Inzicht in informatiebeveiliging

Cybercrime; 12 slachtoffers per seconde, 720 per minuut, 43.200 per uur, 1.036.800 per dag. De wereld is in de ban van cybercrime. Cybercriminelen benutten de afhankelijkheid van data waarbij de mens een makkelijke digitale prooi is geworden.

Dit resulteert onder andere in nieuwe wet- en regelgeving. Zo gaat in mei 2018 de nieuwe privacy wetgeving 'General Data Protection (GDPR)' van kracht.

Informatiebeveiliging gaat niet alleen om technische beveiliging, beveiliging gaat verder dan alleen techniek. Zie GDPR in en breder plaatje: inzicht in informatiebeveiliging.

Maak nu een afspraak voor een gratis consult

Stap 1: Doel bepalen

- ✓ Doel: Waar moet alle moeite die je er in steekt aan bijdragen? (Wetgeving, commercieel doel?)
- ✓ Scope: Een afdeling, het hele bedrijf of een bedrijfsproces? Bepaal de gewenste scope en formuleer je hoofddoel ten aanzien van informatiebeveiliging.

Stap 2: Richtlijn bepalen

- ✓ Kies een norm, set van richtlijnen of een handreiking die je helpt bij het behalen van je doel.
- ✓ Er leiden meerdere wegen naar Rome: ISO 27001/27002, NEN7510, Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG), NIST 800-53.

Stap 3: Risicoanalyse

- ✓ Voer een risicoanalyse aan de hand van de gekozen norm of richtlijn.

Stap 4: Actieplan

- ✓ Vertaal risico's naar te nemen organisatorische, procesmatige en/of technische te nemen stappen.

Stap 5: Communiceren

- ✓ Breng je medewerkers op de hoogte van de genomen maatregelen.
- ✓ Creëer awareness!
- ✓ Zwakste schakel is de mens, totdat je hem informeert.