GapSolutions

Projektmodel informationssikkerhed

Projektmodel

1

Hvad er GapSolutions' projektmodel?

Projektmodellen er et værktøj, der anvendes af GapSolutions' informationssikkerhedsafdeling og giver et klart sæt mål for hver projektfase for at sikre en smidig proces hele vejen igennem. Projektmodellen består af 3 faser:

1. Kortlægning
2. Risikostyring
3. Revision

Kortlægning

Fase 1 - Kortlægning: Forståelse og dokumentation af din organisation

Den første fase af vores proces fokuserer på at opnå en dyb forståelse af din organisation. Gennem interviews, inspektioner og de materialer, du stiller til rådighed, skaber vi et holistisk billede af din virksomheds struktur og drift. Det sikrer, at alt er fuldt dokumenteret og tilgængeligt via vores sikre portal, så hele projektet er gennemsigtigt og sporbart.

Nøgleaktiviteter i fase 1:

1) Trusselprofilering: Vi arbejder tæt sammen med dig om at skabe en skræddersyet trusselsprofil, der tager højde for faktorer som:

- **Offentlig eksponering:** Er du en højt profileret organisation, der kan tiltrække forskellige cybertrusler?
- **Økonomisk status:** Organisationer med stærk økonomisk opbakning kan være mere attraktive for kriminelle aktører.
- **Risiko for aktivisme:** Beskæftiger din organisation sig med følsomme emner som menneskerettigheder eller miljøproblemer?
- **Politisk eksponering:** Hvis du er involveret i politiske anliggender, kan du blive udsat for mere avancerede trusler.
- **Påvirkning af infrastruktur:** Spiller din organisation en vigtig rolle i den lokale, regionale eller nationale infrastruktur?
- **Angrebsflade:** Vi evaluerer dine potentielle sårbarheder, herunder netværk, enheder, servere og meget mere.

2) Kortlægning af nøgleområder: Vi indsamler vigtige oplysninger fra interviews og materialer for at forstå din organisation:

- **Processer:** Dokumentation af jeres kerneforretning og støtteprocesser.
- **Aktiver:** Identificering af værdifulde aktiver som hardware, software, intellektuel ejendom og omdømme.
- **Leverandører:** Forstå dine kritiske tredjepartsrelationer, og hvordan de er knyttet til din virksomhed.
- **Sikkerhedsforanstaltninger:** Gennemgang af dine nuværende sikkerhedspolitikker, -procedurer og -teknologier.

3) Dokumentation af portalen: Alle indsamlede data indtastes i vores sikre portal, hvilket sikrer, at alle relevante oplysninger er tilgængelige for fremtidige trin og detaljeret dokumentation.

Risikostyring

Fase 2- Risikostyring: Beskyttelse af din organisation

Vores risikostyringsmodel følger bedste praksis fra ISO 27005:2022 og NIST RMF (800-30-serien). Processen er opdelt i nøglefaser for at sikre en grundig og effektiv evaluering af din organisations risici og hjælpe dig med at prioritere, hvad der betyder mest.

Nøgleaktiviteter i risikostyringsfasen:

1) Etablering af en risikomodel: Vi begynder med en samarbejdsworkshop for at afpasse vores tilgang til jeres specifikke risikostyringspræferencer. I løbet af denne session vil vi definere:

- **Metode til risikovurdering:** Om du foretrækker en kvalitativ, kvantitativ eller hybrid tilgang.
- **Risikoskala:** Beslutte, hvordan risici skal vurderes, f.eks. ved hjælp af en skala fra 1-5 (fra lav til høj), finansielle målinger eller et andet system.
- **Risikoappetit:** Vi diskuterer, hvor stor en risiko din ledelse er villig til at acceptere.
- **Katalog over risici/trusler:** Vi udfærdiger en liste over de største trusler mod din virksomhed.

Alt dette konsolideres i en omfattende risikostyringspolitik, skræddersyet til dine behov.

2) Risikoevaluering: Når risikomodellen er etableret, vurderer vi dine it-aktiver og øvrige systemer - startende med de kritiske, der blev identificeret i fase 1 (kortlægning). Vi evaluerer hvert aktiv baseret på:

- **Sandsynlighed og konsekvens:** For hver identificeret trussel estimerer vi sandsynligheden for at den opstår, og hvad den potentielle skade er.
- **Kategorisering af aktiver:** Vi klassificerer dine aktiver med et system til at identificere de mest kritiske systemer og de mindst vigtige for så vidt angår opretholdelse af forretningsdriften.

Derefter arbejder vi med de identificerede aktiver, kortlægger eksisterende trusler og udarbejder detaljerede risikovurderinger i GapPortalen. Når alle aktiver er evalueret, bygger vi en komplet, holistisk risikobaseret kortlægning af din organisation.

Risikostyring

4

Risikominimering og overdragelse: Når vi har evalueret risiciene, identificerer vi afhjælpningsstrategier for at reducere dem. Hver afhjælpning er knyttet til et **restrisikoniveau**, der udtrykker den risiko, der er tilbage, efter at disse foranstaltninger er anvendt.

Vi gennemgår dette sammen med dig i en afsluttende workshop, hvor vi:

- Diskuterer resultaterne, særligt eventuelle **højkritiske** risici.
- Sikrer, at jeres ledelse er klar til at påtage sig ansvaret for håndteringen af disse risici.
- Planlægger eventuelle yderligere tiltag, før vi går videre til næste fase af projektet.

Denne fase sikrer, at alle risici er grundigt vurderet, og at der er indført effektive afhjælpningsforanstaltninger, som sikrer din ledelse den nødvendige indsigt til at beskytte organisationen.

Revision

Fase 3 - Revisionsprojekt: Sikring af compliance og styrkelse af sikkerheden

Audit-fasen i projektmodellen er den tredje fase i vores projektplan for informationssikkerhed, og følger afslutningen af risikostyringsfasen. Denne fase fokuserer på intern revision af din organisations overholdelse af vigtig lovgivning, standarder og eksisterende politikker, og sikrer at dine sikkerhedsforanstaltninger er effektive og opfylder de nødvendige krav.

Aktiviteter i auditfasen:

1) Revisioner i GapPortalen: Ved hjælp af vores GapPortal sammenligner vi data indsamlet i fase 1 og 2 med centrale sikkerhedskrav fra rammer og direktiver som f.eks:

- **ISO 27001**
- **NIS2-direktivet**
- **CIS Critical Security Controls v8 (CIS18)**
- **CER**

Hver audit linker til specifik dokumentation og bevismateriale, f.eks:

- **Kontrolserier**
- **Filer**
- **Risikovurderinger**
- **Informationsaktiver**
- **Auditmål**

Dette sikrer fuld sporbarhed og dokumentation for overholdelse af hvert krav.

Revision

6

1) Træning af ledelsen: Vi tilbyder ledelsestræning, der opsummerer de vigtigste sikkerhedsresultater, risici og oplysninger om hændelseshåndtering, og hjælper ledelsen med at træffe informerede beslutninger. Dette inkluderer:

- **Risikoanalyse:** Fremhæver trusler og sårbarheder gennem risikovurderinger.
- **Overensstemmelsesrapportering:** Demonstration af overholdelse af lovkrav gennem specifikke audits.
- **Vejledning i katastrofegendannelse og hændelseshåndtering:** Træning af ledelsen i, hvordan organisationen bedst forbereder sig på et potentielt katastrofe- eller nødscenarie.

Dette sikrer gennemsigtighed, ansvarlighed og informeret beslutningstagning på alle niveauer i organisationen.

2) Politikker og procedurer: I denne fase gennemgår og sikrer vi, at din organisation har de nødvendige politikker og procedurer på plads for at efterleve både juridiske og standardbaserede krav. Disse politikker udgør grundlaget for din informationssikkerhedsramme og omfatter:

- **Politik for informationssikkerhed**
- **Politik for risikostyring**
- **Politik for genopretning efter katastrofer og håndtering af hændelser**

Disse dokumenter styrer din organisations sikkerhedstilgang og sikrer overholdelse af relevante standarder som **ISO 27001** og **NIS2**.

I samarbejde med jer sikrer vi, at GapPortalen er organiseret på en måde, der understøtter de eksisterende sikkerheds- og compliance-aktiviteter, og strømliner de tilbagevendende arbejdsopgaver ved hjælp af vores årshjulsværktøj. Årshjulet giver rapportering, dokumentation og notifikation om, hvilke opgaver der skal udføres, så dine medarbejdere bedst muligt kan medvirke til governance- og compliance-aktiviteter.

Kontakt os for at sikre, at din organisations sikkerhed er robust og overholder den seneste lovgivning. Vores løsninger til risikostyring, revision og hændelseshåndtering hjælper dig med at navigere i komplekse sikkerhedsstandarder, minimere risici og styrke din overordnede sikkerhedsposition. Lad vores informationssikkerhedseksperter guide din organisation til forbedret beskyttelse og compliance.

GapSolutions

Kontakt:
GapSolutions A/S
Uraniavej 6
8700 Horsens

Telefon: 8844 0808
Hjemmeside: www.gapsolutions.dk