Hvordan bruger man mest fornuftigt de første 100.000 kr. på informationssikkerhed?

V/Jacob Barlach - CTO

GapSolutions
WE FIX IT

Min baggrund

- Intern ansvarlig for informationssikkerhed
  - ISO 27001 certificeret
  - ISAE 3000 auditeret
- Ansvarsområder og seneste projekter som ekstern konsulent:
  - ISO 27001: Klargøring til certificeret, internt auditør,lead implementor og generel rådgivning
  - NIST: Auditering efter 800-53, lead implementor
  - CIS18: Rådgivning og auditering
  - NIS2: Rådgivning og implementering af 'ISMS-light'
- Baggrund
  - Udvikler
  - Microsoft konsulent

Jacob Barlach – CTO
GapSolutions A/S

Præmis

- Når I starter op på informationssikkerhed, skal I ofte bruge penge på:
  - Interne ressourcer (f.eks. arbejdstid, licenser og hjælp fra andre afdelinger)
  - Eksterne konsulenter (rådgivning og udførende)
  - Værktøj (f.eks. software, hardware og OT)
- 100.000 kr. er vejledende
  - Små virksomheder kan nogle gange komme i mål
  - Store virksomheder kommer ikke igennem præsentationens indhold
- Dette er en generel tilgang, så der kan være undtagelser
  - Foranstaltningsbaseret compliance (NIST 800-53, ISO 27002, CIS18)

Fundament

Informationssikkerhed består af nogle grundlæggende komponenter.

Deres formål er at skabe de bedste forudsætninger for sikkerhed over reel sikkerhed.

Starter I med foranstaltninger er budgettet måske brugt, før I ved hvor den største risiko er.

Fundamentet består af:

- Kortlægning
  - Hvilke elementer er vigtige?
- Risikostyring
  - Hvilke elementer er truet?
- Compliance
  - Efterlever vi krav og/eller best-practise?

GapSolutions

Kortlægning - Hvilke elementer er vigtige?

Vi har brug for at vide:

- Processer – hvad er kerne, og hvad er støtteaktiviteter?
- Aktiver – hvilke aktiver er nødvendige for at vores processer fungerer?
- Samarbejdspartnere – hvem har vi brug for hjælp fra, før vores processer fungerer?
- Sikkerhedsforanstaltninger– Hvordan sikres elementerne, og er foranstaltningerne effektive?

Ovenstående kan man arbejde med til bevidstløshed, så derfor er det nødvendigt med et princip for, hvordan opgaven tackles bedst muligt.

Proportionalitetsprincippet

Mange informationssikkerhedsstandarder bygger på et princip om, at ressourcerne skal stå mål med de udfordringer, organisationen står overfor.

Det er en indbygget del af, hvordan der auditeres efter blandt andet ISO og ISAE standarder, men er også beskrevet i forskellig lovgivning for sikkerhed, som f.eks. GDPR og NIS2.

Hvad betyder det så i praksis?

GapSolutions

Anvendelse af klassifikation

Klassifikation har nogle iboende egenskaber, der gør den til et godt styreredskab for proportionalitetsprincippet:

- Prioritet
  - Højeste klassifikation = højeste prioritet
- Detaljeringsgrad
  - Højeste klassifikation = højeste detaljeringsgrad
- Regel-inkluderende
  - Der kan laves regler på baggrund af klassifikationen, som f.eks. alle 'kritiske' aktiver skal efter X niveau af sikkerhed

Klassifikationsskalaer

Når det kommer til klassifikationsskalaer, er der generelt to valg:

1. Hvor mange punkter skal vi bruge?
   - Tre eller fire er de mest almindelige valg– jeg foretrækker fire da det giver en ‘mere’ og ‘mindre’ vigtig for kerne- og støtteprocesser
2. Hvad kalder vi skalaen?
   - Eksempler: A, B, C og D. Kritisk, Vigtig, Betydelig og Øvrig.

Risikostyring

Påstand: Formålet med risikostyring er at reducere risiko mest muligt med de ressourcer, der er tilgængelige. Ikke at alle risikovurderinger skal være 'grønne'.

For at komme i mål med dette skal vi bryde risikostyring ned i primære elementer:

- Trusselsidentifikation
- Risikovurderingsmetoder
- Risikobehandling

GapSolutions

Risikostyring

Risikostyring kan være overvældende. Særligt hvis man læser ISO 27005 eller lignende tilgange.
Så hvordan træffer vi nogle valg, der gør processen lettere?

Trusselsidentifikation

- Fra trusselskatalog til trusselskategorier

Risikovurderingsmetoder

- Hvor mange og hvilke?

Risikobehandling

- Hvilke foranstaltninger har den største positive effekt på risikobilledet?

Risikovurderingsmetoder

Alle vurderinger behøver ikke at være konsekvensanalyser, og det er ikke et krav, at der kun anvendes én type risikovurdering.

Kan der skabes sammenhæng mellem vurderingsmetoden og klassifikation, får man noget at vurderingen foræret.

Konsekvensskaler

- Impact Level
- Financial Loss
- Reputational Damage
- Regulatory Compliance
- Operational Disruption

Sandsynlighedsskalaer

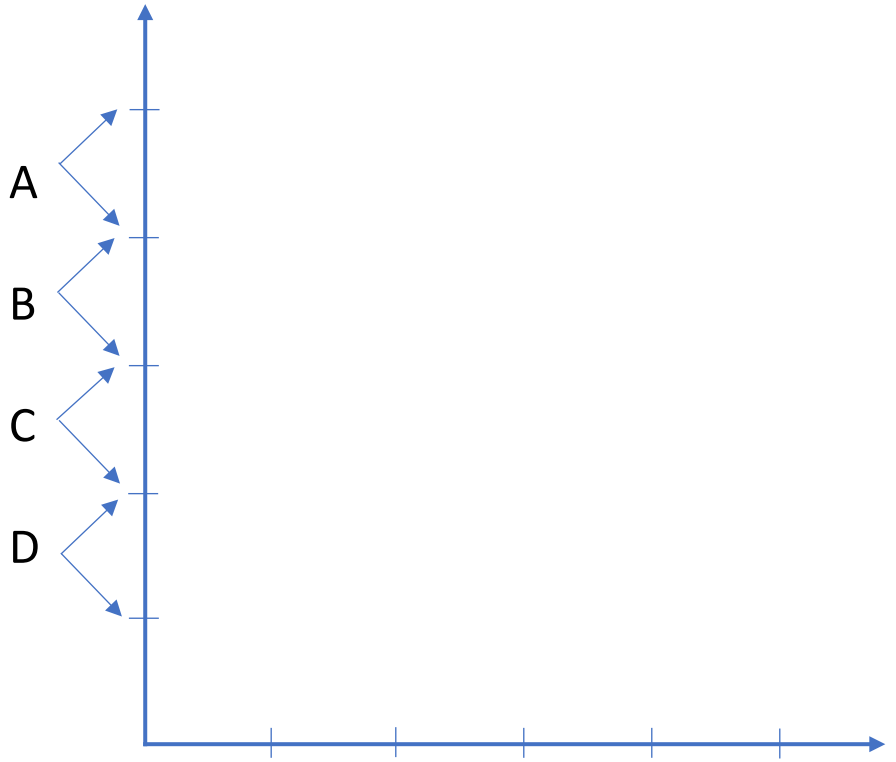
- Frequency
- Probability
- Threat Actor Capability
- Vulnerability Exposure
- Control Effectiveness

GapSolutions

Sammenhæng mellem skala og klassifikation

Generelt vælges der imellem følgende skalaer:

- 3 punkt (ternary scale)
- **4 punkt (forced choice scale)**
- **5 punkt (Likert scale)**
- **7 punkt (semantic differential scale)**
- 10 punkt (decile scale – mest teoretisk)



Opsummering

100.000 kr. er for de fleste virksomheder én måneds koncentreret arbejde, lidt ekstern support til at komme rigtigt i gang og et værktøj til at strukturere arbejdet.

Alle virksomheder (uanset størrelse og indenfor ressourceforbruget) burde kunne kortlægge de mest kritiske processer samt de aktiver, leverandører og sikkerhedsforanstaltninger, der er nødvendige for processernes virke, og identificere de mest relevante risici.

Herfra kan arbejdet modnes og udbygges, så det til sidst er dækkende for de krav, organisationen stilles overfor.

GapSolutions

Kontakt

Ønsker du at vide mere om, hvordan vi kan hjælpe jer med mest fornuftigt at bruge de første 100.000 kroner på informationssikkerhed?

Så tøv ikke med at tage kontakt til vores Sales Manager - Christian Højer.

Christian kan også tilbyde jer at lave en online fremvisning af vores digitale GRC-platform.

ch@gapsolutions.dk

Tlf. 7174 8583

www.gapsolutions.dk

GapSolutions A/S
Uraniavej 6
8700 Horsens
www.gapsolutions.dk