



Hvordan kan vi hjælpe virksomheder i gang med at arbejde risikobaseret

DS Cyberdag 5. oktober 2023

RISIKOSTYRING

MICHAEL STAUSHOLM
PRINCIPAL SECURITY ARCHITECT

Sammen kommer vi #foran**digitalt**

Kom foran digitalt



IOT OG SMARTE PRODUKTER



DIGITAL GRØN OMSTILLING



CYBERSIKKERHED



KUNSTIG INTELLIGENS

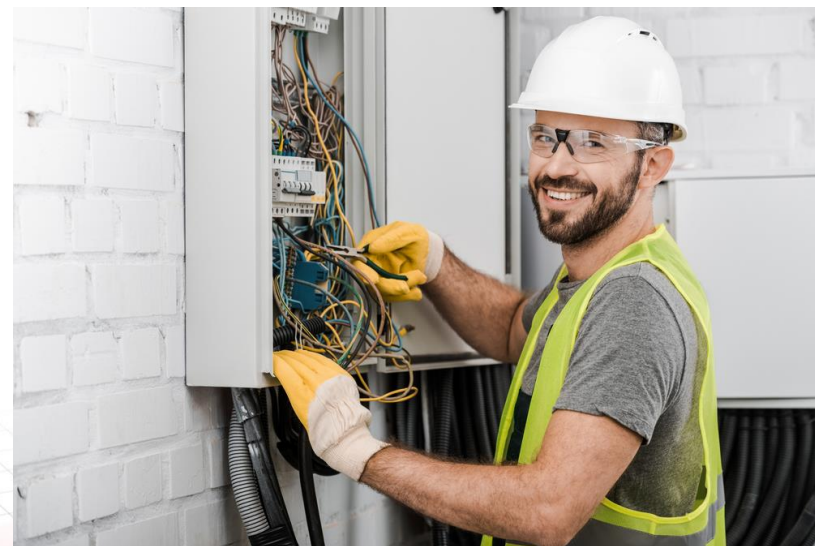


DIGITAL SUNDHED



COMPUTERGRAFIK, VISION OG
SIMULERING

Alle laver risikostyring



Hvorfor risikostyring?


- “Perfekt” cybersikkerhed findes ikke





”

Vi har dygtige ansatte, så
selvfølgelig er vores
systemer sikre...



“Vi ved godt der er problemer med X, Y og Z. Vi skal også i gang med W, men har ikke haft tid endnu.”

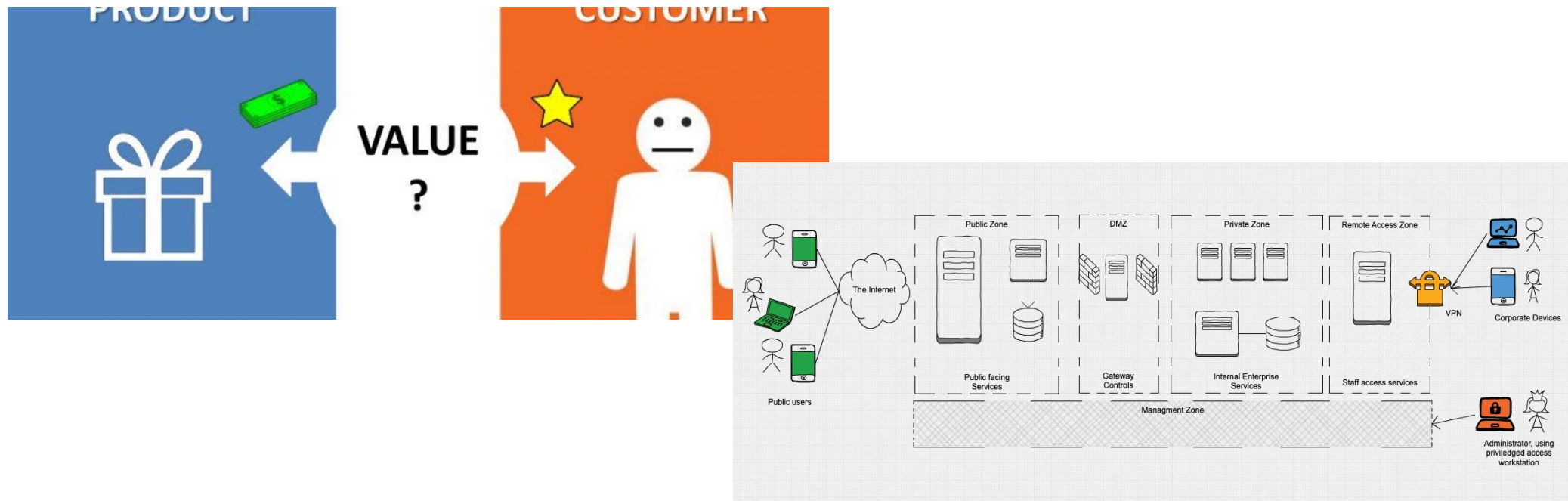
Hvordan ser processen ud?

- Hvad handler sikkerhed om for virksomheden?
 - Er der særlige hensyn?



Hvordan ser processen ud?

- Undersøg virksomheden og systemerne
 - Hvad er vigtigt og skaber værdi? Hvad er mindre vigtigt?
 - Hvordan kan det påvirkes?



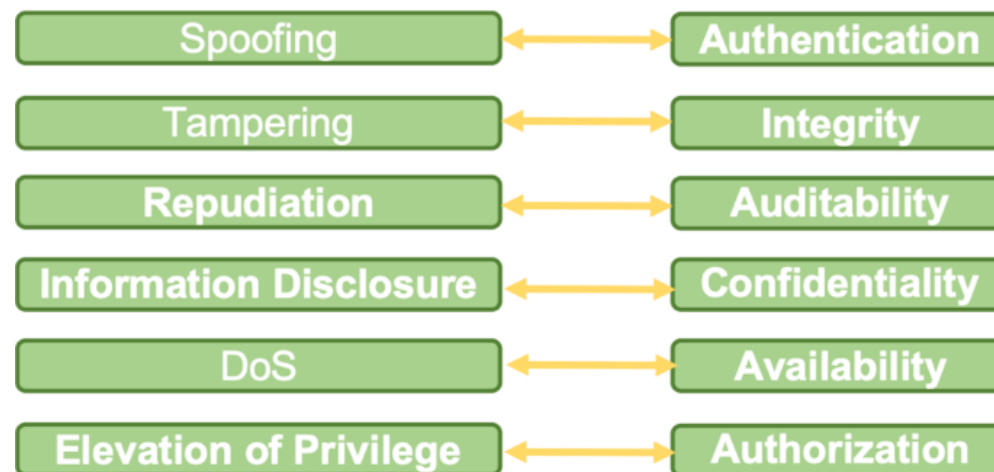
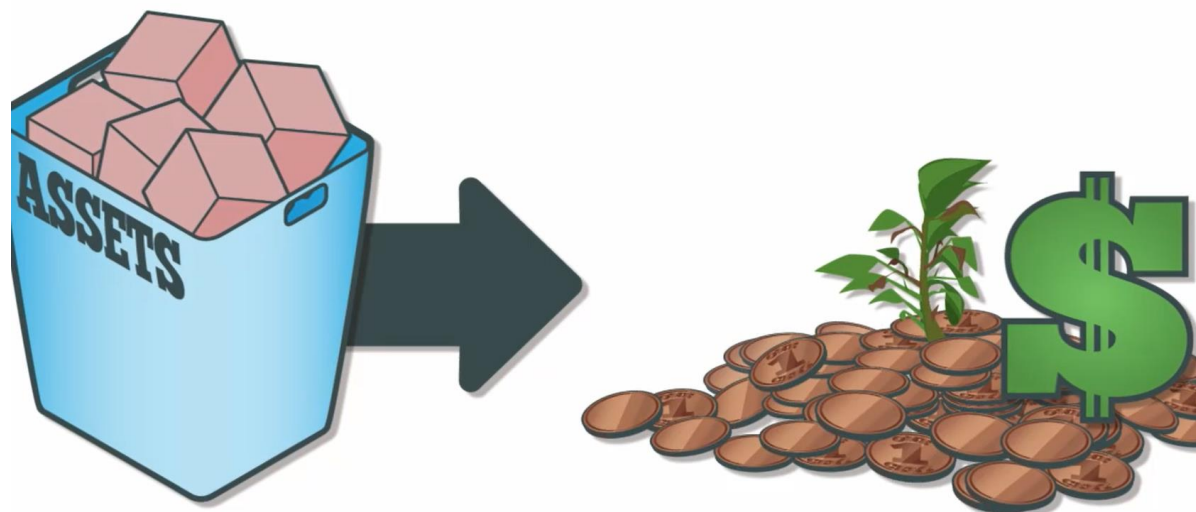
Hvordan ser processen ud?

- Hvad skal forbedres og hvordan?



Udfordringer vi ser i praksis?

Der kan være mange (nye)
tekniske begreber i
litteraturen



Udfordringer vi ser i praksis?

Trusselskataloger(!)

Sub-Category	ID	Threat	Description
Conflict	LIC1	Sabotage	Struggle resulting from incompatible or opposing needs, drives, wishes, or emotions.
	LIC2	Terrorism	Deliberate actions aimed to cause disruption or damage to information and/or IT assets, but not for religious, or ideological aim.
	LIC3	Vandalism	The use of violence as a means to create terror among masses of people; or religious, or ideological aim.
	LIC4	Warfare	Deliberate destruction or damage to information and/or IT assets, but not for religious, or ideological aim.
Misappropriation	LIM1	Embezzlement	Damage to assets, facilities, and employees due to war or armed conflict.
	LIM2	Extortion	Dishonestly or unfairly taking for one's own use.
	LIM3	Fraud	To appropriate something, such as property entrusted to one's care, fraudulently through fraud.
	LIM4	Theft	The act of obtaining money, property, or services from an organization through force or intimidation to obtain compliance.
	LIN1	Abuse of Authorizations	Deliberate deception to secure unfair or unlawful gain, or to deprive a victim of property.
	LIN2	Address Space Hijacking	The act of logically stealing and/or removing property with intent to deprive the victim of property.
	LIN3	Alteration of Software	Flagrant breaching of time-honored laws and traditions of conduct.
	LIN4	Anonymous Proxies	Using authorized access to perform illegitimate actions.
	LIN5	Autonomous System Hijacking	The illegitimate takeover of groups of IP addresses.
	LIN6	Brute Force	Unauthorized modifications to code or configuration data, attacking its integrity.
	LIN7	Code Injections	Access of websites through chains of HTTP proxies (obfuscation), bypassing traditional security measures.
	LIN8	Command Injection	Overtaking, by the attacker, the ownership of a whole autonomous system or network.

T Threat Catalog

- > TC TC.1: Spoofing
- > TC TC.1a: Identity spoofing when logging in (with a password)
- > TC TC.1b: Resource Location Spoofing
- > TC TC.2: Tampering
- > TC TC.2a: Exploitation of software weaknesses
- > TC TC.3: Repudiation
- > TC TC.4: Information Disclosure
- > TC TC.4a: Interception
- > TC TC.4b: Data extraction
- > TC TC.4b1: Firmware extraction
- > TC TC.4c: Reverse Engineering
- > TC TC.5: Denial of Service
- > TC TC.5a: Flooding
- > TC TC.5b: Jamming
- > TC TC.5c: Excessive Allocation of Resources
- > TC TC.6: Elevation of privilege
- > TC TC.6a: Man-in-the-Middle Attack

Name	Type	Description
WEP Shared Key Cracking	AA	802.11 shared key authentication with a cracked shared key or default WEP keys.
WPA-PSK Cracking	AA	Recovering a WPA PSK from captured key handshake frames using dictionary attack tools.
Application Login Theft	AA	Capturing application layer credential information such as email account and password by capturing clear text transmissions.
AP Theft	DoS	Physically removing an AP from a public space.
RF Jamming	DoS	Transmitting noise at the same frequency as the target WLAN.

interfered 802.11 beacon frames to find a legitimate

to prevent delivery of ACKs for deleted

/SSH tunnels in the

d AP by beaconing

the frame body and the MAC part of the frame. Attacker use bit

Consistency



SUCCESS

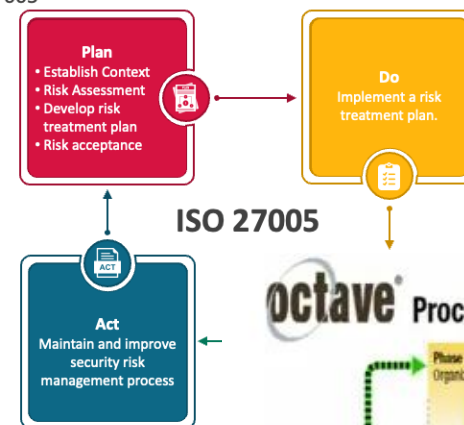
is key to success

Næste trin?

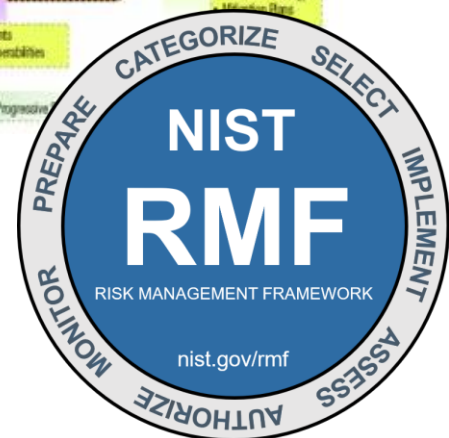
- Gør jer nogle erfaringer
 - Start småt og uformelt...
 - ... og begynd derefter at formalisere
- Standarder og frameworks er gode
 - De skal tilpasses virksomheden
- Selv en uformel gennemgang kan sætte ændringer i gang

ISO 27005

Overview of ISO 27005



octave Process



Guide til risikostyring

Risikostyring i forhold til cyber- og informationssikkerhed for smv'er

Alexandra Instituttet
Dansk Standard

Dansk Standard har gode erfaringer med at udvikle guides, der skal hjælpe virksomheder med at forstå og arbejde med standarder



Hvorfor er informationssikkerhed særligt relevant for SMV'er?



40% af de danske smv'er har et for lavt digitalt sikkerhedsniveau i forhold til deres risikoprofil

24% af de danske smv'er opdaterer ikke deres styresystemer eller har backup af data

Kilde: <https://erhvervsstyrelsen.dk/digital-sikkerhed-i-danske-smver-2021>

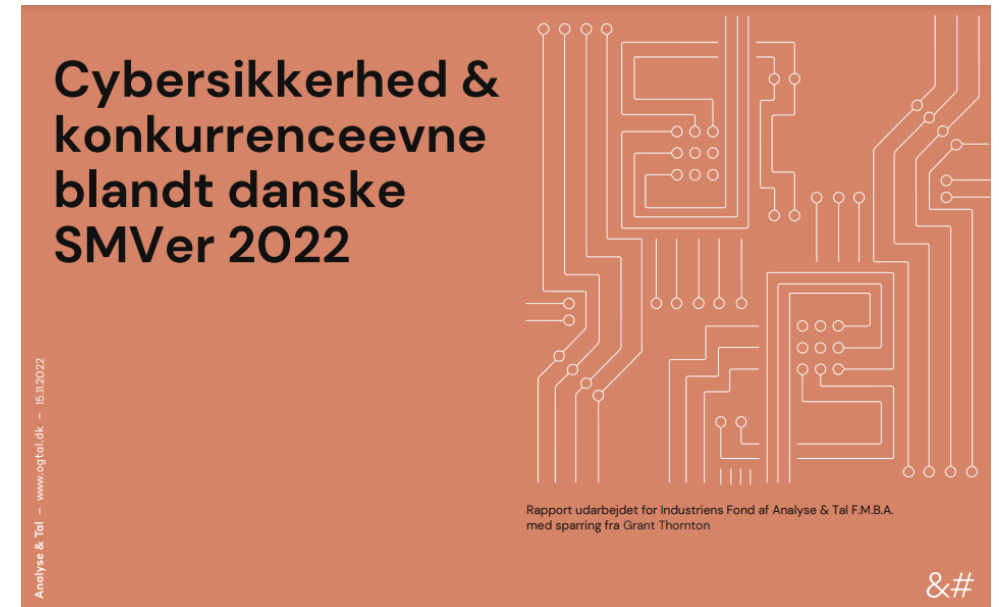
Cybertruslen mod Danmark

- Truslen fra cyberspionage er **MEGET HØJ**
- Truslen fra cyberkriminalitet er **MEGET HØJ**
- Truslen fra cyberaktivisme er **HØJ**
- Truslen fra destruktive cyberangreb er **LAV**
- Truslen fra cyberterror er **INGEN**

Cybersikkerhedstiltag skaber konkurrencefordele for virksomhederne

To af hovedindsigterne fra ny dansk rapport viser at:

- Flere cybersikkerhedstiltag fører til flere konkurrencefordele
- Cybersikkerhed fører til konkurrencefordele i alle brancher



NIS2 direktivet

Ingen direkte krav til standarder, men anbefalinger om at kigge i den retning.



NIS2

Artikel 25

Standardisering

1. For at sikre en samordnet gennemførelse af artikel 21, stk. 1 og 2, tilskynder medlemsstaterne til at benytte europæiske og internationale standarder og tekniske specifikationer, der er relevante for sikkerheden i net- og informationssystemer, uden at de påtvinger eller forskelsbehandler til fordel for anvendelse af en bestemt type teknologi.

Koblingen til NIS2 direktivet

Med NIS2 fastsættes der en række minimumskrav til foranstaltninger, der bl.a. indebærer at udarbejde politikker for **risiko**analyse og informationssikkerhed, håndtere hændelser og sikre driftskontinuitet (artikel 21).

"En risikostyringskultur, der indbefatter risikovurderinger og gennemførelse af foranstaltninger til styring af cybersikkerhedsrisici, som står i forhold til de foreliggende risici, bør fremmes og udvikles." (betragtning 77)

Guide for risikostyring i forhold til cyber- og informationssikkerhed

HVAD

Gode råd og redskaber til at arbejde konkret og systematisk med risikostyring i forhold til cyber- og informationssikkerhed.

HVORFOR

Hjælpe danske smv'er i gang med at arbejde med risikostyring og dermed ruste dem mod f.eks. cyberangreb og it-kriminalitet og samtidig bidrage til at styrke danske smv'ers konkurrencefordel.

HVEM

Danske smv'er der gerne vil i gang med risikostyring, men ikke nødvendigvis har den store forhåndsviden.

HVORDAN

Gennemgang af risikostyringsprocessen trin for trin suppleret med virksomhedseksempler.



Parametre der har indflydelse på risikostyringsprocessen

Digitalisering af virksomheden

Fortrolighed af data anvendt i virksomheden

Virksomhedens placering i leverandørhierarkiet

Antallet af brugere

Guiden benytter sig af tre virksomhedseksempler

VIRKSOMHED A Autoværkstedet



Mindre autoværksted

Mindre grad af digitalisering. Ingen fortrolige/personfølsomme data. Har private kunder og forskellige leverandører af materialer. Dog ikke kunder med særlige krav. Relativt få brugere.

VIRKSOMHED B Produktionsvirksomheden



Mellemstor virksomhed

(omkring 85 ansatte), der producerer og installerer videoovervågningssystemer. Høj grad af digitalisering. Stor mængde fortrolige data. Stor snitflade med mange brugere; kunder, samarbejdspartnere, leverandører mm. Leverer til kritisk infrastruktur.

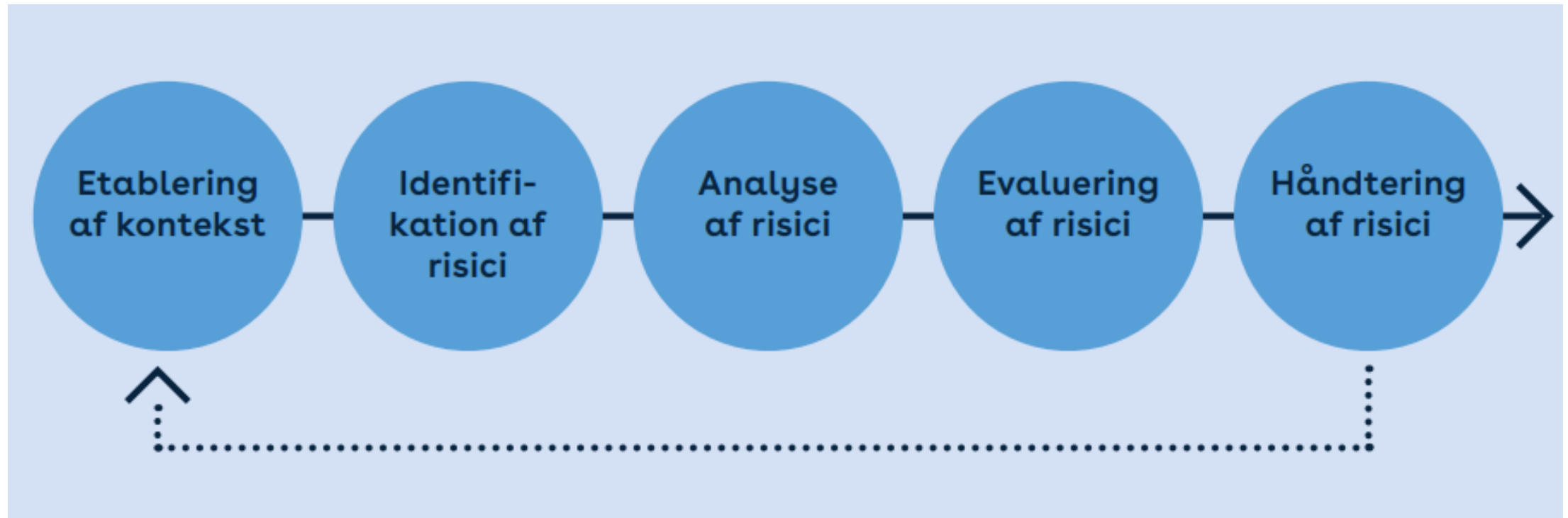
VIRKSOMHED C Webshoppen



Lille virksomhed

(fire ansatte), der importerer vin. Høj grad af digitalisering (100 % webshop). Mange brugere af webshoppen. Nogen grad af fortrolige data. Benytter sig i høj grad af leverandører i forhold til IT-driften.

Guiden gennemgår risikostyring trin for trin



Få konkrete input til at arbejde med sandsynlighed og konsekvens

KONSEKVENSSANDSYNLIGHED

	Lav	Middel	Høj
Lav	Lav/Lav	Middel/Lav	Høj/Lav
Middel	Lav/Middel	Middel/Middel	Høj/Middel
Høj	Lav/Høj	Middel/Høj	Høj/Høj

Brug af persondata

DDoS-angreb


Få konkrete input til at arbejde med sandsynlighed og konsekvens

KONSEKVENSS

	SANDSYNLIGHED				
	10-års hændelse	Årligt	Kvartalsvist	Ugentligt	Dagligt
0-50.000 kr.	1	2	3	4	5
50.001-125.000 kr.	2	4	6	8	10
125.001-500.000 kr.	3	6	9	12	15
500.001-2.500.000 kr.	4	8	12	16	20
2.500.001+ kr.	5	10	15	20	25

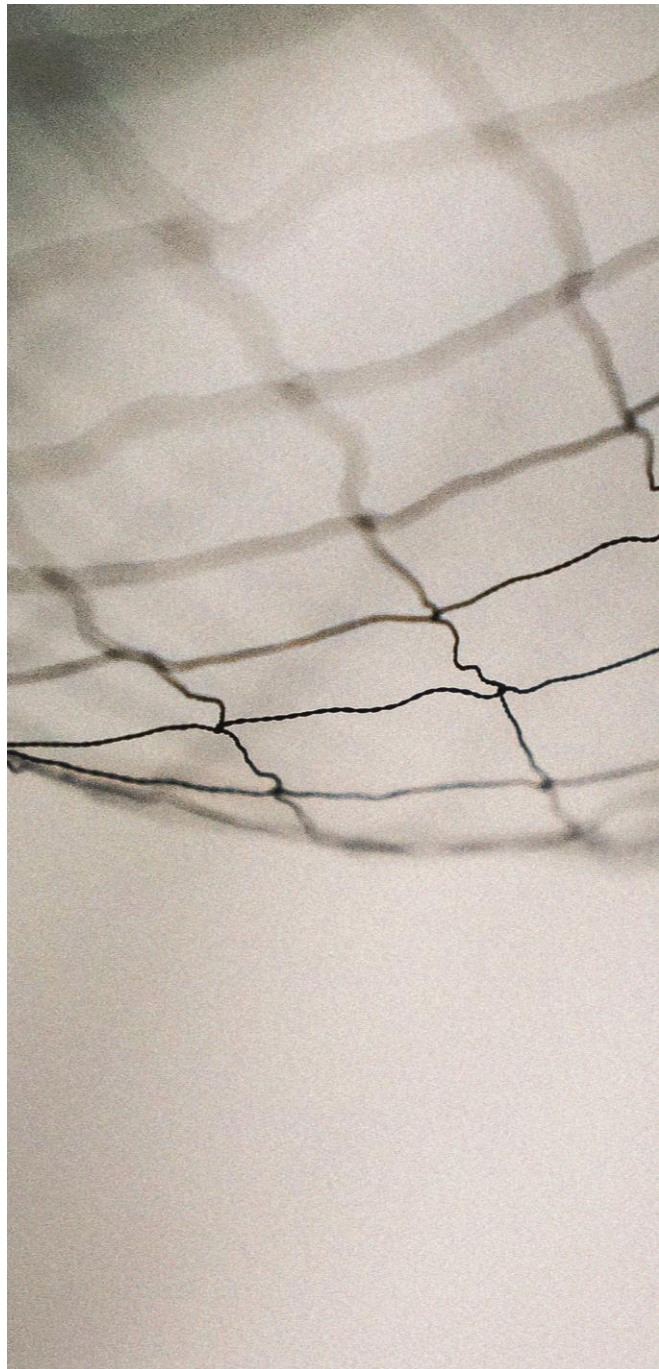
Manglende ekspertise ifm. et cyberangreb

Manglende validering af hvor data stammer fra



Guiden trækker på anerkendte standarder og rammeverk for risikostyring

- ISO/IEC 27005 Information security, cybersecurity and privacy protection – Guidance on managing information security risks
- ISO/IEC 29134 Information technology – Security techniques – Guideline for privacy impact assessment
- OCTAVE Allegro
- NIST SP 800-30, SP 800-37 og SP 800-39
- STRIDE/DREAD
- OWASP Risk Rating Methodology
- Erhvervsstyrelsens IT-risikovurderingsværktøj
- Erhvervsstyrelsens Sikkerhedstjek



Giver guiden værdi?

"Mange af de små virksomheder mangler måske nogle it-sikkerhedstiltag, som en specialist ville tænke er helt banale. Men der er bare mange andre ting, der fylder i hverdagen ude hos virksomhedsejerne".

"Vi tager imod sådan nogle initiativer [guiden], der skal hjælpe virksomhederne, med kyshånd - særligt, når de samtidig også er pædagogiske. Der sidder ikke særlig mange it-specialister ude i virksomhederne."

Citat: Lasse Lundquist, konsulent og digitaliseringsansvarlig, SMV Danmark

"For os har det været en øjenåbner at arbejde konkret med risikovurdering, og hvad det betyder for vores forretning. Det giver stor værdi at tage udgangspunkt i vores virkelighed og hvad der rent faktisk kan påvirke os, fremfor at tage udgangspunkt i generiske risici."

Citat: Anne Dorte Bach, projektleder og DPO hos Magenta

The background of the image is a light gray color, overlaid with a complex, white, stylized circuit board pattern. The pattern consists of numerous thin lines, some straight and some curved, connecting various small circles and dots, resembling a network or a digital circuit. The lines and dots are distributed across the entire frame, with a higher density towards the edges.

Hent guide for risikostyring her:
<https://www.ds.dk/risikostyring>

Tak



Michael Bladt Stausholm

E: michael.stausholm@alexandra.dk

M: 20 29 63 22



Berit Aadal

E: baa@ds.dk

M: 26 22 46 96



Q&A