Waarom lukt het niet (zuinig) te beveiligen?

Ir. P. Kornelisse RE CISA

Dit artikel is een vervolg op het artikel 'Zuinig beveiligen' ([Korn03]), dat reeds eerder in Compact is verschenen. In het voorgaande artikel is aangegeven op welke wijze organisaties zuinig de beveiliging kunnen realiseren. In het thans voorliggende artikel wordt ingegaan op de oorzaken waardoor (zuinig) beveiligen bij menige organisatie toch (nog) niet is gelukt.

Inleiding

Ir. P. Kornelisse RE CISA
is director bij KPMG IT Advisory in Amstelveen en verantwoordelijk voor IT Security Dienstverlening. Hij is in het bijzonder verantwoordelijk voor de groep die zich richt op de beveiliging en beheersing van ICT-infrastructuren, in de vorm van zowel advies- als auditdiensten. Dit betreft onder andere ethical hacking, QA- en beoordelingsdiensten inzake netwerk- en platformbeveiliging (security baselines), zoals voor internetomgevingen, Windows en Unix.

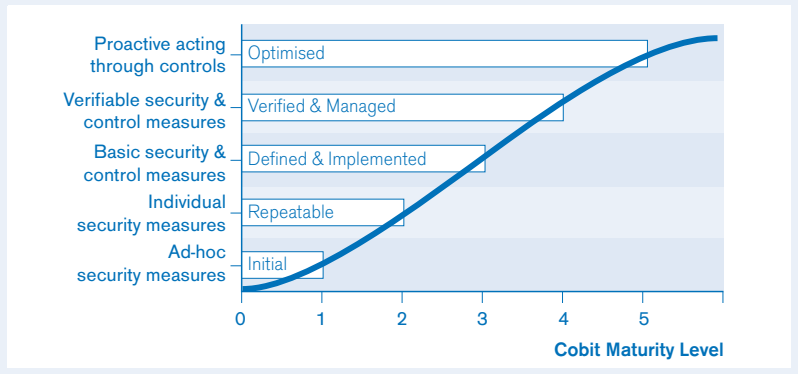
kornelisse.peter@kpmg.nl

Organisaties hebben in de praktijk ten minste enige mate van IT-beveiliging gerealiseerd. Daarmee is in vele gevallen echter nog geen effectieve beveiliging tot stand gebracht, omdat vaak nog beveiligingslekken aanwezig zijn die vanaf extern of intern kunnen worden doorbroken.

In het voorgaande artikel over zuinig beveiligen ([Korn03]) zijn adviezen gegeven om essentiële beveiligingsmaatregelen te treffen, opdat met beperkte middelen toch een effectieve beveiliging kan worden gerealiseerd:

- *Fase 1 – Inrichten versterkte preventieve beveiligingsmaatregelen*
  - opstellen van informatiebeveiligingsbeleid en inrichten van de beveiligingsorganisatie;
  - selecteren van (hoog)gevoelige informatie en IT-middelen;
  - instrueren van gebruikers over informatiebeveiliging;
  - formaliseren van kritieke beheerprocessen;
  - versterken van de beveiliging van de IT-infrastructuur.
- *Fase 2 – Versterken monitoring van beveiliging*
  - kanaliseren van verantwoordingsinformatie betreffende de gerealiseerde kwaliteit van informatiebeveiliging;
  - testen van de effectiviteit van de getroffen maatregelen.

Het blijkt voor organisaties moeilijk de eerstgenoemde fase te doorlopen en daarmee een effectieve beveiliging te realiseren, terwijl hiermee in de praktijk nog niet eens het volwassenheidsniveau van *aantoonbare beheersing* (zie figuur 1) betreffende IT-beveiliging wordt gerealiseerd. En juist dat niveau van volwassenheid van de IT-beveiliging is nodig in bijvoorbeeld SOX- ([USSE03]) en



Figuur 1. Volwassenheidsniveaus van IT-beveiliging.

Tabaksblat-gerelateerde ([Cocg03] omgevingen, evenals in de financiële sector ([DNB01]).

Het blijkt moeizaam het niveau van *aantoonbare beheersing* van de IT-beveiliging te halen, laat staan op een efficiënte wijze en economisch verantwoord. Toch, een aantal organisaties is in staat gebleken *aantoonbare beheersing* van IT-beveiliging op effectieve én efficiënte wijze te realiseren. Uit onze ervaring gedurende de afgelopen jaren blijkt dat organisaties die hierin slagen, met name de volgende kenmerken hebben:

- Deze organisaties gaan uit van eigen kracht en richten IT-beveiliging in uit vrije wil en wachten niet op wet- en/of regelgeving.
- De gewenste wijzigingen worden gerealiseerd in een eigen tempo, waardoor in plaats van kortetermijn- direct langetermijnoplossingen tot stand worden gebracht.
- Deze organisaties kunnen wijzigingen absorberen, omdat deze stapsgewijs worden ingevoerd, in plaats van (te) veel wijzigingen tegelijkertijd.
- Er wordt door deze organisaties onderkend dat IT-applicaties en gegevens verschillende gevoeligheden kunnen hebben betreffende beschikbaarheid, integriteit en vertrouwelijkheid. Op basis hiervan vindt risicogebaseerd scoping van relevante ICT plaats, vervolgens vindt compliancegebaseerd implementatie van beveiligingsmaatregelen plaats.

Tabel 1. Kenmerken van ambitieniveaus.

Ambitieniveau	Toelichting
Geoptimaliseerd	– Organisatie heeft aantoonbare beheersing ingericht – Lerende organisatie wordt tot stand gebracht
Aantoonbare beheersing	– Door organisatie zelf gecontroleerd of gedefinieerde processen daadwerkelijk operationeel zijn
Gedefinieerde processen	– Organisatie heeft IT-beheerprocessen en beveiligingsstandaarden voor ICT-componenten gedocumenteerd
Herhaalbaar	– Organisatie stabiel ingericht – Processen redelijk consequent uitgevoerd op basis van ervaring
Ad hoc	– Organisatie instabiel – Veelal kortetermijnacties gedefinieerd – Vaak 'brandjes' geblust

Ambitieniveaus

Veel organisaties hebben, door wijzigingen in wet- en regelgeving, evenals de cultuur in de samenleving, een cultuurverandering ervaren als gevolg waarvan de volwassenheid van IT-beheersing en daarmee IT-beveiliging diende te worden verhoogd naar het niveau van *aantoonbare beheersing*, onder andere onder invloed van SOX en Tabaksblat. Het ambitieniveau van *aantoonbare beheersing* is daarmee een gegeven. Veel organisaties bevonden zich echter op een grote afstand van dit gewenste niveau, namelijk op het niveau tussen *ad hoc* en *gedefinieerde processen*.

Er is voor die organisaties dan ook een grote stap te maken. Organisaties die onder invloed van SOX in korte tijd van tussen *herhaalbaar* en *gedefinieerde processen* naar *aantoonbare beheersing* dienden te groeien, ervoeren hierbij dan ook groeipijnen. Er ontstond veel druk in deze organisaties en wijzigingen werden nogal eens 'kort door de bocht' gerealiseerd, waardoor inefficiënties optraden.

Het is van belang voor organisaties vast te stellen welk ambitieniveau betreffende de volwassenheid van IT-beheersing gewenst is, gegeven de geldende wet- en regelgeving en de gewenste risicobeheersing binnen de organisatie.

Er was ook veel onduidelijkheid over de implicaties van het gedefinieerde ambitieniveau:

- Voor welke beheerprocessen en ICT-objecten geldt het ambitieniveau van *aantoonbare beheersing* (scoping)?
- Welke eisen dienen te worden gesteld aan de ICT-objecten binnen de scope?

Deze onderwerpen worden hierna behandeld.

Scoping

Het blijkt moeizaam voor organisaties om op adequate wijze de relevante scope vast te stellen betreffende de ICT-beheerprocessen en ICT-componenten die op het niveau *aantoonbare beheersing* dienen te zijn ingericht ([Korn05]). In de praktijk dient een organisatie hiertoe de relevante IT-applicaties vast te stellen, door per IT-applicatie het materiële risico voor het bijbehorende bedrijfsproces te bepalen, bijvoorbeeld door het evalueren van operationele risico's en risico's betreffende financiële rapportages.

Op basis van de onderkende IT-applicaties kunnen eenvoudig de applicatiespecifieke ICT-componenten worden vastgesteld; dit zijn de aan de IT-applicaties gerelateerde applicatie- en databaseservers.

Voor generieke ICT-infrastructuurcomponenten (ICT-componenten die door meerdere applicaties worden gebruikt, zoals bedrijfsnetwerken en beheerplatforms) blijkt dit moeizamer, met name door druk binnen de organisatie om ICT-componenten out-of-scope te verklaren, waardoor *aantoonbare beheersing* eenvoudiger haalbaar lijkt te worden.

Bij het selecteren van de relevante generieke ICT-infrastructuur is het van belang af te wegen welke ICT-componenten op de paden van de eindgebruikers tot de data en van de beheerders tot de te beheren objecten liggen. Dit vraagt om een complexe en uitgebreide analyse. Efficiënter en effectiever blijkt het de essentiële beveiligingsarchitectuur van de ICT-infrastructuur te definiëren, hetgeen veelal resulteert in een scoping van het interne netwerk, identity management en security monitoring.

Weliswaar is daarmee de scoping van de generieke ICT-componenten slagvaardig uitgevoerd, echter, de meeste organisaties ervaren deze drie ICT-componenten als lastig om in scope te verklaren. De reden hiervoor ligt veelal in het feit dat *aantoonbare beheersing* voor deze ICT-componenten thans niet is gerealiseerd.

Bijvoorbeeld netwerkkoppelingen met derde partijen worden vaak als risicovol gezien en verdienen veelal een aantoonbare beheersing. Toch, diverse organisaties hebben geen juist en volledig overzicht van deze externe netwerkkoppelingen en controleren externe netwerkkoppelingen ook niet op gestructureerde wijze.

Voor scoping is het van belang eerst de bij de relevante bedrijfsprocessen behorende essentiële IT-applicaties te selecteren. Op basis van de onderkende essentiële IT-applicaties worden de onderliggende applicatiespecifieke IT-componenten geselecteerd. Tevens worden de generieke ICT-componenten geselecteerd, die samen de essentiële beveiligingsarchitectuur van de organisatie vormen. De bij de IT-applicaties en ICT-componenten horende IT-beheerorganisaties en -processen horen tot slot ook binnen de scope.

Veelvoorkomende knelpunten

Procesmatige knelpunten

Tot de knelpunten van dit type behoren:
- Identity & Access Management;
- ICT-component security;
- Change management.

Identity & Access Management
Identity & Access Management dient te borgen dat alleen volgens een strikte procedure de eindgebruikers en beheerders met passende bevoegdheden in de systemen worden geïmplementeerd, en dat periodiek wordt gerapporteerd en gecontroleerd of alleen de juiste eindgebruikers en beheerders en bevoegdheden zijn geïmplementeerd.

Het is moeilijk de relevante scope van beheerprocessen en componenten vast te stellen

Veel organisaties werken bij eindgebruikers (nog) niet (integraal) met single sign-on en Role Based Access Control, met als gevolg dat het verkrijgen van een volledig overzicht van gebruikers en hun bevoegdheden niet effectief en efficiënt kan plaatsvinden. Bijgevolg ontvangen applicatie-eigenaren en afdelingshoofden niet of niet regelmatig overzichten en worden daardoor de geïmplementeerde gebruikersaccounts en gebruikersbevoegdheden niet periodiek gecontroleerd.

Voor beheerders ligt dit vaak nog moeilijker. Voor elke ICT-component, van database tot server tot netwerkcomponent, is het gewenst de beheerderaccounts en beheerderbevoegdheden te controleren. Echter, de beheerderaccounts zijn veelal niet eenduidig geadministreerd en worden veelal ook niet regelmatig gerapporteerd.

Het is van belang Identity & Access Management voor eindgebruikers en beheerders dusdanig op te zetten, dat op effectieve en efficiënte wijze verantwoordingsinformatie kan worden opgeleverd.

Naast het rapporteren en controleren van bevoegdheden wordt nogal eens onderkend dat bij diverse organisaties de beheerders met hoge bevoegdheden een vertrouwensfunctie hebben, hetgeen betekent dat een beheerder activiteiten kan uitvoeren die niet door een ander (kunnen) worden gecontroleerd. Dit is niet gewenst voor het ambitieniveau van *aantoonbare beheersing*.

ICT-component security
Het aantoonbaar beveiligen van ICT-componenten vraagt om twee belangrijke activiteiten:
- implementatie van ICT-componenten volgens security baselines;
- patch management voor alle ICT-componenten.

Het is gewenst voor elk type van de aanwezige ICT-componenten een security baseline te hebben, de ICT-componenten conform de gedefinieerde security baselines te implementeren en periodiek te controleren of ICT-componenten conform baselines zijn geïmplementeerd.

Diverse organisaties blijken echter niet te beschikken over (alle relevante) security baselines, bijvoorbeeld doordat bepaalde ICT-componenten zoals mainframes en netwerkcomponenten slechts in beperkte mate voorkomen.

Daarnaast hebben veel organisaties controle van de compliance van ICT-componenten aan de bijbehorende security baselines niet ingeregeld en/of geautomatiseerd, waardoor controle van compliance aan security baselines niet plaatsvindt of dusdanig inefficiënt blijkt te zijn dat deze niet voldoende regelmatig plaatsvindt.

Wat betreft patch management blijkt dat organisaties nieuwe patches niet of laat analyseren en niet of niet tijdig implementeren, waardoor de organisaties meer gevoelig zijn voor virussen en inbrekers.

ICT-component security is één van de voornaamste preventieve maatregelen om te voorkomen dat derden (personen van buiten de organisatie) of interne medewerkers op ongeautoriseerde wijze de ICT-omgeving van de organisatie binnendringen. Om dit te voorkomen dienen ICT-componenten conform security baselines te worden geïmplementeerd, hetgeen ook periodiek dient te worden gecontroleerd, in samenhang met de geïmplementeerde patches.

Change management

Veel organisaties hebben voor change management een duidelijke procedure vastgesteld. In de praktijk wordt echter onderkend dat naast reguliere changes ook plaatsvinden:

- urgente changes met beperkte tot geen goedkeuring vooraf, die achteraf dienen te worden verantwoord, evenals
- kleine wijzigingen in de productieomgeving, die niet via change management verlopen.

Het lastige van urgente changes en kleine wijzigingen in de productieomgeving is, dat het niet altijd duidelijk is wanneer een change als urgent of klein mag worden geclassificeerd. Dit vraagt om duidelijke spelregels, die echter nogal eens ontbreken en/of niet eenduidig zijn.

Het is niet altijd duidelijk wanneer een change als regulier, urgent of klein mag worden geclassificeerd

De meeste organisaties zijn niet in staat ongeautoriseerde changes te detecteren door het ontbreken van hulpmiddelen hiertoe, terwijl dergelijke hulpmiddelen wel bestaan (bijvoorbeeld checksumprogrammatuur van TripWire).

Wijzigingen dienen adequaat te worden getest, en bijgevolg zijn gelijke omgevingen gewenst voor het testen van wijzigingen en verwerking in productie. Echter, in de praktijk zijn deze omgevingen niet altijd in voldoende mate gelijk, waardoor de kwaliteit van het testen wordt beperkt.

Bij een change zijn diverse medewerkers betrokken, die allen een deel van de documentatie verzorgen en een deel van een change testen. Daardoor komt het nogal eens voor dat voor een change niet alle documentatie betreffende ontwerpen en testen is gebundeld, hetgeen controle van een change achteraf bemoeilijkt.

Bij change management dienen duidelijke spelregels te zijn vastgesteld voor reguliere, urgente en kleine wijzigingen. Voor kritieke bestanden dient te kunnen worden vastgesteld of zich wijzigingen hebben voorgedaan.
Betreffende alle wijzigingen dient de bijbehorende documentatie te worden verzameld en bewaard, opdat achteraf een change kan worden gecontroleerd.

Technische knelpunten

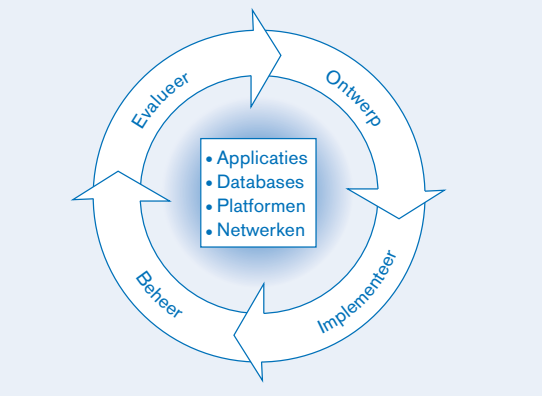
Als gevolg van onvolwassenheid van beheerprocessen, zoals het ontbreken of het niet adequaat inrichten van een aantal beheerprocessen, ontstaan nogal eens technische knelpunten die de beveiliging van de ICT-omgeving ondermijnen. Op technisch gebied is het daarom van belang een eenvoudige securityarchitectuur en IT-infrastructuur te handhaven. Dit vereist het proactief ontwerpen van benodigde IT-voorzieningen, bijvoorbeeld netwerkfiltering (extern en intern), authenticatievoorzieningen (Active Directory, Radius) en security monitoring (verzamelen, controleren en rapporteren inzake logging, evenals controleren van systeemconfiguraties, verzamelen en rapporteren inzake afwijkingen).

Een organisatie dient een eenvoudige securityarchitectuur en IT-infrastructuur te ontwerpen, te implementeren en in stand te houden.

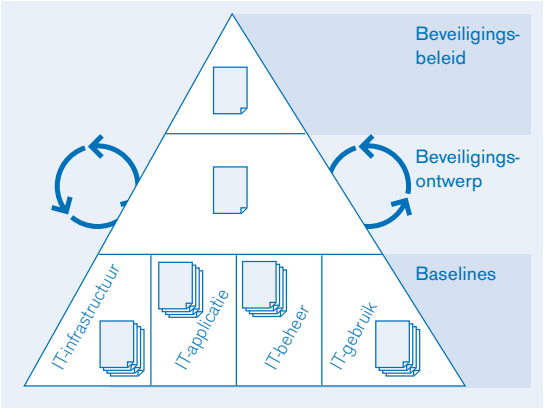
Oorzaken van geconstateerde knelpunten

Op basis van onze ervaringen bij vele organisaties blijkt het gerealiseerde volwassenheidsniveau van IT-beveiliging steeds weer te worden beïnvloed door vier aspecten, die juist een basis voor IT-beveiliging zouden kunnen leggen:

- Sponsoring en leiderschap betreffende IT-beveiliging ontbreekt, waardoor gestructureerde beheersing van IT-beveiliging uitblijft. Ad hoc worden bij strikte noodzaak onsamenhangende beveiligingsoplossingen gerealiseerd.



Figuur 2. Cyclus van IT-beveiliging.



Figuur 3. Inrichting van IT-beveiliging.

• Beveiliging is veelal IT-gedreven; de business is niet of onvoldoende betrokken, waardoor beveiliging niet wordt gebaseerd op het risicoprofiel van de organisatie en haar bedrijfsprocessen.
• Een organisatie heeft geen ambitieniveau vastgesteld betreffende de beheersing van IT-beveiliging, waardoor het belang van het vastleggen van procedures en beveiligingsstandaarden niet wordt erkend, evenals het belang van controle op naleving hiervan.
• Een organisatie onderkent IT-beveiliging niet als een continu proces maar als een eenmalige gebeurtenis. Als gevolg hiervan ontbreekt veelal een gestructureerd (jaar)plan om IT-beveiliging op niveau te houden. In figuur 2 is IT-beveiliging als een continu proces weergegeven.

Als een adequaat ambitieniveau voor IT-beveiliging niet is vastgesteld, dan resulteert dit veelal in de diverse gebreken, zoals:
• Rapportage betreffende IT-beveiliging vindt niet plaats, waardoor zowel de werkvloer als het verantwoordelijke management niet worden geïnformeerd over mogelijke operationele knelpunten en de gevolgen daarvan.
• Structurele voorzieningen ontbreken, zoals een documentbeheersysteem en registratie- en rapportagevoorzieningen, waardoor informatie niet efficiënt en effectief toegankelijk is.
• Bij uitbesteding worden door de organisatie geen concrete eisen gesteld in contracten en/of SLA's.
• Bij nieuwe ontwikkelingen, bijvoorbeeld het gebruik van USB-geheugens, wordt geen beleid opgesteld en geïmplementeerd, waardoor nieuwe risico's ontstaan.

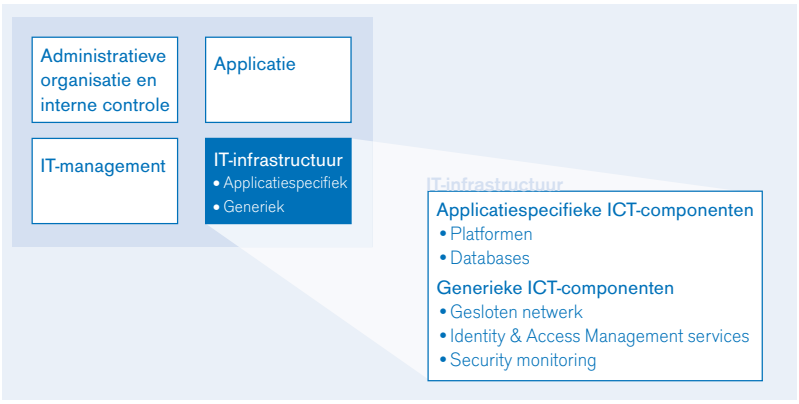
Aandachtspunten voor de organisatie

Afwachten tot wet- en/of regelgeving op een organisatie afkomt, vraagt om het behalen van een bepaalde mate van beveiliging in (te) korte tijd en werkt dan kostenverhogend. Door proactief zelf beveiliging ter hand te nemen, kunnen direct langetermijn- in plaats van kortetermijnoplossingen worden ingeregeld en kunnen tevens beveiligingsrisico's veelal efficiënter en effectiever worden gemitigeerd.

Een organisatie dient hiertoe de aansturing van IT-beveiliging te borgen. Dit vraagt om sponsoring vanuit de leiding van de organisatie en leiderschap van de verantwoordelijke voor IT-beveiliging. Voor de sturing zijn een informatiebeveiligingsbeleid en tactische beveiligingseisen nodig. Deze dienen op operationeel niveau te worden vertaald naar onder andere IT-beheerprocedures en systeemconfiguraties van IT-infrastructuurcomponenten.

Naast een adequate inrichting van IT-beveiliging is het van belang het ontworpen huis periodiek te evalueren, via interne controle (bijvoorbeeld op het punt van registraties en systeeminstellingen), risicoanalyses, penetratietests en IT-audits. Hiertoe is het van belang jaarlijks vast te stellen welke mate van zekerheid gewenst is betreffende IT-beveiliging, zowel wat de IT-beveiligingsprocessen als de feitelijk ingerichte IT-beveiliging op operationeel niveau aangaat.

Op het operationele niveau is het van belang voor de essentiële IT-applicaties de ontworpen en geïmplemen-



Figuur 4. Operationele aandachtsgebieden.

teerde maatregelen te inventariseren en te evalueren. Hierbij worden onderzocht: administratie en interne controle, IT-applicatieve maatregelen, IT-infrastructurele maatregelen en IT-beheermaatregelen (zie figuur 4).

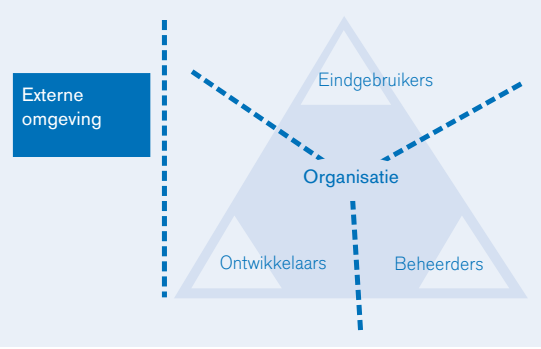
De wijze waarop IT-beheerprocessen en beveiligingsstandaarden worden gedocumenteerd en gedistribueerd, bepaalt mede de effectieve en efficiënte inzet van deze middelen binnen een organisatie.

In de praktijk blijken organisaties die expliciet eisen voor het opstellen van interne documentatie hebben gedefinieerd en voor distributie bijvoorbeeld een intranet hanteren, slagvaardiger te zijn. Dit kan nog verder worden versterkt als registraties en rapportages hierbij worden meegenomen.

Aandachtspunten voor de IT-auditor

Organisaties vragen in veel gevallen aan een IT-auditor om de huidige status van de IT-beveiliging te beoordelen. Een perfecte situatie wordt in de praktijk niet vaak aangetroffen, en de IT-auditor zal veelal diverse (operationele) bevindingen en aanbevelingen kunnen rapporteren.

Knelpunten betreffende de operationeel gewenste maatregelen dienen te worden gerapporteerd, bijvoorbeeld risico's betreffende IT-beheerprocessen en ongewenste systeeminstellingen van ICT-componenten.



Figuur 5. Vereiste functiescheidingen.

Daarnaast is het van belang aan het management van de organisatie de risico's te rapporteren ten aanzien van vertrouwelijkheid, betrouwbaarheid en continuiteit, onder andere door aan te geven welke functiescheidingen kunnen worden doorbroken, hoe groot de kans daarop is en met een inschatting van de mogelijke impact (bijvoorbeeld welke gegevens kunnen worden ontsloten, en/of welke gegevens en programma's kunnen worden gewijzigd, en/of welke bedrijfsprocessen kunnen worden verstoord).

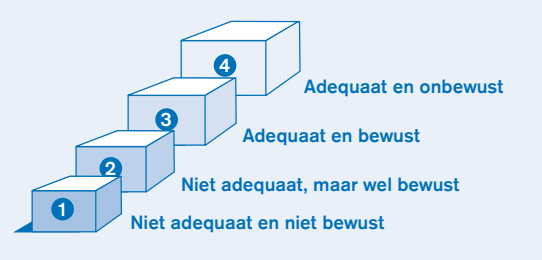
Het is ook van belang te beseffen wat de organisatie na het rapporteren door de IT-auditor vervolgens wenst, namelijk risico's onderkennen en keuzen maken betreffende de mate van en de wijze waarop aanbevelingen dienen te worden opgevolgd. Om te voorkomen dat een organisatie alleen geconstateerde operationele knelpunten oplost, dienen in het bijzonder ook de oorzaken van deze pijnpunten te worden geadresseerd. Hiertoe dient de IT-auditor te deduceren welke oorzaken ten grondslag liggen aan de geconstateerde operationele knelpunten. Dit betreft nogal eens het volgende:

- IT-beveiliging is niet gestructureerd ingericht, bijvoorbeeld richtlijnen, procedures en/of beleid (op onderdelen) ontbreken.
- Rapportages betreffende IT-beveiliging ontbreken, waardoor het management zich niet bewust is van risico's en prioriteitstelling betreffende verbeteringen niet adequaat plaatsvindt.
- IT-security is niet ingericht als een continu proces, bijvoorbeeld beveiligingsproblemen worden geïsoleerd opgelost.
- Gestructureerde vastlegging van documenten vindt niet plaats, waardoor het gebruik ervan beperkt blijft.

Tot slot

In de loop der jaren blijken diverse organisaties een hoog niveau van IT-beveiliging te hebben kunnen bereiken. Ook zijn er diverse organisaties die al jaren aan de slag zijn en bewust pogen een hoger niveau van beveiliging te realiseren, maar het lukt hen (nog) niet. Hierbij is veel geld tevergeefs uitgegeven en is mogelijk schade opgelopen.

Figuur 6. Ontwikkeling van besef inzake IT-beveiliging.



Het is van groot belang de consequenties van adequate IT-beveiliging onder ogen te zien, namelijk dat hierbij keuzen dienen te worden gemaakt, de flexibiliteit kan worden beperkt, maar ook het kwaliteitsbesef kan worden verhoogd, en dat daardoor nogal eens de efficiëntie en de effectiviteit en de slagvaardigheid van de organisatie kunnen worden verbeterd.

Alle betrokkenen van de organisatie dienen te beseffen dat IT-beveiliging een continu proces is en dat zij IT-beveiliging adequaat dienen te ondersteunen. IT-beveiliging blijft echter mensenwerk, hetgeen betekent dat individuen binnen de organisatie een transitie dienen te ondergaan van onbewust niet adequaat naar onbewust adequaat (zie figuur 6) betreffende IT-beveiliging. Hiermee wordt gestimuleerd dat de medewerkers van de organisatie op het punt van IT-beveiliging spontaan proactief handelen en op alle functies beveiliging verder brengen.

Wacht dan ook niet af, maar bepaal de eigen koers van de organisatie voor een efficiënte en effectieve beveiliging.

Literatuur

[Cocg03] Commissie corporate governance, *De Nederlandse corporate governance code*, 9 december 2003.

[DNB01] DNB, *Regeling organisatie en beheersing*, 29 maart 2001.

[Korn06] Ir. P. Kornelisse RE CISA en H. IJkel RE CISA CISSP, *Een inleiding tot integrated audit*, Compact 2006/2.

[Korn05] Ir. P. Kornelisse RE CISA, R.P.J. van den Berg RA en A.A. van Dijke, *SOX – Scoping van de relevante ICT*, Compact 2005/3.

[Korn04] Ir. P. Kornelisse RE CISA, *Security monitoring – De IT-infrastructuur aantoonbaar in control*, de EDP-auditor 2004/4.

[Korn03] Ir. P. Kornelisse RE, *Zuinig beveiligen?*, Compact 2003/4.

[USSE03] US Securities and Exchange Commission, *Final Rule: Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports*, Release Nos. 33-8238; 34-47986; IC-26068; File Nos. S7-40-02; S7-06-03, USA, June 2003.