



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

SITUATIONSANALYSE AF BYGGESTEN TIL CYBERSIKKERHED

Byggesten: Forretningsudvikling

Hovedspørgsmål 1:

Hvordan arbejder virksomheden med sammenhøngen mellem forretningen og cybersikkerhed?

Svar:



Hjælpe spørgsmål

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

Har virksomheden planer om videreudvikling af IoT-løsningerne?

Afdeling 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 sammenhøngen mellem forretningen og cybersikkerhed?

Svar:



Hjælpe spørgsmål

Er der risiko for et cyberangreb?

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

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 sammenhøngen mellem forretningen og cybersikkerhed?

Svar:



Hjælpe spørgsmål

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?





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

SITUATIONSANALYSE AF BYGGESTEN TIL CYBERSIKKERHED

Byggesten: Teknisk

Hovedspørgsmål 1:

Hvordan arbejder virksomheden med tekniske opgaver inden for IoT-cybersikkerhed?

Svar:



Hjælpe spørgsmål

Hvad er jeres prioriteter i forhold til teknisk IoT-sikkerhed? Hvad er inden for og uden for scope?

Hvordan balancerer I produktperformance og produktion i forhold til IoT-cybersikkerhed vs indtjening?

Udfører virksomheden metodiske risikovurderinger og/eller trusselsmodellering af teknisk IoT-cybersikkerhed?

Udfører virksomheden 1) patch management, 2) logning og overvågning af trafik, og 3) indsatsretter mod brugeradfærd?

Hovedspørgsmål 2:

Hvorfor arbejder virksomheden med de tekniske opgaver inden for IoT-cybersikkerhed på denne måde?

Svar:



Hjælpe spørgsmål

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?

Overvåger/observerer virksomheden resultaterne af sin IoT-cybersikkerhed?

Hovedspørgsmål 3:

Hvordan vil virksomheden arbejde videre med sin tekniske tilgang til IoT-cybersikkerhed?

Svar:



Hjælpe spørgsmål

Hvordan kunne virksomheden arbejde systematisk med at opbygge IoT-cybersikkerhed i overensstemmelse med forretnings behov og revidere IoT-cybersikkerheden med bestemte intervaller?

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

Er der brug for strukturerede procedurer for risikovurdering og modellering af trusler?

Har kunder og partnere fokus på IoT-cybersikkerhed?





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: Kvalitet

Hovedspørgsmål 1:

Hvordan arbejder virksomheden med lovgivning og standarder for cybersikkerhed?

Svar:



Hjælpe spørgsmål

Er IoT-cybersikkerhed en del af virksomhedens løbende kvalitetsstyring?

Bruger virksomheden standarder for cybersikkerhed? (eller vejledninger)

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

Er virksomheden klar over lovkraft, der er på vej?

Hovedspørgsmål 2:

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

Svar:



Hjælpe spørgsmål

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:



Hjælpe spørgsmål

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

Bliver det et problem, hvis virksomheden ikke anvender standarder for cybersikkerhed? Fx for kunder og leverandører

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

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

SITUATIONSANALYSE AF BYGGESEN TIL CYBERSIKKERHED

Byggesten: Organisation

Hovedspørgsmål 1:

Hvordan arbejder virksomheden med organisering af arbejdet med cybersikkerhed?

Svar:



Hjælpe spørgsmål

Er ansvar for cybersikkerhed placeret hos en eller flere personer i virksomheden/til en ekstern partner?

Har virksomheden adgang til relevante IoT-cyber sikkerhedskompetencer?

Har virksomheden lavet en struktureret plan, der indeholder både midl og konkrete tiltag med henblik på cybersikkerhed i virksomheden? Dette kan også inkludere overvågning af, hvordan den eventuelle eksterne partner håndterer IoT-cyber sikkerhed.

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:



Hjælpe spørgsmål

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

Er der i virksomheden afsat tid og ressourcer til at opbygge interne kompetencer om cybersikkerhed?

Atspejler 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:



Hjælpe spørgsmål

Arbejdes der vedholdende på virksomhedens cybersikkerhed for IoT-løsninger?

Skal cybersikkerhed kobles sammen med den øvrige kvalitets sikring i virksomheden?

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

Er det relevant med en plan for intern kompetenceudvikling i cybersikkerhed?

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

