23. august 2022

Cybersikkerhed i IoT produkter – basiskrav og risikostyring

Alexandra Instituttet
Force Technology
Dansk Standard

Dagens program

14:00 **Velkommen og status på det aktuelle trusselsbillede**
v/ Jeppe Pilgaard Bjerre, Force Technology og
Berit Aadal, Dansk Standard

14:20 **Grundlæggende krav til cybersikkerhed i IoT produkter – introduktion til EN ETSI 303 645**
v/ Jeppe Pilgaard Bjerre, Force Technology

14:45 **Risikostyring og cybersikkerhed i IoT produkter**
v/ Michael Stausholm, Alexandra Instituttet

15:10 **Spørgsmål**

15:30 **Tak for i dag**

Om Dansk Standard

Hvem er Dansk Standard

- Danmarks officielle standardiseringsorganisation
- Erhvervsdrivende fond, grundlagt i 1926
- 168 medarbejdere (jan. 2021)
- Erhvervspolitisk partnerskab med Erhvervsministeriet

Vi er medlem af:

En stærk platform af solide brands:

Dansk specifikation for cybersikkerhed i IoT-produkter

HVAD

Et samlet overblik over de væsentligste internationale og europæiske standarder inden for cybersikkerhed i produkter (IoT). Fokus på horisontale standarder.

HVORFOR

Hjælpe danske SMV'er med at identificere relevante standarder til deres arbejde med cybersikkerhed i produkter (IoT) og bidrage til at højne cybersikkerheden i dansk erhvervsliv.

HVEM

Danske SMV'er der har fokus på cybersikkerhed i produkter; producenter og aftagere.

HVORDAN

Kort præsentation og vurdering af 12 standarder og standard-serier ud fra en række udvalgte kriterier. Standarderne er placeret i en livscyklusmodel for IoT-produkter. Involvering af fageksperter igennem tre workshops samt offentlig kommenteringsrunde.

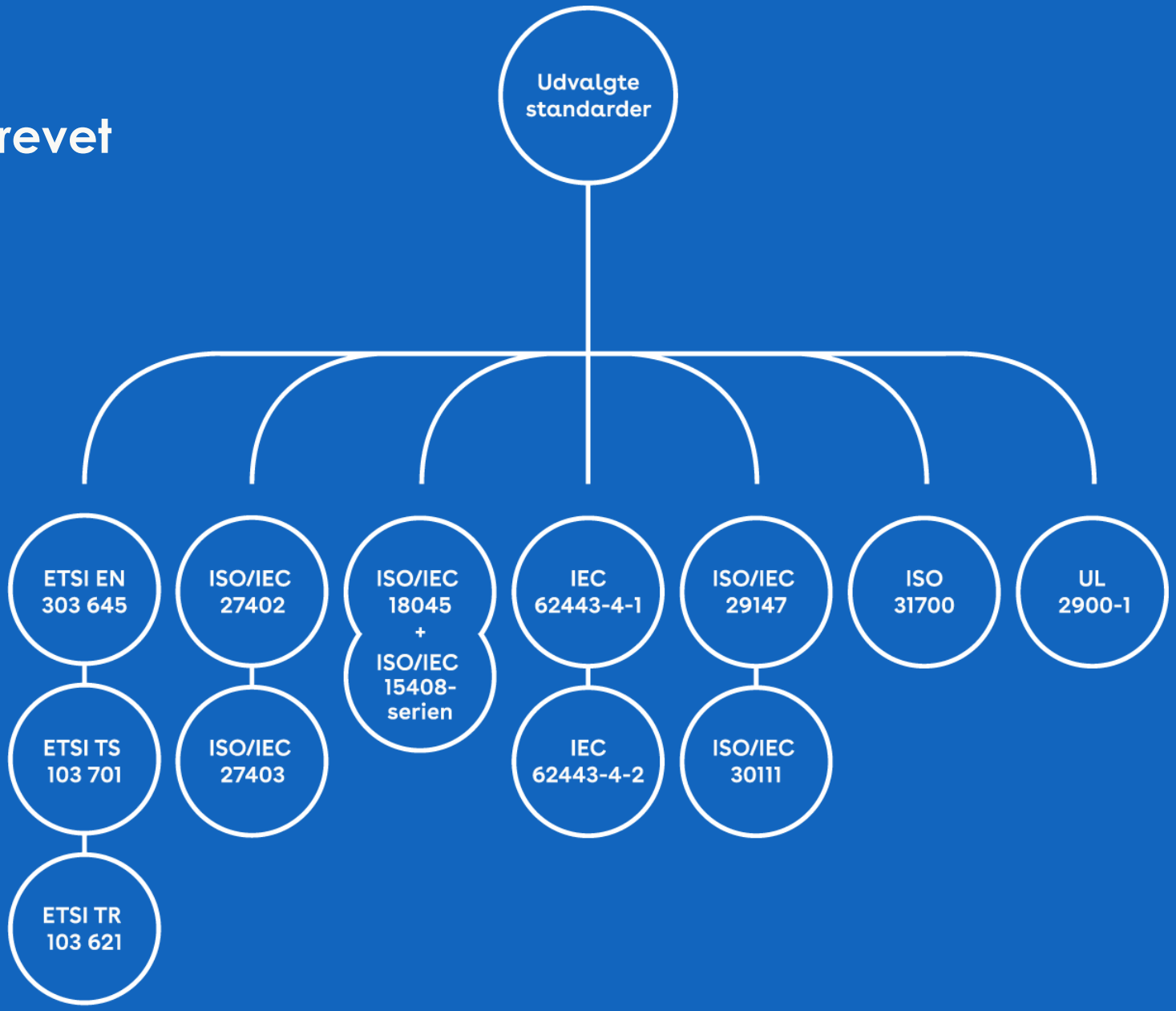
Specifikationen er støttet af cyber hub og ERHVERVSSTYRELSEN

Behovet for en specifikation

- Virksomheder ønsker, at deres IoT-produkter er sikre.
- Imødekomme et behov for overblik over eksisterende og kommende internationale standarder inden for cybersikkerhed i IoT-produkter.
- Standarder kan bidrage til, at virksomheder arbejder mere systematisk med cybersikkerhed i IoT-produkter – udgangspunkt i et livscyklusperspektiv.
- Hjælp til at definere hvilke krav til cybersikkerhed, man kan og bør stille til leverandører.
- Bidrage til, at danske virksomheder prioriterer arbejdet med cybersikkerhed i IoT-produkter.
- Understøtte danske virksomheders konkurrencekraft i forhold til cybersikkerhed i IoT-produkter.

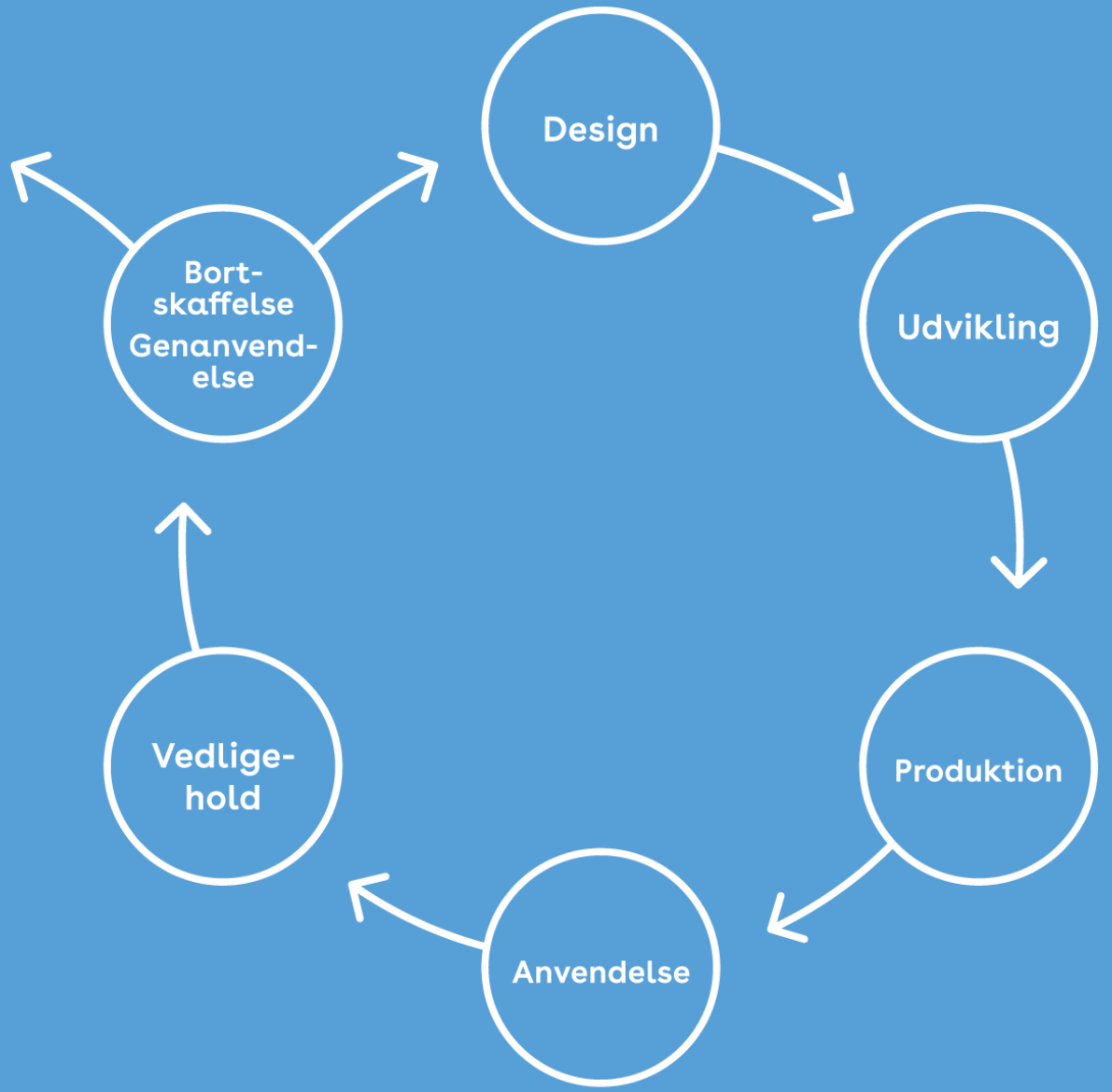
Ambition: Højne cybersikkerheden blandt danske SMV'er.

Standarder og standardserier beskrevet i specifikationen



Figur fra specifikationen.

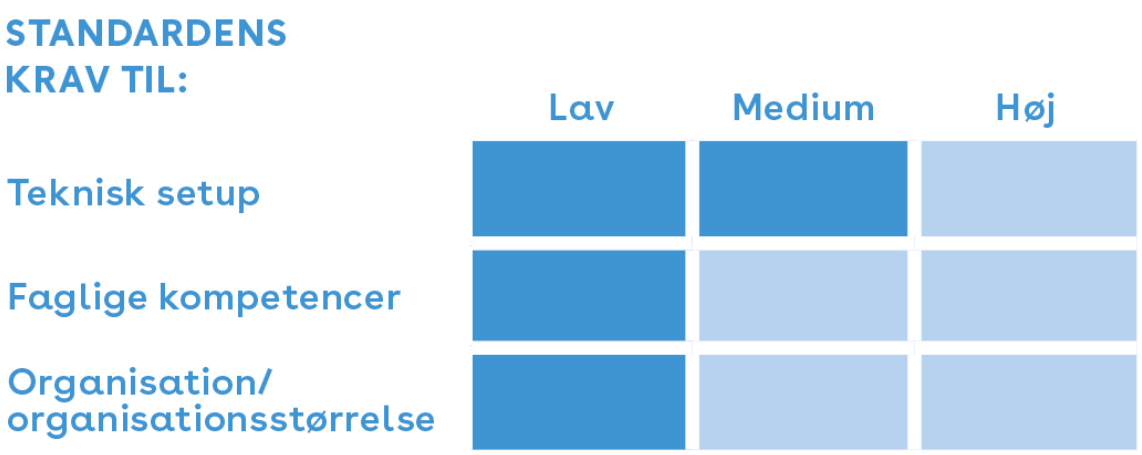
Specifikationen tager udgangspunkt i en livscyklus-model for IoT-produkter

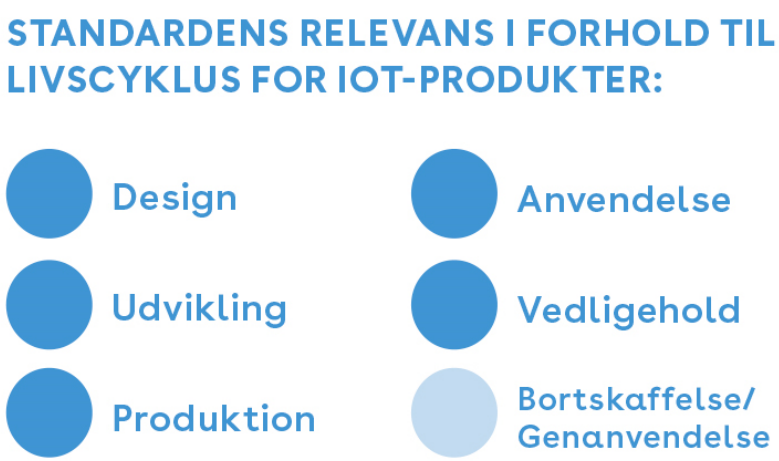


Figur fra specifikationen.

Få et hurtigt overblik over standarderne

Specifikationen indeholder to gennemgående figurer, der kan bruges til at sammenligne standarderne på tværs





Eksempel fra specifikationen.

DANSK STANDARD

Hent specifikationen gratis i vores webshop: www.webshop.ds.dk

Tak

Berit Aadal

E: baa@ds.dk

M: 26 22 46 96

Er det farligt?

(ja)

24 August, 2022

Udfordringen

- Potentielt mange enheder
- Forskellige netværk / fysiske lokationer
- Ofte konkurerende på pris
- Enheder kan være kritiske for drift
- Etc
- Etc
- ...

CfCS siger (Juni 2022):

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

Kilde: CfCS trusselsvurdering:Cybertruslen mod Danmark 2022

Hvad ændre sig?

- IT, OT og IoT mødes
- Botnet / ransomware
- AI / ML tilgængelighed

Hvad ændre sig?

- IT, OT og IoT mødes
- Botnet / ransomware
- AI / ML tilgængelighed

Opkoblede sensorer / aktuatorer i processer bliver mere udbredt og kobler på tværs af IT/OT opsætninger så grænser udvidskes.

OT rammes af de samme problemstillinger som IT har håndteret i en periode

Hvad ændre sig?

- IT, OT og IoT mødes
- Botnet / ransomware
- AI / ML tilgængelighed

Øget tilgængelighed af sårbare IoT enheder er med til at gøre det lettere at opbygge botnets til ex DDoS angreb eller låse vha ransomware.

Ligeledes bliver ransomware dyrere. Fra 2016 til 2021 er prisen per GB låst data cirka steget med en faktor 10

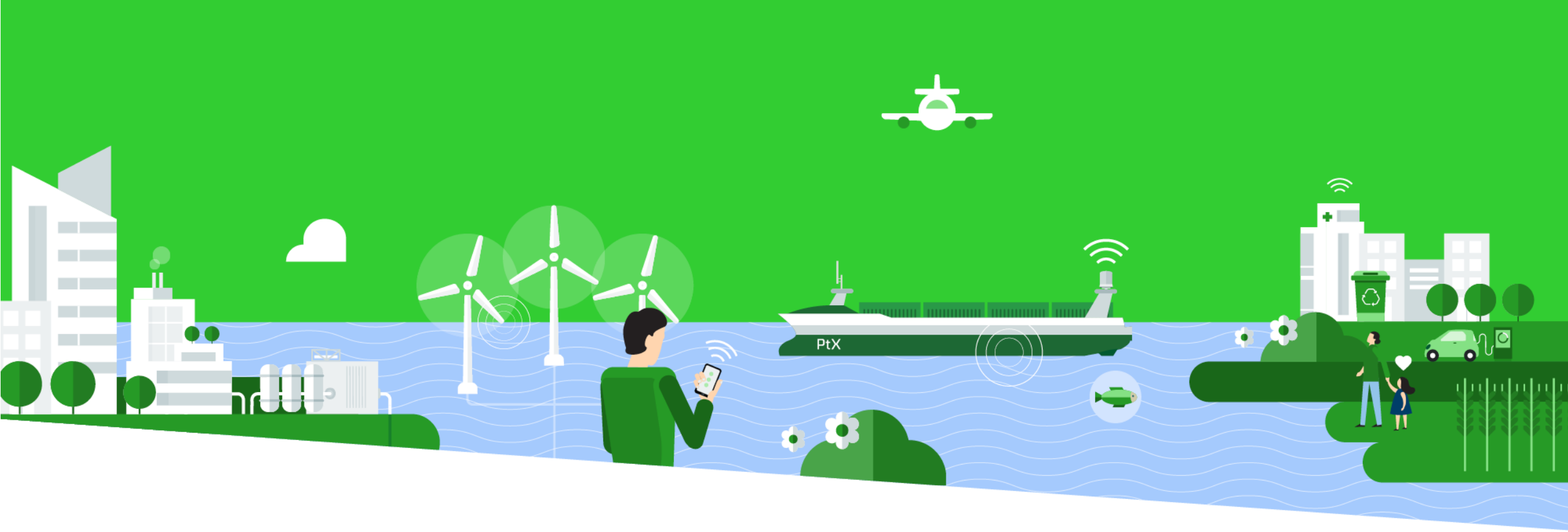
Kilde: Sectrio – Global threat landscape 2022

Hvad ændre sig?

- IT, OT og IoT mødes
- Botnet / ransomware
- AI / ML tilgængelighed

Udviklingen inden for AI er med til at
køre exploits mere kompekse og dynamiske
I forhold til at undgå detektion og højne
succesraten for et angreb

Questions



ETSI EN 303 645

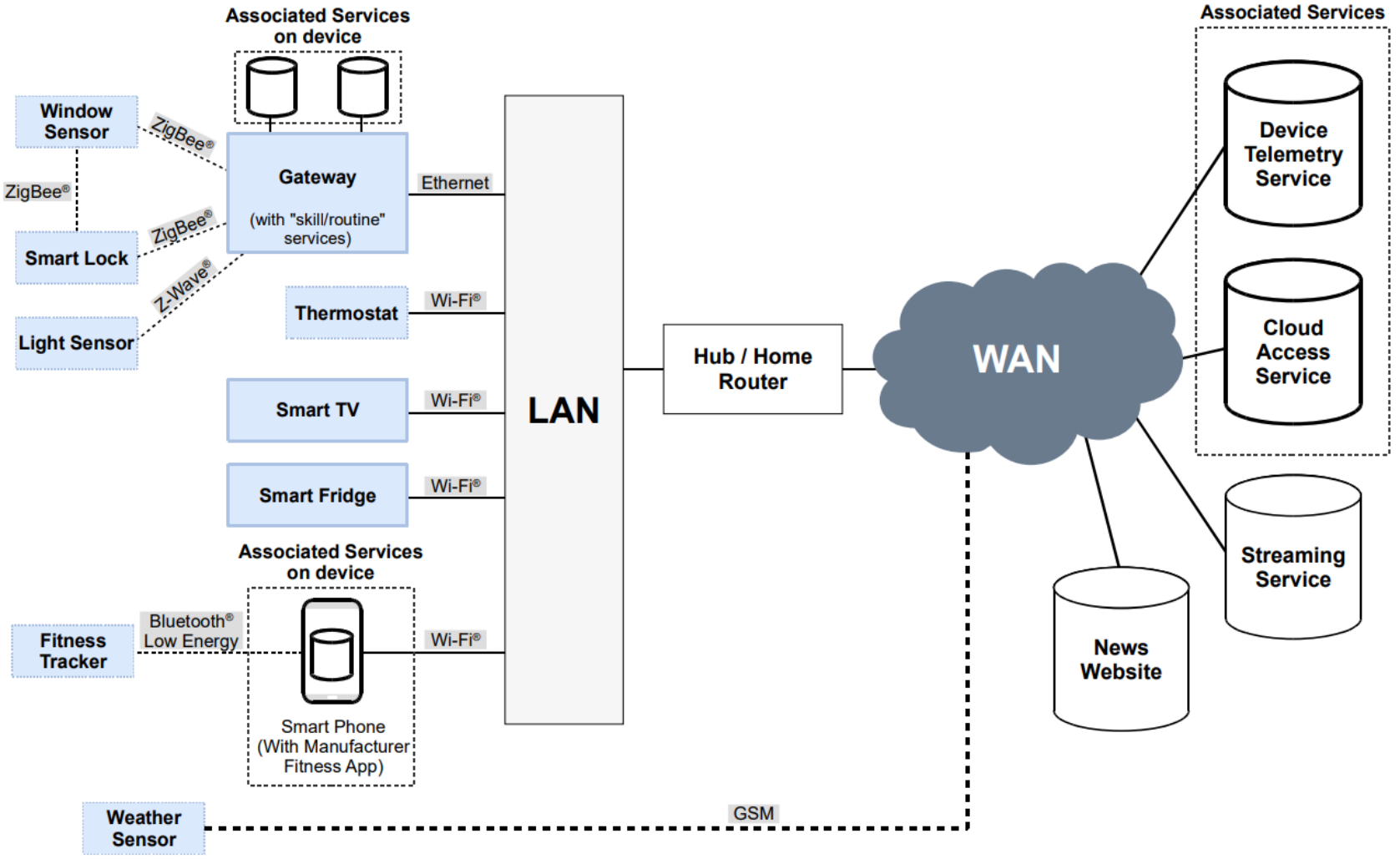
Jeppe Bjerre

Compliance specialist

FORCE Technology

24 August, 2022

Scope – EN 303 645 / TS 103 701



Source: ETSI EN 303 645

EN 303 645

EN 303 645 - Cyber Security for Consumer Internet of Things: Baseline Requirements

Source: ETSI EN 303 645

RISIKOSTYRING OG CYBERSIKKERHED I IOT PRODUKTER

Michael Stausholm

Senior Security Architect, Alexandra Instituttet A/S

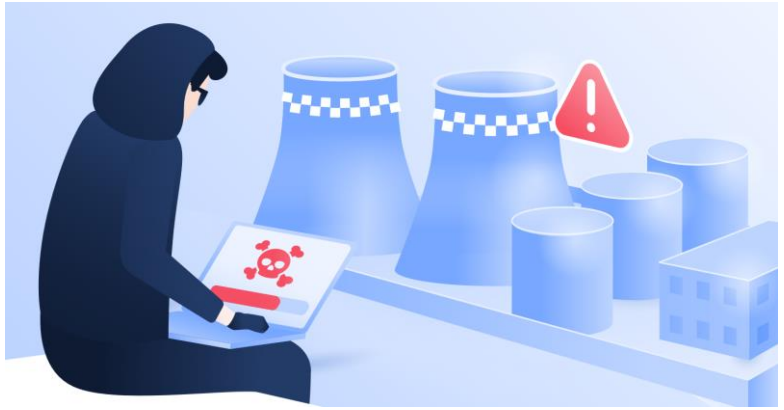
ALEXANDRA INSTITUTTET

The Alexandra Institute is a non-profit company
that works with applied IT research.

Our mission is to merge research, innovation, IT and business
to create value, growth and welfare in society.

WHAT CAN BE HACKED – WILL GET HACKED

- Alt kan hackes, hvis hackerne har resourcer nok!
  - Eksempelvis Stuxnet og det Iranske atom program
- Hvor sikre skal produkterne så være?



- Risikostyring er et centralt værktøj til at sikre balancen
  - og samtidigt en vigtig del af mange sikkerhedsstandarder

ALEXANDRA INSTITUTTET

GRUNDLÆGGENDE RISIKOANALYSE

Risiko = Sandsynlighed x Konsekvens

- Sandsynlighed:
  - Angribers motivation +
  - Angribers kompetencer +
  - Systemets styrke –
- Konsekvens:
  - Teknisk
  - Forretningen

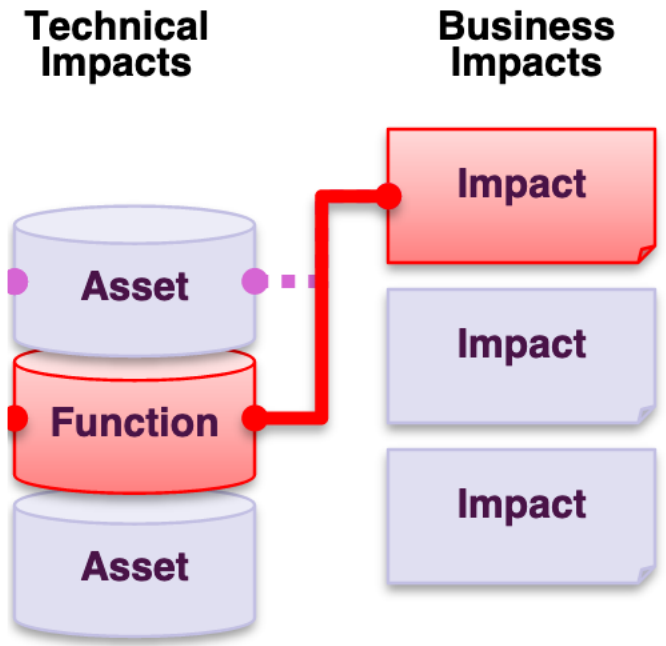
SANDSYNLIGHED	Meget lav	Lav	Medium	Høj	Meget høj
Meget lav	2	3	4	5	6
Lav	3	4	5	6	7
Medium	4	5	6	7	8
Høj	5	6	7	8	9
Meget høj	6	7	8	9	10

KONSEKVENS

ALEXANDRA INSTITUTTET

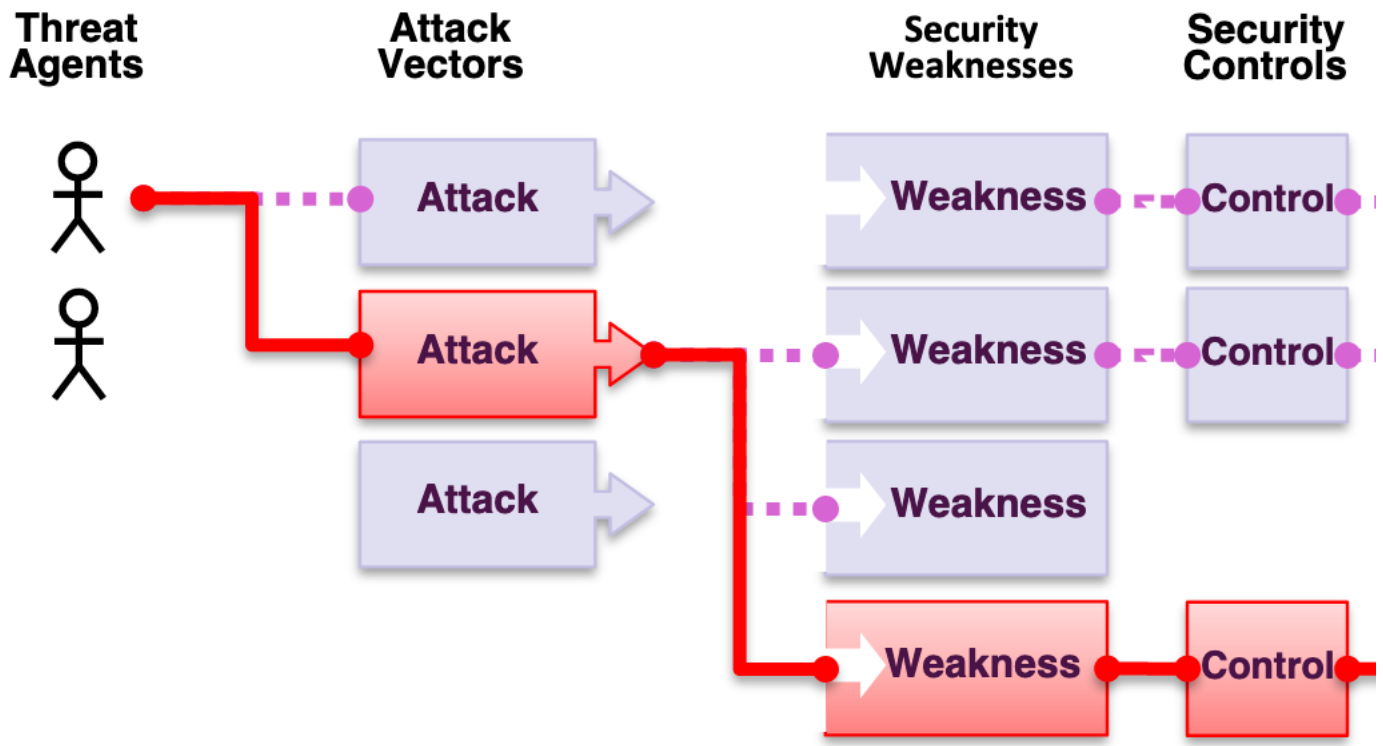
RISIKO – KONSEKVENSEN

- Teknisk konsekvens
  - Uautoriseret adgang til data
  - Uautoriseret adgang til funktion
  - Ødelægge noget
  - …
- Eksterne parter?
- I sidste ende forretningen
  - Tab af kunder
  - Bøder
  - Tid og ressourcer for at rydde op
  - ...



ALEXANDRA INSTITUTTET

RISIKO – SANDSYNLIGHED



- Agenten
  - Motivation
  - Kompetencer
    - Teenager
    - Organisede kriminelle
    - Fjendtlige nationer
    - Konkurrenter
    - Et mix
- Styrke af systemet
  - Undgå svagheder
  - Sikkerhedskontroller

ALEXANDRA INSTITUTTET

RISIKOANALYSE: MÅL FOR METODEN

- Output skal være så objektivt som muligt
  - Skal sikre sammenlignelighed over tid og på tværs af systemer
- Der findes allerede mange standarder og frameworks at støtte sig til
  - ISO/IEC 27005, OCTAVE Allegro, NIST SP-800-30 og mange flere
- (Endnu) en guide fra DS under udvikling omkring risikostyring

ALEXANDRA INSTITUTTET

RISIKOANALYSE: UDFORDRINGER

- Det kan være meget svært at vurdere sandsynligheden for en hændelse
  - Øvelse, flere øjne og indsamling af erfaringer
- Der kan være uventede konsekvenser
  - Strava Fitness app
- Håndtering af skalerbarhed

- Det kan være vanskeligt at vurdere konsekvens på vegne af andre
  - Hvor kritisk er produktet for kunderne?

ALEXANDRA INSTITUTTET

RISIKOANALYSE: VARIANTER

- Asset eller hændelses baseret?
  - Tager man udgangspunkt i egne systemer og hvordan man kan tilgå de kritiske dele?
  - Eller tager man udgangspunkt i mulige hændelser og vurderer hvad de har af konsekvens?

- Er der behov for en egentlig risikovurdering?
  - Kan konsekvensanalyse eller trusselsmodellinger være nok?

ALEXANDRA INSTITUTTET

RISIKOSTYRING

- Hvordan håndteres risici?
  - Risiko appetit
  - Mindske sandsynlighed og/eller konsekvens
  - Forsikring og/eller accept

- Husk ledelsen!

SANDSYNLIGHED	Meget lav	Lav	Medium	Høj	Meget høj
Meget lav	2	3	4	5	6
Lav	3	4	5	6	7
Medium	4	5	6	7	8
Høj	5	6	7	8	9
Meget høj	6	7	8	9	10

KONSEKVENS

ALEXANDRA INSTITUTTET