Dubex:

Cybersikkerhed anno 2024 - regulering, praksis og perspektiv

Det aktuelle trusselsbillede – Trends og kommende udfordringer

Jacob Herbst, CTO, Dubex A/S

DI, Industriens Hus

Den 27. februar 2024

Agenda

01 Cyberrisikoen for digitale virksomheder

02 Truslen fra digitale mafiagrupper

03 Virksomheder i en ny geopolitisk virkelighed

04 Fremtiden & opsamling

Dubex:

Agenda

01 Cyberrisikoen for digitale virksomheder

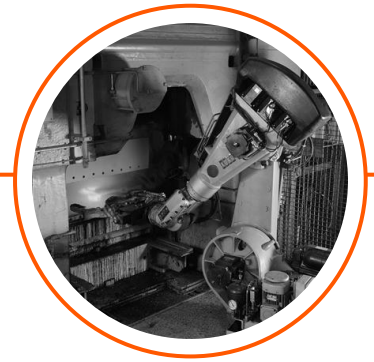
02 Truslen fra digitale mafiagrupper

03 Virksomheder i en ny geopolitisk virkelighed

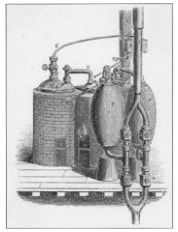
04 Fremtiden & opsamling

Dubex:

The industrial revolutions - the short story

”Industry 0.0” – crafts	Industry 1.0	Industry 2.0	Industry 3.0	Industry 4.0	Industry 5.0
					
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 - Cyber-physical systems (CPS)	**Human-Centric** Man and machines working together - Personalisation and collaborative robots

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:

70%

of new value created globally will be digitally enabled, according to the World Economic Forum

According to Goldman Sachs, Generative AI could raise global GDP by

7%

Dubex:

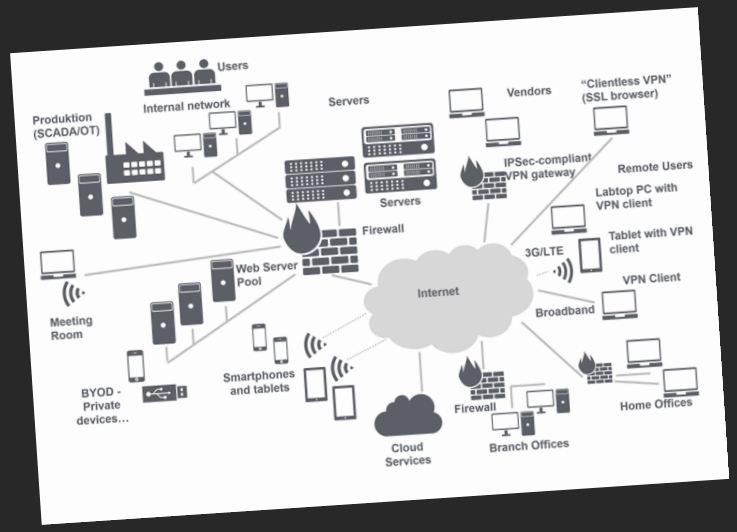
ALL COMPANIES ARE DIGITAL COMPANIES

– SOME JUST DON'T KNOW IT

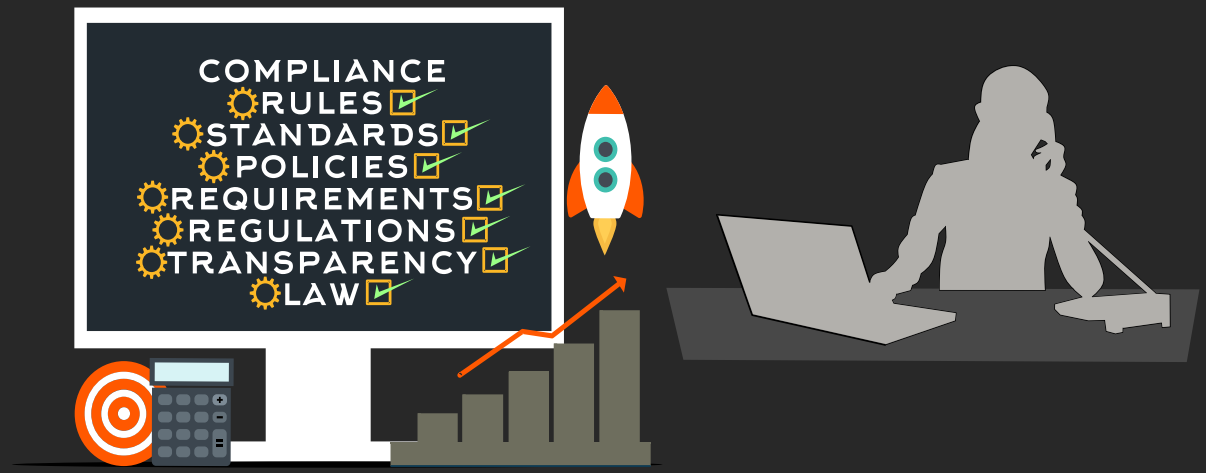
…if cybersecurity breaks down, technology breaks down and the business breaks down…

Dubex:

Avancerede løsning og kompleksitet

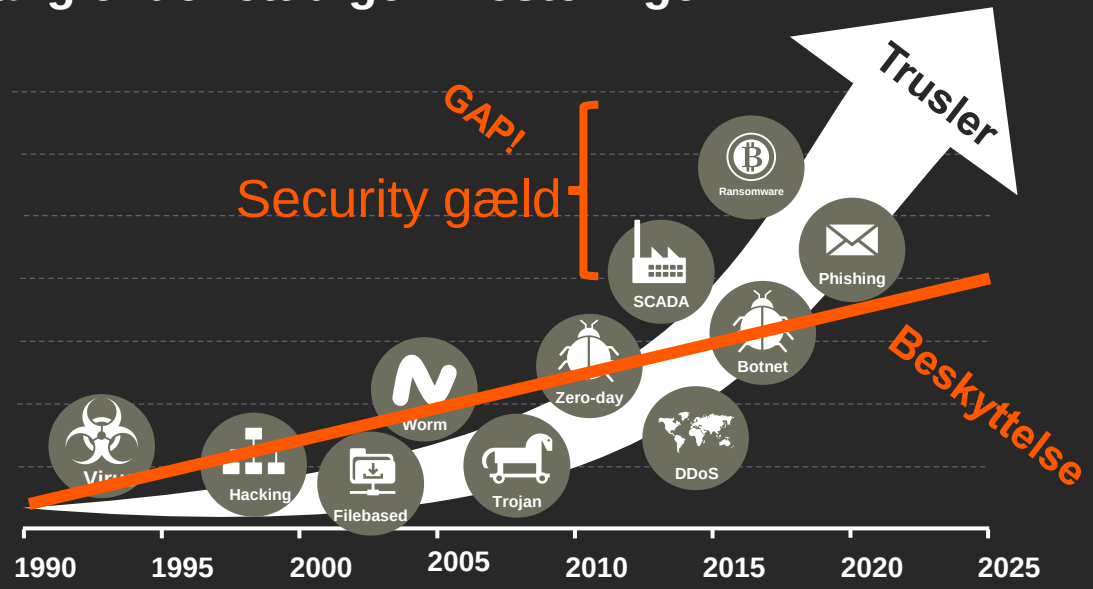


Krav fra forretningen – Voksende afhængighed



Mangel på kompetencer og ressourcer

Manglende rettidige investeringer



Dubex:

Konsekvenser – eksempler

Omkostninger til incident response

Mistede kunder og indtjening

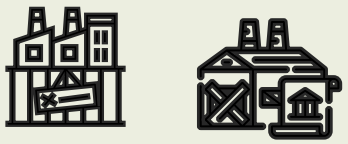
Skadet omdømme & brand – mistet tillid

Tabt omsætning og produktivitet

Mistet data & stjålne personoplysninger

Mistede intellektuelle værdier

Usikkerhed & uvished



Konkurs og lukning

Bøder & erstatninger

Spredning af falske oplysninger

Nu → Kort sigt → Lang sigt

Dubex:

Netcompany – Kursudvikling efter datalæk

ING/VERSION2

Hackere lækker kildekode og passwords fra Netcompany: Truer den danske stat

Cybersikkerhed | 23. februar kl. 14:20 | 11

Berlingske

VIRKSOMHEDER

Nyheden om angrebet på dansk gigant blev udgivet klokken 14.20. Så faldt markedsværdien med cirka 400 millioner kroner på en eftermiddag

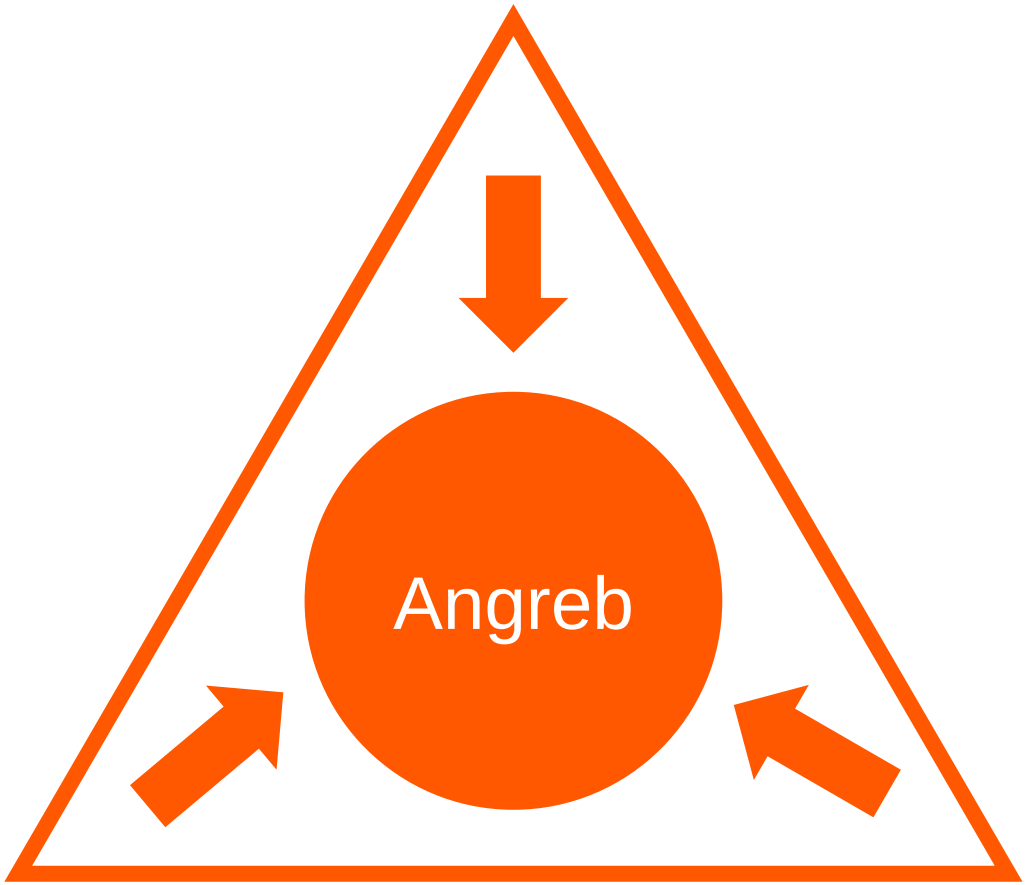
Investorerne har reageret prompte på et nyt hackerangreb, som it-giganten Netcompany er blevet ramt af.

netcompany

Fredag d. 23. februar 2024

Dubex:

Aktør & motiv



Evner & metoder

Mulighed

Dubex:

Cybertruslen mod Danmark 2023

Formålet med denne trusselsvurdering er at informere beslutningstagere i danske myndigheder og virksomheder om cybertruslen mod Danmark. Trusselsvurderingen redegør for de forskellige typer cybertrusler, Danmark står over for. Vurderingen kan bl.a. indgå som en del af grundlaget for myndigheders og virksomheders risikovurderinger på cybersikkerhedsområdet.

Hovedvurdering

- Truslen fra cyberspionage mod Danmark er **MEGET HØJ**. Truslen er koncentreret om udenrigs- og sikkerhedspolitiske forhold såsom Arktis, NATO og EU, selvom også kritisk infrastruktur er udsat for truslen.
- Cyberspionage kan underminere danske interesser, både politisk, økonomisk og sikkerhedsmæssigt. Det er sandsynligt, at fremmede stater benytter cyberspionage som forberedelse af destruktive cyberangreb.
- Truslen fra cyberkriminalitet mod Danmark er fortsat **MEGET HØJ**. Velorganiserede ransomware-grupper går efter alle dele af samfundet.
- CFCS vurderer, at langt de fleste cyberkriminelle fortsat er økonomisk motiverede, arbejder opportunistisk og er uafhængige af stater.
- Truslen fra cyberaktivisme mod Danmark er **HØJ**. Det er sandsynligt, at danske virksomheder og myndigheder vil blive ramt af aktivistiske cyberangreb på kort sigt. Pro-russiske cyberaktivister har et højt aktivitetsniveau mod NATO-lande, herunder Danmark, og har i stigende grad formaliseret deres angrebsmodus og forøget deres kapacitet.
- Truslen fra destruktive cyberangreb er **LAV**. Det er mindre sandsynligt, at fremmede stater på nuværende tidspunkt har til hensigt at udføre destruktive cyberangreb mod Danmark. CFCS vurderer dog, at hackergrupper tilknyttet fremmede stater forbereder sig for at kunne udføre destruktive angreb med kort varsel.
- Danske organisationer, der har aktiviteter i Ukraine eller leverer produkter og tjenester relateret til krigen i Ukraine, kan være udsat for en højere risiko for at blive ramt af et destruktivt cyberangreb eller følgevirkningerne af et angreb, der er rettet mod Ukraine.
- Truslen fra cyberterror er **INGEN.** Militante ekstremister har kun begrænset hensigt og ingen kapacitet til at udføre cyberangreb, der kan sidestilles med konventionel terror.

CENTER FOR CYBERSIKKERHED

- Truslen fra cyberspionage mod Danmark er **MEGET HØJ**. Truslen er koncentreret om udenrigs- og sikkerhedspolitiske forhold såsom Arktis, NATO og EU, selvom også kritisk infrastruktur er udsat for truslen.
- Cyberspionage kan underminere danske interesser, både politisk, økonomisk og sikkerhedsmæssigt. Det er sandsynligt, at fremmede stater benytter cyberspionage som forberedelse af destruktive cyberangreb.
- Truslen fra cyberkriminalitet mod Danmark er fortsat **MEGET HØJ**. Velorganiserede ransomware-grupper går efter alle dele af samfundet.
- CFCS vurderer, at langt de fleste cyberkriminelle fortsat er økonomisk motiverede, arbejder opportunistisk og er uafhængige af stater.
- Truslen fra cyberaktivisme mod Danmark er **HØJ**. Det er sandsynligt, at danske virksomheder og myndigheder vil blive ramt af aktivistiske cyberangreb på kort sigt. Pro-russiske cyberaktivister har et højt aktivitetsniveau mod NATO-lande, herunder Danmark, og har i stigende grad formaliseret deres angrebsmodus og forøget deres kapacitet.
- Truslen fra destruktive cyberangreb er **LAV**. Det er mindre sandsynligt, at fremmede stater på nuværende tidspunkt har til hensigt at udføre destruktive cyberangreb mod Danmark. CFCS vurderer dog, at hackergrupper tilknyttet fremmede stater forbereder sig for at kunne udføre destruktive angreb med kort varsel.

https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/cybertruslen-mod-danmark/


Demant


Vestas


ISS


7-ELEVEN


KALUNDBORG
FORSYNING

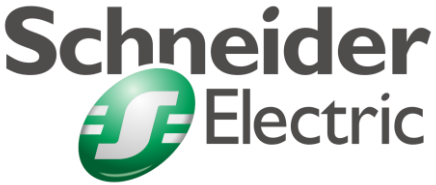

Colonial Pipeline Company


AK TECHOTEL


AZERO
.CLOUD


SEKTOR CERT


coop


Schneider
Electric


EDC


Copenhagen Airports
CPH


DSB


FORSVARSMINISTERIET

Agenda

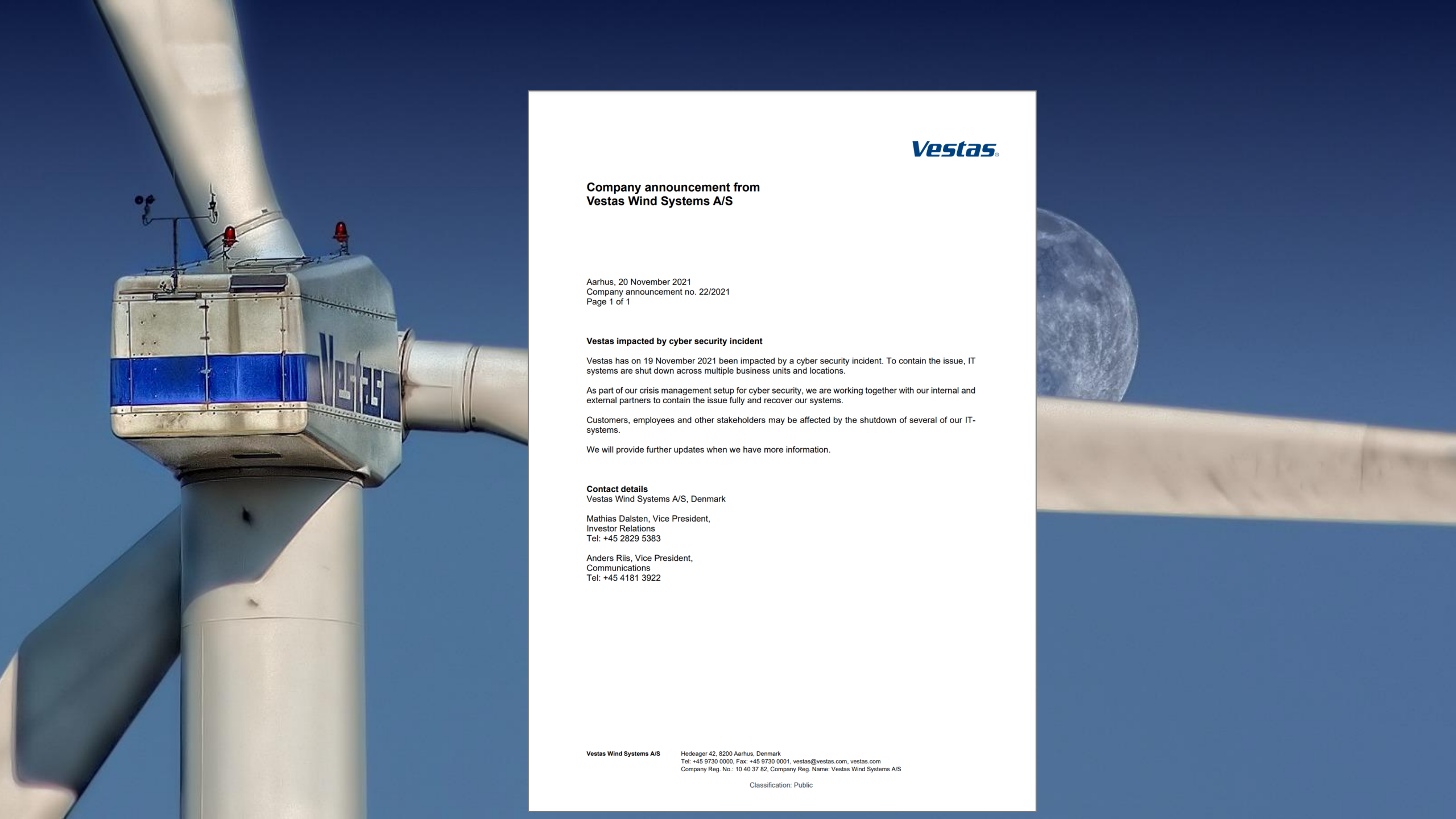
01 Cyberrisikoen for digitale virksomheder

02 Truslen fra digitale mafiagrupper

03 Virksomheder i en ny geopolitisk virkelighed

04 Fremtiden & opsamling

Dubex:



Company announcement from Vestas Wind Systems A/S

Aarhus, 20 November 2021
Company announcement no. 22/2021

Vestas impacted by cyber security incident

Vestas has on 19 November 2021 been impacted by a cyber security incident. To contain the issue, IT systems are shut down across multiple business units and locations.

As part of our crisis management setup for cyber security, we are working together with our internal and external partners to contain the issue fully and recover our systems.

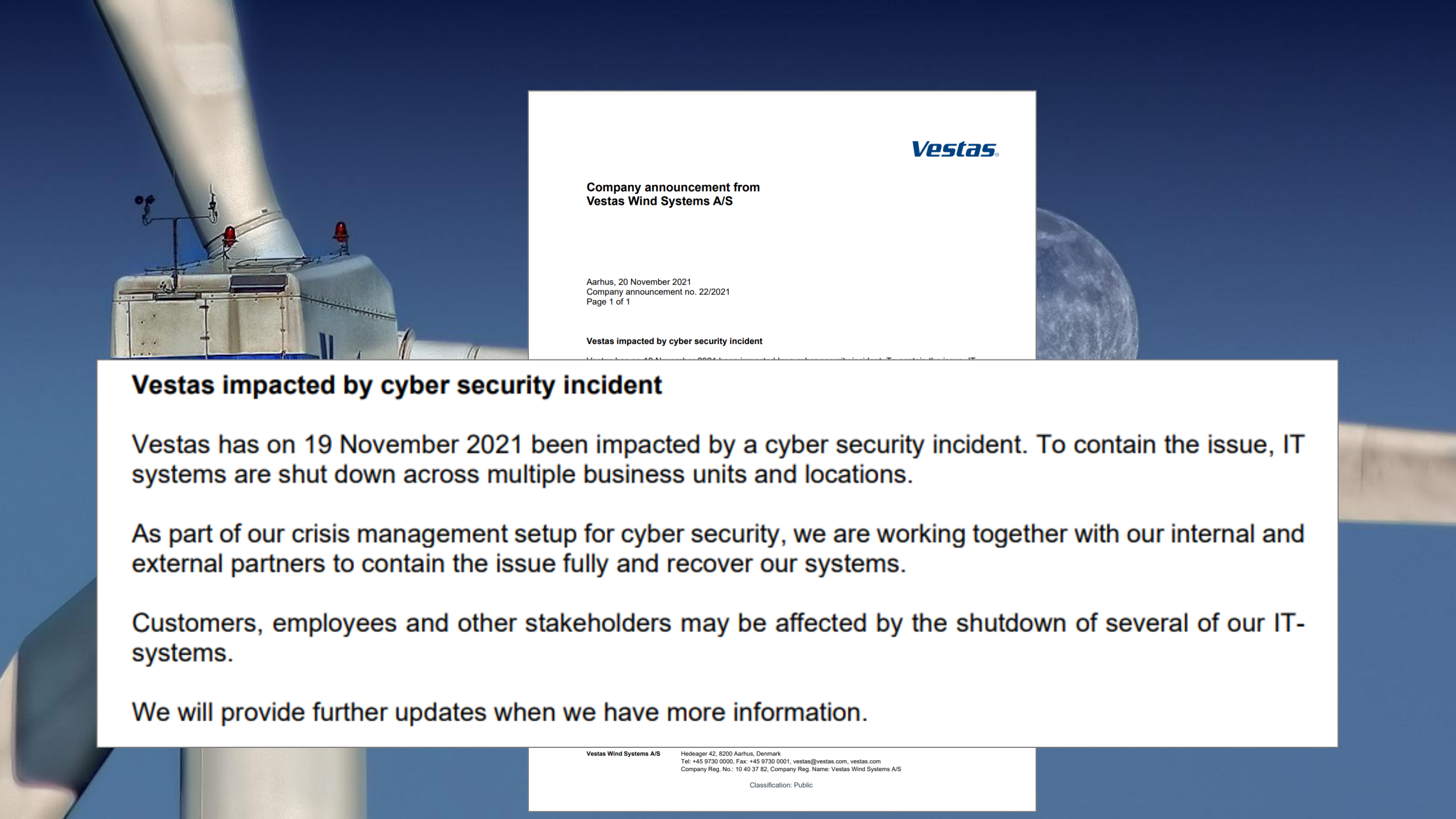
Customers, employees and other stakeholders may be affected by the shutdown of several of our IT-systems.

We will provide further updates when we have more information.

Contact details
Vestas Wind Systems A/S, Denmark

Mathias Dalsten, Vice President,
Investor Relations
Tel: +45 2829 5383

Anders Riis, Vice President,
Communications
Tel: +45 4181 3922



Vestas

Company announcement from
Vestas Wind Systems A/S

Aarhus, 20 November 2021
Company announcement no. 22/2021
Page 1 of 1

Vestas impacted by cyber security incident

Vestas impacted by cyber security incident

Vestas has on 19 November 2021 been impacted by a cyber security incident. To contain the issue, IT systems are shut down across multiple business units and locations.

As part of our crisis management setup for cyber security, we are working together with our internal and external partners to contain the issue fully and recover our systems.

Customers, employees and other stakeholders may be affected by the shutdown of several of our IT-systems.

We will provide further updates when we have more information.

Vestas Wind Systems A/S Hedeager 42, 8200 Aarhus, Denmark
Tel: +45 9730 0000, Fax: +45 9730 0001, vestas@vestas.com, vestas.com
Company Reg. No.: 10 40 37 82, Company Reg. Name: Vestas Wind Systems A/S

I GÅR KL. 17:22

Vestas efter 'cybersikkerhedshændelse': 'Indtil videre er vindmøller ikke påvirket'

LÆS OP ORDBOG TEKST

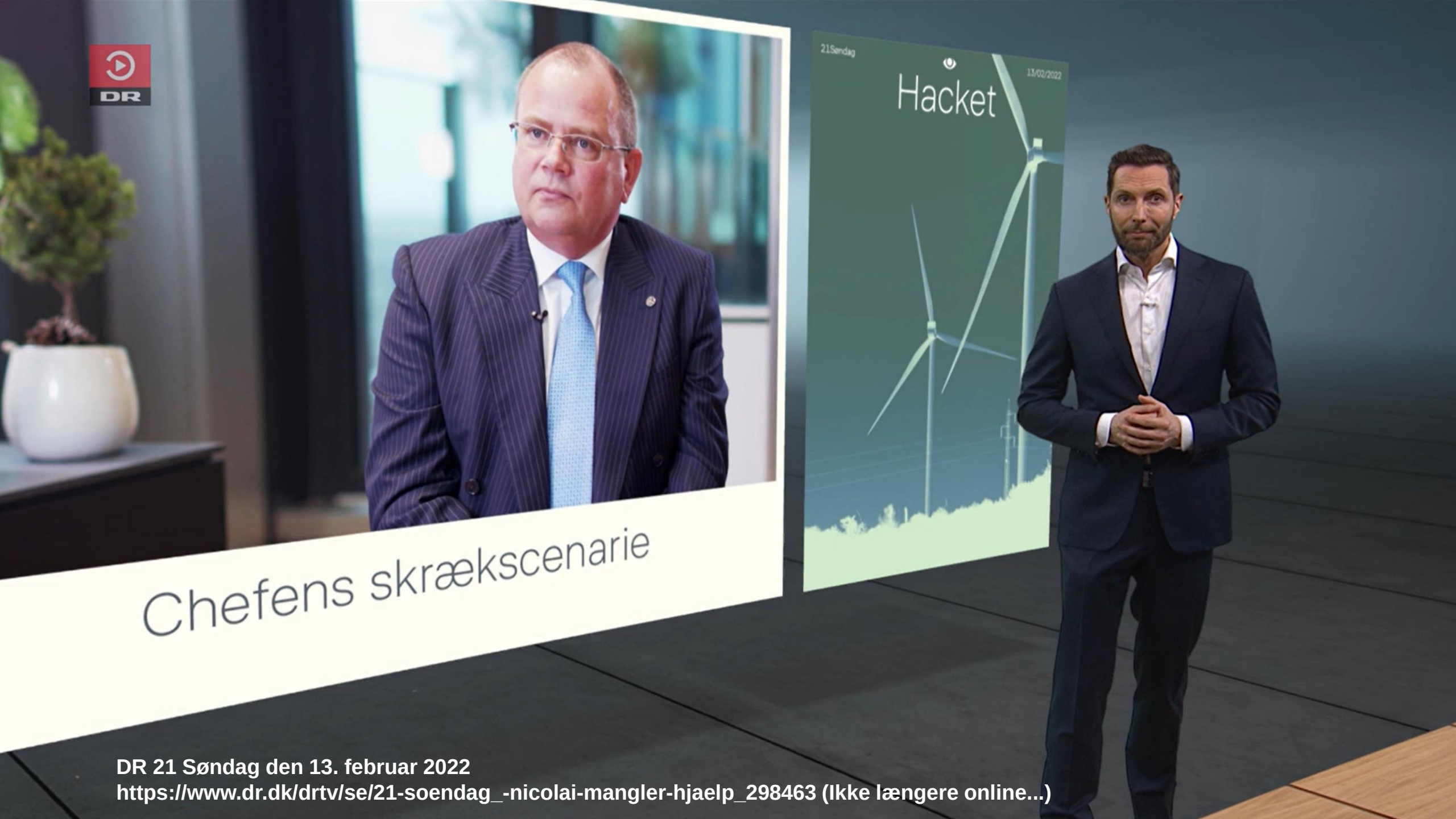
AF
Mathias Oldager

Selvom Vestas tidligere i dag meldte ud, at de er ramt af en "cybersikkerhedshændelse", så er selskabets møller umiddelbart ikke ramt.

Det oplyser virksomheden overfor DR Nyheder.

- Indtil videre er vindmøller ikke påvirket af situationen, og selvom det er for tidligt at udelukke noget, vurderes risikoen som lav, skriver Anders Riis, kommunikationsdirektør i Vestas.

It-systemer på tværs af



DR 21 Søndag den 13. februar 2022
https://www.dr.dk/drtv/se/21-soendag_-nicolai-mangler-hjaelp_298463 (Ikke længere online...)

Velorganiserede cyber-kriminelle

Målrettet afpresning

- Cyber kriminalitet er en lukrativ forretning, og det er nemt at starte
- Afpresning via krypto-ransomware og datatyveri målrettet mod virksomheder – skiftet væk fra private/enkelte brugere
- Metoder som tidligere kun blev brugt i målrettede angreb anvendes nu af almindelige kriminelle
- Automatisering der tillader spredning internt i virksomhedens netværk og systemer
- Krav om markant højere løsesummer og påvirkning af aktiekurser med mulighed for spekulation

Seksdobbelt afpresning

1. Låsning af data
2. Tyveri af data & trusler om offentliggørelse
3. Denial-of-service angreb
4. Kontakt til kunder og samarbejdspartnere
5. Kontakt til konkurrent for at sælge data
6. Anmeldelse til tilsynsmyndigheder

Dubex:

Your network has been infected!

Your documents, photos, databases and other important files **encrypted**

To decrypt your files you need to buy our special software - **General-Decryptor**

Follow the instructions below. But remember that you do not have much time

General-Decryptor price

the price is for all PCs of your infected network

You have 2 days, 23:38:14

* If you do not pay on time, the price will be doubled
* Time ends on **Jul 5, 14:15:38**

Current price **24435.5 XMR** ≈ 5,000,000 USD

After time ends **48871 XMR** ≈ 10,000,000 USD

Monero address:

* XMR will be recalculated in 5 hours with an actual rate.

Black Basta Blog

REDACTED

Basta News

Support

search

etude-villa.fr

Etude Villa Florek - legal services

SITE: *www.etude-villa.fr*

ADDRESS
18 Rue Néricault Destouches
37013 Tours
France

Published 100% | Visits 220

Read more

arenaproducts.com

Reusable Bulk Packaging Solutions

***Arena Products** is a leading packaging, design and pooling company in North America. With 30 years of experience, we provide a full spectrum of services for the*

Data exposure in: 2 d 13:27:32

Read more

agrovi.dk

*[EN] **Agrovi** provides finance, auditing, trade and counselling services for the agricultural sector.*

*[DK] **Agrovi** yder rådgivning til landmænd, landboer og andre erhvervsdrivende. Vi er specialister i regenerativt landbrug og holder os selv og vores kunder opdateret med den nyeste teknologi, der*

Data exposure in: 2 d 13:25:20

Read more

maytec.de

MayTec 100% privately owned family entity. LIT Group owns 17 companies across the USA, Canada, and Europe Company complex covering approximately 13,000 sq. m. Medium-sized international company with subsidiaries in the USA and

Data exposure in: 3 d 8:46:22

Read more

edc.dk

*[EN] **EDC** is a real estate company that specializes in buying, selling and valuing real estate.*

[DK] Vi er Danmarks største ejendomsmæglerkæde, og det er vi stolte af. Vi tror på, at det er en position, man kun kan forsvare

Data exposure in: 4 d 3:31:11

Read more

shopbentley.com

***Bentley & Co LTD's** great adventure began in 1987 in St. John's, Newfoundland, CA. Since that time, our growth and advancement has never stopped. We continue to reinvent ourselves to provide our customers with the best experience on the market and peace of mind with our everyday*

Published 100% | Visits 919

Read more

uchlogistics.co.uk

***UCH** Logistics is a dynamic, customer focused provider of specialist transport services to the airfreight industry. Having been established in this industry since the year 2000, we have built a reputation for offering reliable*

Published 100% | Visits 958

Read more

boulangerieauger.com

Boulangerie Auger is first and foremost a story of family and traditions. We are inspired by our heritage to offer current products and develop breads that Quebecers and Ontarians will love tomorrow.

Published 100% | Visits 1328

Read more

rekord.de

REKORD ist meisterlicher Fachbetrieb für Fenster Sonderbau, Sprossenfenster und Denkmalschutzfenster. Damit können Sie sicher sein, ein handwerklich meisterhaftes und technisch perfektes Einzelstück zu erhalten. Eine Qualität, die bei uns von rekord seit über 100 Jahren gute Tradition ist. Unsere Produkte tragen das bekannte

Published 0% | Visits 1293

Read more

cmcsheetmetal.com

CMC Sheet Metal is a premier sheet metal fabrication facility located in Capitol Heights, Maryland providing the highest quality HVAC Construction Services to our clients and the industry. During that time we have preformed individual

Published 100% | Visits 1280

Read more

Black Basta Blog

REDACTED

Basta News

Support

edc.dk

[EN] ***EDC*** *is a real estate company that specializes in buying, selling and valuing real estate.*

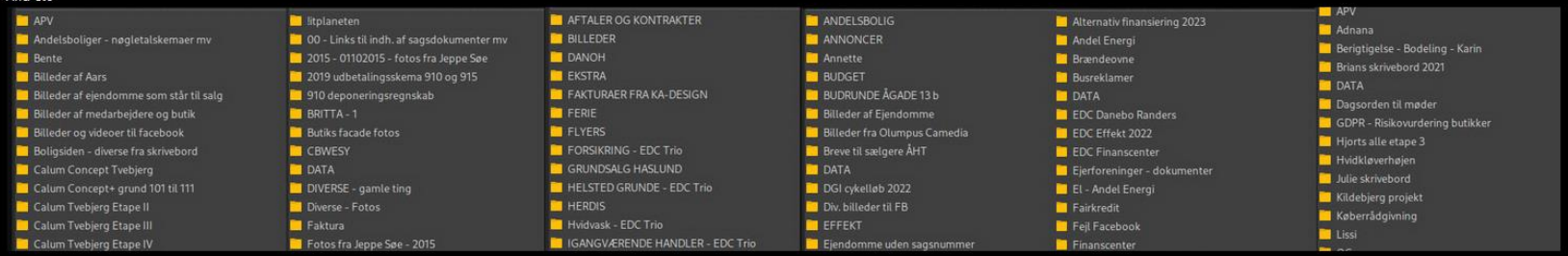
[DK] Vi er Danmarks største ejendomsmæglerkæde, og det er vi stolte af. Vi tror på, at det er en position, man kun kan forsvare gennem 50 år ved at gøre sit bedste, og derfor gør vi os umage hver eneste dag.
*EDC har over 230 selvstændige butikker over hele landet og cirka 1.600 medarbejdere. Det betyder, at der altid er en lokalkendt mægler i nærheden af dig, der kan hjælpe dig med din bolighandel - uanset om du skal købe, sælge eller bare er nysgerrig på boligmarkedet. *

SITE: *www.edc.dk*

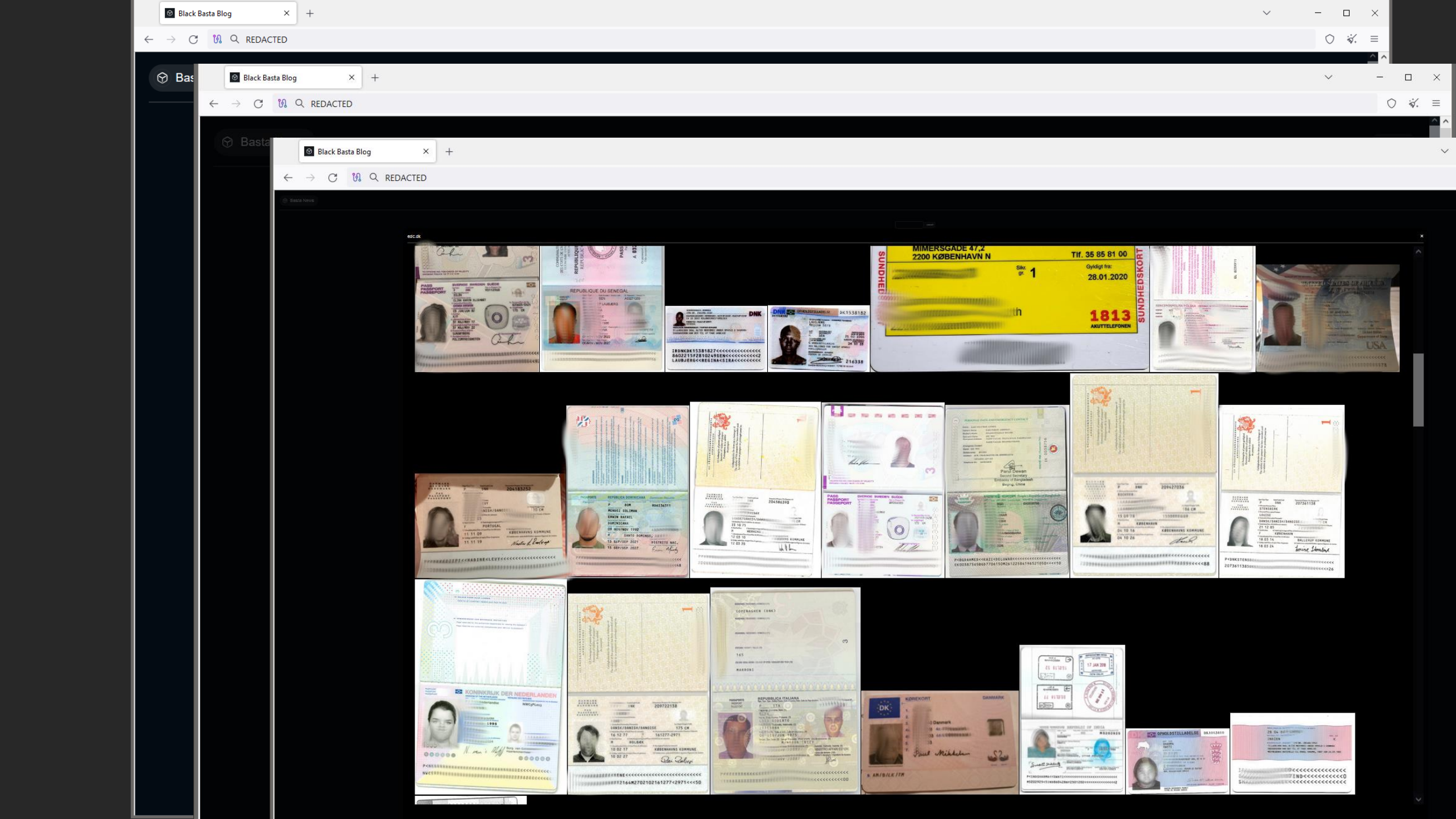
ADDRESS:
EDC Gruppen A/S
Mynstersvej 5, 1827 Frederiksberg C
Tlf.: 33 26 77 77

ALL DATA SIZE: 2.5tb
1. Administration
2. Human Resources
3. Client files
4. GDPR
5. Finance

And etc



Data exposure in:


Black Basta Blog
REDACTED
Black Basta Blog
REDACTED
Black Basta Blog
REDACTED
edc.dk
MIMERSGADE 47,2
2200 KØBENHAVN N
Tlf. 35 85 81 00
SUNDHEDSKORT
Gyldigt fra:
28.01.2020
1813
AKUTTELEFONEN
REPUBLIQUE DU SENEGAL
KONINKRIJK DER NEDERLANDEN
REPUBBLICA ITALIANA
KØREKORT
DANMARK

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

Conti (tidl. Ryuk)

Russisk it-virksomhed med innovative forretningsmodeller…

Branche:
Organiseret kriminalitet

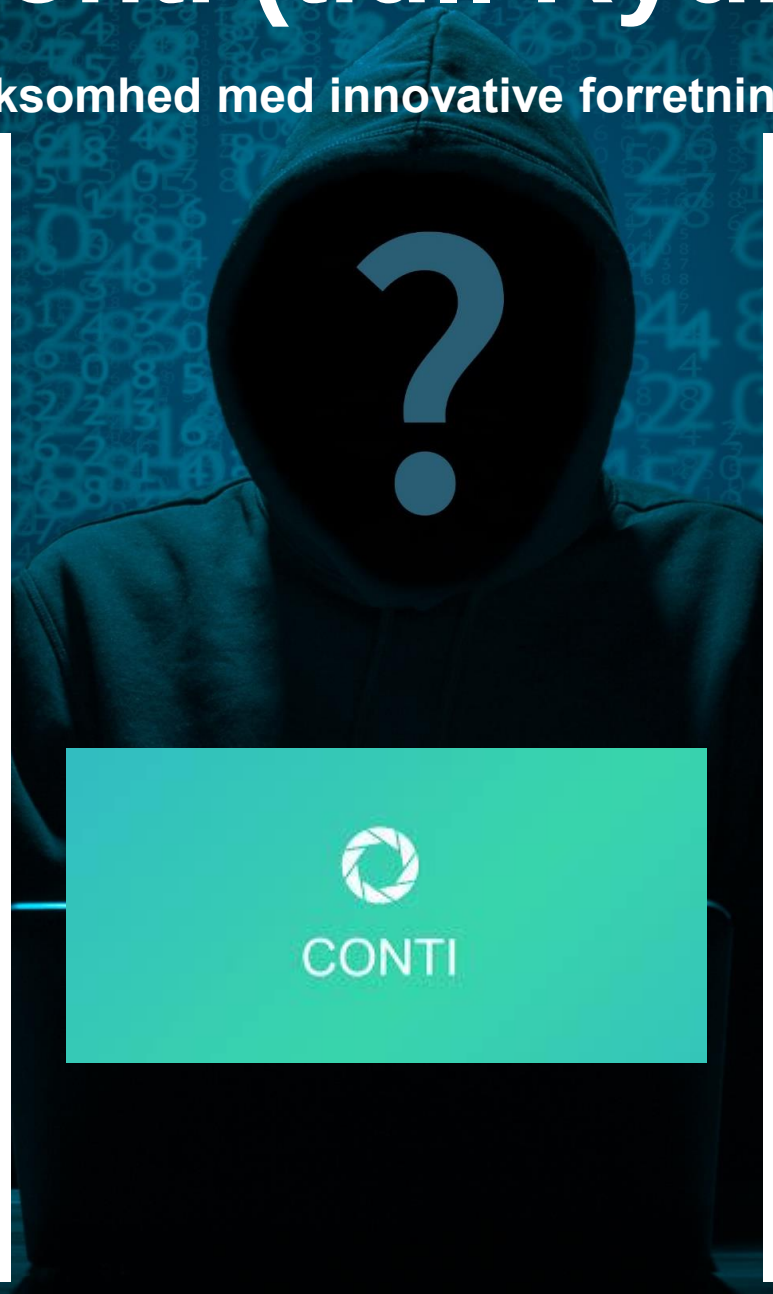
Balance/egenkapital:
?

Omsætning:
$180 million (2021)

Resultat før skat:
Ukendt men stort

Salg:
Ransomware-as-a-Service
Datalæg og afpressning

Kunder:
1000+ Virksomheder og organisationer primært i Vesteuropa og USA (Hospitaler, butikskæder, produktion, rådgivning m.m.)



Ansatte:
62 FTE (Juli 2021)
Konsulenter

Værdier:
Ingen…

IT:
Egen IT platform
Kompromitterede systemer

Underleverandører:
Trickbot og Emotet crimeware-as-a-service platforme

Ejerkreds:
Russiske kriminelle

Ledelse og bestyrelse:
“Tramp,” “Dandis,” “Mango,” “Professor” og “Reshaev.”

Conti organization

HR Cyber-criminal Recruitment	Penetration Testers/Hackers
Coders Malware Writer	Testers
Reverse Engineers	Network and System Admin
Offensive Team	OSINT Specialists
Crypters	Negotiation Staff

CNBC

Leaked documents show notorious ransomware group has an HR department, performance reviews and an ‘employee of the month’

THE SITE IS NOW UNDER CONTROL OF LAW ENFORCEMENT

This site is now under the control of The National Crime Agency of the UK, working in close cooperation with the FBI and the international law enforcement task force, 'Operation Cronos'.

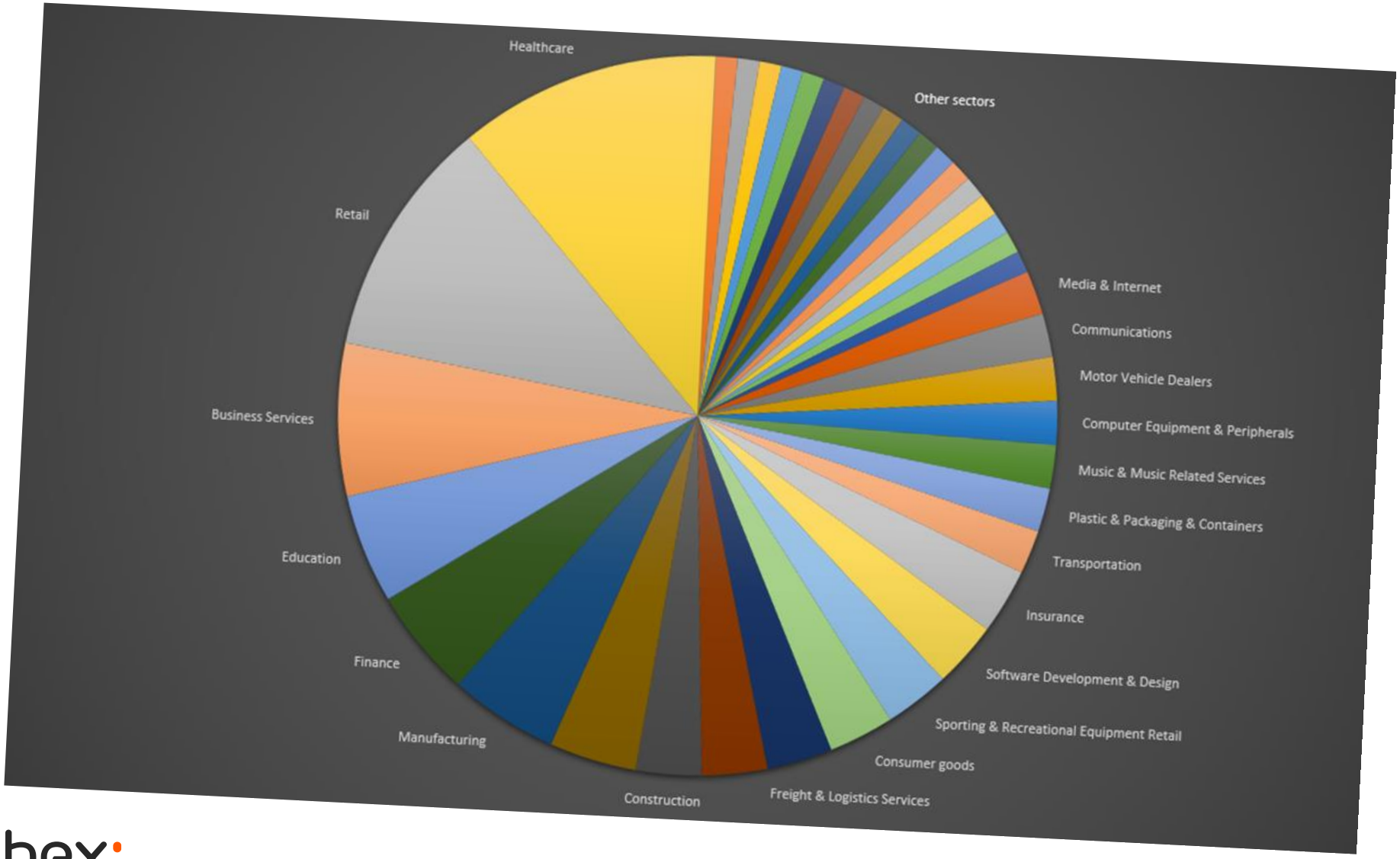
We can confirm that Lockbit's services have been disrupted as a result of International Law Enforcement action – this is an ongoing and developing operation.

Return here for more information at:

11:30 GMT on Tuesday 20th Feb.

NCA National Crime Agency
SOUTH WEST ROCU
METROPOLITAN POLICE
EUROPOL
POLITIE
Bundeskriminalamt
Kanton Zürich
Gendarmerie nationale
OFAC
SH Schleswig-Holstein Landeskriminalamt
POLIISI

Conti - Hvem bliver ramt af ransomware?

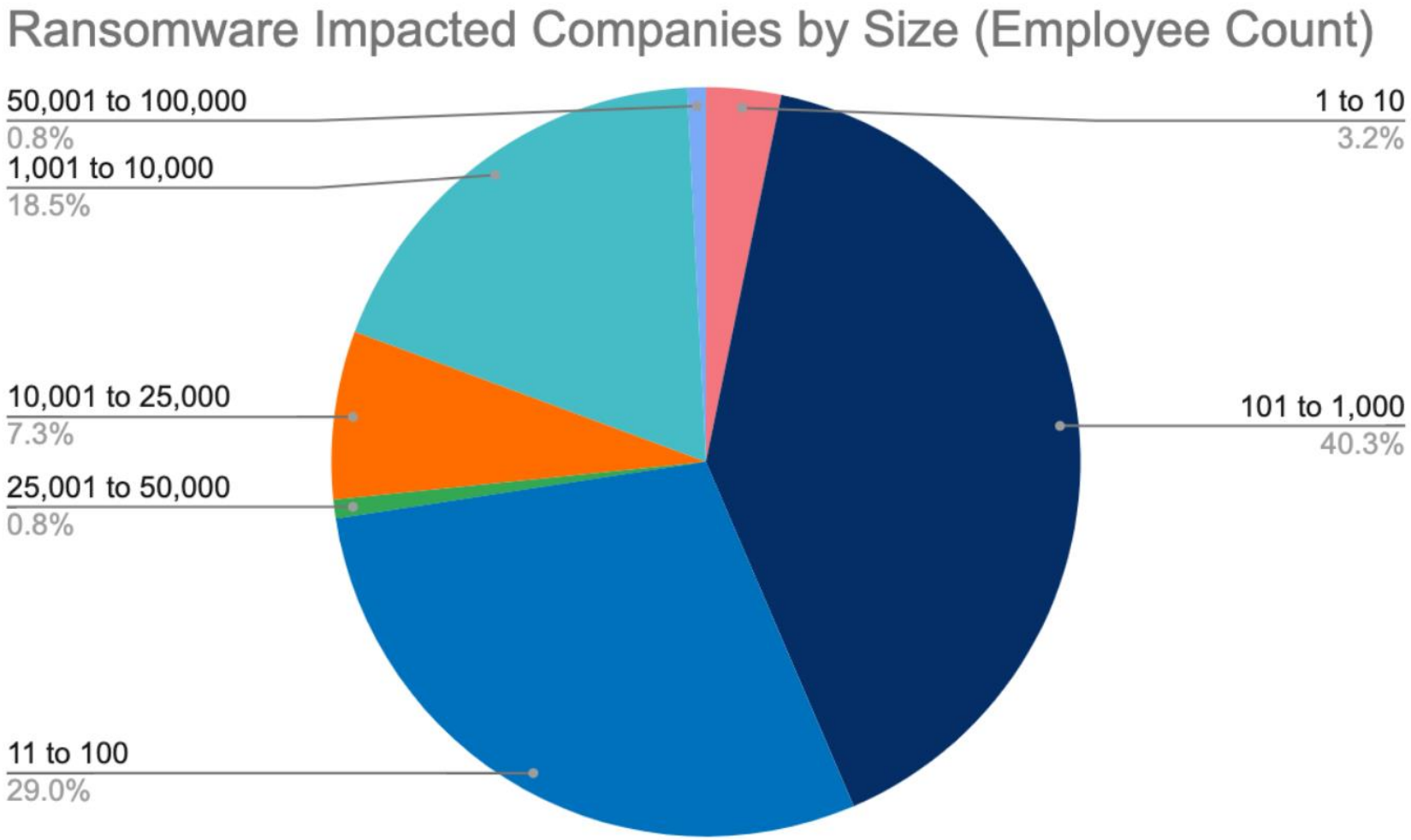


The chart gives an overview of the Conti's potential victims by sector

Dubex:

Trellix https://www.trellix.com/en-au/about/newsroom/stories/research/conti-leaks-examining-the-panama-papers-of-ransomware.html

Hvem bliver ramt?



Dubex:

https://www.coveware.com/blog/2023/1/19/improved-security-and-backups-result-in-record-low-number-of-ransomware-payments

Her tjener de kriminelle de fleste penge…

Business E-Mail Compromise - CEO/CFO Svindel

- Svindel rettet mod de ansatte der må overføre penge
- Rammer 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

Kærlighedssvindel

- Falsk profiler på en dating- eller social medieplatforme – falske billeder
- Foregiver ønske om romantisk forhold med det intetanende offer
- ”Social engineering”, hvor svindlerne bruger stærke følelser og overbevisende manipulation til at opnår ofrets tillid og skabe en alternativ virkelighed, hvor ofret sidder fast
- Social manipulation får offeret til at sende penge, gaver eller personlige oplysninger
- Ofrene for kærlighedssvindel oplever ofte alvorlige fødselsmæssige konsekvenser

Afpressning o.a. svindel

- Porno-afpresning hvor der trues med offentliggøre af kompromitterende video optaget, mens personen har set (børne)porno
- MitID Svindel med falske mails og SMS’er og telefonopkald
- Online shopping svindel via falske webshop der sælger kopivare eller decideret stjæler penge
- Phishing med falske e-mails eller SMS’er fra legitime virksomheder der beder om at klikke på et link

Agenda

01 Cyberrisikoen for digitale virksomheder

02 Truslen fra digitale mafiagrupper

03 Virksomheder i en ny geopolitisk virkelighed

04 Fremtiden & opsamling

Dubex:

Stater og efterretningstjenester

- Cyberangreb er billige, nemme, effektive og risikofri
  - Cyber-spionage
  - Destruktive cyberangreb - sabotage
  - Propaganda og indblanding - påvirkning på bl.a. sociale medier
  - Samarbejde mellem stater og kriminelle

- Alle lande kan udføre angreb med små midler
  - Angrebsværktøjer kan købes som kommercielle produkter
  - 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?

Globale statslige aktører

Rusland har omfattende kapaciteter til at udføre alle former for cyberangreb herunder cyberspionage og destruktive angreb.

Rusland har udvist stor villighed til at anvende cyberangreb til at understøtte både politiske og militære målsætninger. Cyberkriminelle grupper kan de facto opererer sikkert fra Rusland.

Rusland både politisk, strategisk og teknologisk interesse i at angribe Danmark.

Iran har i de senere år udviklet deres kapaciteter til at udføre cyberangreb, herunder cyberspionage og destruktive angreb.

Iran har udvist stor villighed til at anvende destruktive cyberangreb mod særligt regionale og vestlige mål.

Iran har primært en spionagemæssige interesse (både teknologisk og politiske) i at angribe Danmark.

Kina råder over omfattende kapaciteter til at udføre alle former for cyberangreb, men er primært aktive indenfor cyberspionage.

Kina har udvist stor villighed til at anvende cyberspionage til at fremme politiske, millitære og økonomiske mål.

Kina har primært en spionagemæssige interesse (både teknologisk og politiske) i at angribe Danmark.

Nord Korea har i de senere år udviklet deres kapaciteter til at udføre cyberangreb, herunder spionage, politiske og destruktive angreb samt økonomisk motiverede angreb.

Nord Korea har udvist stor villighed til at anvende destruktive cyberangreb mod særligt regionale og vestlige mål.

Nord Korea har begrænset interesse i at angribe Danmark.

Dubex:

Ruslands cyberoperationsgrupper

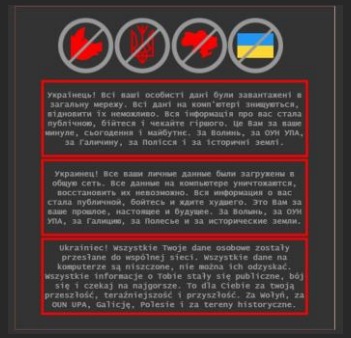
- Rusland er en stærk cyberaktør med lang erfaring
- Bred vifte af mål
  - Spionage og rekognosceringsaktiviteter
  - Angreb mod forsyningskæder og service udbydere
  - Målrettede angreb mod kritisk infrastruktur
- Angrebsmetoder - Bruger mange forskellige TTP'er
  - Destruktive malware- og ransomware-operationer
  - DDoS-angreb
- Påvirkning, desinformation og propaganda
- Kombiner forskellige koordinerede angreb i cyber- og fysisk domæne for at nå sine strategiske mål
- I øjeblikket de fleste angreb på Ukraine, risikoen for følgeskader er reel (NotPetya)

FSO	FSB	SVR	GRU
Russian Federal Protective Service	Federal Security Service of the Russian Federation	Foreign Intelligence Service	Main Directorate of the General Staff
	ACTINIUM Phishing, data theft **BROMINE** Data theft **KRYPTON** Reconnaissance, phishing TURLA	**NOBELIUM APT29** Password spray, phishing (Ukrainian and NATO member diplomatic targets)	**STRONTIUM** Data theft, phishing (military targets) Sandworm **IRIDIUM APT 29** Destruction: FoxBlade wiper; CaddyWiper, Industroer2 **DEV-0586** Destruction: WhisperGate wiper, data theft, influence operations

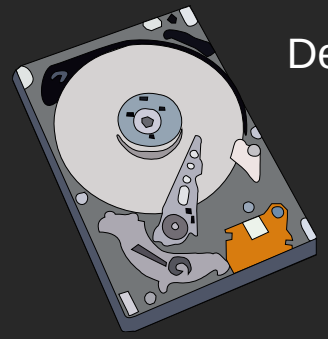
Cyberkriminelle aktører

Dubex:

DDoS and defacement on Government, Military, Financial and Telco



DDoS



Wiper Malware

Destructive wipers – 10+ e.g.:
- WhisperGate (13 Jan 2022)
- HermeticWiper/FoxBlade (23 Feb 2022)
- ACIDRAIN – satellite modems (24 Feb 2022)
- IsaacWiper/HermeticWizard (1 Mar 2022)
- DesertBlade (1 Mar 2022)
- CaddyWiper (14 Mar 2022)
- DoubleZero (mid-Mar 2022)
- Industroyer2 – PowerGrid (8 Apr 2022)

Destructive attack on private company Viasat to disable Internet connectivity

КИЇВСТАР

Destructive attack on mobile telco Kyivstar (12 Dec 2023)

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

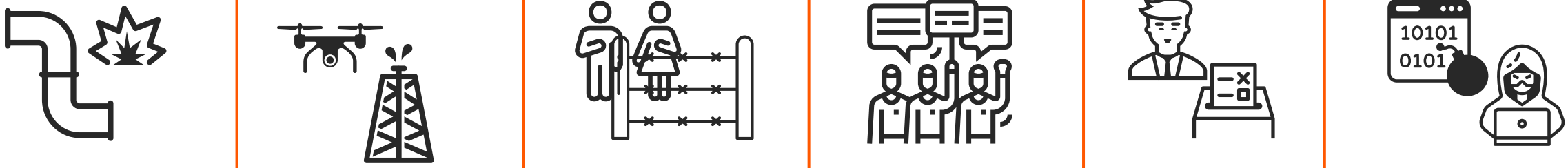
Attacks from Ukraine IT Army and anonymous against Russia – DDoS, Deface, information theft, anti-Russian hacktivism etc.

Infamous Chisel malware targeting Ukranian soldiers Android phones (CISA Alert AR23-243A)

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

Truslen om eskalering

Hybridkrig



Sabotage | Intimidering | Flygtninge | Protester | Politikere | Cyberangreb

Dubex:

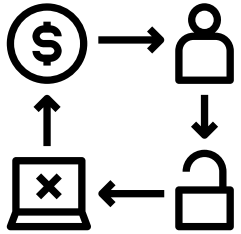
Refleksiv kontrol er et koncept, hvor man påvirker en modstanders beslutninger ved at påtrykke dem antagelser, der ændrer den måde, de handler på

Konsekvenser for virksomheder

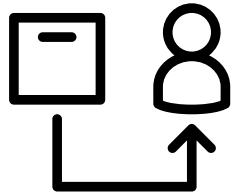
En ny ustabil og udfordrende geopolitisk virkelighed	Magtfulde lande med autokratiske ledere og geopolitiske ambitioner	Økonomi, energi og teknologi anvendes som våben	Globalisering i bakgear – kontrol med fokus på kortere supply chains	Kriminelle grupper finder beskyttelse i – og hjælper - autokratiske lande

Hybridkrig på Internettet

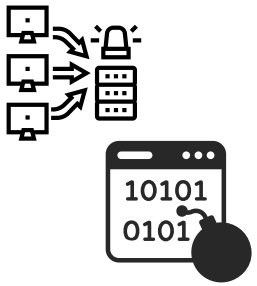
Spionage



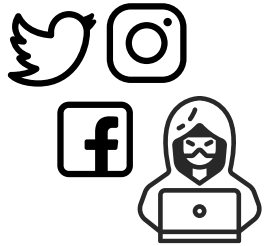
Kriminalitet som våben



Supply Chain



Destruktive angreb



Desinformation & Påvirknings-angreb

Cyberwar

Dubex:

Alle virksomheder er nødt til at forholde sig til at ændrede geopolitiske forhold også ændre trusselsbilledet væsentligt i negativ retning…

REUTERS® World Business Markets Sustainability Legal Breakingviews Technology Investiga

Aerospace & Defense

Rheinmetall in talks on building tank factory in Ukraine - report

Reuters

March 4, 2023 12:36 PM GMT+1 · Updated 6 months ago

Daryna Antoniuk

April 14th, 2023

Briefs

German arms manufacturer Rheinmetall confirms cyberattack

German automotive and arms manufacturer Rheinmetall suffered a cyberattack on Friday, the company said.

The attack hit Rheinmetall's business unit that serves industrial customers, particularly in the

RHEINMETALL

POLITIK

Danmark garanterer støtte til Ukraine de næste ti år: 'Hvis vi ikke står sammen, står Europa potentielt ikke'

Som det første land i Norden laver Danmark en aftale om 'sikkerhedstilsagn' til Ukraine.

LÆS OP ORDBOG TEKST

AF Tobias Leth Klinge

CFCS
@Cybersikkerhed

Flere hjemmesider under Forsvarsministeriets koncern kan i øjeblikket være utilgængelige som følge af et overbelastningsangreb (ddos-angreb).
CFCS er i dialog med de relevante parter om afbødende tiltag.

11:49 AM · Feb 23, 2024 · **5,482** Views

Prorussisk hackergruppe tager ansvaret for at lægge hjemmesider ned: »Vi giver Danmark en uforglemmelig weekend«

Flere danske lufthavne, herunder Københavns Lufthavn, og øvrige hjemmesider er søndag ramt af massive hackerangreb. Prorussisk hackergruppe kan stå bag.

Fra Telegram

Agenda

01 Cyberrisikoen for digitale virksomheder

02 Truslen fra digitale mafiagrupper

03 Virksomheder i en ny geopolitisk virkelighed

04 Fremtiden & opsamling

Dubex:


HUSK:
Udviklingen i trusselbilledet sker ikke revolutionært, men evolutionært
... så med lidt fremsynethed og sund fornuft kan vi være foran…

Threats 2024 and beyond

1. AI and Large Language Model
2. Evolving Ransomware – and other cyber extorsion
3. Evasive phishing cyber attacks – using AI and deepfake
4. Disinformation, cyberwar & hybrid-war – attacks on elections & destructive attacks
5. Disruptive hacktivism e.g. DDoS
6. Use of zero-day vulnerabilities - and targeting edge devices
7. Supply chain attacks on the rise (software and services)
8. Clouds and identities under attack
9. Internet of Things and devices
10. Mobile device attacks

Dubex:

Artificial intelligence and cyberattacks

North Korean Hackers Using AI in Advanced Cyberattacks

U.S.-Led Sanctions Do Little to Curtail North Korea's Development of AI

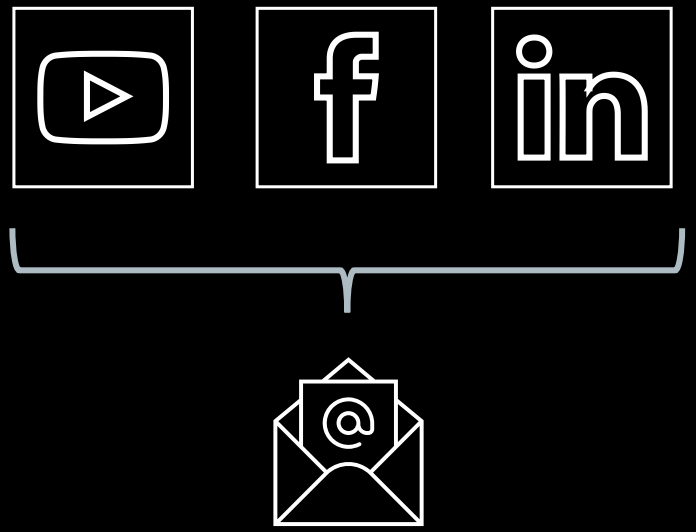
Jayant Chakravarti (@JayJay_Tech) • January 24, 2024

https://www.databreachtoday.com/north-korean-hackers-using-ai-in-advanced-cyberattacks-a-24184

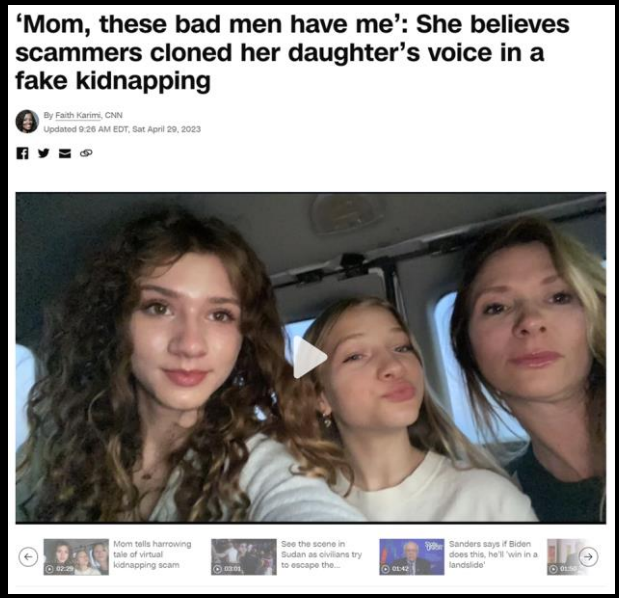
WormGPT - ChatGPT's Evil Twin
Large Language Model

Malware development

AI assisted phishing



Deepfake



Dubex:

Nation-state hackers are exploiting ChatGPT

Crimson Sandstorm (CURIUM)

LLM-supported social engineering: phishing emails, attacker-built website on feminism.

LLM-enhanced scripting techniques: generate code to web dev, remote servers, web scraping

LLM-enhanced anomaly detection evasion

Emerald Sleet (THALLIUM)

LLM-assisted vulnerability research: better understand publicly reported vulnerabilities

LLM-enhanced scripting techniques

LLM-supported social engineering: generation of spear-phishing campaigns against individuals

LLM-informed reconnaissance: identify think tanks, government organizations, or experts on North Korea

Charcoal Typhoon (CHROMIUM) & Salmon Typhoon (SODIUM)

LLM-informed reconnaissance: research and understand specific technologies, platforms, and vulnerabilities

LLM-enhanced scripting techniques: generate, automate and refine scripts

LLM-supported social engineering: translations and communication to manipulate targets

LLM-refined operational command techniques: advanced commands, deeper access, and post-compromise behaviour

Forest Blizzard (STRONTIUM)

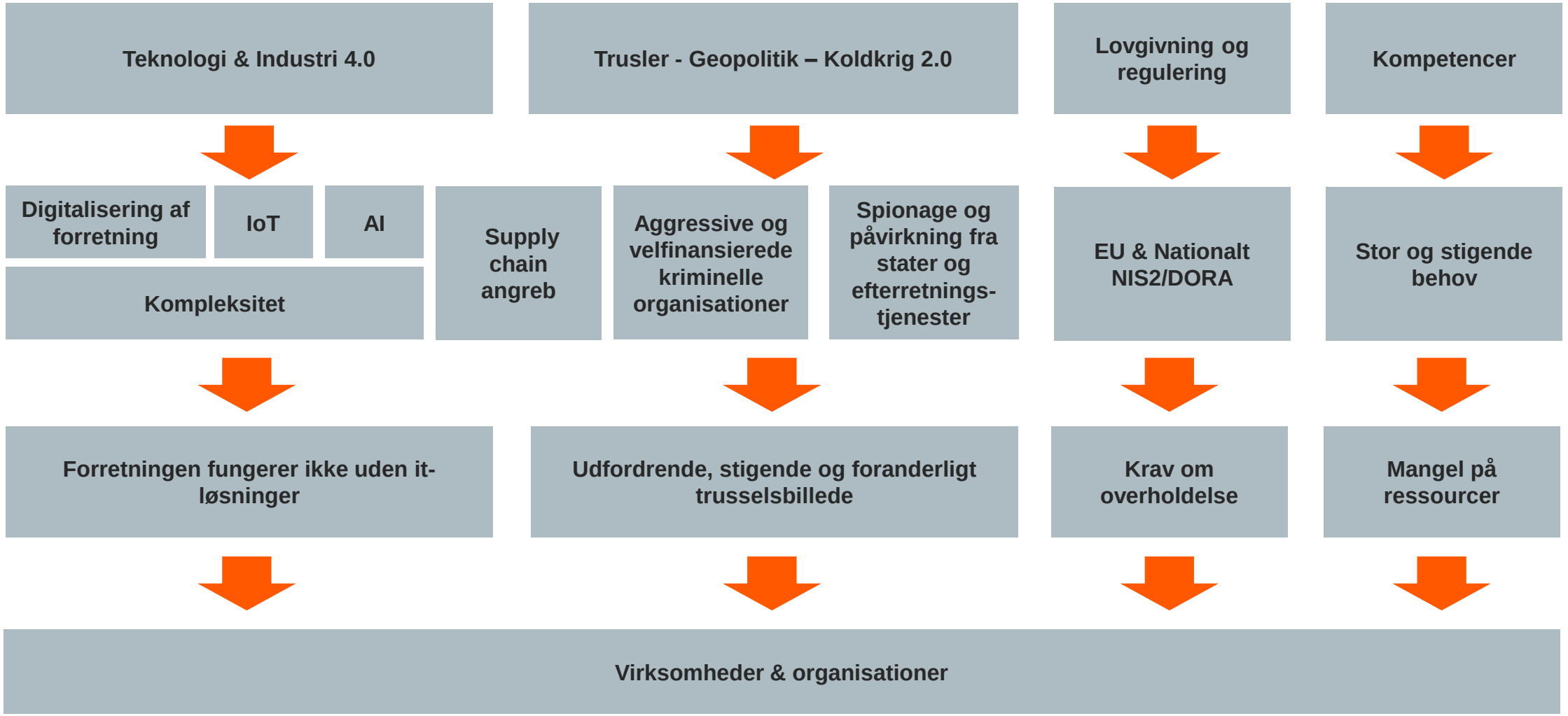
LLM-informed reconnaissance: Understand satellite communication protocols, radar imaging technologies, and specific technical parameters

LLM-enhanced scripting techniques: Assistance in basic scripting tasks, including file manipulation, data selection, regular expressions, and multiprocessing

Dubex:

https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/

Udfordringen for virksomheder & organisationer

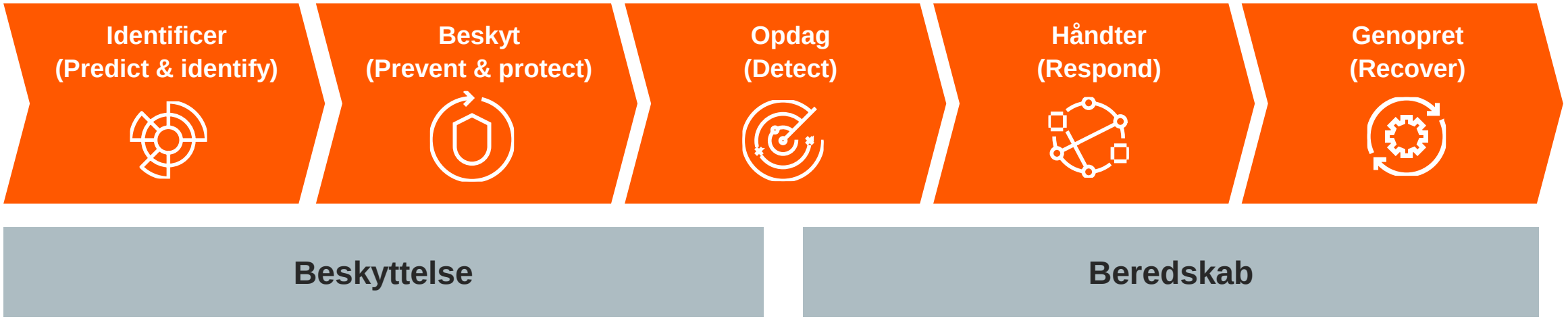


Dubex:

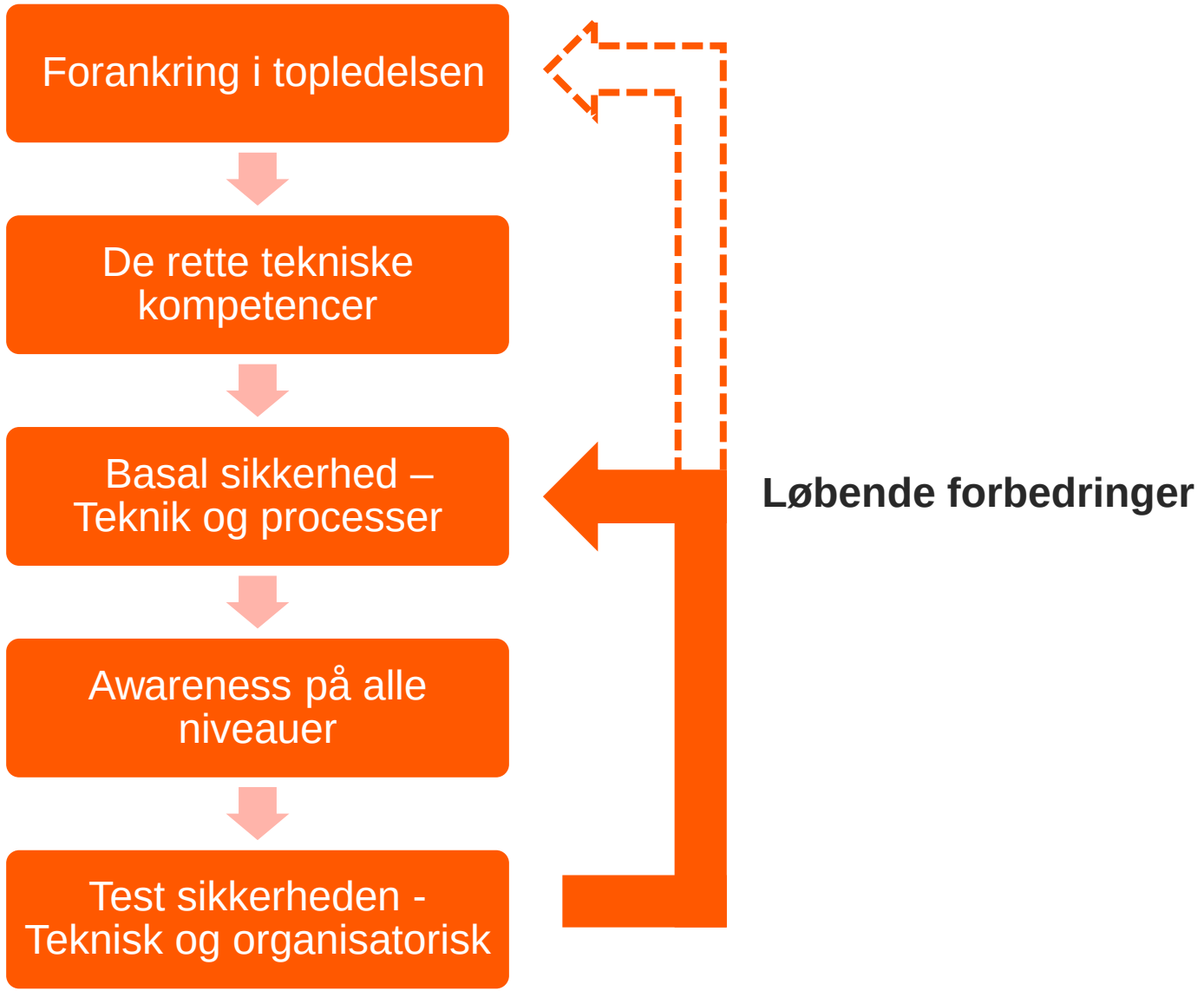
Ledelsens udfordring

- Alle virksomheder er under angreb og risikerer at blive ramt af en alvorlig cyber-incident (erkendelse)
- Alle virksomheder er nødt til at forholde sig til et forøget geopolitisk trusselsbillede (erkendelse)
- De færrest virksomheder har et tilstrækkeligt sikkerheds- og/eller beredskabsniveau (erkendelse)
- Med NIS2 og DORA bliver ledelsen personligt og direkte ansvarlige for virksomhedens cybersikkerhed
- Virksomheden og ledelsen skal kunne dokumentere at der er gjort tilstrækkeligt

Dubex:


Identificer
(Predict & identify)
Beskyt
(Prevent & protect)
Opdag
(Detect)
Håndter
(Respond)
Genopret
(Recover)
Beskyttelse
Beredskab

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:

Top fem anbefalinger – kom i gang nu

Multi-faktor brugervalidering til al ekstern adgang

Overblik - se virksomheden udefra

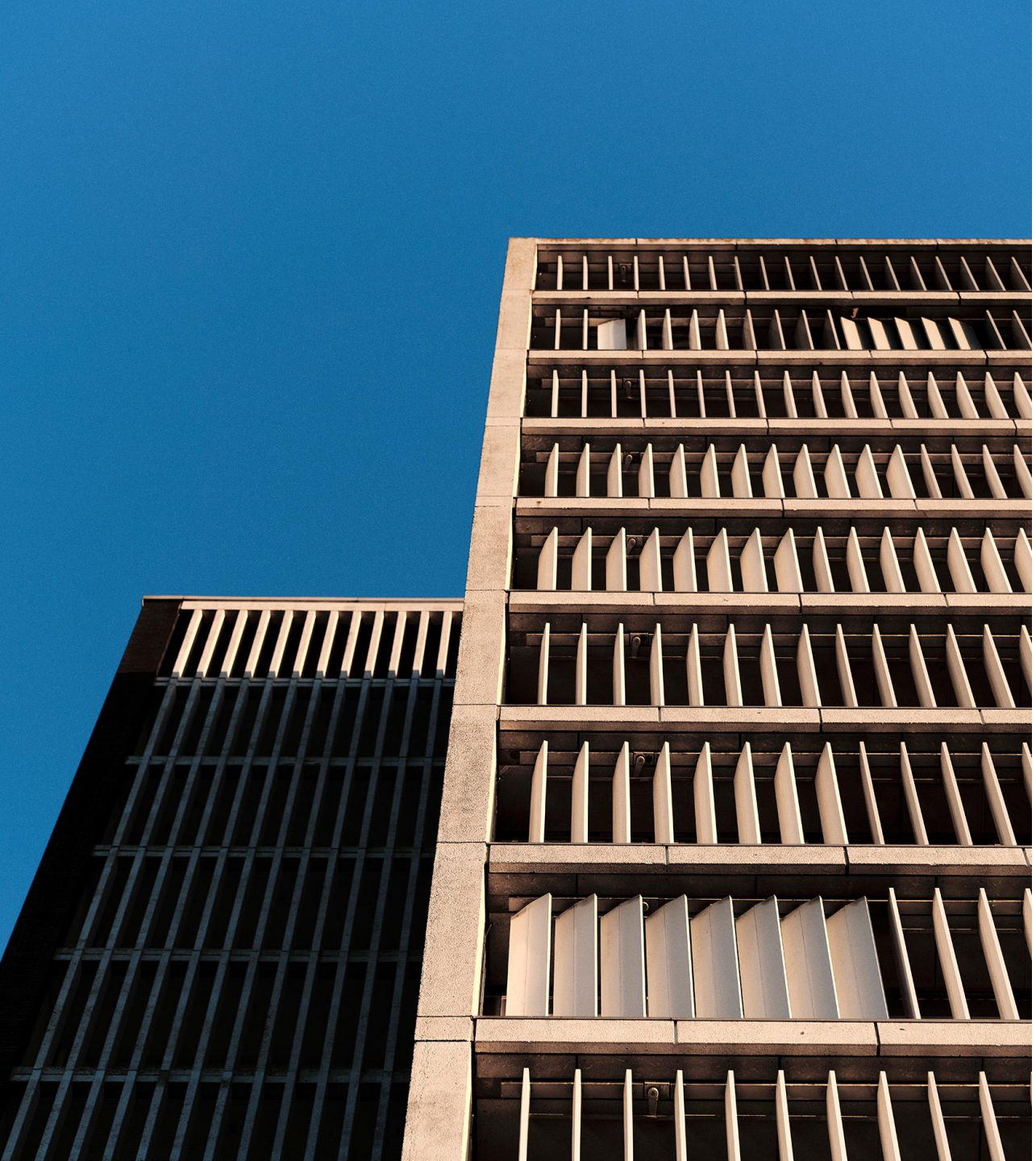
Opdater programmer – fjern sårbarheder

Backup – og helst offline

Beredskabsplan - husk at teste

… og så brug din sunde fornuft

Dubex:



Tak!

Jacob Herbst, CTO

jhe@dubex.dk

+45 2083 0430

Under attack?

+45 32 83 04 03

Dubex A/S

Gyngemose Parkvej 50

DK-2860 Søborg

Denmark

www.dubex.dk

+45 3283 0430

info@dubex.dk

Follow us on X (Twitter), LinkedIn and Facebook