

Informatiebeveiliging:

Informatiebeveiliging is een soort hygiëne: het speelt altijd. In veel gevallen zonder dat iemand erbij nadenkt, maar intussen is iedereen wel degelijk verantwoordelijk voor zijn eigen handelen. We hebben allemaal van onze moeder geleerd wát, hóe en waarom we onze handen moeten wassen op bepaalde momenten. En dat is allemaal vanzelfsprekend geworden... [HANS LABRUYÈRE *](#)

Informatiebeveiliging is voor alle betrokkenen in een organisatie vaak een lastig onderwerp. Ze associëren het met IT, met fysieke beveiliging of besluiten dat het hen überhaupt niet aangaat. De term beveiliging moet er eigenlijk ook af; die is alleen maar storend in de communicatie. Beter is: bescherming van informatie, dat is een stuk duidelijker. Bovendien heeft elke organisatie ook nog te maken met culturele aspecten: zeg tegen een Duitser linksaf te gaan en hij zal antwoorden met: 'Jawohl' – geef een Nederlander dezelfde opdracht en hij vraagt: 'Waarom?'

Relevantie

Waar staat informatiebeveiliging nu eigenlijk voor? Organisaties kunnen drie vragen stellen:

1. Welke kernprocessen hebben wij eigenlijk?
2. Welke informatiestromen zijn noodzakelijk voor de continuïteit van dat kernproces? Dat zijn niet alleen digitale informatiestromen, maar ook papieren informatiestromen, menselijke informatiestromen.
3. Hoe gaan personeelsleden om met de bescherming van die informatiestromen in het kader van integriteit, vertrouwelijkheid, beschikbaarheid?

Het antwoord op deze vragen geeft al een veel beter beeld van informatiebeveiliging en de relevantie daarvan voor de organisatie. Als de keuze wordt gemaakt: 'Nee, dat risico dekken we niet af', is dat overigens een prima antwoord. Maar dan wel graag een 'nee' met de goedkeuring en de handtekening van iemand van de leiding, zodat men daarop kan terugvallen als

het alsnog verkeerd gaat. Men kan dit indekken noemen, maar bij een *realistische* afweging van risico's gaat het om *realiteitszin*.

De leiding moet de verantwoordelijkheid nemen en leiding geven. Dat betekent knopen doorhakken. Aan de hand van gegevens en argumenten die alleen de leiding in zijn totaliteit kan afwegen.

In het echelon onder de leiding zal de security manager beleid uitwerken, auditen op de uitvoering, en proactief bezig zijn met het onderwerp. Maar beslissingen nemen... nee. Beslissingen nemen op het gebied van informatiebeveiliging is de taak van een echelon hoger.

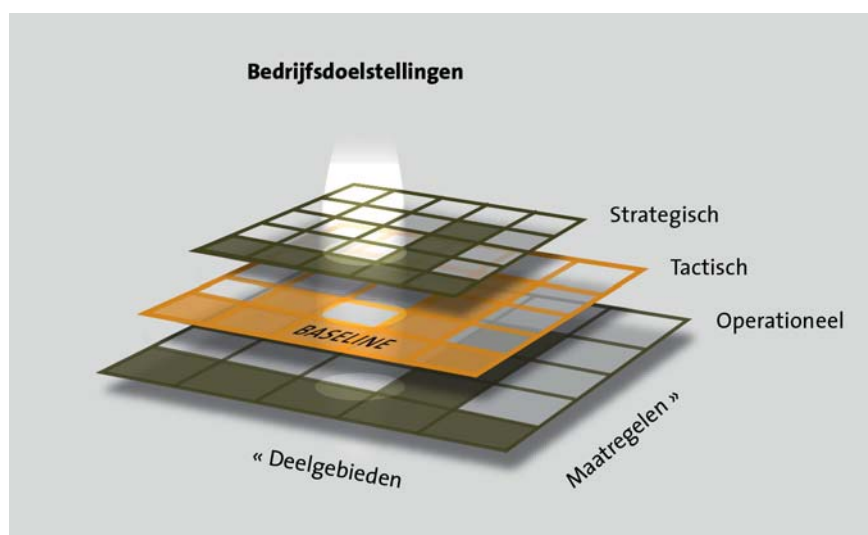
Beleid

Beslissingen dienen te worden vervat in een beleidsdocument. Met een geaccordeerd beleidsdocument is het mogelijk een communicatieplan voor

medewerkers en directie te maken. Alleen met gecommuniceerde regels en protocollen kan men van medewerkers vragen zich aan die regels te houden en kan men van de directie vragen de juiste middelen te verschaffen. En alleen met een gedocumenteerd beleid is het meetbaar óf de informatiebeveiliging werkt en in hoeverre het werkt. Beleid is dus onmisbaar en vormt de spil van het succes in informatiebeveiliging.

Beleid dient te worden gedragen door zowel management als medewerkers. Dat houdt onder andere in dat het uitwerken van dat beleid een pragmatische, voor alle betrokkenen begrijpelijke, complete oefening dient te zijn. Met heldere resultaten.

Voor veel organisaties is het moment dat het beleid concreet wordt uitgewerkt de eerste keer dat zij met het onderwerp informatiebeveiliging in aanraking komen. Het is dus zaak om de



'Nee' is een prima antwoord.

waar te beginnen?

verwachtingen over en weer van management en leidinggevenden helder te krijgen. En om met elkaar een heldere perceptie te krijgen over 'Waar staan we nu en waar moet het naar toe?' Toch is dit een lastige opgave, want hoe krijg je als security management de directie bij elkaar over een onderwerp dat a priori geen aandacht heeft?

Methodiek

Om een beleidsdocument op te zetten zijn diverse methoden beschikbaar, zoals het Verbeterplan Informatiebeveiliging. In het kort houdt dit in:

- » Scope bepalen: alleen ICT-gerelateerde informatie, of ook menselijk gerelateerd? En hoe zit het met papierstromen?
- » De juiste mensen betrekken, op het juiste moment.
- » De IST-situatie (feitelijk aangetroffen situatie) bepalen.
- » De SOLL-situatie (wenselijke situatie) bepalen. Daar hoort bij dat de visie van directie en management wordt bepaald en vastgelegd. Dat er wordt bepaald aan welke wet- en regelgeving men dient te voldoen. Dat er een beeld wordt gevormd van het gebruik van informatie in de diverse bedrijfsprocessen.
- » Risicoanalyse uitvoeren.
- » Het verschil tussen IST en SOLL bepalen met een voor de organisatie passend normenkader. De verschillende kaders kunnen naar keuze van de situatie gebaseerd zijn op maatregelen, productgeoriënteerd zijn, of gebaseerd zijn op processen en/of best practices.
- » Plan van aanpak op hoofdlijnen vaststellen en laten goedkeuren door de directie.
- » Het lijnmanagement een projectplan van aanpak laten maken (SMART).
- » Zicht houden op de uitvoering van die plannen: *plan-do-act-control*.

Scope

Even terug naar het begin van dit artikel, waarin drie informatiestromen worden gedefinieerd: papieren, digitale



en menselijke. Informatiebeveiliging bestaat ook uit drie onderdelen: technische, organisatorische en menselijke elementen. Door alle processen heen is deze driehoek in wisselende verhoudingen terug te vinden.

Techniek/Organisatie

Wat technisch niet hoeft, moet men achterwege laten. Ook daarbij is beleid behulpzaam: als er is vastgelegd dat het dragen van een toegangspas verplicht is, valt te overwegen een slimmere kaart aan te schaffen die ook andere

Zo ja, weten medewerkers daar dan van? Handelen ze daar dan ook naar? En als er iets misgaat, zou dat dan (op tijd) worden opgemerkt? Is er daarna dan nog iets aan te doen? Wat is de schade? Wat is het risico (kans x impact)?

Door in een Verbeterplan uit te gaan van de wenselijke situatie (SOLL) en de feitelijk aangetroffen situatie (IST), is het mogelijk een verschil vast te leggen. Het totaal van de bevindingen wordt dan gespiegeld aan een normen-

Beleid is de spil van het succes in informatiebeveiliging

functies kan hebben. Op die manier zijn medewerkers eerder geneigd de kaart ook daadwerkelijk mee te nemen, in plaats van hem tijdens de lunch op het bureau te laten liggen.

Organisatie/Mens

Is informatiebeveiliging georganiseerd?

kader (bijvoorbeeld de Code voor Informatiebeveiliging), om aldus inzicht te verkrijgen in datgene wat er volgens de organisatie zou moeten zijn, maar wat er feitelijk niet is. Op die manier komen prioriteiten tot stand, zodat op een pragmatische manier het plan van aanpak wordt ontwikkeld. »



Mens/Techniek

Pas als medewerkers weten 'waar het voor is', zijn ze bereid na te denken OF ze de regel willen opvolgen. Overigens is 50 procent van het antwoord: 'Nee, ik wil niet.' Maar als er beleid is, als de risico's in de organisatie zijn bekeken en gewogen, is het een weloverwogen 'nee', compleet met zicht op mogelijke risico's (kans x impact). Natuurlijk kun je ook die bereidheid tot medewerking meten, beïnvloeden, sturen. Er zijn legio *awareness*-programma's ontwikkeld, waarvan sommige ook nog best goed werken.

Verschillen in inzicht

Een aldus ontstaan plan van aanpak kan er voor verschillende afdelingen heel anders uitzien: voor HRM geldt wellicht een ander gevoel van veiligheid inzake informatie dan voor een operationele afdeling. Voor de directie kan een andere werkelijkheid gelden dan voor uitvoerende afdelingen. Reden ook waarom *corporate* plannen van aanpak zelden werken. Die zijn ook veelal te complex. Laat afdelingen vooral zelf nadenken over hun gevoel van veiligheid, hun ervaringen, hun dreigingen en oplossingen. Je zult zien dat voor veel dreigingen al een oplossing is aangedragen. In veel gevallen dient een en ander alleen nog in een eenduidig document te worden gegoeten en te worden afgetekend.

Aandacht

Toegegeven, zo eenvoudig is het niet altijd. Met name beslissers kunnen soms horende doof zijn en ziende

blind. 'Het gebeurt wel, maar mij niet'. En als er dan wat gebeurt, is het huis te klein en worden alle *resources* geactiveerd om een incident waarvan de kans dat het nóg een keer gebeurt nul is, in het vervolg te voorkomen. Aan de andere kant: incidenten werken dus wel. Alleen brengen ze een hoop onrust en onmin, imagoschade en bedreiging van de continuïteit, precies de zaken die iedereen wil vermijden.

Vooropgezet incident

Een vooropgezet incident heeft dat nadeel niet en heeft eigenlijk alleen voordelen:

- » het toont dat het niet alleen kán gebeuren, maar dat het ook deze organisatie en deze medewerkers kan overkomen;
- » het geeft organisaties de gelegenheid te tonen dat ze weten wanneer zich een incident aandient, en wat ze moeten doen bij een incident;
- » je hebt het als opdrachtgever in de hand: het betreffen vaak goed geregisseerde acties, die door ervaren professionals worden uitgevoerd.

Een vooropgezet incident kan verschillende gedaanten hebben. Het kan *BlackBox* geschieden, zonder enige voorinformatie, waarbij de 'aanvaller'

of fysiek (insluiper die probeert papieren en/of menselijke informatiestromen te vinden en te beïnvloeden) worden uitgevoerd. Telefonische of fysieke *social engineering* kan onderdeel uitmaken van de opdracht.

Een combinatie van deze elementen is voor de meeste organisaties fataal, maar daar gaat het niet om. Waar het om gaat is dat medewerkers incidenten kunnen herkennen en zich kunnen afvragen wat de waarde is van de informatie waar zij op dat moment de beschikking over hebben. En een '*real life*' actie is daarbij een goed middel. De reactie die een dergelijke actie bij medewerkers geeft, treedt ook op bij beslissers. Die zullen zich op hun beurt rekenschap geven van nut & noodzaak van goed gecommuniceerde regels en procedures. Er dient beleid te komen, als dat er nog niet is. De cirkel is rond.

Spin-off

Overigens is er nog een positieve spin-off van dergelijke geregisseerde incidenten te onderkennen: de security manager komt op een positieve manier 'in the picture' te staan: medewerkers weten hem te vinden, ze begrijpen wat hij doet, en vooral waarom. Het is zeker dat na een dergelijke actie inzicht, aandacht en uitvoering van beveiliging

Beveiliging van informatie is een 'ongoing proces'

gebruikmaakt van toeval, ervaring, list & bedrog. Er kan *CrystalBox* worden gewerkt, waarbij een opdrachtgever een bepaald proces of element van de bedrijfsvoering aanwijst als doelobject en alle mogelijke voorinformatie overhandigt om de oefening zo effectief mogelijk te laten zijn. Incidenten kunnen digitaal (hacker),

van informatie sterk verbeteren. Dat duurt overigens maar kort, maar toch is een dergelijke bewustwordingsimpuls waardevol. Beveiliging van informatie is een ongoing proces – je kunt niet te vroeg beginnen. Wel te laat. «

* Hans Labruyère is partner bij LBVD (www.lbvd.nl)

Samenvatting

- » **Informatiebeveiliging** is voor organisaties vaak een lastig onderwerp.
- » Door antwoord te geven op de vragen wat de **kernprocessen** zijn, welke **informatiestromen** hierbij noodzakelijk zijn en hoe **personeelsleden** omgaan met de bescherming van die informatiestromen wordt een beter beeld verkregen van informatiebeveiliging en de relevantie daarvan voor de organisatie.