REFERENCEARK: 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

Opmærksomhed

- Overvåger drift, evt. brug af driftsdata til rapportering eller effektivisering.
- Data og øvrige aktiver i IoT-løsningen er ikke vigtige i forretningsudviklingen.
- Fordele ved øget IoT-cybersikkerhed afvejes altid op imod ulemper for brugerne hos kunderne.
- Hvis der er overvejelser om services bygget på data sammen med andre virksomheder og partnere, så fylder IoT-cybersikkerhed ikke ret meget heri.
- Kritikalitet for driftsdata italesættes ofte som **fortrolighed** og GDPR-compliance.

Praksis

- Fokus på automatisering, optimering og driftssikkerhed samt indsigter om produktionen.
- Fokus på forretningspotentialet i systematisk at hente data hjem med integritet, der er tilgængelige og fortrolige. Stor interesse for cloud-løsninger i forretningen med fokus på at afklare sikkerheden, hvis der indgår en cloud-løsning eller en digital platform i IoT-løsningen.
- Overvejelser om IoT-cybersikkerhed som en gevinst i form af fx øget salg og bedre konkurrenceevne og et solidt omdømme.
- Sammenstilles med fokus på, hvad der er et økonomisk effektivt niveau af IoT-cybersikkerhed.
- Kunderne stiller flere krav og spørgsmål til IoT-cybersikkerheden, og virksomheden har mere og mere fokus på leverandørens sikkerhed.
- Der er typisk fokus på især datas tilgængelighed og integritet i forhold til at holde produktionen i gang. Fortrolighed synes ikke relevant i forhold til produktionsdata.

Struktur

- Fokus på automatisering samt at koble produkter og enheder sammen med services. Større fokus på at levere udstillede/modellerede data til kunder, fx via en digital platform.
- Nye forretningsmodeller baseret på service samt data som en handelsvare. Cloud-løsninger og digitale platforme til kunderne er implementeret, og der er øget deling af data.
- IoT-cybersikkerhed er et konkurrenceparameter og et 'selling point', der differentierer virksomheden fra konkurrenterne; en central brand-værdi, der koster penge og ressourcer.
- Samarbejdet om IoT-løsninger og deres sikkerhed er ofte formaliseret og dokumenteret.
- Fokus på at håndtere, at IoT-cybersikkerhed varierer fra løsning til løsning, herunder risikoappetit i forhold til tilgængelighed, integritet og fortrolighed af data. De nye digitale løsninger på tværs af virksomheder kan aktualisere fortrolighed, fordi der kan være kundedata involveret.

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

INDUSTRIENS FOND

"CyPro", støttet af Industriens Fond.

REFERENCEARK: 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

Opmærksomhed

- Virksomhederne i denne fase forholder sig afventende og har ofte endnu ikke arbejdet med standarder.
- Indledende arbejde med sikkerhedsreviews og dokumentation af praksis.
- Ingen eller få daglige rutiner, processer og procedurer på tværs af virksomheden.
- Der laves mange ad hoc- løsninger, og det øger systemets kompleksitet.
- Standarder ses som en mulighed for at undgå særtilpasninger, men standardiseringsprocessen opfattes som overvældende.

Praksis

- Har måske – eller ønsker at opnå – en domænespecifik eller en generel ISO-certificering eller bruger dele af standarder som systematik.
- Standarderne bidrager til at skabe et fælles sprog om sikkerhed – både internt i virksomheden og eksternt i samtalen med kunder.
- Arbejdet med sikkerhed går fra at være afhængigt af enkeltkunders krav og spørgsmål til at lægge sig op ad generaliserede niveauer og målsætninger.
- Der er stigende fokus på sikkerheden i det samlede system frem for individuelle løsninger.
- Motivationen for struktureret arbejde med standarder er, at det vil styrke kommunikationen med kunderne om sikkerhed, og giver en valid baggrund for de trufne IoT-cybersikkerhedsbeslutninger.

Struktur

- Har typisk flere ISO-standarder og domænespecifikke standarder, samt it-standarder og enkelte (del)standarder for cybersikkerhed.
- Standarder og/eller rammeværk for IoT-cybersikkerhed er et struktureret grundlag for at opstille krav og skabe et fælles sprog på tværs af afdelinger. Disse indgår i dialog med ledelsen om risikovurderinger og ressourcer til sikkerhed.
- Typisk har virksomhederne i denne fase tænkt dokumentation ind fra starten af udviklingsprocessen.
- Motivationen for standardisering er, at certificering opfattes som en konkurrencefordel og en systematisk måde at kommunikere internt og eksternt om IoT-cybersikkerhed. Samtidig letter standarderne arbejdet med at leve op til lovkrav.

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

UGLA INSIGHTS
FORCE TECHNOLOGY
DAMRC
ALEXANDRA INSTITUTTET
DEPARTMENT OF BUSINESS DEVELOPMENT AARHUS UNIVERSITY BSS

REFERENCEARK: 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

Opmærksomhed

- Ansvaret for IoT-cybersikkerhed er ikke i fokus eller er uafklaret.
- Ingen eller få interne kompetencer i IoT-cybersikkerhed. Måske interne kompetencer hos en opmærksom teknisk ildsjæl. Ofte afhængig af eksterne rådgivere og leverandører til at sparre med og til at levere IoT-cybersikkerhed.
- Der kan være oplæg fra tekniske ildsjæle om IoT-cybersikkerhed til ledere/direktion. Det er en stor formidlings-opgave at få forretningen til at forstå konsekvenserne af et givent risikoniveau/risikoappetit.
- Internt tales der i IoT-projekter primært om funktionalitet ud fra et teknisk/fagligt perspektiv, hvilket i nogle tilfælde kan inkludere IoT-cybersikkerhed.
- Har ikke beredskabsplaner for IoT.
- Generelt en tilgang til IoT-cybersikkerhed, hvor man primært forholder sig til det som svar på kundernes spørgsmål om IoT-cybersikkerhed.

Praksis

- En eller flere personer har en formaliseret rolle med ansvar for IoT-cybersikkerhed, enten internt eller eksternt (fx IoT-leverandøren).
- Der er nogle interne kompetencer i IoT-cybersikkerhed og sparring med eksterne som konsulenter, partnere og leverandører. Får evt. gennemført ekstern risikovurdering af hensyn til kvalitet.
- Ledelsen bakker op om IoT-cybersikkerhed og har en klar holdning til det under hensyntagen til økonomi i sikkerhedsinvesteringer. Ledelsen modtager rapporteringer om IoT-cybersikkerhed og afsætter budget til det.
- Intern kommunikation har fokus på, at alle har en fælles forståelse af IoT-cybersikkerhed, hvilket bygger på hyppig dialog.
- Har beredskabsplaner for it, men ikke eksplicit for IoT. Ville trække på leverandør eller partner, hvis der skete en hændelse.
- I gang med internt at opbygge procedurer for IoT-cybersikkerhed (fx for beredskab, risikovurdering, rapportering samt IoT-cybersikkerhed i løsningens livscyklus).

Struktur

- Ansvaret for IoT-cybersikkerhed er forankret internt suppleret med eksterne rådgivere. Klar organisering af roller, og hvordan de arbejder sammen, inkl. forretning, drift og strategi.
- Har adgang til de nødvendige IoT-cybersikkerhedskompetencer, både internt og eksternt.
- Ledelsen er med til at vurdere risici og konsekvenser på et informeret grundlag, så de kan bevillige ressourcer eller acceptere risikoen. Hovedopgaven med IoT-cybersikkerhed er at udvikle forretningen.
- Intern kommunikation er tværfaglig med fokus på videndeling, politikker, guidelines mv. Klar kommunikation fra ledelsen om betydningen af IoT-cybersikkerhed.
- Har beredskabsplaner for de kritiske IoT-systemer.
- Struktureret proces for IoT-cybersikkerhed og risikovurdering fra ide til implementering, inkl. økonomiske konsekvenser, bl.a. for produktets pris. Kortlægger som en del af risikovurderingen alle produkter, evt. i samarbejde med leverandørerne.

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

REFERENCEARK: TEKNISK 1/2

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

Opmærksomhed

- Fokus er på at forstærke og udbygge den fælles opmærksomhed på IoT-cybersikkerhed. Det grundlæggende risikobillede er, at IoT-løsningens funktioner og data ikke som sådan er kritiske.
- Det primære fokus er, at der er sikkerhed omkring dét, der er allermest kritisk for lige præcis dette produkt, hvilket ofte er driftssikkerhed.
- Den generelle sikkerhedstiltag er ikke nået til IoT endnu, og der er ikke en fælles tilgang til IoT-cybersikkerhed i virksomheden.
- De IoT-komponenter, der indgår i løsningerne, er måske købt hos en specialiseret leverandør, som man har tiltro til, har styr på sikkerheden.
- Den fysiske dimension af IoT-løsningen er ofte ikke sikret eller vurderes ikke som værende relevant.
- Kan sende opdateringer ud til løsningen, men det sker meget håndholdt, og i nogle tilfælde sker det slet ikke, eller virksomheden er afhængig af, at underleverandøren sørger for det.

Praksis

- Virksomheden arbejder sig væk fra ad hoc-tilgangen til IoT-cybersikkerhed og har en målsætning om at skabe et ensartet, risikobaseret IoT-cybersikkerhedsniveau og en fælles forståelse af sikkerhedspraksis på tværs af virksomheden.
- Sikkerheden er enten blevet bygget ind i IoT-løsningen fra starten eller bliver opgraderet løbende, efterhånden som der opnås større indsigt.
- De nødvendige IoT- sikkerhedskompetencer er til stede internt, men der benyttes eksterne kompetencer, hvor der vurderes at være behov for det.
- Den fysiske dimension af IoT-løsningen vurderes særskilt: Er der adgang til data fysisk? Hvad er risikoen ved en sådan adgang? Hvordan kan risici mitigeres?
- Der arbejdes hen imod at skabe både tekniske rammer og procedurer for at sende opdateringer ud løbende. Der arbejdes på at lave et struktureret overblik over, hvilke kendte sårbarheder, der findes, hvordan de kan patches, og hvilke enheder der er opdateret af virksomheden selv eller leverandøren.

Struktur

- Der arbejdes ud fra en helhedsorienteret tilgang, hvor sikkerheden tænkes igennem for alle brugsscenarier og kontekster for løsningen.
- Ledere og medarbejdere arbejder med IoT-cybersikkerhed ud fra fælles og strukturerede tekniske processer, og der er dedikerede ressourcer til det.
- Til- og fravalg i opbygningen af sikkerheden baseres på en struktureret og kontinuerlig risikovurdering omkring hele produktets værdikæde og levetid.
- Der er lagt flere lag af sikkerhed ind i løsningen, så der både er et ydre forsvar og et lag af sikkerhed i dybden, som skal begrænse skadesomfanget ved et evt. brud.
- Det står klart for virksomheden, at hvis man ikke har kontrol over fysisk adgang til løsningen, så har man ikke styr på sikkerheden.
- Det meste er bygget, så det kan opdateres, og der sendes løbende opdateringer ud. Der er mål for, hvor lang tid der må gå, fra en sårbarhed opdages, til løsningen bliver patchet.

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

"CyPro", støttet af Industriens Fond.

INDUSTRIENS FOND

UGLA INSIGHTS
FORCE TECHNOLOGY
DAMRC
ALEXANDRA INSTITUTTET
DEPARTMENT OF BUSINESS DEVELOPMENT AARHUS UNIVERSITY BSS

REFERENCEARK: TEKNISK 2/2

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

Opmærksomhed

- Nogle virksomheder har ingen logning, nogle ser det som en opgave, der ligger hos leverandøren, og andre igen har logs, som de kun bruger sporadisk.
- Der er primært fokus på at sikre brugeradgangen til platformen og ikke så meget til selve enheden.
- Kryptering bruges ad hoc, ud fra hvad allerede valgte platforme understøtter, eller udviklerne er bekendte med. Fx krypteres kommunikation med HTTPS(TLS) uden overvejelse om understøttede cipher-modes og nøglehåndtering.

Praksis

- Der er sat systemer op, som overvåger mønstre i systemet og udløser en alarm ved afvigelser.
- Overvågningen er især sat op med driftsstabilitet for øje, fx fejllogs.
- Der er sikkerhed omkring den måde, brugeren opretter sig i systemet, og der er sporbarhed ift., hvad brugere gør i systemet, og hvad de må gøre.
- Udviklerne kender best practice og anvender kun 'sikre' algoritmer. Komponenter/platforme fravælges, hvis ikke et tilstrækkeligt niveau af algoritmer understøttes.

Struktur

- Systemet overvåges konstant og systematisk, og der arbejdes ud fra faste responstider.
- Indbygget styring af adgang til løsningen – også fysisk. Fx skal brugere autentificere sig selv via to eller tre faktorer.
- Valg af kryptografiske algoritmer er registreret og gennemgås periodisk med henblik på at identificere evt. nye sårbarheder. Komponenter vælges således, at kryptografiske algoritmer kan udskiftes efter behov.

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

UGLA INSIGHTS
FORCE TECHNOLOGY
DAMRC
ALEXANDRA INSTITUTTET
DEPARTMENT OF BUSINESS DEVELOPMENT AARHUS UNIVERSITY BSS