

VERBETERPLAN INFORMATIE BEVEILIGING

Het verbeterplan informatiebeveiliging (VIB) is een dienst uit het LBVD-dienstmodel '**Komen tot**', en heeft tot doel om te komen tot een situatie waarin een organisatie beschikt over een complete opzet voor een informatiebeveiligingsproces. Deze opzet omvat een aantal componenten, waaronder:

- Een eerste informatiebeveiligingsbeleid;
- Inzicht in de materie voor betrokkenen;
- Inzicht in de huidige situatie;
- Projectplan om de gewenste situatie te bereiken.

PLAN VAN AANPAK

Iedere organisatie is uiteraard anders – dit komt natuurlijk ook tot uitdrukking in de resultaten. Hoewel de vorm van een VIB standaard is, is de feitelijke uitvoering in hoge mate onafhankelijk van het soort organisatie. En dat is wat uw organisatie voordeel oplevert.

Een VIB bestaat uit de volgende onderdelen (waarbij sommige delen naar believen kunnen worden overgeslagen, bijvoorbeeld omdat deelgegevens van een assessment al door de accountant zijn verzameld, of omdat delen van het norm interview reeds in het kwaliteits management zijn opgenomen):

- Intake;
- Assessment;
- Gap-analyse;
- Opzetten eerste strategisch (vervolg) beleid;
- Opstellen projectplan 'komen tot'.

(diverse onderdelen van VIB kunnen desgewenst ook los worden geleverd).

1. **Intake.** Hier wordt de scope van het project bepaald, en een referentiekader aangenomen (Code voor Informatiebeveiliging, I7799 etc);
2. **Assessment.** In deze fase wordt aan de hand van een aantal vooraf te bepalen incidenten de kwetsbaarheid van de organisatie vastgesteld. Zonder er waarde aan te hechten wordt de huidige status bepaald aan de hand van gangbare referentiekaders en/of de eigen geldende regelgeving.
3. **Gap-analyse.** Dit deel van het Verbeterplan levert inzicht in drie deelgebieden:
 - (a) risico's die zijn afgedekt;
 - (b) risico's die niet, of onvoldoende zijn afgedekt;
 - (c) risicogebieden waar men tijdens het assessment onvoldoende inzicht in kreeg, en: witte vlekken.Deze laatste categorie behoeft wellicht nadere (risico)analyse.

4. **Opzetten eerste strategisch beleid.** Op basis van de in de voorgaande onderdelen gevonden 'grote gemene deler' is een set minimale maatregelen op te stellen. Deze maatregelen vormen de eerste opzet voor het nieuw op te stellen beleid.
5. **Opstellen projectplan 'komen tot'** Gedurende deze periode groeit het beveiligingsproces, en gaat het langzaam aan op eigen benen staan. Hierbij moet o.a. gedacht worden aan:
 - Het inrichten van het proces informatiebeveiliging zoals beschreven in het inmiddels vastgestelde beleid;
 - De invoering van maatregelen uit de set van 'minimale maatregelen', voorzover nog dit niet is gedaan;
 - Het uitvoeren van benodigde risicoanalyses t.b.v. de geïdentificeerde 'witte plekken' en het indien nodig invoeren van aanvullende maatregelen.

RESULTAATVERPLICHTING

Een Verbeterplan Informatie Beveiliging kent een vast aantal duidelijke resultaten:

1. Bewustwording omtrent de noodzaak en de werking van het onderwerp informatiebeveiliging bij een groot deel van de organisatie: variërend van MT tot eindgebruiker;
2. Inzicht in de huidige status van (informatie)beveiliging (IST-situatie);
3. Kennisopbouw aangaande normenkaders met betrekking tot de eigen organisatie;
4. Eerste opzet van een werkend informatiebeveiligingsbeleid. Werkend, omdat het vanuit de eigen organisatie is opgezet – vanuit begrip voor nut en noodzaak;
5. Een werkend informatiebeveiligingsplan. Helder, communicatief, en geaccepteerd door alle betrokkenen. Hierdoor is de effectiviteit van het plan al bij voorbaat hoog!
6. Bewustwording omtrent voortzetten van het proces bij beleidsmakers.

De Gartner Group zei het al in 1999: *"It's not about the destination – it's far more about the willingness to take the travel"*.

MEER WETEN?

NEEM CONTACT OP MET LBVD VOOR
DE TARIEFSTELLING EN BIJZONDERE
MOGELIJKHEDEN