SITUATIONSANALYSE AF BYGGESTEN TIL CYBERSIKKERHED

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

Byggesten: Sammenhæng mellem forretning og sikkerhed

Hovedspørgsmål 1:

Hvordan arbejder virksomheden med sammenhængen mellem forretningen og cybersikkerhed?

Svar:

Hjælpespørgsmål

Er det forretningsmæssige mål med brugen af IoT-løsninger klart?

Har virksomheden planer om videreudvikling af IoT-løsningerne?

Afklaring af hvor kritisk cybersikkerhed er for forretningen. Hvad må ikke ske, fordi det kan skade forretningen? Hvis virksomhedens...

- data bliver offentlige.
- data i systemer/maskiner er utilgængelig for virksomheden.
- data bliver ændret

Hovedspørgsmål 2:

Hvorfor arbejder virksomheden på den måde med sammenhængen mellem forretningen og cybersikkerhed?

Svar:

Hjælpespørgsmål

Er der risiko for et cyberangreb?

Er der konsekvenser for forretningen af et IoT-sikkerhedsbrud? Fx image hos kunder og samarbejdspartnere, forsinkelser.

Tillægger virksomheden cybersikkerhed forretningsmæssig værdi?

Er der et pres/krav udefra for at have mere cybersikkerhed? Fx fra kunder, leverandører eller lovgivning.

Hovedspørgsmål 3:

Hvordan vil virksomheden arbejde videre med sammenhængen mellem forretningen og cybersikkerhed?

Svar:

Hjælpespørgsmål

Kan virksomheden tjene flere penge med en cybersikker IoT-løsning? Kan det fx give adgang til andre kunder.

Bliver det i højere grad et problem fremover, hvis virksomhedens data bliver offentlige, I ikke kan få adgang til data og systemer, eller udefrakommende ændrer data?

Er cybersikkerhed forretning eller forsikring for virksomheden?

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

SITUATIONSANALYSE AF BYGGESTEN TIL CYBERSIKKERHED

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

Byggesten: Tilgang til sikkerhed og risiko

Hovedspørgsmål 1:

Hvordan arbejder virksomheden med sit mindset for risiko og tilgang til cybersikkerhed?

Svar:

Hjælpespørgsmål

Er der sat mål for cybersikkerhed/indsatser vedrørende cybersikkerhed i virksomhedens IoT-løsninger?

Laver virksomheden en struktureret risiko-vurdering?

Modellerer virksomheden trusler på en struktur-eret måde?

Hovedspørgsmål 2:

Hvorfor arbejder virksomheden på den måde med sit mindset for risiko og sin tilgang til cybersikkerhed?

Svar:

Hjælpespørgsmål

Er virksomheden et mål for et cyberangreb?

Har virksomheden aktivt taget stilling til trusler og risiko for indbrud i systemet og data?

Er virksomhedens arbejde med cybersikkerhed baseret på konkrete risici og trusler?

Hovedspørgsmål 3:

Hvordan vil virksomheden arbejde videre med sit mindset for risiko og sin tilgang til cybersikkerhed?

Svar:

Hjælpespørgsmål

Kan det være en fordel for virksomheden at have en fælles risikoopfattelse for indbrud i systemer og data blandt ledere og medarbejdere?

Bliver det et problem, hvis virksomheden ikke har fælles viden og holdninger til risiko og cyber-sikkerhed?

Er der brug for strukturerede procedurer for risiko-vurdering og modellering af trusler?

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 AND TECHNOLOGY AARHUS UNIVERSITY

SITUATIONSANALYSE AF BYGGESTEN TIL CYBERSIKKERHED

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

Byggesten: Lovgivning og standarder

Hovedspørgsmål 1:

Hvordan arbejder virksomheden med lovgivning og standarder for cybersikkerhed?

Svar:

Hjælpespørgsmål

Bruger virksomheden standarder for cybersik-kerhed? (eller vejledninger)

Er der lovgivning om cybersikkerhed, som virksomheden skal være opmærksom på?

Er virksomheden klar over lovkrav, der er på vej?

Er cybersikkerhed en del af virksomhedens løbende kvalitetssikring?

Hovedspørgsmål 2:

Hvorfor arbejder virksomheden på den måde med lovgivning og standarder for cybersikkerhed?

Svar:

Hjælpespørgsmål

Har virksomheden aktivt taget stilling til lovgivning (eksisterende og ny lovgivning på vej)?

Har virksomheden aktivt forholdt sig til standarder for cybersikkerhed?

Har virksomheden allokeret ressourcer til at arbejde med vejledninger og standarder for cybersikkerhed i virksomhedens løsninger, produkter og services?

Tillægger virksomheden standarder for cybersikkerhed værdi i forretningen?

Hovedspørgsmål 3:

Hvordan vil virksomheden arbejde videre med lovgivning og standarder for cybersikkerhed?

Svar:

Hjælpespørgsmål

Hvad vil være en relevant måde at bruge standarder og lovgivning på i virksomheden?

Bliver det er problem, hvis virksomheden ikke anvender standarder for cybersikkerhed? Fx for kunder og leverandørere

Er det et problem, hvis virksomheder ikke lever op til lovkrav og standarder?

Har virksomheden en god størrelse til at arbejde med standarder og/eller vejledninger for cybersikkerhed?

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 AND TECHNOLOGY
AARHUS UNIVERSITY
BSS

SITUATIONSANALYSE AF BYGGESTEN TIL CYBERSIKKERHED

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

Byggesten: Processer og forankring i organisationen

Hovedspørgsmål 1:

Hvordan arbejder virksomheden med organisering af arbejdet med cyber-sikkerhed?

Svar:

Hjælpespørgsmål

Er ansvaret for cybersikkerhed placeret hos en eller flere personer i virksomheden?

Er ansvaret for cybersikkerhed placeret hos en ekstern leverandør?
- Følger virksomheden med i, hvordan den eksterne partner håndterer virksomhedens cybersikkerhed?

Har virksomheden lavet en struktureret plan, der indeholder både mål og konkrete tiltag med henblik på cybersikkerhed i virksomheden?

Håndteres IT-sikkerhed (fx i forbindelse med kontor IT) sammen med cybersikkerhed, eller ser virksomheden det som to forskellige ting?

Hovedspørgsmål 2:

Hvorfor arbejder virksomheden på den måde med organisering af arbejdet med cybersikkerhed?

Svar:

Hjælpespørgsmål

Er det afklaret i virksomheden, om der er behov for, at en eller flere faste personer har ansvaret for cybersikkerhed?

Er der i virksomheden afsat tid og ressourcer til at opbygge interne kompetencer om cyber-sikkerhed?

Afspejler organiseringen af cybersikkerhed den betydning som sikkerheden har for forretningen?

Hvordan/hvornår taler I i virksomheden om cybersikkerhed?

Hovedspørgsmål 3:

Hvordan vil virksomheden arbejde videre med organisering af arbejdet med cybersikkerhed?

Svar:

Hjælpespørgsmål

Arbejdes der vedholdende på virksomhedens cybersikkerhed for IoT-løsninger?

Skal cybersikkerhed kobles sammen med den øvrige kvalitetssikring i virksomheden?

Er der brug for at inddrage medarbejderne i tiltag for cybersikkerhed i virksomheden?

Er det relevant med en plan for intern kompetence-udvikling i cybersikkerhed?

Er det vigtigt at være i dialog med den eventuelle eksterne leverandør om virksomhedens krav til cybersikkerhed?

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 AND TECHNOLOGY AARHUS UNIVERSITY