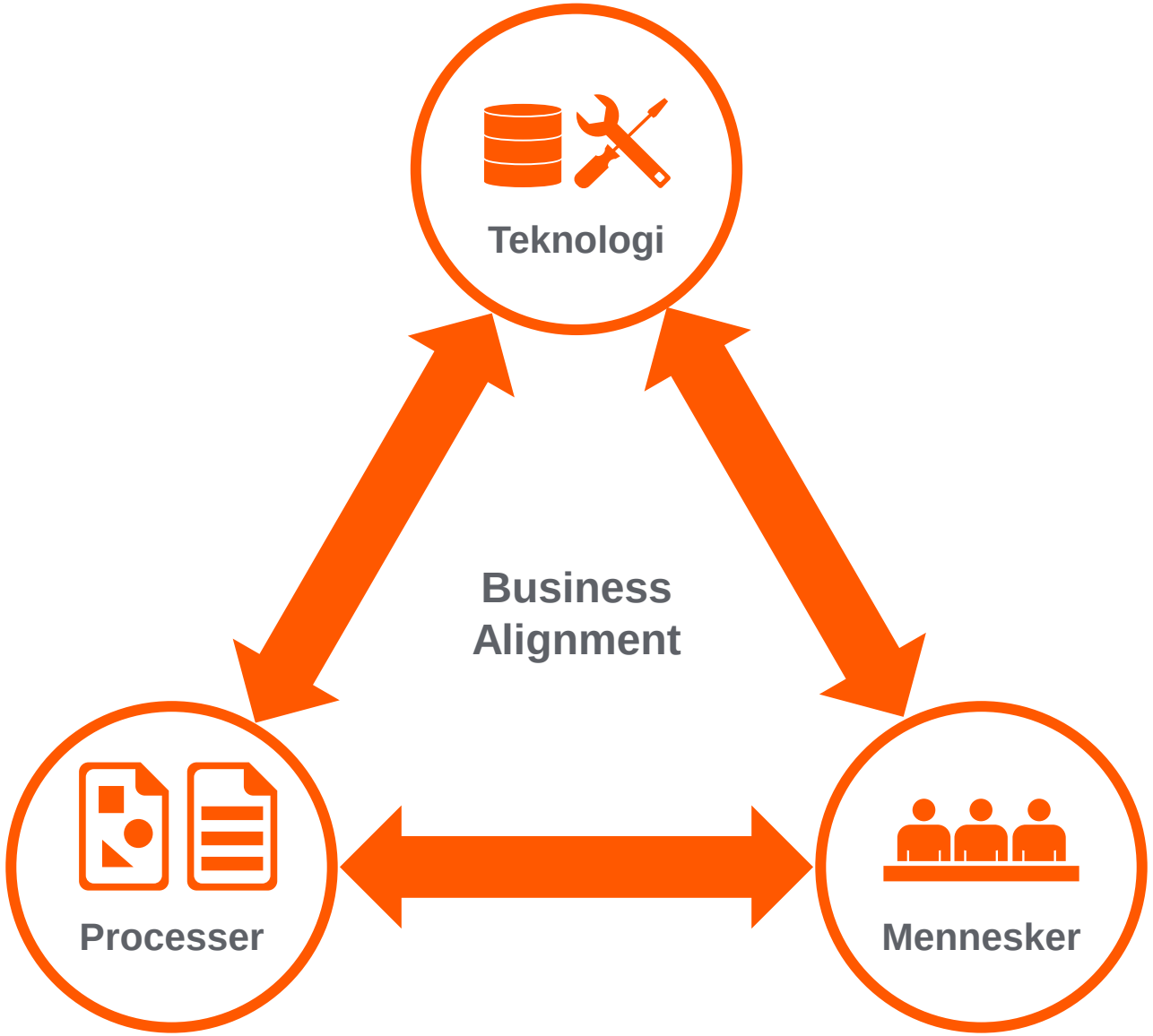
Global Machine-to-Machine Growth
Kilde: Cisco

Cheap software

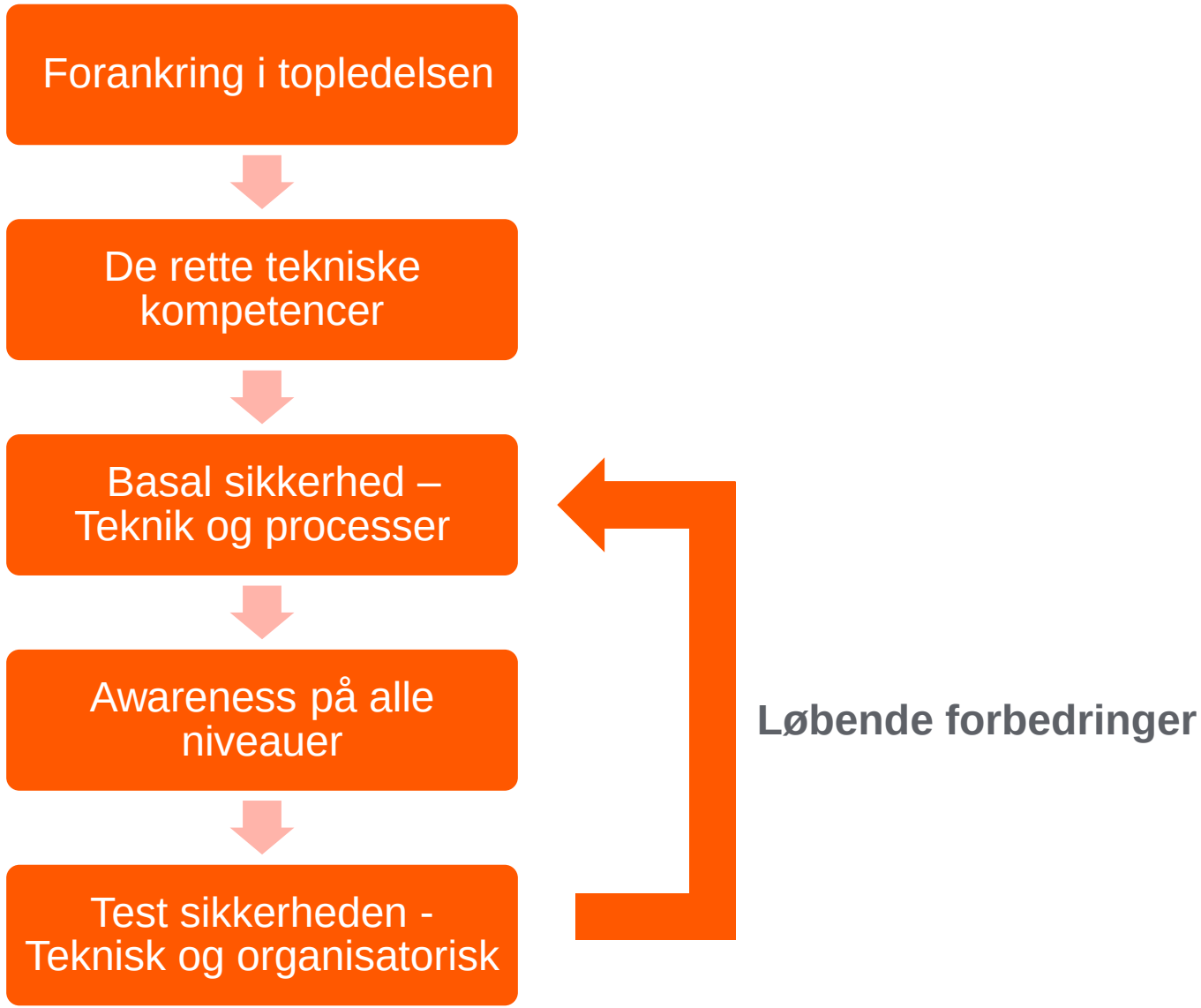


Dubex:

Dubex:



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:

BESTYRELSESFORENINGEN
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/

Hvad kan vi gøre? - Praktiske anbefalinger (1)

- **Sikkerhed i dybden**: Anvend forskellige og overlappende sikkerhedsforanstaltninger, så der beskyttes med single-point-of-failure i enkelte foranstaltninger eller teknologier
- **Basale kontroller**: Hold fokus på basale kontroller – husk den løbende opfølgning
- **Overvågning**: Mange organisationer opdager først brud på sikkerheden, når de får et opkald fra politiet eller en kunde. Overvågning af logfiler og change management kan give tidligere advarsel
- **Antivirus er ikke nok**: Antivirus fanger stadig mange angreb, men mange angreb anvender unik malware og udnytter dag-0-sårbarheder, som kræver andre værktøjer
- **Endpoint-beskyttelse**: Endpoints skal beskyttes af mere end antivirus - husk opdateringer, begrænsede rettigheder, websikkerhed, device kontrol, overvågning og incident response muligheder
- **Patch straks**: Angribere får ofte adgang ved hjælp af simple angrebsmetoder, som man kan beskytte sig mod med et opdateret og godt konfigureret it-miljø samt opdateret anti-virus
- **Eksterne services**: Enhver sårbarhed i eksterne services udnyttes lynhurtigt, så begræns eksponerede services mest muligt, fokus på opdatering og konfiguration – brug altid VPN og undgå fx RDP udefra
- **Krypter følsomme data**: Hvis data bliver tabt eller stjålet, er det meget sværere for en kriminel at misbruge
- **Beskyt krypteringsnøgler**: Hvis krypteringsnøglerne kompromitteres, kompromitteres sikkerheden også
- **To-faktor-autentifikation**: Dette vil ikke eliminere risikoen for, at passwords bliver stjålet, men det kan begrænse de skader, der kan ske ved misbrug af stjålne legitimationsoplysninger

Dubex:

Hvad kan vi gøre? - Praktiske anbefalinger (2)

- **Mennesker: Awareness** er stadig vigtigt. Undervis de ansatte i vigtigheden af sikkerhed, hvordan man opdager et angreb, og hvad de skal gøre, når de ser noget mistænkeligt. Husk awareness til ledelsen
- Hold adgangen til data på et ”**need-to-know**” niveau: Begræns adgangen til systemerne til det nødvendige personale. Sørg for, at have processer på plads til at lukke for adgangen igen, når folk skifter rolle eller job
- **Administrativ adgang**: Begræns administrativ adgang mest muligt og overvåg anvendelse af administrative adgange. Hold øje med brugen af administrative værktøjer
- **Husk fysisk sikkerhed**: Ikke alle datatyverier sker online. Kriminelle vil manipulere med computere, betalingsterminaler eller stjæle dokumenter
- **Backup**: Hvis alle andre foranstaltninger fejler, kan en backup redde data. Husk beskyttelse af backup medierne…
- **Incident response**: Planlæg efter, at der vil ske hændelser - følg løbende op på hvordan, og hvor hurtigt, incidents opdages og håndteres, så reaktionen løbende kan forbedres
- **Opfølgning**: Glem ikke de basale kontroller. Hold fokus på bedre og hurtigere opdagelse gennem en blanding af mennesker, processer og teknologi
- **Trusselsbilledet**: Hold øje med trusselsbilledet for løbende at kunne tilpasse sikkerhedsløsningen. Husk at ”one-size fits all” ikke holder i virkeligheden
- **Riskovurdering**: Er du mål for egentlig spionage, så undervurder ikke vedholdenheden, ekspertisen og værktøjerne hos din modstander

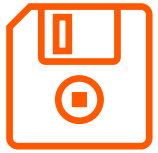
Dubex:

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:

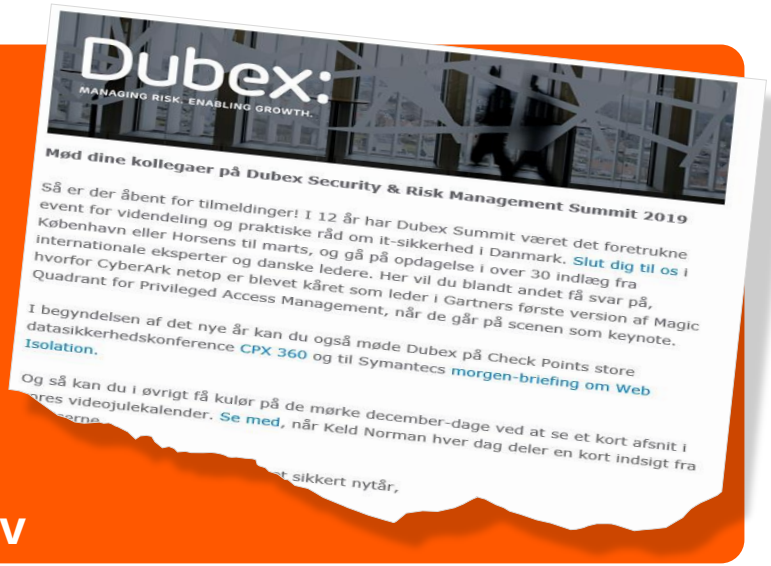
Risikobegrænsning

- Risikoen kan ikke fjernes, kun begrænses
- Sikkerhed kan ikke købes som produkt
- Sikkerhed opnås ved en blanding af
  - Procedure & ledelse (Management issues)
  - Design, værktøjer og tekniske løsninger
  - Løbende overvågning og vedligeholdelse
- Resultat: Formulering af sikkerhedspolitik og implementering af sikkerhedssystem

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.

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