



Op zoek naar een kapstok

ALS HET GOED IS, HOUDT IEDERE ORGANISATIE ZICH BEZIG MET **INFORMATIEBEVEILIGING**. DAARBIJ GAAT HET OM **BESCHIKBAARHEID, VERTROUWELIJKHEID EN INTEGRITEIT**: IS DE INFORMATIE DIE NODIG IS OM DE BEDRIJFSPROCESSEN GOED TE LATEN VERLOPEN OP HET GEWENSTE MOMENT AANWEZIG, IS DEZE **JUIST EN VOLLEDIG**, EN SLECHTS TOEGANKELIJK VOOR PERSONEN VOOR WIE DIT GEWENST EN NOODZAKELIJK IS? DOOR DE JAREN HEEN ZIJN OOK BIJ **ZEELANDIA** OP DIT GEBIED EEN GROOT AANTAL MAATREGELLEN GENOMEN. **BERT DE VOS**, HOOFD ICT-BEHEER VAN HET BEDRIJF, **DEELT ZIJN ERVARINGEN**.

Door Bert de Vos

De keuzes uit de talloze, met name technische maatregelen op het gebied van informatiebeveiliging werden bij Zeelandia veelal gemaakt op basis van logisch nadenken, gezond verstand en algemeen aanvaarde best practices. Doelen en verwachtingspatronen bij de producent en distributeur van bakkerij-ingrediënten 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 beveiligingsniveau.

Structuur

Besloten werd evenwel dat de genomen maatregelen aan een echt beleid en bovenliggende doelstellingen gekoppeld dienden te worden. We zijn bij Zeelandia dus op zoek gegaan naar een '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 bovendien nog verre van compleet.

Een andere conclusie was dat we gespecialiseerde assistentie nodig hadden om dit proces efficiënt en effec-

tief te kunnen 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, die vooral zou dienen als vulling voor de boekenkast. We gingen op zoek naar een partner met een pragmatische aanpak, die op korte termijn kon leiden tot concrete resultaten.

Op de Infosecurity-beurs kwam ik in contact met LBVD, een onafhankelijk adviesbureau op het gebied van informatiebeveiliging. Zij bleken de 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 bestaat uit de volgende onderdelen:

- Intake.
- Vaststellen van de *ist*-situatie door middel van onder andere norminterviews, kwetsbaarheidsscans en bewustzijnspeilingen.
- Formuleren van een strategisch beleid met daaraan gerelateerde organisatiestructuur.
- Vaststellen van de *soll*-situatie aan de hand van onder andere wet- en regelgeving, best practices, vereisten van de bedrijfsvoering, en 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 was het lastigste, maar tevens het belangrijkste onderdeel van het project. In eerste instantie zijn daarbij een beperkt aantal (vier) strategische doelstellingen geformuleerd. Deze zijn onder meer gebaseerd op de door Zeelandia geformuleerde *corporate strategy* en *business principles*. Een aantal gesprekken met stakeholders binnen Zeelandia wer-

den 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. Bovendien is sommige informatie op bijvoorbeeld financieel gebied erg gevoelig of belangrijk; deze mag niet in handen komen van personen of partijen waarvan Zeelandia dat niet wenst. Verder 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.

Kleerhangers

De geformuleerde strategische doelstellingen stonden evenwel nog ver af van de huidige (praktische) 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 ge-

┌ MET BEHULP VAN DE GAP- ANALYSE WORDT DE GARDEROBE GEORDEND ┐

'Wij zijn toch geen bank!'

Beveiliging van informatie is iets waar meer en meer organisaties mee worstelen. "Wij zijn toch geen bank!", is bij informatiebeveiliging LBVD een veelgehoord argument. Wat men vergeet, is dat een bank in veel gevallen de middelen heeft gevolgschade op te vangen. Bij de meeste 'gewone' ondernemers is dat lang niet altijd het geval.

De opdrachtgevers van LBVD zijn in de praktijk afkomstig uit zeer diverse branches. Volgens de 'begeleidend specialist' hebben al deze totaal verschillende organisaties min of meer toch met dezelfde vragen te maken. Bovendien passen daar vaak min of meer vergelijkbare antwoorden en benaderingen bij. Wat dikwijls ontbreekt is een voldoende mate van structuur. Hierdoor is het moeilijk te bepalen of er genoeg aan informatiebeveiliging gedaan is. Als je geen duidelijk doel hebt, kun je namelijk ook niet eenvoudig vaststellen of je het doel bereikt hebt – noch wat eventuele vervolgstappen zouden kunnen zijn.

Vast stramien

Het 'Verbeterplan Informatiebeveiliging' is een vast stramien van activiteiten waarbij de *ist*- en *soll*-situatie worden bepaald, en tegen elkaar afgezet. Alhoewel deze aanpak een vaste vorm kent, biedt het alle flexibiliteit die nodig is om het aan te passen aan de organisatie.

Door de formulering van (een beperkt aantal) beveiligingsdoelstellingen wordt het waarom van informatiebeveiliging verankerd. Deze doelstellingen worden vervolgens in overleg uitgewerkt tot beveiligingsprincipes. Deze principes beschrijven vooral wát bereikt moet worden en niet zozeer hōe dat gedaan zal worden. Dit heeft onder andere tot gevolg dat de betrokken medewerkers, in veel gevallen werkzaam bij de ict-afdeling, de broodnodige kaders krijgen aangereikt en tegelijkertijd worden uitgedaagd hun eigen kennis en vaardigheden in te zetten. Aan hen de taak daadwerkelijk invulling te geven aan het opgestelde beleid.

Stappenplan

1. Kennis omtrent de *ist* (m.b.t. techniek, organisatie en mens).
2. Begrip en kaders omtrent de *soll* (idem).
3. Informatiebeveiligingsbeleid op hoofdlijnen.
4. Plan van aanpak om te komen tot de gewenste kaders.
5. Besef bij de verschillende betrokkenen omtrent hun rol in het proces.
6. Borging van de verschillende maatregelen.
7. Implementatie (bij hoofdvestiging in Nederland).
8. Communicatie omtrent de modus operandi naar (eventuele) andere vestigingen.
9. Bepalen of vergelijkbare activiteiten bij buitenlandse vestigingen noodzakelijk is.
10. Uitvoeren werkzaamheden.
11. Opzetten auditprocessen.

baseerd op best practices en onder andere het beveiligingsproces uit het ISM3 model (information-securitymodel). 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

Garderobe ordenen

Met behulp van de gap-analyse en verbeterplannen kan de bestaande 'garderobe' worden geordend. 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 leiden tot een aantal verbeterplannen om te gaan voldoen aan de strategische doelstellingen en de beveiligingsprincipes.

Door middel van 'borging' kunnen nieuwe jassen op de juiste plaats worden gehangen. Hoewel het Verbeterplan Informatiebeveiliging als project kan worden beschouwd, dient de informatiebeveiliging zelf niet als project maar als proces te worden benaderd. Het is namelijk van belang dat er een organisatie bestaat om het proces informatiebeveiliging continu de aandacht te geven die het verdient en vereist. Rollen en verantwoorde-

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

Conclusie

Zeelandia is een meer dan honderd jaar oud familiebedrijf met een relatief platte organisatiestructuur en een vriendelijke cultuur. Daarbij past de nodige pragmatiek en een grote inbreng van de betrokken medewerkers. Dit is tot uiting gekomen in zowel de aanpak als het eindresultaat van het verbeterplan.

Terugkijkend op de oorspronkelijke uitgangspunten voor het structureren van het onderwerp 'informatiebeveiliging' is bij Zeelandia geconstateerd dat de samenwerking met LBVD, waarvan de doorlooptijd ongeveer een jaar heeft bedragen, niet alleen heeft geresulteerd in een informatiebeveiligingsbeleid met strategische doelstellingen, maar tevens tot 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 dit aan nieuwe ontwikkelingen te toetsen.

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.