Det aktuelle trusselsbillede for danske virksomheder i 2026

V2SECURITY 2026 København

Jacob Herbst

Den 6./7. maj 2026

Conscia
Secure progress

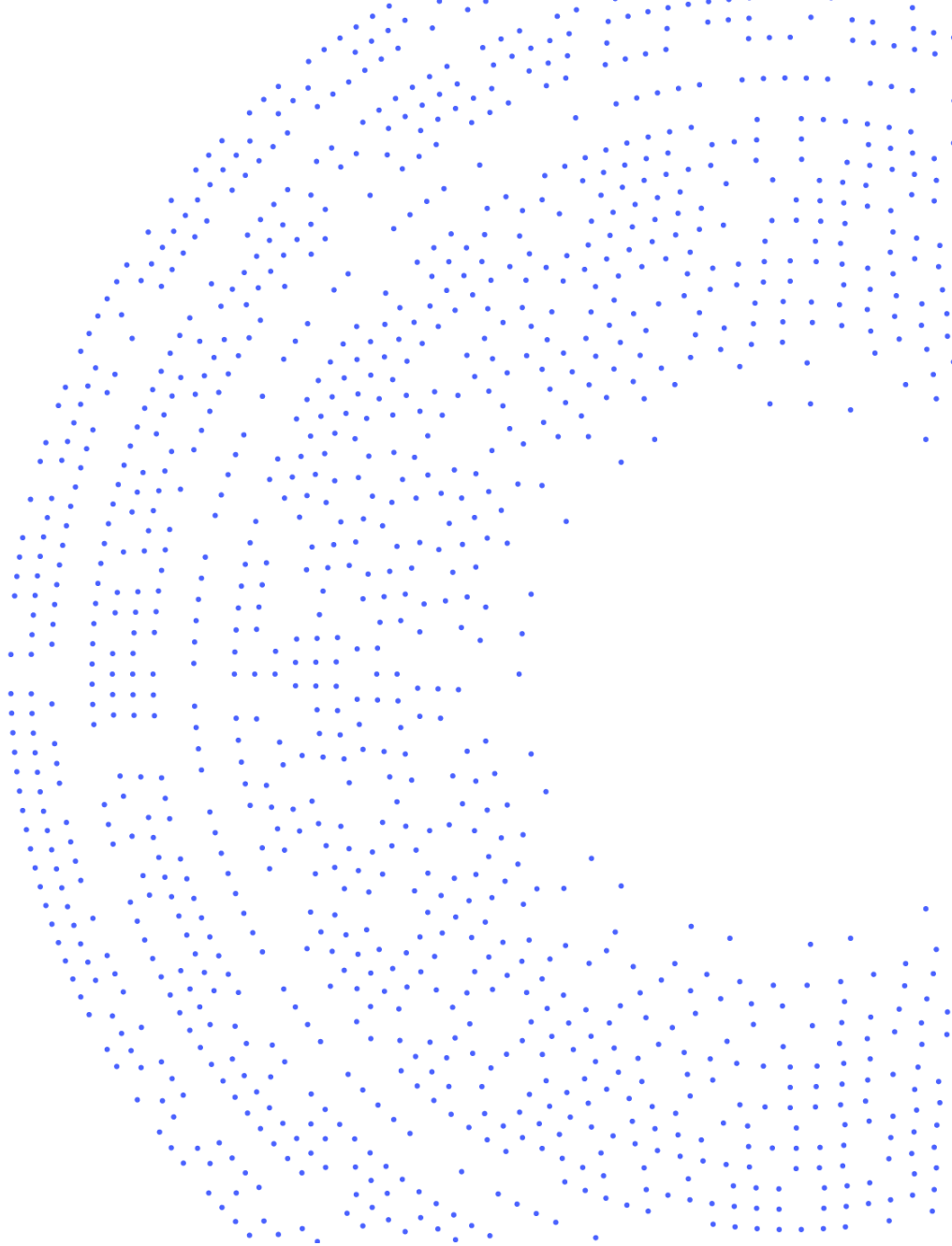
Agenda

01 Cyberrisikoen for digitale virksomheder

02 Truslen fra digitale mafiagrupper

03 Virksomheder i en ny geopolitisk virkelighed

04 Fremtiden & opsamling



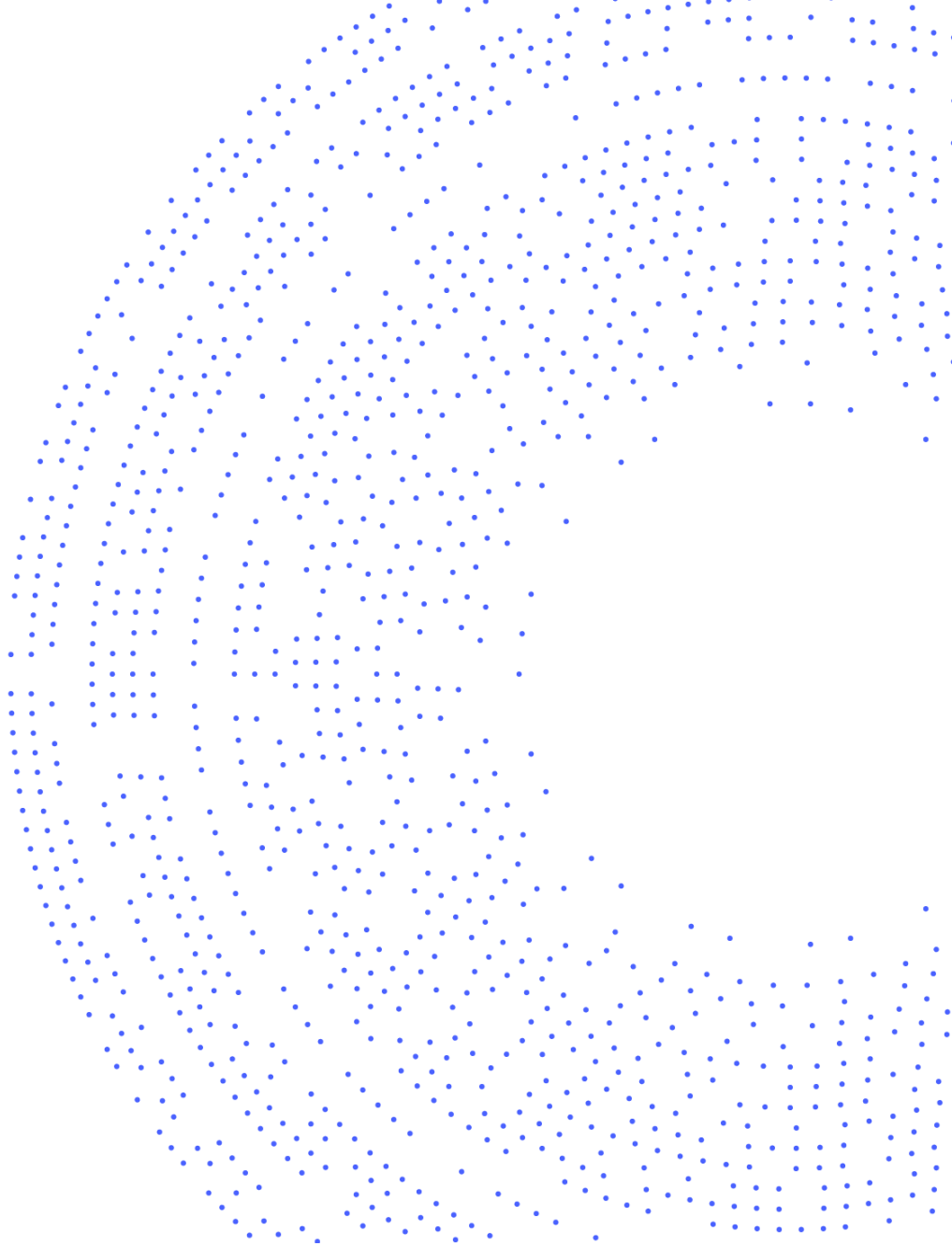
Agenda

01 Cyberrisikoen for digitale virksomheder

02 Truslen fra digitale mafiagrupper

03 Virksomheder i en ny geopolitisk virkelighed

04 Fremtiden & opsamling



Hvorfor er udfordringen større i dag…?

Samfundet er blevet mere kompleks

Digitalisering overalt i samfundet

Kritisk infrastruktur er ejet og drevet af mange aktører

Globalisering – globale teknologi forsynings-kæder

Avancerede tværnationale cybertrusler

Hybride angreb – går efter virksomheder, samfund og livsstil

Manglende erkendelse af truslens kompleksitet

Forbundet digital rygrad i samfundet

Regeringen: Danmark skal have et totalberedskab

Vi skal sikre vores samfund i en usikker tid. Verden forandrer sig, og det skal vores indsats for at passe på Danmark også. Derfor lancerer regeringen et totalberedskab og udmønter over en milliard kroner til en akutpakke til beredskabsområdet.

20.02.2026

https://mssb.dk/nyheder/nyhedsarkiv/2026/februar/pressemeddelelse-regeringen-danmark-skal-have-et-totalberedskab/

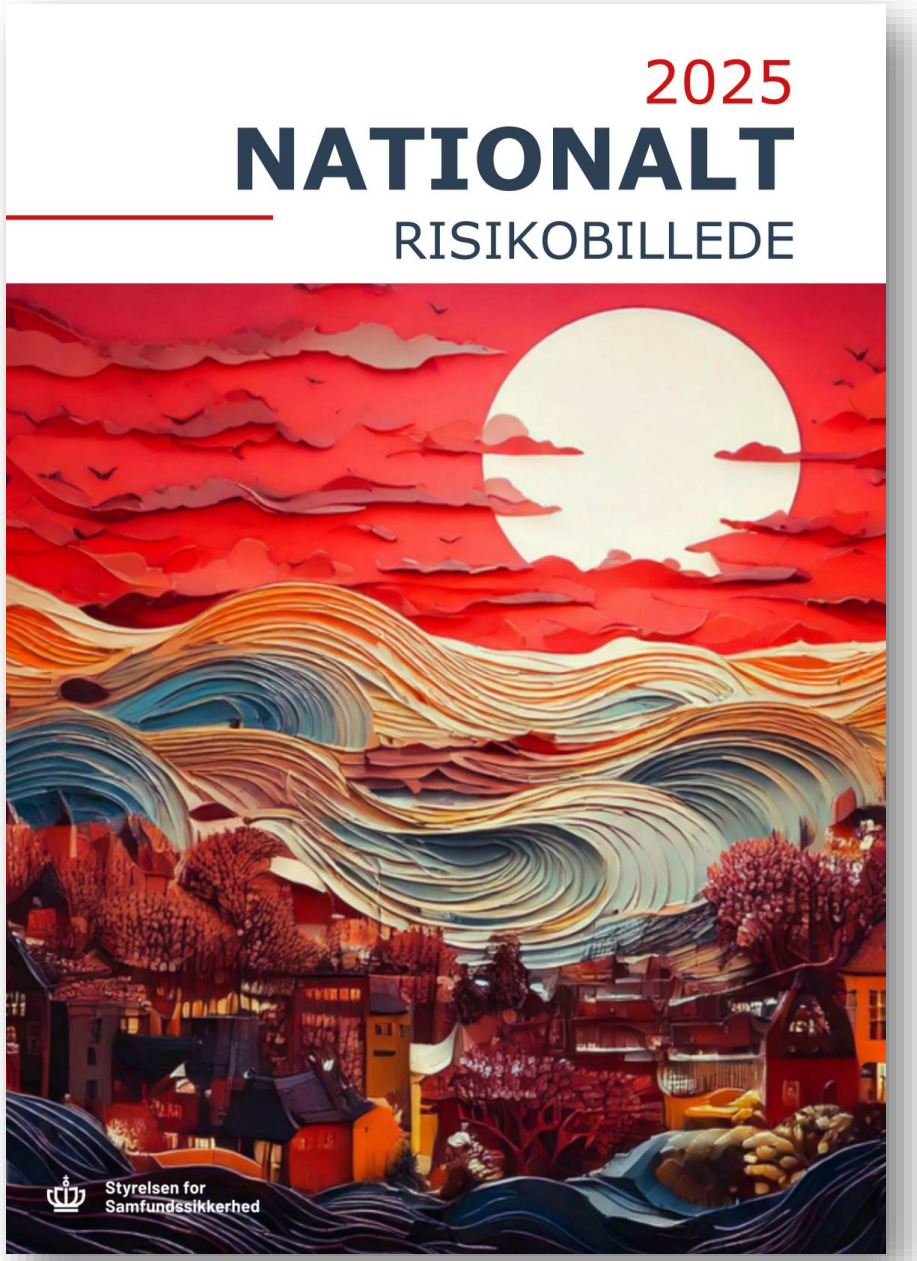
Regeringen

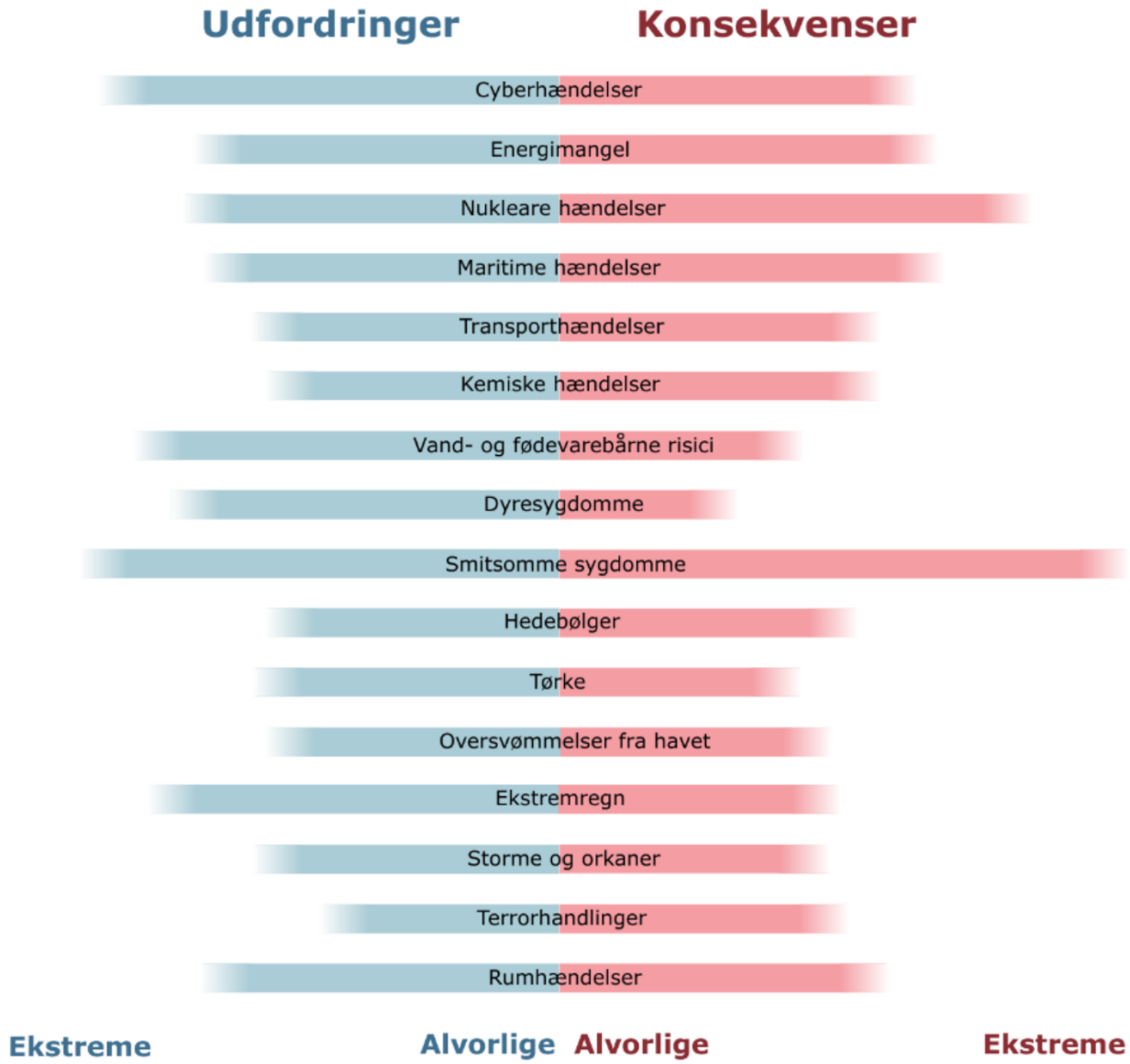
Totalberedskab

Krav til cybersikkerhed og fysisk sikkerhed

- Cybertruslen mod Danmark er alvorlig. Virksomheder udsættes dagligt for cyberangreb.
- NIS 2-loven stiller krav til virksomheders cybersikkerhed i kritiske sektorer. Og med CER-loven øges den fysiske modstandsdygtighed inden for en række samfundsvigtige sektorer.
- Danske virksomheder er i høj grad afhængige af hinanden. Det øger risikoen for cyberangreb og nedbrud, der kan sprede sig gennem leverandørkæder.
- Cybersikkerhed og fysisk sikkerhed er ikke noget, du kun gør for at beskytte din egen forretning. Det beskytter også andre virksomheder og den offentlige sektor.

https://mssb.dk/media/ue3ayelr/beredskabspjece_webfil-a.pdf

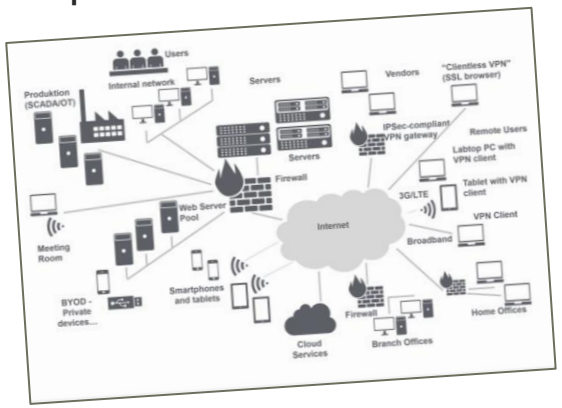




Conscia

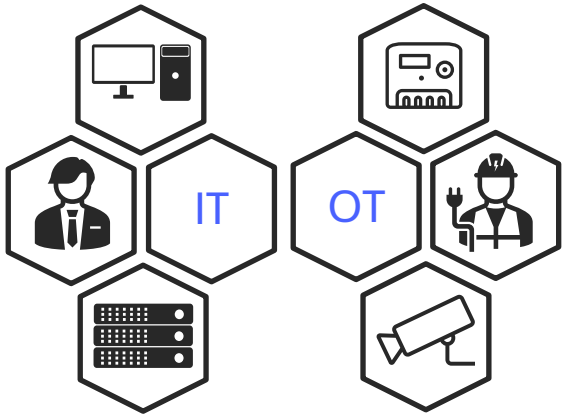
https://samsik.dk/nyt-nationalt-risikobillede-2025/

Avancerede løsning og kompleksitet



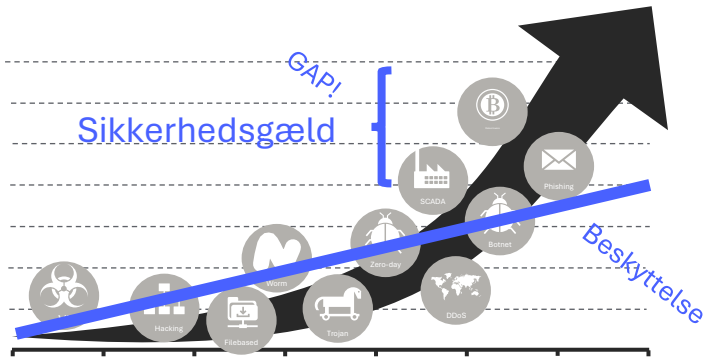
Krav fra forretningen – Voksende afhængighed

Integration mellem IT og OT



Mangel på kompetencer og ressourcer

Manglende rettidige investeringer



Let, billig og tilgængelig Internet of Things

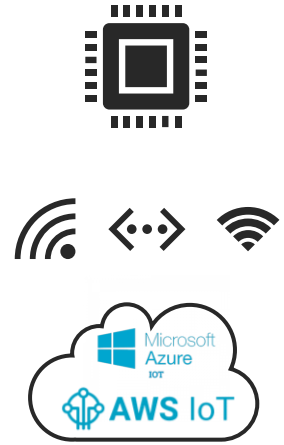
Billig hardware

+

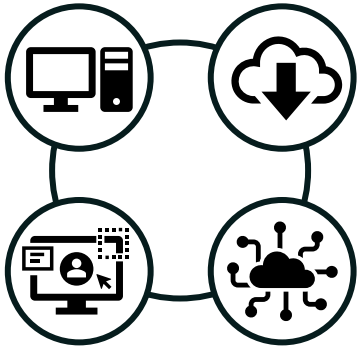
Billig forbindelse

+

Billig software



Aktuelle tendenser – trusler



Forsyningskæder

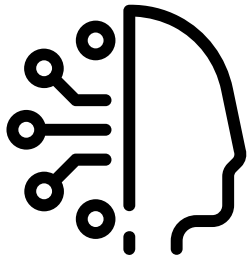
Flere angreb via leverandør- og forsyningskæder

Tredjepartssoftware

Managed Service Providers (MSP) og cloud-afhængigheder udnyttes

Et angreb giver adgang til mange organisationer og data på en gang

Vanskeligt at placere ansvaret



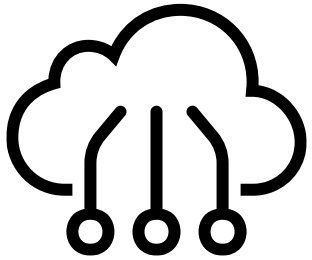
Kunstig intelligens

Meget mere overbevisende phishing og social engineering

Hurtig og effektiv opdagelse og udnyttelse af sårbarheder

Hurtigere udvikling af malware og exploits

Skalerede, tilpassede angreb mod specifikke målgrupper



Cloud-angreb

Udnyttelse af konfigurationsfejl

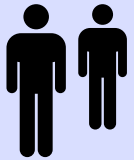
Målrettede angreb mod API'er og tokens

Automatiserede workflows

Manglende klart ansvar forværre risici

Konsekvenser – eksempler

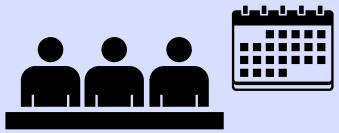
Omkostninger til incident response



Mistede kunder og indtjening

Mistet tillid - Skadet omdømme & brand

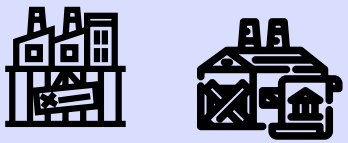
Usikkerhed & uvished



Tabt omsætning og produktivitet

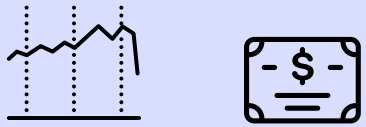
Mistet data & stjålne personoplysninger

Mistede intellektuelle værdier



Konkurs og lukning

Bøder & erstatninger



Værdisætning og aktiekurser

Nu

Kort sigt

Lang sigt

Udgivelsesdato, 25. november 2025

Hovedvurderinger

Aktuelle trusselsniveauer

- Truslen fra cyberkriminalitet er **MEGET HØJ.** Cyberkriminelle rammer hele tiden ofre i Danmark med forskellige cyberangreb, fra omfattende ransomware-angreb til tyveri af sensitiv viden og svindel af den enkelte borger.

- Truslen fra cyberspionage er **MEGET HØJ**. Særligt Rusland og Kina retter løbende cyberangreb mod danske organisationer i forsøg på at få adgang til viden af bl.a. udenrigs- og sikkerhedspolitisk karakter samt indsigt i informationer med betydning for Danmarks forsvar.

- Truslen fra cyberaktivisme er **HØJ.** Særligt pro-russiske hackere rammer løbende danske mål med DDoS-angreb, og i nogle tilfælde gøres også forsøg på at manipulere operationel teknologi (OT), som f.eks. da et dansk vandværk blev ramt i slutningen af 2024. Det er sandsynligt, at nogle pro-russiske hackergrupper har forbindelse til den russiske stat.

- Truslen fra destruktive cyberangreb er **MIDDEL.** Det er særligt Ruslands risikovillighed i forhold til brugen af hybride virkemidler, der kan komme til udtryk i form af wiper-angreb og angreb mod operationel teknologi med begrænsede effekter.

- Truslen fra cyberterror er **INGEN**. SAMSIK vurderer, at ingen militante ekstremister aktører aktuelt har kapacitet til eller intention om at udføre cyberterror mod Danmark.

https://samsik.dk/publikationer/cybertruslen/


Demant


Vestas


ISS


7-ELEVEN


FanøVand


TUREBY-ALKESTRUP
VANDVÆRK


AK TECHOTEL


KALUNDBORG
FORSYNING


SEKTOR CERT


coop


IT-HOTELLET


JLR
JAGUAR
LAND ROVER


Nordea


Arla


United
Healthcare

FanøVand

TUREBY-ALKESTRUP VANDVÆRK

Jyllands-Posten

28. MAR. 2024 KL. 16:57

Vandværk udsat for hackerangreb: Efterretningstjeneste orienteret

Fanø Vand har været udsat for et hackerangreb. Formand for Fanø Vand, Kaj Svarrer, er uforstående over for, hvorfor det lige var dem, der blev ramt.

DEL ARTIKLEN | GEM PÅ LÆSELISTE

Der er stadig vand i hanerne på Fanø, men ikke alt er genoprettet i systemerne efter angrebet. Arkivfoto: Finn Frandsen

MAGNUS HELMS

Natten til mandag blev Fanøs vand- og spildevandsenhed Fanø Vand ramt af et hackerangreb.

»Der gik en alarm i vores system, og så var det med at tage fat i nogen, der kunne ordne det og orientere de relevante myndigheder,« forklarer formand for Fanø vand Kaj Svarrer.

Hackerne forsøgte at trænge ind i selskabets administrative systemer. Det resulterede i, at det ikke var muligt at tilgå systemerne, og den sædvanlige betjening af forbrugerne har ikke været mulig siden:

Jyllands-Posten

24/01/2025 KL. 14.40 | FOR ABONNENTER

»Koden var 1234«: For første gang er dansk vandforsyning blevet angrebet af prorussiske hackere

Et lille vandværk syd for Køge blev kort før jul udsat for et hackerangreb, der fik rørene til at sprænge tre steder i byen. En prorussisk hackergruppe tog æren. Og vandværket fik besøg af fire mand fra FE, som advarer om truslen mod vores vand.

DEL ARTIKLEN | GIV ARTIKLEN | GEM PÅ LÆSELISTE

Det første angreb ramte Tureby-Alkestrup Vandværk den 18. december sidste år. Illustration: Datawrapper

MAGNUS BODING HANSEN

Vandværkspasseren ringer midt om natten:

»Pumperne er gået på nul.«

»Det kan de da ikke,« udbryder Jan Hansen, folkepensionist og formand for Tureby-Alkestrup Vandværk syd for Køge, som denne dag, den 18. december, er udsat for et hackerangreb fra den prorussiske gruppe Z-Pentest, som angiveligt har bånd til Ruslands cyberhær.

Et angreb, de først så småt er ved at have fået ryddet op efter. Og som hackerne pralende lagde fotos ud af inde fra kontrolsystemet.

https://jyllands-posten.dk/indland/ECE16976728/vandvaerk-udsat-for-hackerangreb-efterretningstjeneste-orienteret/,

https://jyllands-posten.dk/indland/ECE17839480/koden-var-1234-for-foerste-gang-er-dansk-vandforsyning-blevet-angrebet-af-prorussiske-hackere/

24/01/2025 KL. 14:40 | FOR ABONNENTER

»Koden var 1234«: For første gang er dansk vandforsyning blevet angrebet af prorussiske hackere

Et lille vandværk syd for Køge blev kort før jul udsat for et hackerangreb, der fik rørene til at sprænge tre steder i byen. En prorussisk hackergruppe tog æren. Og vandværket fik besøg af fire mand fra FE, som advarer om truslen mod vores vand.

DEL ARTIKLEN | GIV ARTIKLEN | GEM PÅ LÆSELISTE

Det første angreb ramte Tureby-Alkestrup Vandværk den 18. december sidste år. Illustration: Datawrapp

MAGNUS BODING HANSEN

Vandværkspasseren ringer midt om natten:

»Pumperne er gået på nul.«

»Det kan de da ikke,« udbryder Jan Hansen, folkepensioni
for Tureby-Alkestrup Vandværk syd for Køge, som denne
december, er udsat for et hackerangreb fra den prorussisk
Pentest, som angiveligt har bånd til Ruslands cyberhær.

Et angreb, de først så småt er ved at have fået ryddet op ef
hackerne pralende lagde fotos ud af inde fra kontrolsyster

Vandværkspasseren, som er landmand, nulstiller pumperne. Byen sover, ingen mærker noget. Men natten efter angriber den prorussiske gruppering igen.

Hackerangrebet kort fortalt

Pumpestyringssystemet var opsat med fjernadgang via et standardmodem fra en teleudbyder, og med fast IP-adresse var der lavet en portforward, som gjorde systemet tilgængeligt via VNC-viewer med en simpel 4-cifret pinkode.

1: Vandtrykket på alle pumper var sat til manuelt tryk på 0 procent. Dette blev rettet kort efter, men resulterede i at ca. 450 husstande stod uden vand i ca. 1 time.

2: Vandtrykket blev igen ændret, denne gang til 100 procent, hvilket resulterede i at et vandrør sprang og efterlod ca. 50 husstande uden vand i cirka 7 timer, hvor skaden blev udbedret.

Fjernadgangen er blevet udskiftet med en sikker VPN-forbindelse, og dermed er en gentagelse af hændelserne afværget.

Af sikkerhedsmæssige årsager beskriver vi ikke i detaljer, hvordan hackerne bar sig ad.

TUREBY-ALKESTRUP VANDVÆRK

https://danskevv.dk/nyheder/vandvaerk-hacket-fjernadgang-var-ikke-sikret-godt-nok/

24/01/2025 KL. 14:40 | FOR ABONNENTER

»Koden var 1234«: For første gang er dansk vandforsyning blevet angrebet af prorussiske hackere

Et lille vandværk syd for Køge blev kort før jul udsat for et hackerangreb, der fik rørene til at sprænge tre steder i byen. En prorussisk hackergruppe tog æren. Og vandværket fik besøg af fire mand fra FE, som advarer om truslen mod vores vand.

DEL ARTIKLEN | GIV ARTIKLEN | GEM PÅ LÆSELISTE

Vandværkspasseren ringer midt om natten:

»Pumperne er gået på nul.«

»Det kan de da ikke,« udbryder Jan Hansen, folkepensionist for Tureby-Alkestrup Vandværk syd for Køge, som denne december, er udsat for et hackerangreb fra den prorussiske Pentest, som angiveligt har bånd til Ruslands cyberhær.

Et angreb, de først så småt er ved at have fået ryddet op ef hackerne pralende lagde fotos ud af inde fra kontrolsyster

Vandværkspasseren, som er landmand, nulstiller pumperne. Byen sover, ingen mærker noget. Men natten efter angriber den prorussiske gruppering igen.

Fjernadgangen er blevet udskiftet med en sikker VPN-forbindelse, og dermed er en gentagelse af hændelserne afværget.

Af sikkerhedsmæssige årsager beskriver vi ikke i detaljer, hvordan hackerne bar sig ad.

TUREBY-ALKESTRUP VANDVÆRK

https://danskevv.dk/nyheder/vandvaerk-hacket-fjernadgang-var-ikke-sikret-godt-nok/

McDonald's AI hiring tool's password '123456' exposed data of 64M applicants

News

Jul 11, 2025 • 5 mins

A security flaw in McHire allowed access to sensitive applicant data via default admin credentials and a vulnerable API. The issue was patched swiftly after disclosure.

https://www.csoonline.com/article/4020919/mcdonalds-ai-hiring-tools-password-123456-exposes-data-of-64m-applicants.html

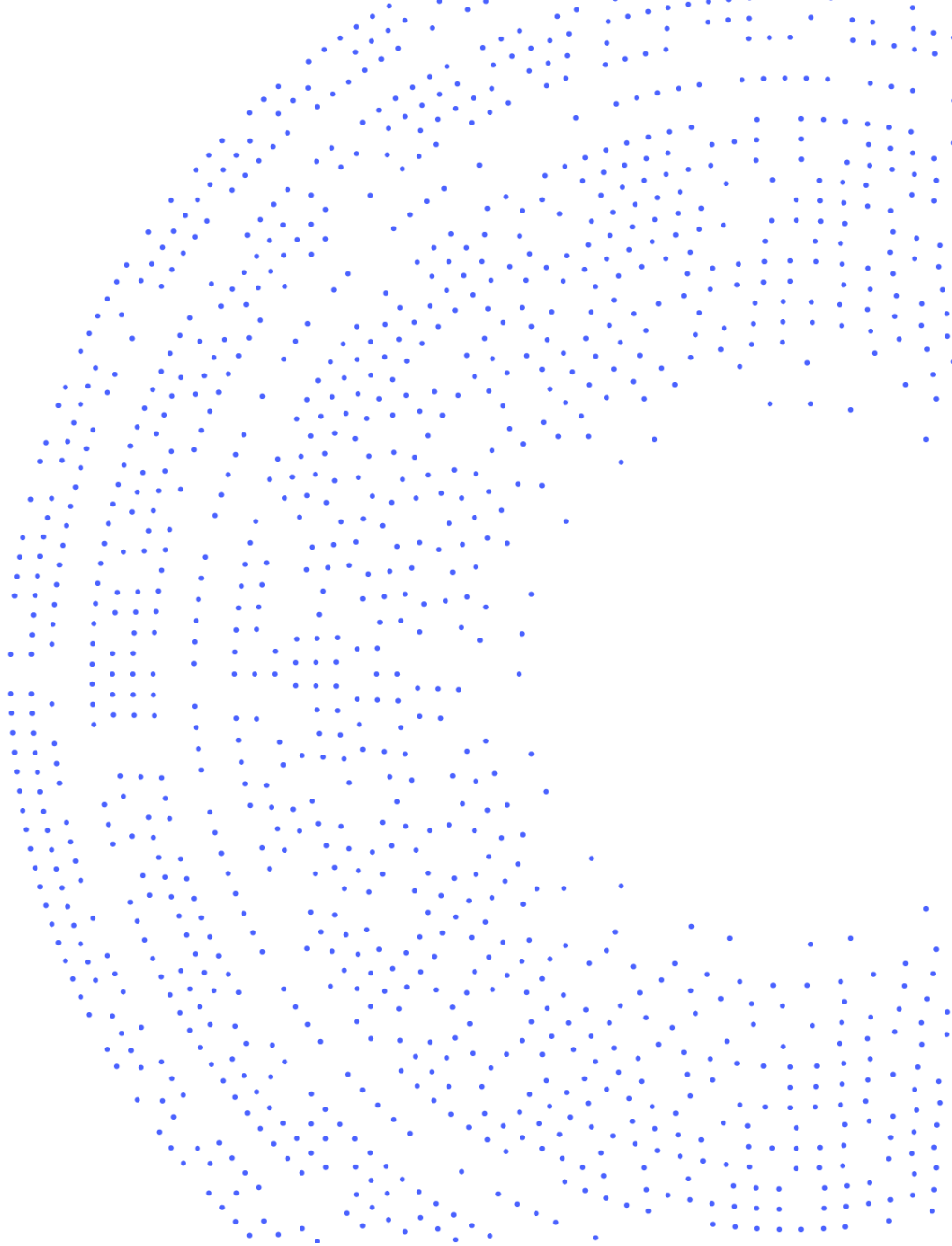
Agenda

01 Cyberrisikoen for digitale virksomheder

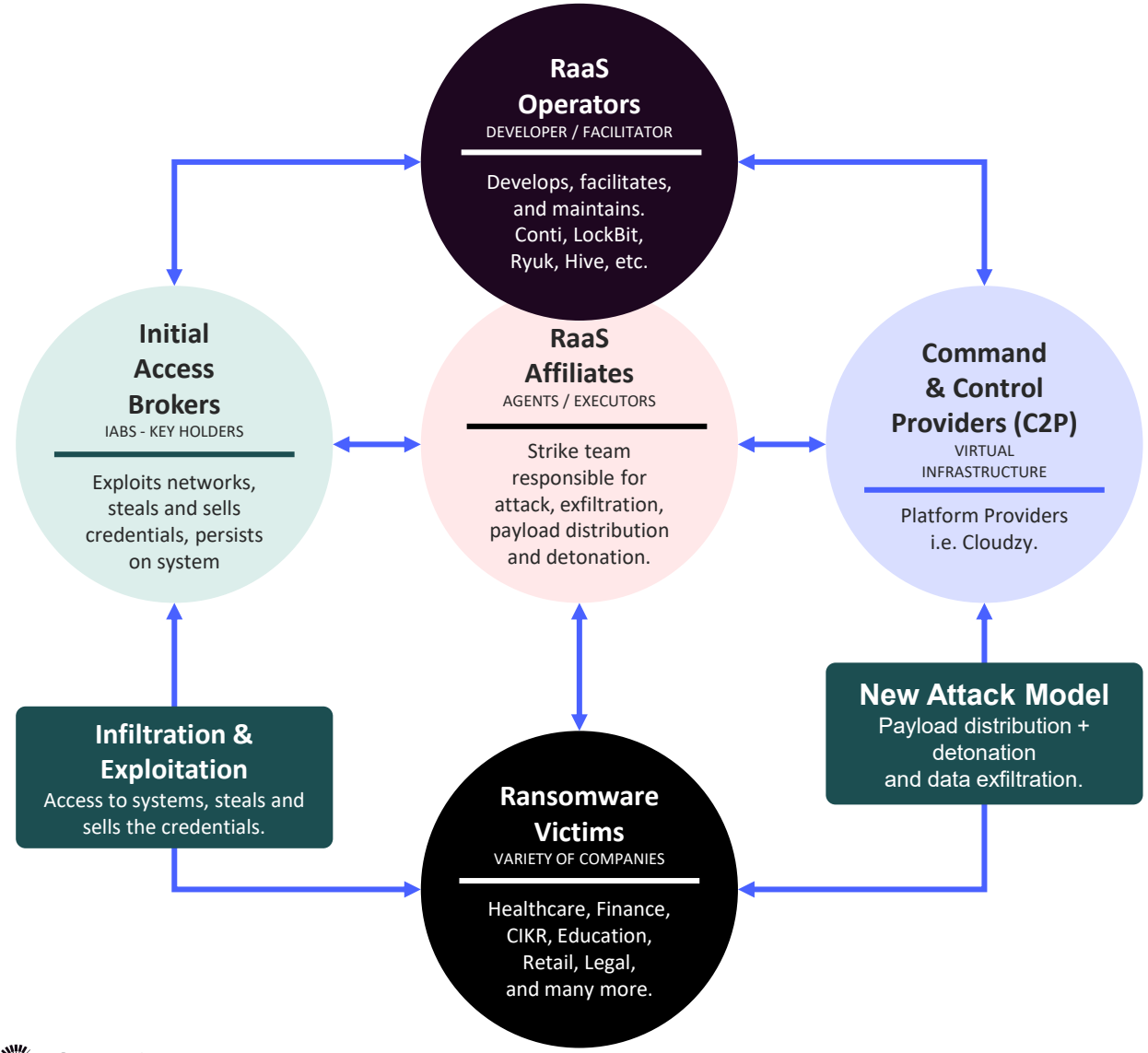
02 Truslen fra digitale mafiagrupper

03 Virksomheder i en ny geopolitisk virkelighed

04 Fremtiden & opsamling



Velorganiserede cyber-kriminelle



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

Chainalysis oplyser, at ransomware-ofre i 2023 betalte hackerne $1.1 milliarder - en ny rekord.

Conscia

Cyberkriminalitet

- Ransomware rammer alle dele af samfundet
- Cyberkriminelle udfører også andre typer af cyberkriminalitet
- Cyberkriminelle udnytter sårbarheder
- Kriminelle hackere udnytter også forsyningskæden
- Phishing
- Udnyttelse af svage eller genbrugte passwords

Arla

Arla ramt af kæmpe cyberangreb: Produktion har ligget stille i en uge

En af Arlas helt centrale fabrikker, der forsyner europæiske supermarkeder med skyr, har været ude af drift i en uge efter omfattende hackerangreb.

15. maj 2025 kl. 12.49

https://www.computerworld.dk/art/291567/arla-ramt-af-kaempe-cyberangreb-produktion-har-ligget-stille-i-en-uge

MARKS & SPENCER

Marks & Spencer and Co-op Ransomware Attack Costs Up to £440 Million – Report

June 23, 2025 by Martin Hinton

https://cyberinsurancenews.org/marks-spencer-cyber-monitoring-centre/

Collins Aerospace

Airport chaos highlights rise in high-profile ransomware attacks, cyber experts say

By **James Pearson**

September 22, 2025 10:45 PM GMT+2 · Updated September 22, 2025

https://www.reuters.com/legal/government/airport-chaos-highlights-rise-high-profile-ransomware-attacks-cyber-experts-say-2025-09-22/

JLR

JAGUAR

LAND ROVER

A hack impacting Jaguar Land Rover was so bad that it hurt the U.K.'s GDP, Bank of England says

The hack is estimated to have cost the company nearly $2.5 billion and delayed manufacturing for weeks.

https://www.berlingske.dk/virksomheder/hackerangreb-mod-jaguar-er-det-dyreste-nogensinde-i-storbritannien

Hi friends,

Whatever who you are and what your title is if you're reading this it means the internal infrastructure of your company is fully or partially dead, all your backups - virtual, physical - everything that we managed to reach - are completely removed. Moreover, we have taken a great amount of your corporate data prior to encryption.

Well, for now let's keep all the tears and resentment to ourselves and try to build a constructive dialogue. We're fully aware of what damage we caused by locking your internal sources. At the moment, you have to know:

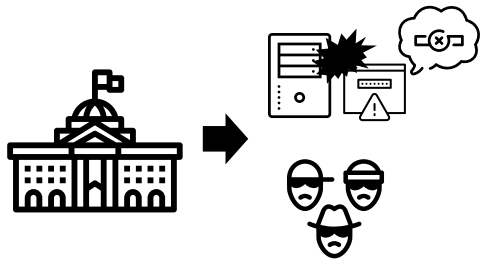
1. Dealing with us you will save A LOT due to we are not interested in ruining your financially. We will study in depth your finance, bank & income statements, your savings, investments etc. and present our reasonable demand to you. If you have an active cyber insurance, let us know and we will guide you how to properly use it. Also, dragging out the negotiation process will lead to failing of a deal.
2. Paying us you save your TIME, MONEY, EFFORTS and be back on track within 24 hours approximately. Our decryptor works properly on any files or systems, so you will be able to check it by requesting a test decryption service from the beginning of our conversation. If you decide to recover on your own, keep in mind that you can permanently lose access to some files or accidently corrupt them - in this case we won't be able to help.
3. The security report or the exclusive first-hand information that you will receive upon reaching an agreement is of a great value, since NO full audit of your network will show you the vulnerabilities that we've managed to detect and used in order to get into, identify backup solutions and upload your data.
4. As for your data, if we fail to agree, we will try to sell personal information/trade secrets/databases/source codes - generally speaking, everything that has a value on the darkmarket - to multiple threat actors at ones. Then all of this will be published in our blog - https://akiral<redacted>.onion.
5. We're more than negotiable and will definitely find the way to settle this quickly and reach an agreement which will satisfy both of us.

If you're indeed interested in our assistance and the services we provide you can reach out to us following simple instructions:

1. Install TOR Browser to get access to our chat room - https://www.torproject.org/download/.
2. Paste this link - https://akira<redacted>.onion.
3. Use this code - XXXX-XX-XXXX-XXXX - to log into our chat.

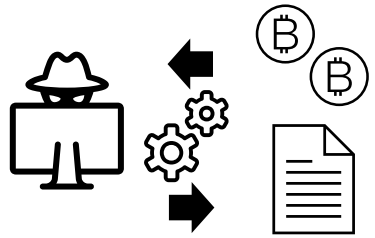
Keep in mind that the faster you will get in touch, the less damage we cause.

Ransomware – tendenser 2026

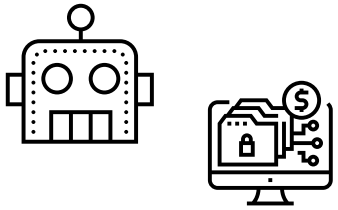


Statsstøttede grupper
Ransomware grupper kommer under statskontrol og angreb bruges som del af hybridkrig

Mange nye RaaS-grupper
Fragmentering og magtkampe blandt kriminelle grupper, føre til konstant opblomstring af nye RaaS-grupper

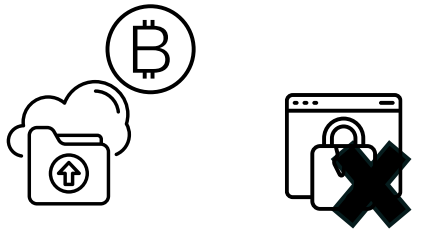


Automatiseret lateral movement og hurtig dataeksfiltration
Automatiseret ransomware bl.a. med AI kan udføre angreb 100 gange hurtigere



AI-drevet ransomware (Agentic AI)
Angreb bliver selvstyrende: AI-agenter planlægger, tilpasser og gennemfører angreb i realtid

Angreb på SaaS- og leverandørkæder
Angreb på software, CI/CD pipelines og SaaS-platforme for at ramme mange organisationer i et angreb



Fokus på dataekstraktion frem for kryptering
Data-eksfiltration og afpresning uden kryptering — backup utilstrækkelige

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

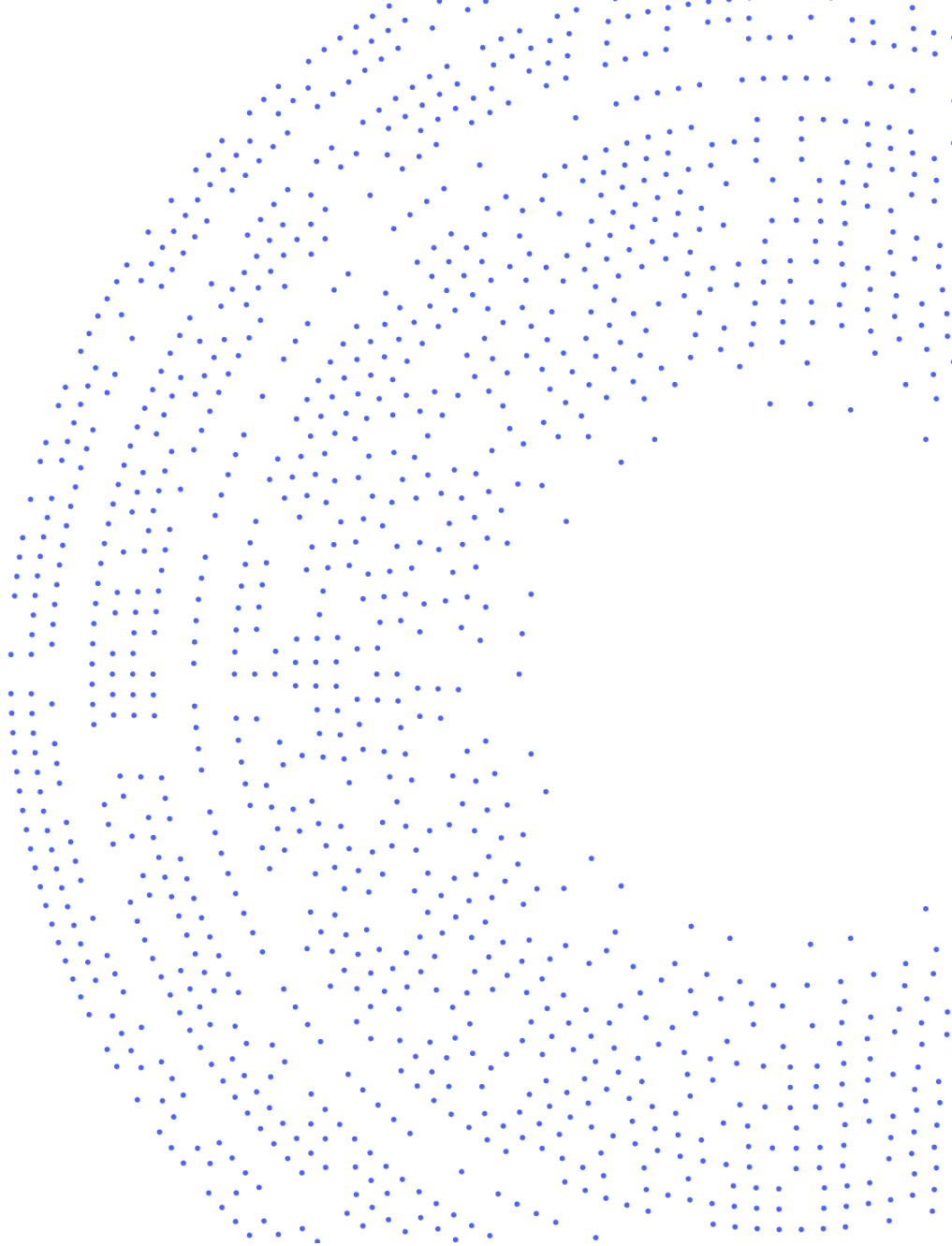
Agenda

01 Cyberrisikoen for digitale virksomheder

02 Truslen fra digitale mafiagrupper

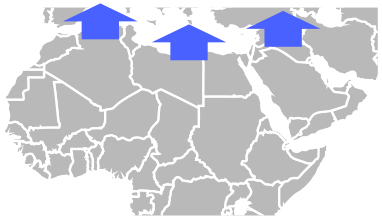
03 Virksomheder i en ny geopolitisk virkelighed

04 Fremtiden & opsamling

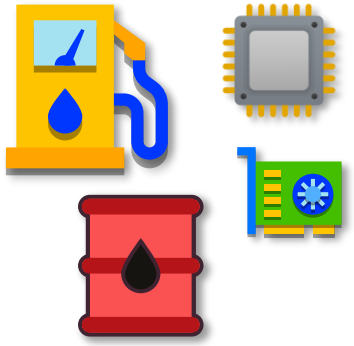


Geopolitiske udfordringer

Usikkerhed om sikkerhedsgarantien i NATO

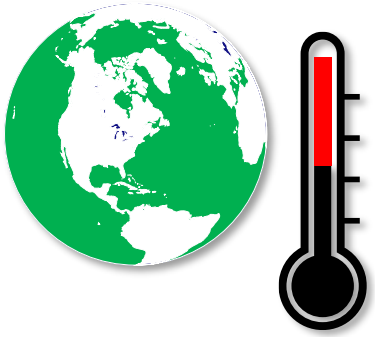


Migration, ustabilitet og konflikter i Mellemøsten og Afrika



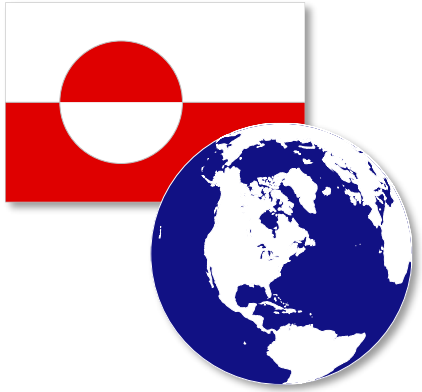
Energi og teknologi som våben

Ophøret af den regelbaserede internationale orden



Klimaforandringer

Ruslands aggression og krigen i Ukraine



Øget militarisering og stormagtskamp i Arktis

EU's sikkerhedspolitiske transformation

Stormagtsrivalisering mellem USA, Kina og Rusland

Kina og Taiwan

Geopolitik & 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 operere sikkert fra Rusland, og samarbejder med myndighederne.

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

Iran har i de senere år udviklet deres kapaciteter til at udføre cyberangreb, herunder cyberspionage og destruktive angreb. Efter etablering af samarbejde med Rusland og Gaza konflikten er Iran blevet endnu mere villig til at anvende cyberangreb.

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 og Europa.

Udfaldet af februar 2026-krigen er i øjeblikket ukendt, men iranske og iransk støttede cyberangreb forventes at stige fremover som resultat af konflikten og de første angreb er observeret.

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, militære og økonomiske mål.

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

Nord Korea har i de senere år udviklet deres kapaciteter til at udføre cyberangreb, herunder spionage, politiske og destruktive angreb samt ikke mindst 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 og Europa, og udfører primært økonomisk motiverede angreb bl.a. ransomware

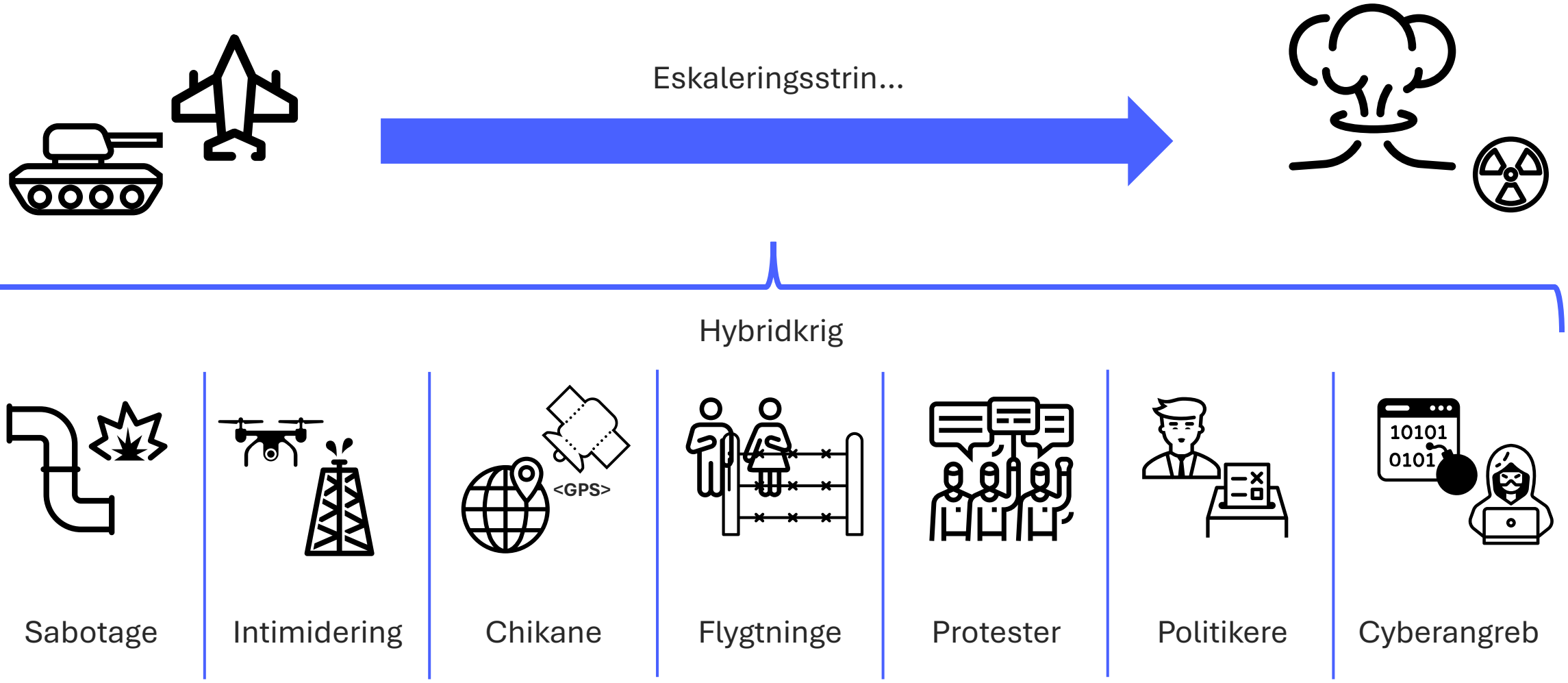
Ruslands cyberoperationsgrupper

- Rusland er en stærk cyberaktør med lang erfaring og 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

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

Russisk hybridkrig - refleksiv kontrol



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

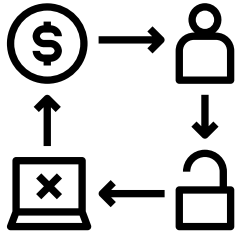
Økonomi, energi og teknologi anvendes som våben

Globalisering i bakgear – kontrol med fokus på kortere supply chains

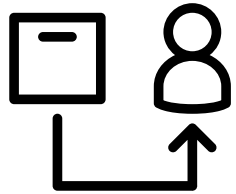
Kriminelle grupper finder beskyttelse i – og hjælper - autokratiske lande

Hybridkrig på Internettet

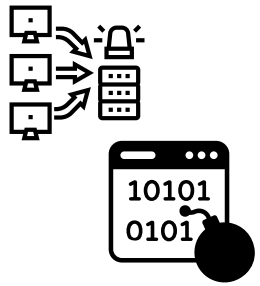
Spionage



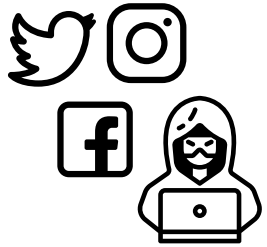
Kriminalitet som våben



Supply Chain



Destruktive angreb



Desinformation & Påvirknings-angreb

Cyberwar

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

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

Afværgede voldsomt cyberangreb mod energiforsyningen: Nu vil Polens premierminister sikre digital autonomi

Op mod en halv million borgere var tæt på at stå uden strøm efter jul efter et særligt cyberangreb fra Rusland. Premierministeren vil sikre digital autonomi for at beskytte sig bedre.

26. januar 2026 kl. 16.45

Russian state hackers likely behind wiper malware attack on Poland's power grid

A major cyberattack that nearly cut electricity to hundreds of thousands of people in Poland late last year was reportedly carried out by Sandworm, a Russia-linked hacking group known for targeting power grids, researchers have determined.

Wiper Malware Targeting Poland's Power Grid Tied to Moscow

Signs Point to Long-Active 'Sandworm' Military Intelligence Hackers at Work

Mathew J. Schwartz (euroinfosec) • January 26, 2026

Share Tweet Share Credit Eligible Get Permission

Polish Prime Minister Donald Tusk on Jan. 15, at a press conference where he first detailed late 2025 Russian cyberattacks targeting his country's power grid. (Image: Polish government)

Russian military intelligence attempted to disrupt Poland's power grid just after the onset of winter using wiper malware, say security researchers.

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.

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

I dag kl. 13.27 NYHEDSVARSEL

Grønlanske hjemmesider ramt af hackerangreb

Der er lige nu såkaldte DDoS-angreb mod grønlandske hjemmesider.

Det oplyser Styrelsen for Samfundssikkerhed til Ritzau.

»Vi følg
Danma
komme

Når der
hjemm

Styrels
om.

5 minutter siden NYHEDSVARSEL

Russisk gruppe tager ansvaret for hackerangreb i Grønland

Den russiske hackergruppe NoName057(16) har taget ansvar for cyberangrebet mod grønlandske hjemmesider.

Det fremgår af gruppens forum på den krypterede beskedtjeneste Telegram, skriver TV 2.

Ifølge mediet skriver gruppen, at det aktuelle angreb sker som hævn for, at Danmark har doneret kampfly til Ukraine.

Ritzau

USA vs. EU

Ukraine & Rusland

Kina

Energi

Kultur & Ytringsfrihed

Big tech

Conscia

Modstandsdygtighed

Sikkerhedsprofil: USA har en tænd-sluk-knap til det danske samfund

Danske aktører bør fremadrettet kigge efter open source- eller europæiske cloud-løsninger, siger formand for Cybersikkerhedsrådet til TV2.

USA kan lukke Danmark ned på en time, siger ekspert

Der er ingen konkret trussel fra USA om at "trække stikket" til Danmark – men eksperter er enige om, at man bør se sig om efter alternativer

VIRKSOMHEDER

Fem amerikanske giganter har sat sig tungt på Danmark – og de kan trække stikket

De seneste fem år har nærmest gjort Danmark og Europa totalt afhængige af fem amerikanske teknologigiganter, selvom der findes europæiske alternativer. Nu vokser et oprør frem af frygt for, at nogen beslutter at trække stikket.

Sanktioner

WORLD NEWS

Trump's sanctions on ICC prosecutor have halted tribunal's work

Frygtet scenarie bliver til virkelighed: Microsoft blokerer europæisk anklagers e-mail efter Trump-indgreb

Frygten for, at de amerikanske teknologigiganter spærrer for europæeres adgang til deres data, har stået som et mareridt, siden Donald Trump blev præsident. Nu har Microsoft lukket Den Internationale Straffedomstols chefanklagers e-mail på ordre fra Trump. Er vi klar herhjemme?

Påvirkning og værdier

US warns tech companies against complying with European and British 'censorship' laws

U.S. tech companies were warned on Thursday they could face action from the Federal Trade
regulat

UK braced for 'free speech' row with JD Vance as far-right websites spurn Online Safety Act

Officials in the United Kingdom are bracing for a clash with the White House as far-right social media platforms dismiss legal requests from British regulators tackling illegal online

TEKNOLOGI

Analyse: Vi bør frygte Trumps alliance med techgiganterne

Techgiganterne har dog i øjeblikket stor interesse i at minimere risiko for misbrug, skriver DR's techkorrespondent

Cybersikkerhed

Hegseth Orders Pentagon to Stop Offensive Cyberoperations Against Russia

The defense secretary's instructions, which were given before President Trump's blowup with the Ukrainian president, are apparently part of an effort to draw Russia into talks on the war.

Spionage

U.S. Orders Intelligence Agencies to Step Up Spying on Greenland

Effort underscores seriousness of Trump's intent to acquire the island from Denmark

SAMFUND | ABONNEMENT

»Det er vilde oplysninger«: Melding om amerikansk spionage i Grønland skaber forargelse i dansk politik

Europa tager ikke længere nogen chancer: Opfordrer topfolk til at udskifte telefoner og computere før møde i USA

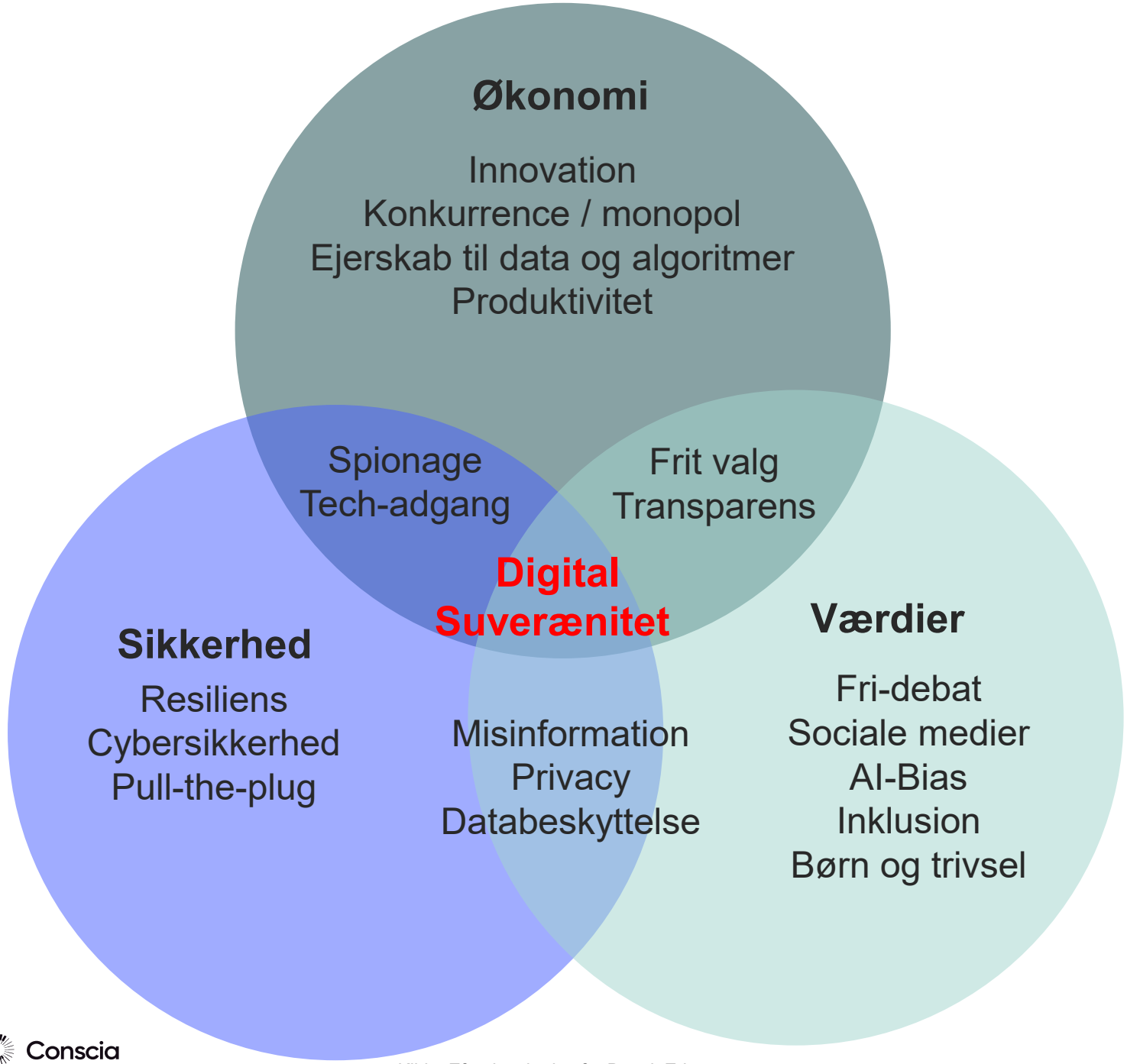
Nye oplysninger afslører, at EUs topembedsmænd og kommissærer nu bliver anbefalet at have burner-telefoner og rensede computere i tasken, når de rejser til USA. Det er endnu et ildevarslende tegn på, hvor skrøbeligt forholdet til Washington er blevet.

Teknologiadgang

Trump Hints U.S. Could Go to War With Allies Someday in Wild Presser

Donald Trump called the press conference to unveil a new fighter jet.

The United States announced that the F-47 fighter jets sold to allies will have their capabilities reduced by 10%, a decision made by President Donald Trump to mitigate risks in case these nations cease to be allies in the future.



AI og kvanteteknologi

Software

Cloud og services

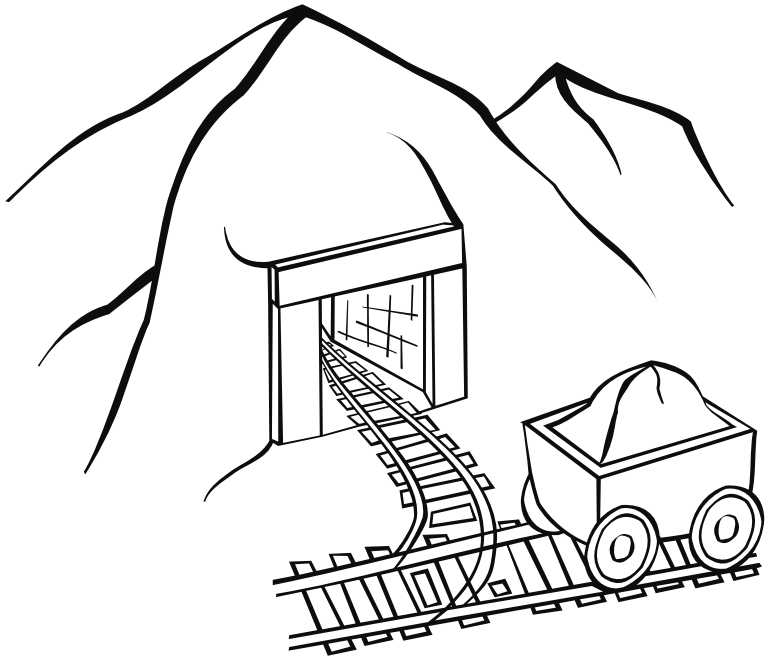
Infrastruktur

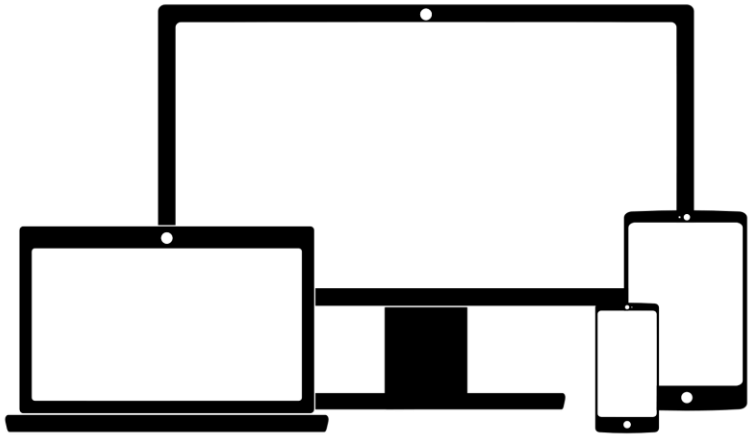
Hardware

Materialer

Conscia

Kilde: Efter inspiration fra Dansk Erhverv





Risikovurderinger og modstands-dygtighed

Rammevilkår, mentalitet (mindset), regulering og alternativer

Efterspørgsel og kommercielt marked for europæiske løsninger

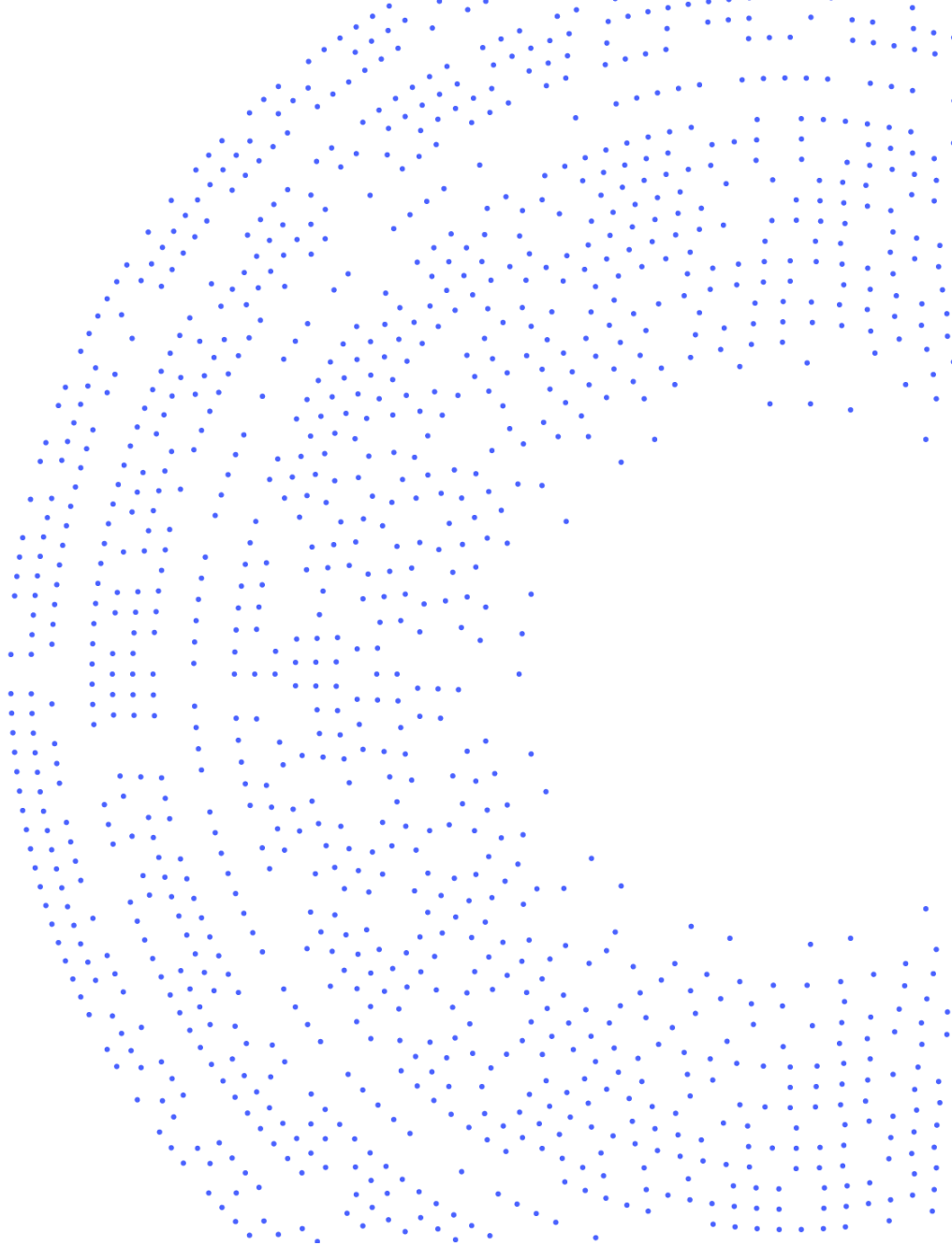
Agenda

01 Cyberrisikoen for digitale virksomheder

02 Truslen fra digitale mafiagrupper

03 Virksomheder i en ny geopolitisk virkelighed

04 Fremtiden & opsamling



EU regulering - NIS2 & DORA

- Væsentlig forandret trusselsbillede – og større erkendelse af problemet omkring cybersikkerhed

- Omfatter flere sektorer og enheder – herunder myndigheder
- Strenge sanktioner og konkrete højere bøder
- Krav om risikostyring og udvidede krav til sikkerhedsforanstaltninger
- Fokus på at styrke sikkerheden i forsyningskæden
- NIS2 skal harmonisere implementeringen mellem medlemsstaterne

- DORA: Fælles regler på tværs af finanssektoren & skærpelse af NIS2

Krav til sikkerhed i NIS2

Krav til ledelsen (§7/Artikel 20)	**Effektiv risikostyring (§6/Artikel 21)**	**Hændelsesrapportering (§12/§13/Artikel 23)**

Kompetencer	**Ansvar**	**Risikoanalyse & Politikker**	**Kontroller**	**Beredskab**	**Opfølgning**	**Håndtering**	**Rapportering**

- A European cybersecurity strategy, including the **establishment of a joint Cybersecurity Unit**, a Review of the Security of Network and Information Systems (NIS) Directive[13] and giving a push to the **single market for cybersecurity**.

Conscia

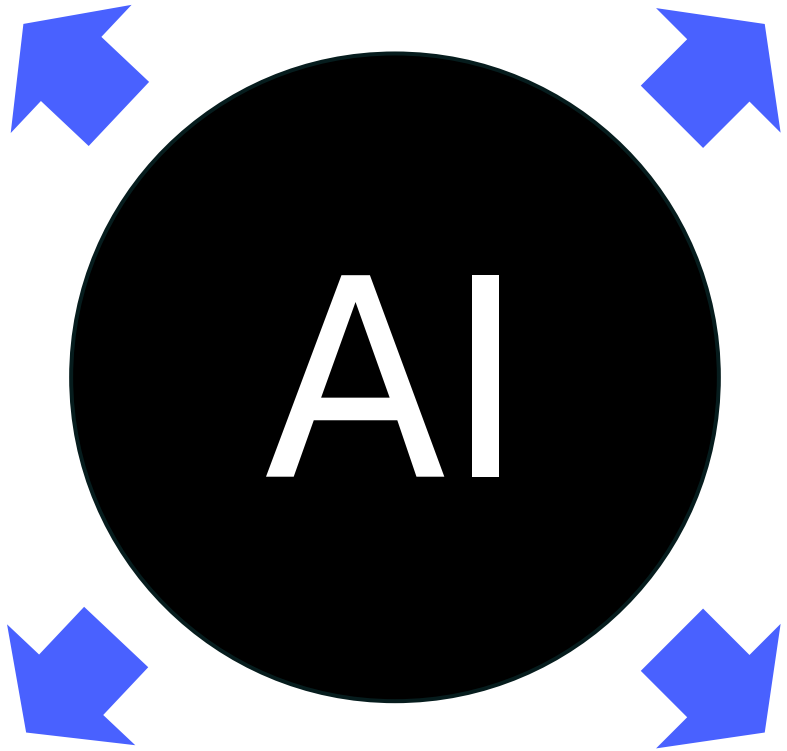
Chips
Resilience
Diplomacy
Strategic
Act
Health
EHDS
Policy
NIS
Union
Intelligence
Markets
Operational
Digital
Artificial
Critical
European
Toolbox
EU
Governance
Cyber
DSA
DMA
ePrivacy
Services
Compass
Space
Directive
Entities
DGA
CER
Data
DORA
Defence
Regulation

The NIS 2 Directive
The European Cyber Resilience Act
The Digital Operational Resilience Act (DORA)
The Critical Entities Resilience Directive (CER)
The Digital Services Act (DSA)
The Digital Markets Act (DMA)
The European Health Data Space (EHDS)
The European Chips Act
The European Data Act
European Data Governance Act (DGA)
The Artificial Intelligence Act
The European ePrivacy Regulation
The European Cyber Defence Policy
The Strategic Compass of the European Union
The EU Cyber Diplomacy Toolbox

Kunstig intelligens og cybersikkerhed

Brugerinteraktion med AI

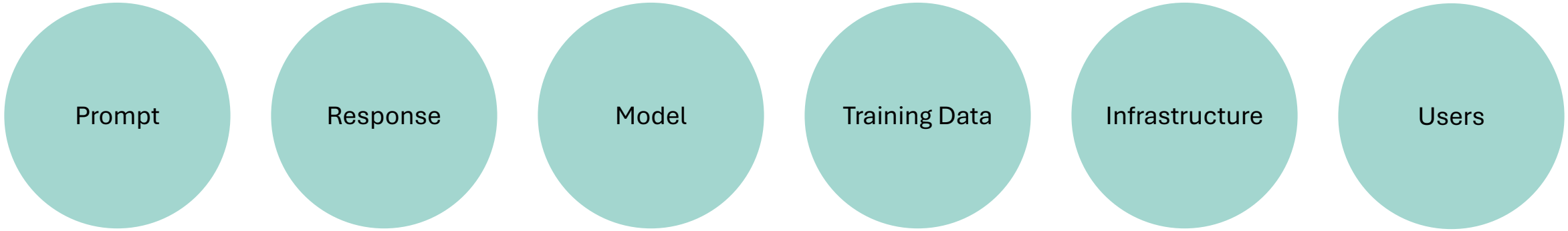
Sikring af AI-modeller (LLM)



AI til cybersikkerhed

AI til cyberangreb

Sikring af AI-modeller (LLM)



Anthropic Claude Mythos

Storbanker væbner sig mod frygtet AI-model: "Vi forbereder os på en række scenarier"

Ny sprogmodel fra Anthropic får banker og sikkerhedseksperter t
avancerede angreb mod finanssektoren.

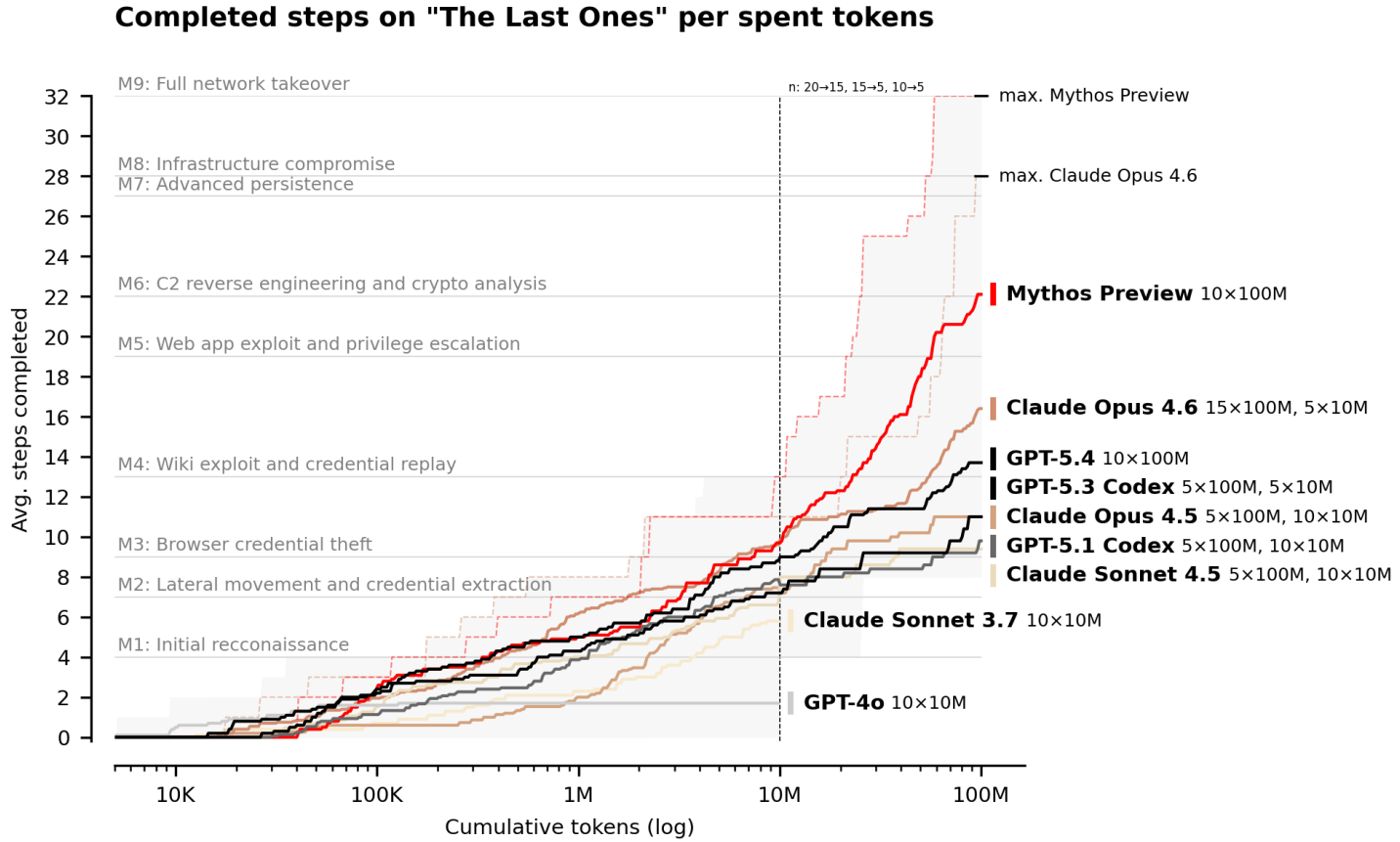
Finder iflg. Anthriopic markant flere sårbarheder end tidligere modeller

Frigivet til begrænset antal aktører – primært store US tech-virksomheder

Risiko for store mængder sårbarheder

Særlig udfordring for mindre software virksomheder

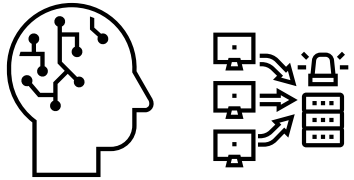
Hvad tilsvarende findes i øvrigt derude?



https://www.aisi.gov.uk/blog/our-evaluation-of-claude-mythos-previews-cyber-capabilities

Conscia

Flere angreb



Kunstig intelligens (AI) vil forøge mængden og konsekvenserne af cyberangreb

Indvirkningen vil være ujævnt fordelt på forskellige angrebsmetoder.

Deepfake

Deepfake kan realistisk efterligne billeder, lyd og video af eksisterende og fiktive personer, hvilket kan bruges i avanceret social engineering angreb

Anvendes i alle angreb

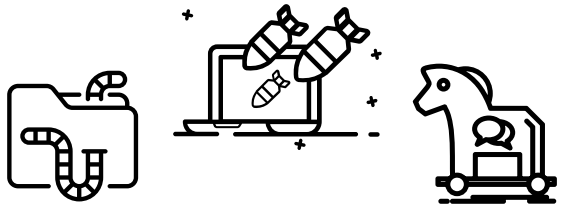
AI anvendes allerede af alle typer trusselsaktører – både statslige og ikke-statslige, kvalificerede og mindre kvalificerede

Mere målrettede angreb

AI medfører et kapacitetsløft inden for rekognoscering og social engineering

Gør angreb hurtigere, mere målrettede, mere effektive og sværere at opdage.

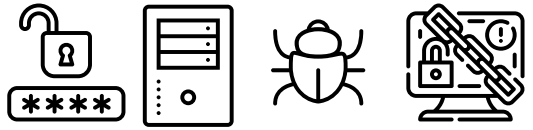
Hurtigere videreudvikling



Cyberangreb udføres hurtigere

Trusselsaktører kan forbedre eksisterende angrebsmetoder og analysere stjålne data hurtigere og mere effektivt og bruge dem til at træne AI-modeller.

Flere farlige aktører



AI sænker barrieren og gør det muligt for uerfarne cyberkriminelle og hacktivister at udføre effektive angreb.

Dette vil medføre en større kriminalitets- og ransomware-trussel.

Den aktuelle sikkerhedssituation

Manglende ledelsesmæssig erkendelse af:

- Højt digitaliseringsniveau og dermed stor digital afhængighed
- Voksende trusselsniveau hvor alle er under angreb og risikerer at blive ramt af en alvorlige cyber-hændelser
- Det aktuelle cybersikkerhedsniveau er formentlig ikke tilstrækkeligt ifht. digitalisering og trusler
- God it-modenhed og god it-hygiejne har stor sikkerhedsmæssige betydning, og teknologisk gæld er en stor udfordring for sikkerheden
- Cybersikkerhed er ikke gratis, men koster investering og har løbende omkostninger
- Manglende investeringer i cybersikkerhed har store langsigtede konsekvenser og er meget dyrt og svært at løse efterfølgende

Trusler mod Danmark og Europa

Kriminelle - afpresning

Kriminelle grupper bliver stadig mere aggressive i deres angreb, hvor særligt forskellige former for ransomware o.a. afpresning typisk anvendes og ofte udløser store økonomiske gevinster til forbryderne.

Cyberkriminelle udnytter sårbarheder f.eks. svage passwords eller svagheder i forsyningskæder. Grupperne opererer ofte i samarbejde med eller under beskyttelse af fremmede stater.

Risiko for angreb på kritisk infrastruktur

Hybride trusler - Russisk hybridkrig mod vesten

Danmark er et af de lande der har støttet Ukraine mest. Udsigt til mulige afslutning af kamphandleringer og at USA trækker sig fra Europa/afslutningen af NATO. Risiko for optrapning af russiske angreb på Europa.

Rusland ønsker gengældelse, at markere sig og afprøve grænser hvor Cyberangreb er et oplagt værktøj til gråzone angreb.

Kritiske infrastruktur er et oplagt mål.

Cyberaktivister

Aktivist grupper der gennemfører forskellige former for angreb med fokus på opmærksomhed – typisk DDoS. Grupperne opererer ofte i samarbejde med eller under beskyttelse af fremmede stater.

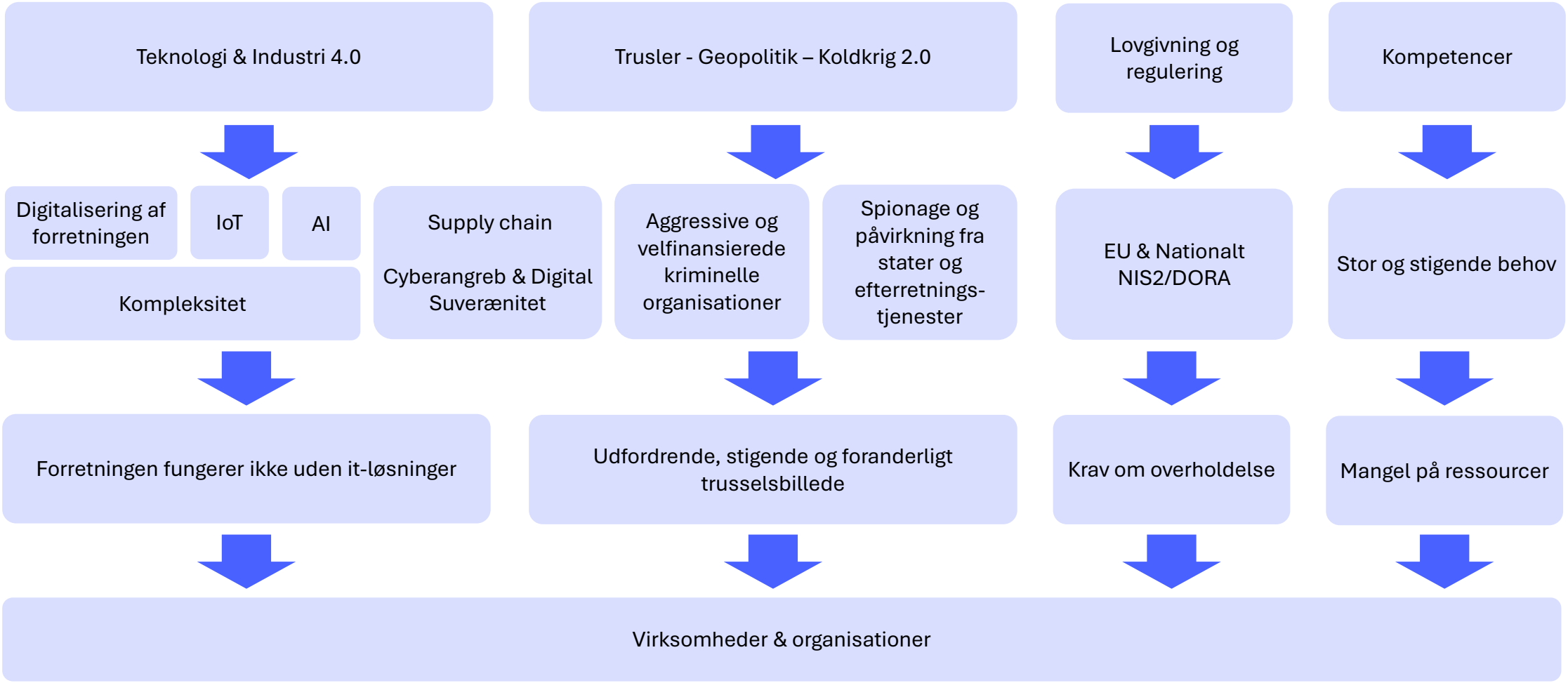
Digitale afhængigheder

Europa er dybt afhængig af ikke europæisk teknologi, hvilket gør Danmark og Europa sårbar overfor teknologisk pression og spionage.

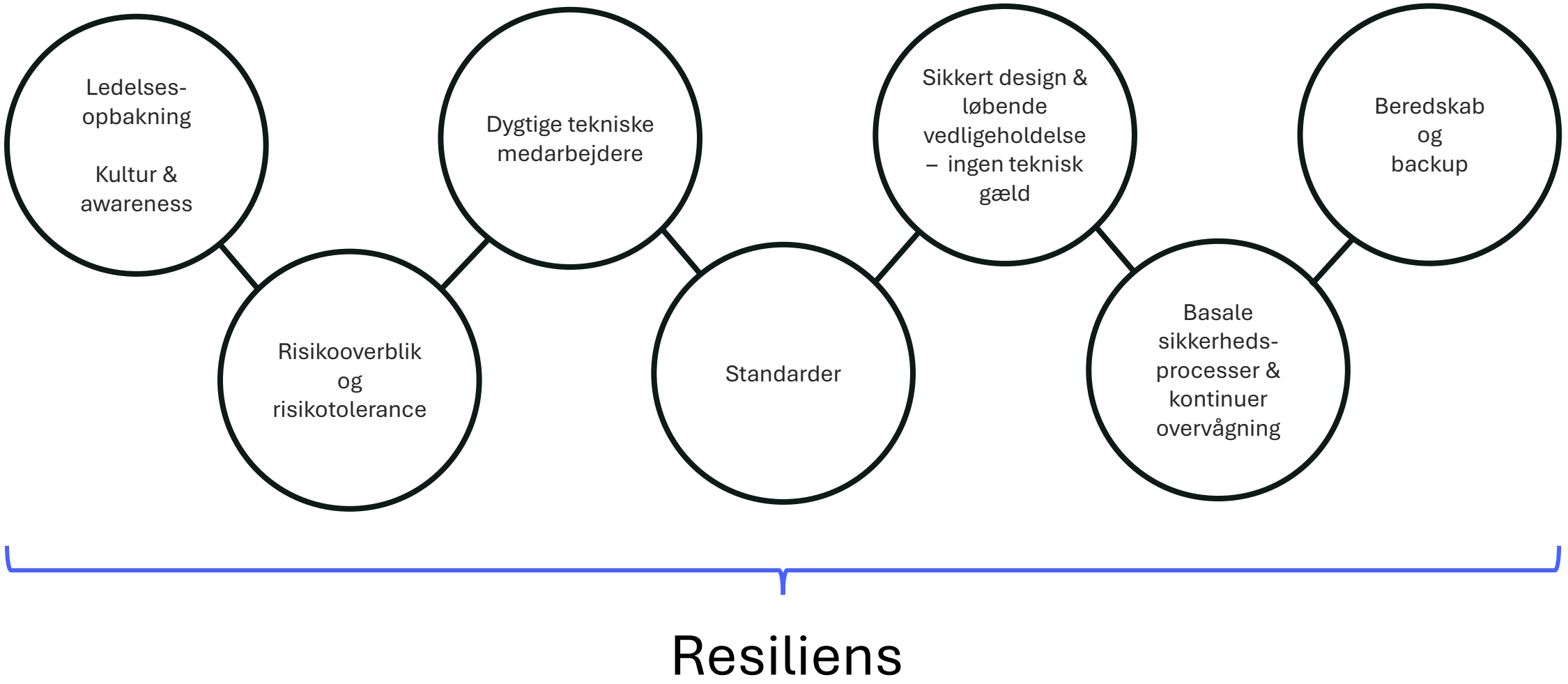
Cyberspionage

Danmark har en strategisk position ved Østersøen, er en vigtig spiller i arktisk og medlem af NATO og EU, hvorfor fremmede stater forsøger at stjæle viden om udenrigs- og sikkerhedspolitik. Rusland udfører cyberspionage for at forberede sig på en militær konflikt. Alt dette gør bl.a. den kritiske infrastruktur i Danmark til at oplagt mål for cyberspionage

Udfordringen for virksomheder & organisationer



En cyberresilient organisation



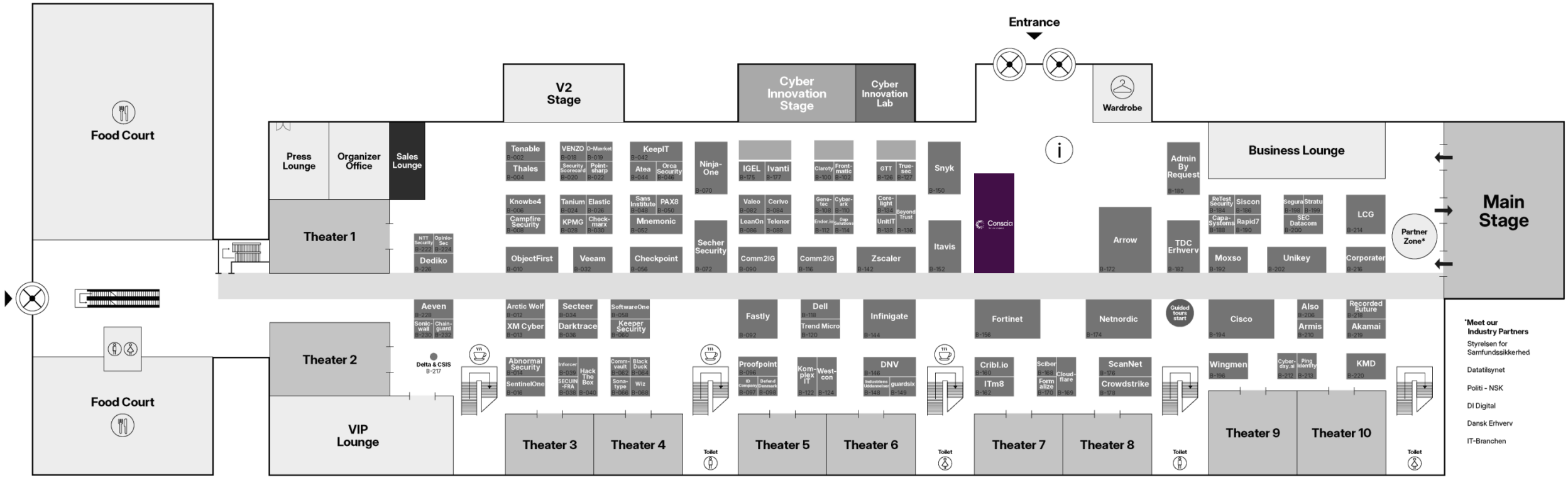
Ses vi?

Conscia Momentum 2026 – Resilience in motion

Den 2. september | Hangaren, Københavns Lufthavn

Conscia
Secure progress

Læs mere på www.conscia.dk/events



*We reserve the right to continuously update the floor plan.

TAK!

Conscia
Secure progress

Cyber attack?
24/7 Incident Response

+45 32 83 04 03

Jacob Herbst
+45 2083 0430