

### AANLEIDING

De bedrijfsprocessen van organisaties, overheden, bedrijven en instellingen zijn sterk afhankelijk van het goed functioneren van de informatievoorziening. Uitval, vermindering of onbevoegde kennisname van gegevens kan grote gevolgen hebben. Een ongestoorde voortgang van de werkzaamheden, waarbij informatie tijdig, correct en volledig op de juiste plek komt, is niet alleen van essentieel belang bij het vervullen van taken en behalen van doelstellingen, maar ook voor het imago van de organisatie. Daarbij hoort ook de zekerheid dat alleen degenen die daartoe zijn geautoriseerd, toegang hebben tot vertrouwelijke informatie.

### PROBLEEMSTELLING

Informatiebeveiliging is een combinatie van weloverwogen organisatorische en technische maatregelen. Dit vereist inzicht in wat men wil bereiken met informatiebeveiliging. Hoe afhankelijk is men precies van de informatievoorziening? Welke risico's zijn aanwezig en moeten verminderd worden? Welke risico's zijn acceptabel? Deze vragen moeten beantwoord worden alvorens het proces informatiebeveiliging correct kan worden geïmplementeerd.

### DOELSTELLINGEN

De doelstellingen van het voorgestelde traject zijn achtereenvolgens:

1. Te komen tot inzicht in de afhankelijkheidsrelatie tussen de organisatie en haar informatievoorziening, gerelateerd aan de strategische doelstellingen van de organisatie;
2. Inzicht te krijgen in de risico's ten aanzien van de informatievoorziening die het behalen van deze doelen en doelstellingen in de weg kunnen staan;
3. Het formuleren van beveiligingsdoelstellingen, gerelateerd aan de eerder geïdentificeerde dreigingen;
4. Op globaal niveau identificeren en beschrijven van de organisatie en beveiligingsmaatregelen welke nodig zijn om de gewenste doelstellingen te behalen;
5. Inzicht verkrijgen in het verschil tussen de huidige situatie en de gewenste situatie;
6. Opstellen van een plan van aanpak om te komen tot de gewenste situatie.

Desgewenst kan overigens hierbij de scope worden beperkt tot de geautomatiseerde informatievoorziening.

### PLAN VAN AANPAK

Aan de start van het traject worden een klankbord groep opgericht bestaande uit managers bedrijfsvoering. Deze groep wordt op gezette tijden geraadpleegd om informatie in te winnen en gedane aannamen of voorstellen te toetsten op correctheid en haalbaarheid. Tevens wordt door de organisatie een project-begeleider aangewezen, welke nauw met de adviseurs van LBVD samenwerkt om te komen tot de feitelijke eindproducten.

Op basis van eventueel reeds beschikbare stukken en gesprekken met de leden van de klankbord groep zal door LBVD een inschatting gemaakt worden m.b.t. de

afhankelijkheidsrelatie aangaande de informatievoorziening. Tevens zal in deze fase een waarderingschaal worden ontworpen ten behoeve van het kwalificeren van risico's.

Vervolgens zal op basis van reeds bij LBVD aanwezige kennis en ervaring een overzicht gemaakt worden van de relevante risico's ten aanzien van de informatievoorziening. Hierbij zal zowel kans op voorkomen van een mogelijk incident als mogelijke impact worden gekwalificeerd. Immers risico is de kans op voorkomen maal de impact van het optredende incident. Tevens wordt een eerste voorzet gegeven van mogelijke beveiligingsdoelstellingen. De geïndiceerde doelstelling(en) alsmede de inschatting van de risico's worden getoetst met de klankbordgroep.

Als overeenstemming is bereikt over de risico's en de doelstellingen worden deze door LBVD, in samenspraak met de aangestelde project-begeleider, vertaald in een concreet beleidsvoorstel en een beveiligingsplan op hoofdlijnen. Aan de hand van deze concepten wordt vervolgens een audit uitgevoerd teneinde het verschil tussen de huidige en de voorgestelde situatie in kaart te brengen. In dit stadium zal een ruwe schatting gemaakt worden van de kosten en inspanningen welke het dichten van het gat met zich meebrengen. Het beveiligingsplan kan nu nog aangepast worden indien de omvang van het verschil hiertoe noopt.

Het beleidsvoorstel, het concept beveiligingsplan en de resultaten van de gap-analyse worden uiteindelijk aan de klankbordgroep voorgelegd ter toetsing. Na instemming van de klankbordgroep zullen de stukken ter formalisatie worden voorgelegd aan de leiding van de organisatie.

De project-begeleider kan nu in samenwerking met LBVD een concreet projectplan opstellen om het gat tussen de huidige en de gewenste situatie te dichten. Na dit moment trekt LBVD zich grotendeels terug en zal nog gedurende één jaar éénmaal per kwartaal (4x) een voortgangsgesprek voeren met de project-begeleider en/of de security officer.

### **DELIVERABLES**

Het voorgestelde traject zal de navolgende deliverables leveren:

1. Informatiebeveiligingsbeleid;
2. Informatiebeveiligingsplan op hoofdlijnen;
3. Plan van aanpak ter dichting van het gat tussen de huidige situatie en de gewenste situatie.

### **VERVOLG**

De organisatie zal aan de hand van het opgestelde plan van aanpak het gat tussen de huidige situatie en de gewenste situatie moeten dichten.

Tevens zal het beveiligingsproces als gedefinieerd in het beleid moeten (op)groeien in de organisatie voor een blijvend resultaat.