

Kapstok gezocht.....(en gevonden)

Wat is informatiebeveiliging?

Iedere organisatie houdt zich bezig met informatiebeveiliging. Bij informatiebeveiliging gaat het om de volgende aspecten van informatie: beschikbaarheid, vertrouwelijkheid en integriteit. Oftewel: is de informatie die nodig is om de bedrijfsprocessen goed te laten verlopen aanwezig op het juiste moment (beschikbaarheid) en is deze informatie juist en volledig (integriteit) en is deze informatie alleen toegankelijk voor personen voor wie dit gewenst en noodzakelijk is (vertrouwelijkheid).

Van weloverwogen ad-hoc.....

Door de jaren heen zijn ook door Zeelandia op bovengenoemd gebied een groot aantal maatregelen genomen. Keuzes uit de talloze (met name technische maatregelen) zijn veelal gemaakt op basis van logisch nadenken, "gezond verstand" en algemeen aanvaarde "best practices". Doel en verwachtingspatronen waren hierbij echter niet altijd even duidelijk.

Interne en externe toetsing op verschillende manieren en momenten gaven wel aan dat door het totaal van maatregelen sprake was van een behoorlijk niveau van informatiebeveiliging.

..... naar structuur

Besloten werd dat de maatregelen aan een beleid en bovenliggende doelstellingen gekoppeld dienden te worden. We zijn dus op zoek gegaan naar de "kapstok" om de maatregelen aan op te kunnen hangen. Dit kwam neer op het formuleren van een formeel informatiebeveiligingsbeleid. Natuurlijk stonden hiervan al losse "flarden" op papier maar het was nog geen samenhangend geheel en was nog verre van compleet. Een andere conclusie was dat we een gespecialiseerde partner nodig hadden om ons daarbij te assisteren om dit proces efficiënt en effectief te laten verlopen. Het op te stellen beleid diende tevens de link naar de praktijk op eenvoudige wijze te faciliteren. Voorkomen moest worden om een onnodige zware "papieren tijger" te creëren om de boekenkast op te vullen. We gingen op zoek naar een partner met een pragmatische aanpak die op korte termijn kon leiden tot concrete resultaten.

Op zoek naar een partner

Op de Infosecurity kwam ik in contact met LBVD, een onafhankelijk adviesbureau op het gebied van informatiebeveiliging. Zij bleken een methode "Verbeterplan Informatiebeveiliging" te hebben ontwikkeld waarbij volgens een gestructureerde aanpak met beperkte middelen en met een korte doorlooptijd de door ons gewenste resultaten geboekt zouden kunnen worden. In mei 2007 zijn we gestart met het verbeterplan dat bestaande uit de volgende onderdelen:

- Intake
- Vaststellen van de IST-situatie middels o.a. norminterviews, kwetsbaarheidsscans en bewustzijnsspelingen
- Formuleren van een strategisch beleid met daaraan gerelateerde organisatiestructuur
- Vaststellen van de SOLL-situatie aan de hand van o.a. wet- en regelgeving, best practices, vereisten bedrijfsvoering rekening houdend met het geformuleerde strategische beleid.
- GAP-analyse
- Opstellen van een projectplan om te komen tot de SOLL-situatie rekening houdend met het geformuleerde beleid

Om de kans op resultaat te vergroten werd besloten de scope te beperken tot het procesmatig inrichten van de informatiebeveiliging binnen de invloedssfeer van de ICT-

afdeling. Een bredere scope verkleinde naar onze mening de kans op zichtbare successen.

De kapstok

Het formuleren van het strategisch beleid en de vertaling naar praktische uitgangspunten is het lastigste maar tevens het belangrijkste onderdeel van het project. In eerste instantie zijn daarbij een beperkt aantal (4) strategische doelstellingen geformuleerd. Deze zijn o.a. gebaseerd op de door Zeelandia geformuleerde corporate strategy en business principles. Een aantal gesprekken met stakeholders binnen Zeelandia werden gevoerd om de strategische doelstellingen te formuleren. Hoewel de geformuleerde doelstellingen “open deuren” lijken te zijn is het vaststellen, uitschrijven en uitdragen daarvan een cruciale stap in het geheel. Deze doelstellingen zijn uiteindelijk vastgesteld door de hoofddirectie. Dit is de basis van de kapstok.

De door Zeelandia geformuleerde strategische doelstellingen zijn de volgende:

- Zeelandia voldoet aan alle relevante wet- en regelgeving. Belangrijk hierbij is dat er ook aangegeven wordt welke dit zijn.
- Zeelandia heeft concurrentievoordeel door unieke kennis die zij heeft verworven. Ook is sommige informatie op bijv. financieel gebied erg gevoelig of belangrijk. Deze kennis en informatie mag niet in handen komen van personen of partijen waarvan Zeelandia dat niet wenst. Bovendien mag deze informatie niet (geheel of gedeeltelijk) verloren gaan.
- Zeelandia dient te voorkomen dat niet-publieke informatie van/over klanten en leveranciers in handen komt van personen of partijen zonder de nadrukkelijke toestemming van betreffende klant/leverancier
- Verstoring of uitval van de (al dan niet digitale) informatievoorziening mag niet leiden tot hinderlijke situaties voor de bedrijfsvoering van klanten.

Beveiligingsprincipes (de kleeftjes)

De geformuleerde strategische doelstellingen stonden nog ver af van de (praktische) huidige situatie en het formuleren van praktische verbeterpunten.

De volgende stap was het definiëren van de beveiligingsprincipes die nodig zijn om de strategische doelstellingen te kunnen realiseren.

De beveiligingsprincipes zijn gebaseerd op best practices en o.a. het beveiligingsproces uit het ISM3 model (Information Security Model). Dit model gaat uit van beveiligingsprocessen en niet van specifieke maatregelen zoals de Code voor Informatiebeveiliging. Dit heeft als voordeel dat processen nog specifiek voor Zeelandia ingericht kunnen worden zolang er wordt voldaan aan de omschreven randvoorwaarden en eindresultaten.

Per beveiligingsproces zijn relevante beveiligingsprincipes gekozen inclusief het bijbehorende basisniveau van beveiliging.

De beveiligingsprincipes zorgen dus voor de overbrugging van de strategische doelstellingen naar de praktische uitvoering. Per principe worden de volgende onderdelen beschreven:

- Toelichting
- Basisniveau
- Verantwoordelijkheid
- Voorbeeld
- Motivatie

GAP-analyse en verbeterplannen (de bestaande garderobe ordenen)

Met de beveiligingsprincipes in de hand is het dus mogelijk om de IST-situatie te toetsen. Tekortkomingen zullen dus inzichtelijk gemaakt dienen te worden waarbij het principe geldt van “pas toe” of “leg uit”. Afwijkingen van het basisniveau zijn dus alleen toegestaan indien dit verantwoord kan worden.

Uiteindelijk zal deze stap dus leiden tot een aantal verbeterplannen om te gaan voldoen aan de strategische doelstellingen en de beveiligingsprincipes.

Borging (nieuwe jassen op de juiste plaats hangen)

Hoewel het “Verbeterplan Informatiebeveiliging” als project kan worden beschouwd dient “informatiebeveiliging” zelf niet als project maar als proces te worden benaderd. Het is n.l. van belang dat er een organisatie bestaat om het proces informatiebeveiliging continu de aandacht te geven die het verdient en vereist.

Rollen en verantwoordelijkheden zijn vastgesteld. Binnen de omvang van Zeelandia betekent dit dat deze rollen door medewerkers worden ingevuld naast hun primaire functie.

Conclusie

Terugkijkend op de oorspronkelijk uitgangspunten voor het structureren van het onderwerp “Informatiebeveiliging” kunnen we constateren dat de samenwerking met LBVD met een doorlooptijd van ongeveer een jaar niet alleen geresulteerd heeft in een informatiebeveiligingsbeleid met strategische doelstellingen maar tevens een zeer praktische vertaling hiervan naar de dagelijkse praktijk. Er bestaat nu een lijst met projecten om te gaan voldoen aan dit vastgestelde beleid en een structuur om nieuwe ontwikkelingen te toetsen aan het beleid.

Daarnaast is er ook een structuur van rollen en verantwoordelijkheden gecreëerd om definitie en controle van het beleid vorm te geven.

Wat ons betreft biedt de kapstok dus inderdaad voldoende houvast en structuur om “alles” aan op te kunnen hangen.....