De inrichting van een informatiebeveiligingsbeleid

Samenvatting
Informatiebeveiliging is het gewogen nemen van beheersbare risico's. Om een gewogen afweging te maken is een gestructureerd informatiebeveiligingsbeleid noodzakelijk.

Inleiding
Een succesvol informatiebeveiligingsbeleid is volgens More-Secure gebaseerd op een aantal essentiële uitgangspunten. Deze uitgangspunten zijn:

- Uitdrukkelijke betrokkenheid van het senior management;
- Een effectieve inbedding van informatiebeveiliging, inclusief de bijbehorende taken, binnen de bestaande organisatie;
- Informatiebeveiliging als een noodzakelijk en continue proces binnen de organisatie kenbaar maken ("security awareness");
- Een duidelijk, herkenbaar en uitvoerbaar informatiebeveiligingsbeleid;
- Het structureel waarderen van informatiemiddelen op basis van een classificatiemethode;
- Het gestructureerd uitvoeren van risico-analyses om te bepalen welke risico's aanwezig zijn;
- Het vaststellen van security baselines waarmee maatregelen op gestructureerde wijze toegepast kunnen worden.

Betrokkenheid van het management
Succesvolle en structurele informatiebeveiliging vraagt om de betrokkenheid van het senior management van de organisatie. Deze betrokkenheid dient verder te gaan dan alleen het verstrekken van de opdracht om informatiebeveiliging in te richten. Het senior management moet zelf geloven in de toegevoegde waarde van het informatiebeveiligingsbeleid en dit ook uitdragen naar de organisatie. Dit betekent niet dat er geen risico's meer genomen mogen worden maar dat de risico's gewogen genomen worden. Deze afweging wordt ondersteund door middelen die voortvloeien uit de uitvoering van het informatiebeveiligingsbeleid.

Informatiebeveiligingsbeleid
Het doel van een gestructureerd informatiebeveiligingsbeleid is het gewogen nemen van beheersbare risico's. Ondernemen is in het algemeen gebaseerd op het nemen van risico's. De verstandige ondernemer neemt die maatregelen om risico's in te perken waarvan de kosten in verhouding staan tot de opbrengst en de risico's die gelopen worden. Informatiebeveiligingsbeleid is een maatregel die helpt om risico's van informatiemiddelen inzichtelijk te maken en om te bepalen welke maatregelen zowel mogelijk als kosteneffectief zijn. Het is de verantwoordelijkheid van de ondernemer om uiteindelijk te beslissen welke risico's afgedekt worden tegen welke kosten. Zelfs als er besloten wordt om bepaalde risico's niet af te dekken, bijvoorbeeld omdat de voorgestelde maatregelen te duur zijn, is in ieder geval bekend welke risico's gelopen worden. Maatregelen zoals verzekeren kunnen dan een mogelijk alternatief zijn.

In het informatiebeveiligingsbeleid komen onder andere de volgende onderwerpen aan bod:

- Hoe wordt er omgegaan met informatie, zowel eigen informatie als de informatie van derden (bijvoorbeeld klanten);
- Het inrichten van verantwoordelijkheden en bevoegdheden rond het informatiebeveiligingsbeleid binnen de organisatie (security management);
- Het waarderen van informatiemiddelen middels een classificatiemethode;
- De borging van het informatiebeveiligingsbeleid door middel van risicoanalyses en audits.

Security baselines
Het informatiebeveiligingsbeleid beschrijft informatiebeveiliging op een strategisch niveau. De weerslag hiervan op het tactische niveau wordt gevormd door zogenaamde "security baselines". Met security baselines wordt een basisniveau gedefinieerd waaraan de informatiebeveiliging binnen de organisatie minimaal moet vol-

doen. Security baselines worden per aandachtsgebied geformuleerd. Aandachtsgebieden kunnen zijn: netwerk, platform, werkplek etc...

Security baselines worden vastgesteld in workshops waarbij sleutelpersonen uit de organisatie betrokken zijn. Dit versterkt het draagvlak voor het informatiebeveiligingsbeleid binnen de organisatie.

Nulmeting
Als de security baselines zijn vastgesteld is het moment aangebroken om een nulmeting uit te voeren. Met de nulmeting wordt de huidige situatie op het gebied van informatiebeveiliging in kaart gebracht (de "ist" situatie). Tevens wordt bepaald welke onderwerpen prioriteit hebben bij het verbeteren van de informatiebeveiliging.

Inbedding
Nadat de huidige situatie in kaart is gebracht zal informatiebeveiliging in de bestaande processen ingebed moeten worden om de gewenste situatie te realiseren (de "soll" toestand). De gewenste situatie is bereikt als er een continue proces is waarin informatiebeveiliging onderdeel uitmaakt van de bedrijfsprocessen en de bedrijfscultuur.

De volgende onderdelen zijn daarbij van belang:
- Het inbedden van het uitvoeren van risico-analyses bij de start van projecten (nieuwbouw);
- Het betrekken van risicoevaluaties bij change management (verbouw);
- Het inbedden van informatiebeveiliging in de beheerorganisatie (ITIL Security Management).

Ondersteuning
Als het informatiebeveiligingsbeleid ingevoerd is in de organisatie is ondersteuning van groot belang. Ondersteuning kan geboden worden in de vorm van:
- Hulpmiddelen bieden zoals sjablonen voor het uitvoeren van een risico-analyse;
- Trainingen;
- Advies aan projecten op het gebied van informatiebeveiliging;
- Het continue stimuleren van beveiligingsbewustzijn onder medewerkers en management door middel van acties.

De Auteur
Ir. Ernst J. Mellink is IT Security Architect en eigenaar van More-Secure BV. Hij adviseert grotere en kleinere organisaties over de wijze waarop IT-beveiliging (technisch en organisatorisch) een onderscheidende factor kan zijn in de markt en in de bedrijfsvoering. Hij is bereikbaar op e.j.mellink@more-secure.nl

Contact
More-Secure BV
Da Costalaan 14
3767GH Soest
T: +31 (0)6 5357 9338
F: +31 (0)35 524 7587
E: info@more-secure.nl
W: www.more-secure.nl