

Als uw organisatie bij ieder ongeluk met de informatievoorziening de rommel snel opruimt, de schuldigen straft, de helden eert en vervolgens overgaat tot de orde van de dag, heeft u een probleem. Het kan zo niet eeuwig doorgaan, zeker niet nu uw organisatie aan alle zijden elektronisch geopend wordt. Het invoeren en verbeteren van informatiebeveiliging vereist structurele maatregelen en gaat alle lagen van de organisatie aan. Het is een proces waarin drie vragen centraal staan: waar staat de organisatie nu, wat is het einddoel en wat is de kortste weg daarheen? Om deze vragen te beantwoorden, beschrijft dit artikel een groeimodel voor de verbetering van informatiebeveiliging. Het uitgangspunt hiervan vormen de leerprocessen van de betrokkenen bij het verbeteren van de informatiebeveiliging. De auteurs grijpen terug op ervaringen die onder andere zijn opgedaan bij het Ministerie van VROM.

Informatiebeveiliging nu of nooit

door Anton Griffioen en Jaap van der Wel

E-commerce, loketten op het Internet; in allerlei verschijningsvormen neemt het belang van de informatievoorziening toe. Informatiebeveiliging wint daardoor aan belang. Ook stellen wet- en regelgeving, denk aan de privacywetgeving, steeds hogere eisen. Dit terwijl bedrijven en overheid voortdurend worden geconfronteerd met informatiebeveiligingsincidenten. Het besef dat informatiebeveiliging veel verder gaat dan een goed wachtwoord dringt gelukkig door bij het management. Maar hoe pakken we het aan?

Geen recept

Helaas, een eenduidig recept bestaat niet. Elke organisatie heeft haar eigen cultuur, haar eigen primaire processen en eigen bedrijfsvoering. Bovendien zijn er grote verschillen in de mate waarin informatiebeveiliging is geïmplementeerd binnen organisaties. Eén kenmerk hebben alle organisaties gemeen: verbeteren van de beveiliging is een veranderingsproces. Op basis van onze praktijkervaring hebben we een instrument ontwikkeld waarmee het begin en het einde van het proces kan worden bepaald alsmede de veranderstrategie voor het bereiken van het einddoel. Dit artikel geeft een eerste aanzet voor dit instrument in de vorm van een groeimodel voor de verbetering van informatiebeveiliging. Uitgangspunt vormen de leerprocessen die de betrokkenen doormaken bij het verbeteren van de informatiebeveiliging en bij het vasthouden van het eenmaal bereikte niveau.

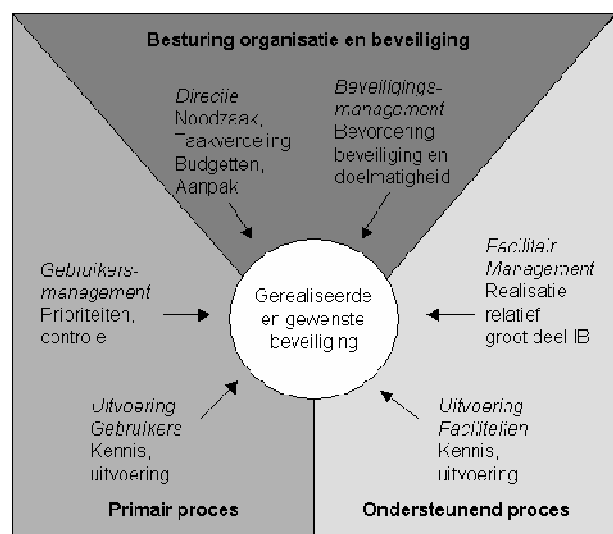
Wie realiseren informatiebeveiliging?

In de meest eenvoudige organisatie van informatiebeveiliging wordt men bij de uitvoering van het werk geconfronteerd met problemen en moet men die maar zien op te lossen. Pas als er zich ongelukken voordoen, ziet het management in dat de uitvoerders dit karwei niet alleen kunnen opknappen en raken steeds meer organisatie-niveaus en specialisten betrokken, te weten:

- *Het facilitair management.* Hieronder valt het management van het rekencentrum, de softwareontwikkel- en beheersorganisatie, de huishoudelijke dienst, de financiële functie, et cetera. Deze groep is verantwoordelijk voor de uitvoering van een relatief belangrijk deel van de beveiligingsmaatregelen.

- *Het lijnmanagement.* Dit management bepaalt het gewenste beveiligingsniveau voor het eigen (deel van het) bedrijfsproces en ziet toe op de uitvoering van de benodigde maatregelen.
- *De directie.* De directie stelt de gewenste betrouwbaarheid vast als onderdeel van een bedrijfsstrategie, stelt prioriteiten, verdeelt taken en wijst budgetten toe. Ook stelt de directie de hoofdlijnen van de aanpak vast.
- *Het beveiligingsmanagement.* Dit coördineert en controleert de beveiligingsactiviteiten. Het verzamelt kennis en ervaring over informatiebeveiliging, waardoor de aanpak van beveiliging effectiever wordt. Deze functie kan bij meerdere organisatieonderdelen zijn belegd maar ook in een gespecialiseerde functie, zoals een IT-security officer.

Elk van de betrokkenen moet de juiste attitude en ervaring hebben op het gebied van informatiebeveiliging. In eerste instantie bakent ieder zijn eigen taken af. Tussen de taken ontstaan daarbij doublures en hiaten; het bereiken van het juiste samenspel kost jaren. Het gedrag van de actoren verschilt in elke fase van het groeimodel.

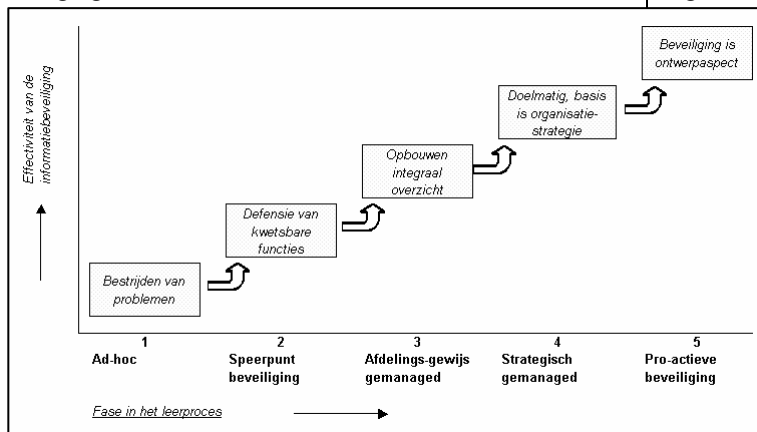


Figuur 1 Betrokkenen en hun rollen bij het realiseren van informatiebeveiliging

Het groeimodel.

Het groeimodel (zie figuur 2) beschrijft de inrichting van de informatie-beveiliging. Het model kent vijf fasen, elk met haar eigen karakteristieken:

- *Fase 1: Ad-hoc*, waarin een organisatie ontstane problemen oplost en overgaat tot de orde van de dag.
- *Fase 2: Speerpunt-informatiebeveiliging*, waarin een organisatie de belangrijkste problemen voorkomt door de meest kwetsbare onderdelen van een beveiliging te voorzien.



Figuur 2: Groeimodel voor de invoering van informatiebeveiliging

- *Fase 3: Afdelingsgewijs gemanaged*, waarbij een organisatie een analyse maakt van de totale bedrijfs-situatie en voor in principe alle afdelingen van het bedrijf de beveiliging inricht met vergelijkbare procedures zoals die van de vorige fase. Iedere afdeling krijgt voor het eerst met een systematische aanpak van beveiliging te maken. Door gebrek aan de noodzakelijke ervaring ontstaat een maatwerk aanpak rondom de al bestaande beveiliging uit de vorige fase.
- *Fase 4: Strategisch gemanaged*, waarbij een organisatie op basis van een strategische visie een doelmatige beveiligingsarchitectuur inricht. Een kenmerkend verschil met de vorige fase is de uitgebreide inzet van classificatienormen en standaardmaatregel-pakketten in plaats van de maatwerkbeveiliging per gebruikersafdeling.
- *Fase 5: Pro-actieve beveiliging*, waarin beveiliging één van de ontwerpaspecten is van nieuwe organisaties, informatievoorzieningen en ICT-architectuur. In plaats van de inhaalslag van de vorige fasen, wordt de beveiliging voor de gehele lifecycle systematisch ingericht.

Gedurende het doorlopen van de fasen ontwikkelt een organisatie de aanpak van informatiebeveiliging van een niet-georganiseerd verband (fase 1), naar een steeds uitgebreidere informatiebeveiliging (fase 2 en 3), totdat de kosten een rem op de ontwikkelingen zetten. Daarop wordt de doelmatigheid en de effectiviteit van de beveiliging bevorderd met rationalisering van de aanpak door de inzet van specialisten, de ontwikkeling van standaards, en dergelijke voor de bestaande systemen

(fase 4). In fase 5 wordt deze aanpak uitgebreid naar de gehele life cycle van organisatie en informatievoorziening, door de beveiliging integraal onderdeel te laten zijn van de ontwikkeling. De kosten van informatiebeveiliging zijn dan niet meer te onderscheiden onderdeel geworden van de realisatiekosten. Figuur 3 brengt de geschetste ontwikkeling kwalitatief in beeld. Enige relativering van deze grafiek is op zijn plaats omdat de inspanning die nodig is om een fase te doorlopen per organisatie verschilt. Een organisatie die al een hoge mate van standaardisatie in de ICT en de bedrijfsvoering heeft, zal sneller naar fase 4 kunnen doorstoten dan een organisatie waar standaardisatie nog geen gestalte heeft gekregen.

Karakteristieken van elke fase.

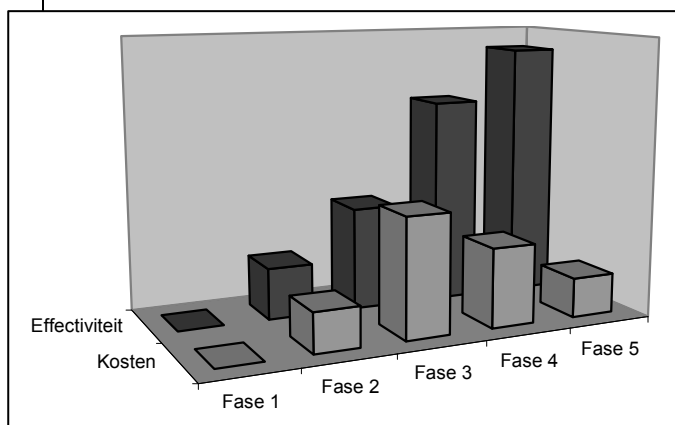
Figuur 4 karakteriseert iedere fase aan de hand van de activiteiten die de betrokken organisatielieden uitvoeren. Voor iedere fase zijn dat de volgende:

Fase 1: Ad-hoc informatiebeveiliging

Aan informatiebeveiliging wordt geen prioriteit gegeven. Op incidenten en calamiteiten wordt gereageerd door het opruimen van de schade, het straffen van de schuldigen en het belonen van helden.

De aanwezigheid van helden, die in het verleden grote ongelukken hebben rechtgetrokken, staat borg voor de informatiebeveiliging.

Toch ontstaat al snel bij organisatieonderdelen die bijzonder afhankelijk zijn van de informatievoorziening de behoefte aan een gestructureerde aanpak om herhaling te voorkomen. Dit vormt de overgang naar een volgende fase.



Figuur 3: Effectiviteit en kosten

Fase 2: De speerpunt-informatiebeveiliging.

In deze fase is informatiebeveiliging voor de meest kwetsbare afdelingen of processen een belangrijk onderwerp. Voorbeelden zijn bescherming van financiële processen met functiescheiding en bescherming van rekencentra met beveiligde gebouwen en dergelijke. Het

	1. Ad-hoc	2. Speerpunt	3. Afdelingsgewijs	4. Strategisch	5. Pro-actief
Directie	---	Schenkt aandacht aan beveiliging	Verantwoordelijkheid budgetten voor beveiliging duidelijk	Infobeveiliging is onderdeel van de organisatiestrategie	idem
Management beveiliging	---	---	Basisbeveiliging: maatregelenpakket beschreven	Hulpmiddelen en Classificatie-norme beschikbaar	Ontwikkeling v informatievoorziening, integraal met de informatievoorziening
Mgt Faciliteiten	---	Organisatie en procedures voor onderhoud en verbetering	idem	Extra beveiliging: standaard maatregelenpakketten beschikbaar	idem
Mgt Gebruikers	---	---	Overzicht van eisen processen, informatiesystemen e beveiliging	Inzet maatregelenpakketten op basis van budgettaire afweging	idem
Werkvloer gebruikers	Voert onbeschreven beveiliging uit	idem	Voert beschreven beveiliging uit	idem	idem
Werkvloer faciliteiten	Voert onbeschreven beveiliging uit	Voert beschreven beveiliging uit	idem	idem	idem

Figuur 4: Kenmerken per fase

afschermen van bedrijfsnetwerken met firewalls tegen het Internet en zijn hackers en crackers, is ook een onderwerp dat thuishoort in deze fase. Het betreffende lijnmanagement heeft het belang van de informatiebeveiliging onderkend en bepleit budgetten voor een betere beveiliging bij de directie.

Deze fase wordt gekenmerkt door de formalisering van financiële procedures en de intrede van ITIL-procedures (of vergelijkbaar) binnen rekencentra en tussen rekencentra en gebruikersafdelingen. Informatiebeveiliging is in deze fase een onderdeel van het kennisgebied van de betreffende afdeling en richt zich daardoor op de technieken van die afdeling, of deze nu financieel of computertechnisch zijn. Risicobeperking vanuit het perspectief van de betrokken afdelingen staat daardoor voorop (defensieve aanpak van informatiebeveiliging). De inhoudelijke kennis over informatiebeveiliging is versnipperd over de ondersteunende functies en is gespecialiseerd. Zo treft men binnen personeelszaken vaak iemand aan met kennis van privacywetgeving, binnen het rekencentrum iemand met kennis van rekencentrumprocedures en dergelijke. De versnippering van deze kennis van informatiebeveiliging over de afdelingen kan tot kennisleemten leiden.

Door de inzet van de betreffende lijnmanager of door externe factoren (bij de overheid: rapport rekenkamer, eisen van klanten, privacywetgeving) wordt de directie

zich bewust van het bestaan van risico's op andere plaatsen in de organisatie. Er groeit op directieniveau behoefte aan een overall inzicht en een overall beveiliging.

Fase 3: De afdelingsgewijs gemanagede beveiliging.

In deze fase wordt de beveiliging uitgerold over de gehele organisatie. Uit oogpunt van haalbaarheid wordt aangehaakt bij bestaande structuren en procedures. Deze fase wordt gekenmerkt door de professionalisering van beveiligingsprocedures bij gebruikersafdelingen. Deze aanpak vereist commitment van

de directie omdat dit een forse omslag van werken met zich meebrengt.

De aandacht verschuift van de techniek naar de bedrijfsdoelstellingen van de informatiebeveiliging die de prioriteiten voor het beveiligingsniveau moeten bepalen. Door ontbrekende beveiligingsnormen blijkt het in de praktijk echter nog lastig om overdreven beveiliging ongedaan te maken of om onaanvaardbare risico's te verhelpen. Zo blijven te sterk beveiligde servers, met hoge beheerskosten, bestaan en worden te grote risico's geaccepteerd met het argument, dat 'we dit al jaren zo doen en dat er nog nooit iets is gebeurd'.

Soms wordt het wiel op meerdere plaatsen tegelijk uitgevonden als lijnafdelingen voor de stafsysteem (financiën, personeel) die zij op hun afdeling gebruiken, beveiligingsprocedures gaan ontwikkelen. De ondoelmatigheden laten de noodzaak zien van een informatiebeveiligingsspecialisatie, die kijkt naar alle facetten van de bedrijfsvoering en regelgeving. Het kennisgebied van de informatiebeveiligers begint te verschuiven ten opzichte van de vorige fase doordat gebruikerswensen moeten worden vertaald in maatregelen in of rondom informatievoorziening. Informatiebeveiliging wordt daardoor meer en meer een kennisgebied, waarin beveiligingsniveaus en maatregelen moeten worden afgeleid uit de bedrijfsbehoefte (een strategische aanpak van de informatiebeveiliging).

Maatschappelijk belang.

De eisen die de maatschappij stelt, zijn niet eenvoudig onder één noemer te vatten. De Wet Bescherming Persoonsgegevens geeft een reeks voorbeelden, zoals het recht om gegevens over jezelf te raadplegen en zo nodig te doen corrigeren. In aanvulling daarop eist het College Bescherming Persoonsgegevens dat biometrische informatie, zoals gegevens over vingerafdrukken en dergelijke, alleen in gecodeerde vorm mag worden geregistreerd op een chipkaart, die eigendom blijft van de betrokkene. Privacybelangen stellen een grens aan de economisch interessante verhandelbaarheid van gegevens.

Betrouwbaarheid kent echter meer aspecten. Zo moeten informatiesysteem soms in staat zijn om de opsporing van strafbare handelingen te ondersteunen, door het registreren en het langdurig bewaren van aanloggegevens. In de jaren vlak voor de millenniumwisseling werd aan organisaties met maatschappelijk belangrijke systemen, zoals banken en ziekenhuizen een verantwoordingsplicht opgelegd over de millenniumbestendigheid van hun informatievoorziening.

Voor organisaties waarin de afdelingen (business units) een zeer hoge mate van autonomie hebben kan dit het eindstation zijn. De hoge kosten van beveiliging leiden er echter vaak toe dat een efficiëncyslag nodig is.

Fase 4: Strategische gemanagede informatiebeveiliging. In deze fase ontstaat aandacht voor de doelmatigheid van informatiebeveiliging. Er worden gezamenlijke, kostenbesparende standaards ontwikkeld en toegepast door de in de vorige fase ontstane discipline van informatiebeveiligers. Ook worden taken en verantwoordelijkheden uit efficiëntie-oogpunt belegd op een andere plaats in de organisatie. Zo ontstaan pakketten van samenhangende maatregelen voor informatievoorziening, huisvesting et cetera voor de verschillende klassen van beveiligingseisen die de organisatie onderkent. Langs deze weg worden ook *make or buy*-beslissingen mogelijk voor onderdelen van de informatiebeveiliging zoals het inrichten en onderhouden firewall-software en het bewaken van de operationele firewall. Het overzicht van beveiligingsmaatregelen in de gehele organisatie, dat in de vorige fase is ontstaan, helpt hierbij doordat hieruit de *best practices* zijn te destilleren. Door de maatregelpakketten van een prijs te voorzien, ontstaat een basis voor nieuwe procedures waarbij gebruikers het gewenste beveiligingsniveau kunnen 'kopen' onder gelijktijdig aangaan van de verplichting in de eigen afdeling aansluitende beveiligingsprocedures in te zetten.

Voor organisaties met een normale afhankelijkheid van ICT kan dit het einddoel van de informatiebeveiliging zijn. Organisaties die zich onderscheiden door het behalen van strategische voordelen uit ICT moeten echter meer toekomstgericht werken. Daarvoor is fase 5.

Fase 5: De pro-actieve informatiebeveiliging.

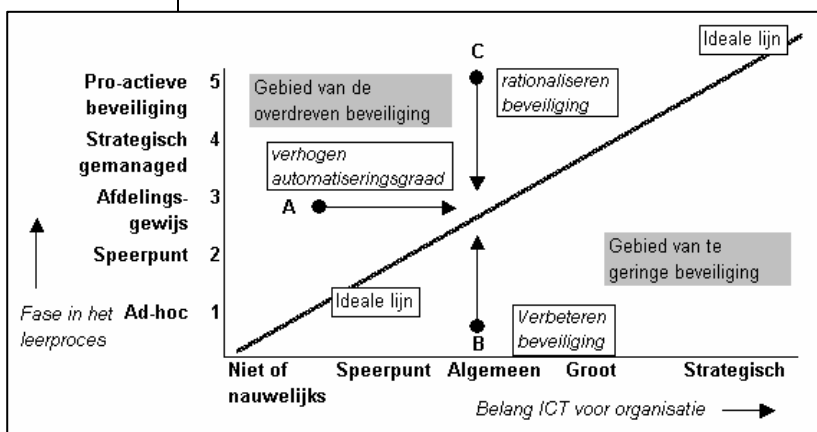
In de laatste fase is informatiebeveiliging meer dan een aanvulling op een reeds ontworpen informatievoorziening: het wordt een ontwerpcriterium. Vanaf het opstellen van de bedrijfsbrede ICT-strategie wordt informatiebeveiliging meegenomen. De organisatie in deze fase volgt trends in de informatiebeveiliging en

anticipeert op risico's. Elke strategie wordt getoetst op potentiële beveiligingsrisico's.

Met de normen en standaardmaatregel-pakketten die zijn ontstaan in de vorige fase, wordt informatiebeveiliging integraal meegenomen in vernieuwingsprojecten. Daardoor is het budget dat expliciet is vrijgemaakt voor informatiebeveiliging relatief gering en voornamelijk bestemd voor onderhoud van hulpmiddelen en trendonderzoek.

Wat is de ideale fase?

Er is een rechtstreeks, positief verband tussen de informatiebeveiliging en het belang van informatievoorziening voor de organisatie (zie figuur 5).



Figuur 5: Het gebruik van het groeimodel bij beleidsbepaling

In het ene uiterste is informatievoorziening nauwelijks van belang en kan de beveiliging zich beperken tot ad hoc maatregelen.

In het andere uiterste (informatievoorziening neemt een strategische positie in) biedt een integrale benadering van ontwerp en beveiliging efficiënte en effectieve mogelijkheden voor bestaande beveiligingsproblemen.

In figuur 5 geeft een rechte lijn het ideale verband weer tussen het belang van informatievoorziening en het niveau van informatiebeveiliging. Deze grafiek is hulpmiddel bij een analyse van de aansluiting van de bestaande beveiliging op het belang van de informatiebeveiliging van de organisatie. Deze lijn scheidt de twee gebieden van te geringe informatiebeveiliging en die van de overdreven informatiebeveiliging.

Betrouwbare informatievoorziening van strategisch belang.

Betrouwbaarheid als eigenschap van een informatiesysteem is een verzamelbegrip voor beschikbaarheid, exclusiviteit en integriteit. Betrouwbaarheid moet adequaat zijn voor de eisen die de bedrijfsvoering stelt. Zo werkt een hapering van een logistiek systeem direct door op een bedrijfsvoering die is gebaseerd op lage voorraden en korte levertijden. In de ogen van de klant heeft betrouwbaarheid ook te maken met vertrouwen. Zo stelde Microsoft recentelijk de hotmail-abonnees op de hoogte van de gang van zaken rondom een serie geslaagde hackpogingen en de inmiddels ondernomen tegenacties. Op deze wijze werd het vertrouwen behouden. Voor organisaties waarin informatievoorziening een belangrijke rol speelt, is betrouwbaarheid een onderdeel van de bedrijfsstrategie omdat falende informatievoorziening zich vertaalt naar verminderd toekomstperspectief. Zo daalde de aandelenkoers van de Amerikaanse Internetveiling Ebay toen de informatievoorziening een aantal malen uitviel.

Het gebruik van het groeimodel

Een verbeterproces van informatiebeveiliging heeft de meeste kans van slagen als de inspanningen zich concentreren op de gebieden waar het grootste rendement te verwachten is. Deze gebieden worden gevonden door de volgende drie vragen te beantwoorden:

1. *Waar staat men op dit moment?*

Met behulp van het voorgaande wordt nagegaan over welke informatiebeveiliging men beschikt en wat men in de organisatie nodig heeft. Het model wordt in deze stap gebruikt als referentiekader bij een toets van de huidige situatie;

2. *Waar moet men, gezien het belang van informatievoorziening, naar toe?*

Uit de risico's van de huidige situatie of uit het bedrijfsbrede ICT-beleid kan het juiste belang van de informatievoorziening worden afgeleid. Het model wordt gebruikt als referentiekader bij de beeldvorming over de toekomstige informatiebeveiliging.

3. *Wat is de meest effectieve veranderstrategie om dit einddoel te bereiken?*

De IST en de SOLL situatie bepalen de aanpak die nodig is om de verandering te bereiken. Daarbij zijn in de praktijk drie hoofdrichtingen te onderkennen (zie figuur 4). Iedere hoofdrichting vereist een geheel eigen motivering door directies om de organisaties mee te laten gaan in de gewenste veranderingsprocessen:

A. *De inhaalslag*, waarin tekortschietende informatiebeveiliging wordt verbeterd. Bij dit soort trajecten heeft de organisatie gewoonlijk al kennisgemaakt met forse problemen. Deze problemen leveren een goed motief voor het verandertraject. Een bijzondere omstandigheid kan zijn dat medewerkers in een organisatie ontkennen of bagatelliseren dat zaken fout lopen. In dat geval zal een aanvullend bewustwordingsprogramma noodzakelijk zijn;

B. *De rationalisering*, waarin overdreven informatiebeveiliging wordt vereenvoudigd; bijvoorbeeld is dit soms nodig bij organisaties die kort geleden zijn begonnen met netwerken en de beveiliging hebben aangepakt zoals dat op een cursus netwerkbeheer wordt verteld, zonder te kijken naar de noodzaak in de specifieke situatie. De betrokken technici vormen gewoonlijk de grootste tegenstanders van rationalisering omdat een verandering al snel het gevoel geeft dat men het in het verleden niet goed gedaan heeft. Een veranderingstraject maakt meer kans op succes als het start met de erkenning dat de te zware beveiliging een noodzakelijk leerproces is geweest;

C. *De sprong voorwaarts*, waarin de afhankelijkheid van de primaire processen van informatievoorziening veel groter wordt, zoals bij de invoering van e-commerce. Een herijking van informatiebeveiliging is hiervoor een noodzakelijke randvoorwaarde. Voor de organisatie kan de sprong voorwaarts overdreven overkomen,

D. zeker als er weinig problemen zijn met de huidige beveiliging. De noodzakelijke motivatie wordt gemobiliseerd door voor de betrokkenen inzichtelijk te maken wat de risico's zijn van een falende informatievoorziening in de nieuwe situatie. Dit kan bijvoorbeeld door te wijzen op de nieuwe bedreigingen en door veel hogere eisen te stellen aan de back-office.

Tot besluit

Verbeteren van informatiebeveiliging is een gecompliceerd proces. Uiteraard is de werkelijkheid altijd ingewikkelder dan het hiervoor geschetste model, dat dan ook met de nodige voorzichtigheid en kennis van zaken moet worden gebruikt. Het model is een eerste aanzet voor een procesmatige benadering van informatiebeveiliging en zal nog veel meer aan de praktijk getoetst moet worden dan nu is gebeurd. De auteurs staan open voor suggesties en andere inzichten.

Anton Griffioen is adviseur informatiebeveiliging van het Ministerie van VROM en Jaap van der Wel is managing partner bij Comfort-IA. Reacties: anton.griffioen@dio.cs.minvrom.nl of jvdwel@comfort-ia.nl.

Dit artikel is eerder verschenen in Informatiebeveiliging Praktijkjournaal, nr. 3/2000, en in IT Beheer Praktijkjournaal, nr. 4/2000.

Literatuur

1. 'Implementatie VIR bij het Ministerie van VROM', Anton Griffioen, Willem Velt en Jaap van der Wel, Informatiebeveiliging Praktijkjournaal nr. 1, 2000, pag. 19.