9. Integrering af supply chain cybersikkerhed gennem hele produktlivscyklussen

www.cyber-smv.dk

Formål, deltagere og anvendelse

- **Formål**
  - At sikre at produkter og serviceydelser sikres mod cyberangreb gennem hele deres livscyklus.
- **Deltagere**
  - Ledelse, IT, indkøb og andre relevante funktioner.
- **Anvendelse**
  - Løbende overvågning.

Livscyklus og cybersikkerhedspraksisser

Livscyklusfase	Fokus	Cybersikkerhedspraksisser iværksat	Dato	Ansvar	Status
Udvikling					
Introduktion					
Vækst					
Modning					
Nedgang					

Eksempler på indholdselementer

Enkelte praksisser kan ligge i forskellige faser

Livscyklusfase	Fokus	Cybersikkerhedspraksisser iværksat
Udvikling	Security by Design – sikre arkitektur fra starten.	- Trusselsmodellering - Sikker kodestandard - Penetrationstest af prototyper - Sikker udviklingspipeline
Introduktion	”Hærdning” og compliance – undgå sikkerhedsfejl ved lancering.	- "Hærdning" af systemer og netværk - Patch managementstrategi - Overholdelse af relevante standarder (ISO 27001, NIST, NIS2, GDPR) - Incident responsplan
Vækst	Skalerbar sikkerhed – beskytte voksende infrastruktur og data.	- Kontinuerlig overvågning og hændelses håndtering - Automatiseret trusselsdetektion - Adgangskontrol og identitets- og adgangsstyring - Databeskyttelse (kryptering, forebyggelse af datatab)
Modning	Optimering og complianceforbedring – holde sikkerhedsniveauet højt.	- Regelmæssige audit og sikkerhedsrevisioner - Opdaterede penetrationstests - Supply chain sikkerhed - Brugernes sikkerhedsuddannelse
Nedgang	Sikker udfasning – beskytte data og undgå efterladte sårbarheder.	- Sikker datasletning - Afvikling af systemer og servere - Fjernelse af adgangsrettigheder - Kommunikation om end-of-life-risici