NØGLEORDSARK: ORGANISATION

Scan QR-koden for at finde en trin-for-trin guide til dette værktøj, digitale forretningsudviklings-cases og mere inspiration på dbd.au.dk

- **Ansvar** er ikke i fokus eller er uafklaret.
- Ingen eller få **kompetencer**, måske ildsjæle. Ledelsen er uinteresseret.
- **Tilgang**: forholder sig til IoT-cybersikkerhed gennem kundernes spørgsmål, ingen beredskabsplaner mv.

- En eller flere personer har formelt **ansvar**.
- Enkelte interne **kompetencer** samt sparring med eksterne fagfolk. Ledelsen interesseret i økonomiske konsekvenser.
- Er ved at opbygge en **tilgang** med planer og procedurer for IoT-cybersikkerhed og er optaget af fælles forståelse.

- Forankret internt **ansvar** og klar organisering af arbejdet.
- Har adgang til alle nødvendige **kompetencer** internt og/eller eksternt. Ledelsen deltager aktivt og informeret i vurderinger.
- Struktureret **tilgang** og proces for beredskab og risikovurdering – alle dele af forretningen.

NØGLEORDSARK: FORRETNING

Scan QR-koden for at finde en trin-for-trin guide til dette værktøj, digitale forretningsudviklings-cases og mere inspiration på dbd.au.dk

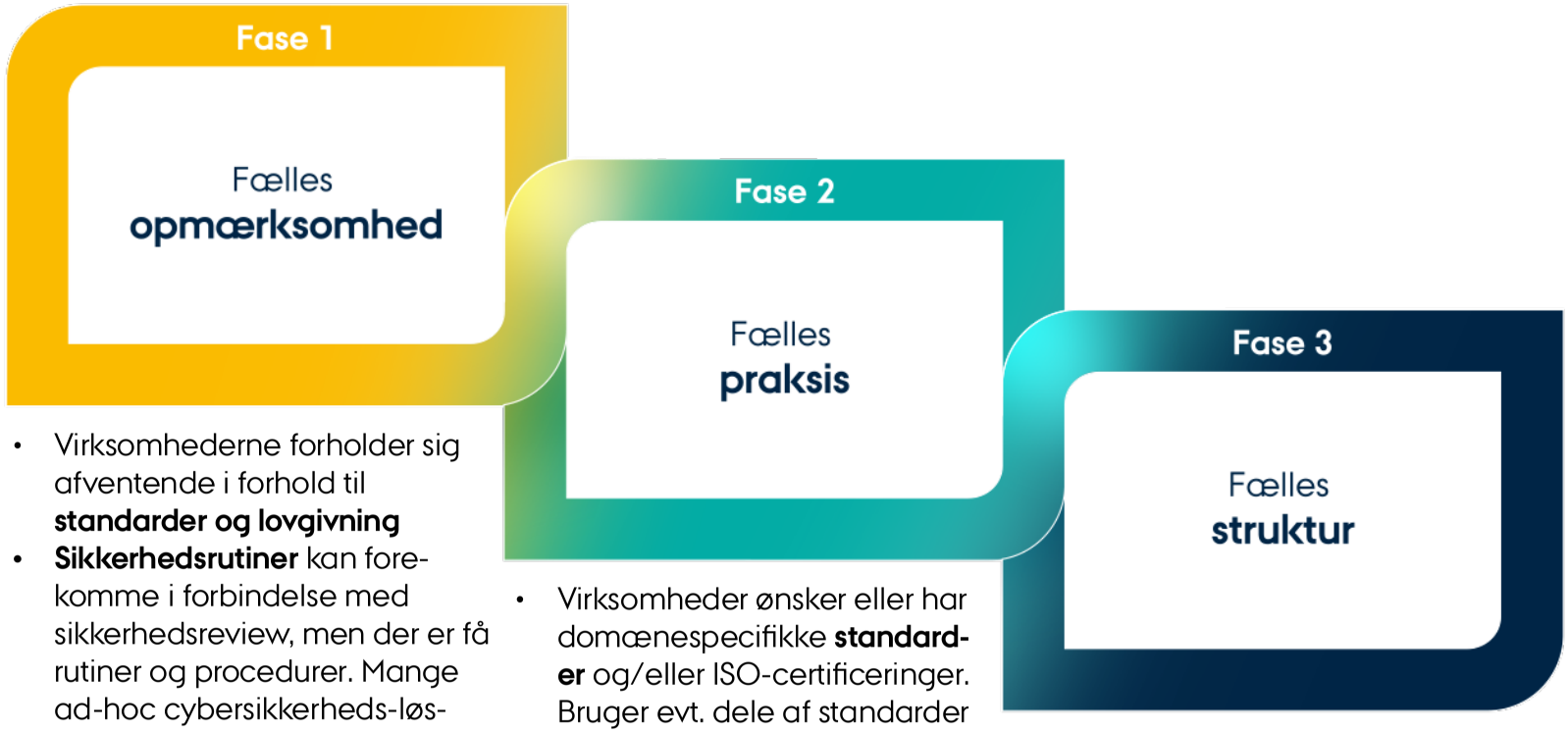
- **Forretningsformål** med IoT-løsninger er typisk at overvåge drift og tage hensyn til fordele og ulemper ved sikkerhedsvalg for kunderne.
- **Kritikalitet** for driftsdata er fortrolighed.
- **Forretningsudvikling** er ikke koblet sammen med IoT-løsningen eller data.

- **Forretningsformål med** IoT-løsninger er automatisering, optimering og driftssikkerhed.
- **Kritikalitet** for data er typisk tilgængelighed og integritet. Fokus på økonomisk effektivt niveau of IoT-cybersikkerhed. **Forretningsudvikling** har fokus på systematisk datahøst, datas integritet og fortrolighed. Stor interesse for potentialer i cloud-løsninger.

- **Forretningsformål** med IoT-løsninger er automatisering og forbundne produkter og services.
- **Kritikalitet** og risikoappetit vurderes og tilpasse løsningerne særskilt.
- **Forretningsudvikling** sker i form af nye forretningsmodeller, fordi IoT-cybersikkerhed er et 'selling-point'. Cloud-løsninger og digitale platforme til kunderne.

NØGLEORDSARK: KVALITET

Scan QR-koden for at finde en trin-for-trin guide til dette værktøj, digitale forretningsudviklings-cases og mere inspiration på dbd.au.dk



- Virksomhederne forholder sig afventende i forhold til **standarder og lovgivning**
- **Sikkerhedsrutiner** kan forekomme i forbindelse med sikkerhedsreview, men der er få rutiner og procedurer. Mange ad-hoc cybersikkerheds-løsninger.
- **Brug af standarder** ses som en mulighed, men standardiseringsprocessen opfattes som overvældende.

- Virksomheder ønsker eller har domænespecifikke **standarder** og/eller ISO-certificeringer. Bruger evt. dele af standarder som en systematik.
- **Sikkerhedsrutiner** lægger sig op ad generaliserede niveauer og målsætninger. Stigende fokus på IoT-cybersikkerheden i det samlede system/løsning.
- **Brug af standarder** ses som et fælles sprog både internt og eksternt og som valid baggrund for sikkerhedsbeslutninger.

- Virksomhederne har typisk flere ISO-**standarder** og domænespecifikke it- og cybersikkerhedsstandarder. Letter arbejdet med at leve op til lovkrav.
- **Sikkerhedsrutiner** og rammeværk er tænkt ind fra start-en af udviklingsprocesserne.
- **Brug af standarder** er et fælles sprog for alle og en konkurrencefordel.

FIND VORES WEBSITE
DIGITAL BUSINESS DEVELOPMENT
PÅ DBD.AU.DK

"CyPro", støttet af Industriens Fond.
Materialet er stillet til rådighed under licens CC BY-SA 4.0

INDUSTRIENS FOND

NØGLEORDSARK: TEKNISK

Scan QR-koden for at finde en trin-for-trin guide til dette værktøj, digitale forretningsudviklings-cases og mere inspiration på dbd.au.dk

- **Tekniske til- og fravalg** afgøres af, at IoT-løsningens funktioner og data ikke opfattes som kritiske for forretningen. Stort fokus på driftssikkerhed.
- **Tekniske aktiviteter** inkluderer ofte ikke IoT-cybersikkerhed. Der er tiltro til, at leverandøren har styr på IoT-sikkerheden. Kan udsende opdateringer. Få har logning. Ikke stort fokus på brugeradgang til enheder.
- **Risikovurdering** er ikke systematisk eller tydelig.

- **Tekniske til- og fravalg** er, at IoT-cybersikkerhed er bygget ind fra starten eller opdateres løbende.
- De nødvendige IoT-sikkerhedskompetencer til **tekniske aktiviteter** er tilgængelige: patch management, logning og monitorering samt bruger-adgang er systematiseret
- **Risikovurdering** ses ved bevægelse væk fra ad hoc-cybersikkerhedstilgang til risikobaseret IoT-sikkerhedsniveau.

- **Tekniske til- og fravalg** er indlejret i en helhedsorienteret tilgang for alle løsningernes scenarier og kontekster.
- **Tekniske aktiviteter** sker i fælles og strukturerede processer. Der er flere lag af IoT-cybersikkerhed bygget ind i løsningerne. Der er dedikerede ressourcer.
- Til- og fravalg baseres på kontinuerlig **risikovurdering**, både ledere og medarbejdere deltager.

FIND VORES WEBSITE
DIGITAL BUSINESS DEVELOPMENT
PÅ DBD.AU.DK

"CyPro", støttet af Industriens Fond.
Materialet er stillet til rådighed under licens CC BY-SA 4.0

INDUSTRIENS FOND