0. Samlet overblik over cybersecurity supply chain risk management værktøjer

www.cyber-smv.dk

Cybersecurity supply chain risk management

- Cybersecurity Supply Chain Risk Management (C-SCRM) handler om at **identificere, vurdere** og **håndtere** de cyberrelaterede risici, der opstår gennem en virksomheds kunder, leverandører, og øvrige samhandelspartnere.
- Det er en disciplin i krydsfeltet mellem cybersecurity og supply chain management, fordi virksomheder i stigende grad er afhængige af komplekse, globale og digitale forsyningskæder.

Formål, deltagere og anvendelse

- **Formål**
  - At skabe et AS-IS billede over opfattelser af konkret praksis indenfor 10 områder af cybersecurity supply chain risk management.
  - At tage stilling til et fremtidigt ønsket niveau for virksomheden (TO-BE).
  - At prioritere indsatsområder og udvikle handleplaner.
- **Deltagere**
  - Ledelse og nøglemedarbejdere.
- **Anvendelse**
  - Bør vurderes løbende – periodiske intervaller f.eks. hvert kvartal.

Fremgangsmåde

- Der knytter sig et værktøj til hver af de 10 konkrete praksisser med cybersecurity supply chain risk management (se slide 5).
- Er det første gang, der arbejdes med værktøjet, udvælges de værktøjer, man ønsker at sætte fokus på.
- På baggrund af (nødvendige) værktøjer, der er anvendt, vurderes det for hvert værktøj, hvor virksomheden ligger i dag (AS-IS) på en skala fra 1 (i meget lav grad) 5 (i meget høj grad). Skriv IB (ikke brugt), hvis et værktøj ikke anvendes. Vurderinger markeres i tabellen.
- Herefter plottes virksomhedens ønskede niveau ind for hvert værktøj (TO-BE).
- Derefter identificeres, og prioriteres, de tiltag der er nødvendige for at komme fra AS-IS til TO-BE.
- Til slut udvikles en handleplan (se slide 7) for hvert indsatsområde.

#	Praksis	1	2	3	4	5	TO-BE	Gab
1	En strategi for risikostyring af cybersikkerhed i forsyningskæderne er etableret og accepteret af virksomhedens interessenter.							
2	Cybersikkerhedsroller og ansvarsområder for leverandører, kunder og samarbejdspartnere fastlægges, kommunikeres og koordineres internt og eksternt.							
3	Risikostyring af cybersikkerhed i forsyningskæderne er integreret i virksomhedens generelle risikostyring og forbedringsprocesser.							
4	Leverandører er kendte og prioriteret efter, hvor kritiske de er.							
5	Krav til håndtering af cybersikkerhedsrisici i forsyningskæder fastlægges, prioriteres og integreres i kontrakter og andre typer aftaler med leverandører og andre relevante tredjeparter.							
6	Planlægning og due diligence (detaljerede undersøgelser) gennemføres for at reducere risici, inden der indgås formelle leverandør- eller andre tredjepartsrelationer.							
7	Risici forbundet med en leverandør, dens produkter og tjenester samt andre tredjeparter identificeres, registreres, prioriteres, vurderes, besvares og overvåges i løbet af relationen.							
8	I tilfælde af hændelser (incidents) inddrages relevante leverandører og andre tredjeparter i planlægning, i modsvar og i aktiviteter med at genoprette praksis.							
9	Sikkerhedspraksis i forsyningskæderne er integreret i vores generelle risikostyring og produkters og serviceydelsers performance overvåges gennem hele deres livscyklus.							
10	Planer for styring af cybersikkerhedsrisici i forsyningskæderne inkluderer bestemmelser for aktiviteter, der finder sted efter ophør af et partnerskab eller en serviceaftale.							

IB = ikke brugt; 1 = i meget lav grad, 2 = i lav grad, 3 = i nogen grad, 4 = i høj grad, 5 = i meget høj grad

Handleplaner: Overordnet

Nr.	Indsatsområde	Beskrivelse	Målsætning	Prioritet	Ansvarlig	Deadline

Handleplan indsatsområde

Indsats	Navn på indsatsområde
Formål	
Målsætning	
Aktiviteter	
Ansvarlig	
Investering	
Risici	
Deadline	
Rapportering/ opfølgning	