Zuinig beveiligen?

Ir. P. Kornelisse RE

In dit artikel worden handvatten aangereikt waarmee een organisatie de beveiliging naar een hoger niveau kan brengen. Hierbij wordt het belang van specifieke maatregelen aangeduid op basis van opgedane ervaringen.

Inleiding

Beveiligen en Zeeuws Meisje gaan niet samen. Beveiligen is namelijk geen activiteit waarmee je zuinig kunt omgaan. Het is als onderdeel van risicomanagement een continu proces en geen eenmalige of tijdelijke activiteit.

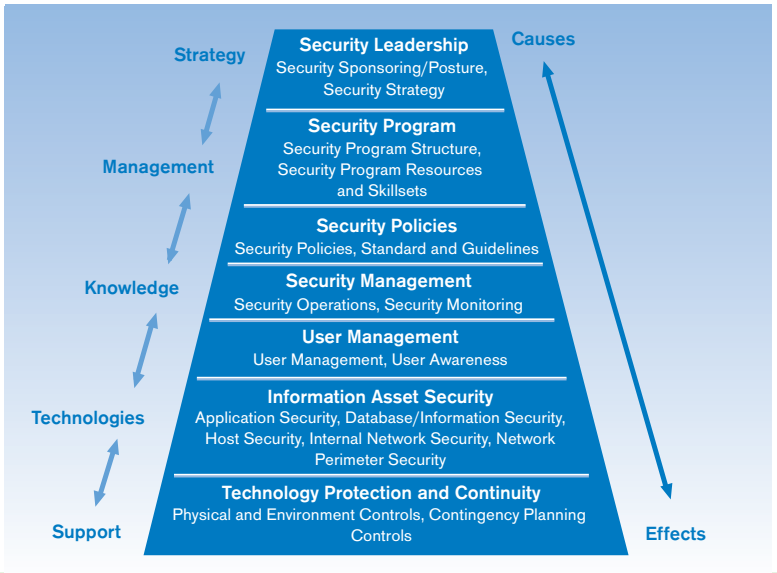
Beveiliging vraagt om het treffen van diverse maatregelen. In het KPMG Security Capabilities Model (figuur 1) zijn deze maatregelen aangegeven.

Een organisatie die beveiliging adequaat en efficiënt wil oppakken, zal alle lagen van het model ook daadwerkelijk moeten invullen en periodiek dienen vast te stellen in welke mate zij ten aanzien van informatiebeveiliging *in control* is.

Maar zou het niet mogelijk zijn zonder al te veel inspanning en kosten toch vooruitgang te boeken op het gebied van beveiliging? We weten uit de praktijk dat de realisatie van verbeteringen in de beveiliging op drie verschillende manieren mogelijk is, te weten:

- via grote projecten, zoals de implementatie van Public Key Infrastructure (PKI) en een Intrusion Detection System (IDS);
- via structurele projecten, die beveiliging topdown optuigen en structureel verankeren in de organisatie;
- via quick win-projecten, waarmee direct resultaat kan worden bereikt.

Figuur 1. KPMG's Security Capabilities Model.



Wellicht dat de laatste categorie, de quick win-projecten, mogelijkheden biedt. In dit artikel zal nader op deze categorie worden ingegaan. Uiteraard bevelen wij aan beveiliging uiteindelijk structureel op een dusdanige wijze op te tuigen, dat de organisatie aantoonbaar *in control* van haar beveiliging is en blijft.

Het nut van beveiliging binnen organisaties

Organisaties hebben bewust en onbewust vele redenen om beveiliging te regelen. Deze redenen zijn gerelateerd aan de impact die (onvoldoende) beveiliging kan hebben op de bedrijfsvoering. Hierbij kan worden gedacht aan het volgende:

- Een organisatie zal haar eigendommen en die van haar klanten willen beschermen. Denk aan bijvoorbeeld het intellectueel eigendom en bestanden met daarin klantgegevens.
- Een organisatie zal de van toepassing zijnde wet- en regelgeving willen volgen. Dit betreft bijvoorbeeld de Wet computercriminaliteit en de Wet bescherming persoonsgegevens, evenals de Regeling Organisatie en Beheersing voor het bankwezen.
- Beveiliging kan voor organisaties een onderscheidend kenmerk zijn, bijvoorbeeld voor hostingbedrijven van websites en andere dienstverleners, waardoor de selling points worden versterkt en meer omzet kan worden gerealiseerd.
- Als gevolg van adequaat getroffen beveiligingsmaatregelen wordt mede de continue beschikbaarheid van services ondersteund, bijvoorbeeld doordat ongewenste wijzigingen in de programmatuur worden voorkomen en inbrekers de computersystemen niet kunnen ontregelen.

Functiescheidingen

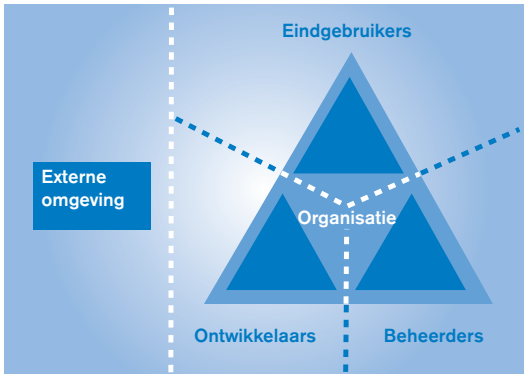
In de praktijk heeft beveiliging als nut dat een aantal gewenste functiescheidingen wordt gerealiseerd. In figuur 2 zijn deze functiescheidingen weergegeven.

In de eerste plaats dient een organisatie een functiescheiding te realiseren tussen de externe omgeving en de eigen organisatie. Dit betreft onder andere de beveiliging van externe koppelingen, zoals die met het internet. Een bedrijf heeft tegenwoordig echter vele externe koppelingen die dienen te worden beveiligd, zoals huurlijnen, ADSL-verbindingen en draadloze netwerken.

Binnen de eigen organisatie is het van belang dat eindgebruikers geen directe invloed kunnen uitoefenen op de gebruikte informatiesystemen en gegevens. Daarom is een functiescheiding tussen de eindgebruikers- en de automatiseringsorganisatie (bestaande uit ontwikkelaars en beheerders) van belang.

Daarnaast kennen we binnen de automatiseringsorganisatie de functiescheiding tussen ontwikkelaars en beheerders, om te waarborgen dat wijzigingen in de productieomgeving alleen volgens de geldende change-managementprocedures kunnen plaatsvinden.

Tot slot kennen we nog functiescheidingen tussen verschillende beheerders, zoals die voor het netwerk, specifieke servers, applicaties en databases.



Figuur 2. Functiescheidingen.

Beveiliging en risicobeheersing

Wat is eigenlijk het beveiligingsrisico als functiescheidingen niet afdoende worden gerealiseerd?
Het beveiligingsrisico kan worden bepaald met behulp van de volgende formule:

Beveiligingsrisico =
Kans van optreden bedreiging × Impact van bedreiging bij optreden

De kans van optreden van een bedreiging is afhankelijk van zowel de mogelijke omvang van de groep die de bedreiging effectueert als de eenvoud waarmee een bedreiging kan worden uitgevoerd.

Organisaties zullen bij het implementeren van beveiligingsmaatregelen 'zuinig' kunnen beveiligen, door met name maatregelen te treffen voor de gegevens en IT-middelen die een hoge(re) impact hebben als een bedreiging daadwerkelijk optreedt. Het is dan ook van belang om voor de gebruikte gegevens en de toegepaste IT-middelen de gevoeligheid te bepalen (zie kader 1).

Kader 1. Gevoeligheid van gebruikte gegevens en toegepaste IT-middelen.

Bij het bepalen van de gevoeligheid worden gewichten toegekend: **H**oog, **G**emiddeld en **L**aag voor de kwaliteitsaspecten continuïteit, betrouwbaarheid en vertrouwelijkheid. Uit pragmatische overwegingen zijn hier betrouwbaarheid en vertrouwelijkheid samengevoegd, immers beide leiden tot te treffen beveiligingsmaatregelen.

Continuïteit
De inschatting van de gevoeligheid inzake continuïteit richt zich op de tijd gedurende welke een informatiesysteem kan worden gemist (door uitval) zonder dat ernstige gevolgen optreden. Bij deze inschatting wordt rekening gehouden met de meest kritische periode waarin het informatiesysteem wordt gebruikt. Ook kan een onderscheid worden gemaakt tussen kleine en grote calamiteiten.

Hoog
Herstel is vereist binnen enkele minuten.

Gemiddeld
Herstel is vereist binnen enkele uren.

Laag
Herstel is vereist binnen langere tijd.

Betrouwbaarheid en vertrouwelijkheid
De gevoeligheid betreffende de betrouwbaarheid wordt beïnvloed door de schade die kan worden geleden in geval van toepassing van onbetrouwbare informatie en door de periode die nodig is om onjuist vastgelegde informatie te herstellen. Aantasting van de betrouwbaarheid kan plaatsvinden door het muteren van via het netwerk verzonden gegevens.

De gevoeligheid betreffende vertrouwelijkheid richt zich ten eerste op door derden opgelegde verplichtingen tot geheimhouding en de mate waarin financieel verlies zou kunnen worden geleden (indirect verlies door uiteindelijk verlies van marktaandeel, direct verlies door een reductie van opbrengsten of een verhoging van kosten).
De aandacht gaat hierbij voornamelijk uit naar kennisnemen van informatie door derden, veroorzaakt door het lezen van via het netwerk getransporteerde gegevens.

Hoog
Beslissingen op basis van onjuiste gegevens kunnen ernstige gevolgen hebben. Denk hierbij aan het productieproces, informatie van personeel en kritische financiële systemen. Een schending van een wettelijke verplichting tot behoud van vertrouwelijkheid (privacywetgeving) zou kunnen plaatsvinden.
Openbaar worden van gegevens zou een structureel verlies tot gevolg hebben.

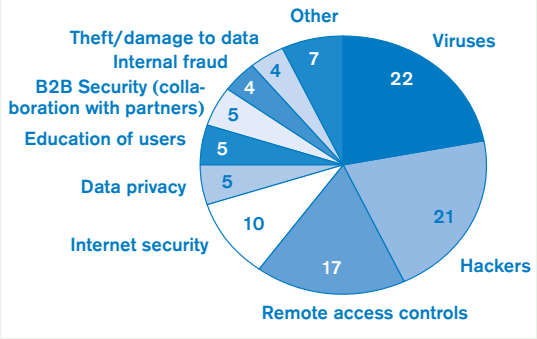
Gemiddeld
Onjuiste gegevens kunnen leiden tot foutieve beslissingen, maar de gevolgen zijn van beperkte omvang (lage kosten, relatief korte hersteltijd). Kennisnemen van gegevens door onbevoegden zou een incidenteel verlies veroorzaken.

Laag
Onjuiste gegevens zijn niet kritisch, kennisnemen van gegevens door onbevoegden heeft geen ernstige gevolgen.

In het navolgende wordt op basis van ervaringen geïnventariseerd wat op hoofdlijnen de kans van optreden van een bedreiging is, en welke maatregelen kunnen worden getroffen om deze kans van optreden te verkleinen.

Aard van de bedreigingen

Op basis van diverse security surveys kan worden gesteld dat met name externe bedreigingen als serieus worden ervaren. Uit een survey ([KPMG02]) blijkt dat maar liefst zeventig procent van door organisaties ervaren bedreigingen afkomstig is van buiten af en met name vanaf het internet.



Figuur 3. Door organisaties ervaren bedreigingen in procenten ([KPMG02]).

In de praktijk betreft dit met name de volgende bedreiging:

Te beperkt bewustzijn bij gebruikers van activiteiten die leiden tot het uitbreken van virussen en manipulatie van systemen
Eindgebruikers beseffen niet wat eigen handelingen tot effect kunnen hebben. Hierbij gaat het onder andere om het downloaden van programma's vanaf het internet en het openen van e-mailberichten van onbekende verzenders, waardoor virussen worden losgelaten op de werkplek van de eindgebruiker.
Virussen slagen overigens veelal in het doorbreken van beveiligingsmaatregelen doordat beschikbare patches niet of niet adequaat zijn geïmplementeerd.

Op basis van vele uitgevoerde penetratietests (ethical hacks) blijkt dat organisaties – ongeacht branche of omvang – blootstaan aan veelal dezelfde typen van bedreigingen. Dit betreft met name de volgende operationele bedreigingen:

Niet-gepatchte computers
Hierbij gaat het om computers waarop recente (en soms zelfs oude) patches die leveranciers beschikbaar stellen, niet zijn geïmplementeerd. Uit diverse bronnen blijkt dat met name een beperkt aantal zwakheden in programmatuur herhaaldelijk heeft geresulteerd in computerinbraken ([SANS03]).

Onvoldoende beveiligde beheeromgevingen
Kritieke servers en pc's van gebruikers worden veelal bewust beveiligd. Echter, de delen van de technische infrastructuur die via andere computers en netwerkcomponenten worden beheerd, vallen vaak tussen wal en schip.

Onbewust niet toegepaste beveiligingsparameters
Tijdens audits en penetratietests is vaak gebleken dat triviale beveiligingsopties niet waren geactiveerd, zoals het afsluiten van niet-gebruikte netwerkservices op computers.

Niet-versleutelde wachtwoorden van beheerders die worden getransporteerd over het netwerk
Een beheerder heeft verregaande bevoegdheden en deze kunnen worden overgenomen als het wachtwoord van een beheerder wordt bemachtigd. Het is daarom van belang dat beheerderswachtwoorden niet kunnen worden afgeluisterd via het netwerk.

Niet-actieve accounts
Tijdens onderzoeken is diverse malen gebleken dat niet-actieve accounts van gebruikers en beheerders op servers en binnen applicaties waren gedefinieerd. Veelal was ook niet duidelijk welke medewerkers deze accounts eventueel nog konden benutten.

Gevolgen van bedreigingen

Het is erg lastig de schade als gevolg van beveiligingsincidenten in detail in kaart te brengen. Wel is een trend in de door organisaties ervaren schade af te leiden uit de survey-uitkomsten (zie tabel 1).

In de praktijk onderkennen bedrijven als voornaamste schades de effecten van virussen, de kosten door het verlies van IT-middelen (apparatuur en programmatuur) bij diefstal en de schade bij uitval van systemen. Kijken we naar de oorzaken van deze schades, dan blijkt schade met name te worden veroorzaakt door:

Niet-geïmplementeerde patches
Dit fenomeen komt niet alleen naar voren als een door organisaties ervaren bedreiging, maar ook als een bedreiging met een grote (financiële) impact. Het moge dan ook duidelijk zijn dat bij 'zuinig beveiligen' patchmanagement toch een hoge prioriteit dient te krijgen.

Ontbreken van afdoende beveiligingsbewustzijn
Het beveiligingsbewustzijn blijkt niet alleen van belang te zijn voor het veilig houden van de inhoud van pc's en laptops, ook de pc's en laptops zelf verdienen deze beveiliging. Deze computers moeten fysiek worden beveiligd en de logische toegang tot deze computers dient te worden afgeschermd met behulp van ten minste een opstartbeveiliging en harddiskversleuteling.

Bouwhuis van beveiligingsmaatregelen

In het voorgaande zijn diverse bedreigingen uit de praktijk aan bod gekomen. Deze bedreigingen komen echter met name voort uit knelpunten die de beveiliging op strategisch en tactisch niveau betreffen. Het is dan ook raadzaam niet alleen de operationele bedreigingen aan te pakken, maar ook de oorzaken ervan op het strategische en het tactische niveau. In de beveiligingspiramide zijn

Security incidents	#Organisations reporting breaches	%Suffering breaches	Average days lost per year	Average US$ lost per year [in k$]	Highest reported US$ lost/year [in m$]
Virus incident	390	61%	65	162	10,0
Theft of IT equipment	246	38%	21	98	3,0
Email intrusion (e.g. spam)	183	29%	12	16	0,2
Loss of software	102	16%	19	104	3,0
Denial of service attack	91	14%	24	53	0,5
Website intrusion (e.g. hacking)	79	12%	84	32	0,2
Critical system failure	79	12%	80	155	4,0
Loss of company documents (hardcopy)	76	12%	11	37	0,2
Loss of confidential data	35	5%	18	197	1,5
Tampering on input and output	23	4%	14	14	0,1

Tabel 1. Financiële schade als gevolg van beveiligingsincidenten ([KPMG02]).

deze op de bovenste twee niveaus weergegeven (figuur 4).

De beveiligingspiramide is een model met de te treffen maatregelen op strategisch, tactisch en operationeel niveau, en omvat ook de op te stellen documenten op basis waarvan het beveiligingsbouwhuis adequaat kan worden gefundeerd.

Het is op strategisch niveau gewenst een beveiligingsbeleid te formuleren, waarin met name het leiderschap en eigenaarschap, evenals het proces van security management worden ingevuld.
In de praktijk vraagt het invullen van het leiderschap voor informatiebeveiliging om een bewuste keuze, aangezien de binnen de organisatie aan te wijzen persoon naast kennis van informatiebeveiliging ook dient te beschikken over een aantal persoonlijke eigenschappen zoals initiatief, trekkracht en uithoudingsvermogen, evenals kennis van de toegepaste bedrijfsprocessen.
De kracht van het beschikbaar hebben van een informatiebeveiligingsbeleid borgt de ondersteuning die het hoogste management geeft aan het optuigen van het bouwhuis voor informatiebeveiliging.
Onthoud dat een beveiligingsbeleid niet hoeft te resulteren in een lijvig document, maar met name gericht moet zijn op de organisatorische inbedding en de wijze van beheersing van informatiebeveiliging.

Als onderdeel van security management is het gewenst het tactische niveau van informatiebeveiliging nader in te richten door het opstellen van een beveiligingsontwerp voor de te treffen maatregelen, bijvoorbeeld op basis van de Code voor Informatiebeveiliging (BS7799).

Voor het operationele niveau zijn in het voorgaande al diverse maatregelen aangeduid, zoals het implementeren van security patches en het versterken van het beveiligingsbewustzijn. Een organisatie kan dergelijke te treffen maatregelen opnemen in baselines (beveiligingsstandaarden) voor de IT-infrastructuur, de IT-applicatie, het IT-beheer en het IT-gebruik.

Het zal duidelijk zijn dat het opstellen van een compleet stelsel van beveiligingsdocumenten een wezenlijke activiteit vormt. Daarom worden alleen essentiële documenten als onderdeel van zuinig beveiligen opgesteld, waaronder het beveiligingsbeleid.

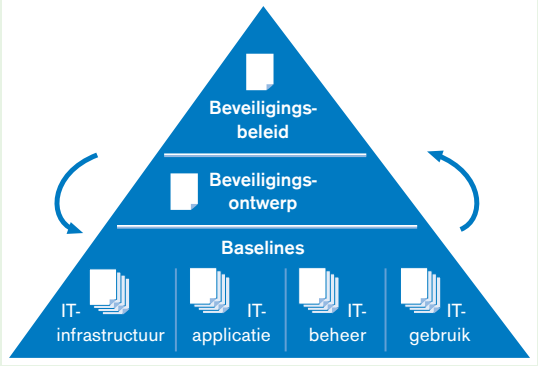
Essentiële beveiligingsmaatregelen als quick win

Een organisatie kan als kleinschalig quick win-project in twee fasen de beveiliging wezenlijk verbeteren door het treffen van een aantal essentiële beveiligingsmaatregelen. Deze fasen zijn:

Fase 1 – Inrichten versterkte preventieve beveiligingsmaatregelen
Deze fase omvat:
* opstellen van het beleid en inrichten van de organisatie;
* 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
Deze fase omvat:
* kanaliseren van verantwoordingsinformatie betreffende de gerealiseerde kwaliteit van informatiebeveiliging;
* testen van de effectiviteit van de getroffen maatregelen.

In kader 2 zijn de essentiële beveiligingsmaatregelen in detail uitgewerkt.



Figuur 4. Beveiligingspiramide.

Realiseren van essentiële maatregelen

Fase 1 – Inrichten versterkte preventieve beveiligingsmaatregelen

* *Opstellen van het beleid en inrichten van de organisatie*
  1. Opstellen en accorderen van beveiligingsbeleid, en benoemen van de security manager.
* *Selecteren van (hoog)gevoelige informatie en IT-middelen*
  2. Uitvoeren van een pragmatische gevoeligheidsanalyse, waarmee wordt bepaald welke gebruikte gegevens en toegepaste IT-middelen met name dienen te worden beveiligd.
* *Instrueren van gebruikers over informatiebeveiliging*
  3. Stimuleren van beveiligingsbewustzijn, met name met betrekking tot:
     – clear desk-beleid;
     – download van programmatuur;
     – gebruik van e-mail;
     – gebruik van webbrowsers;
     – beveiliging van apparatuur.
* *Formaliseren van kritieke beheerprocessen*
  4. Inrichten van het proces van patchmanagement, opdat patches direct na het bekendmaken door de leverancier worden geëvalueerd en zo nodig geïmplementeerd.
  5. Volgen van ontwikkelingen voor wat betreft de beveiliging op internet.
* *Versterken van de beveiliging van de IT-infrastructuur*
  6. Filteren van alle verkeer dat via externe koppelingen de organisatie kan binnendringen (waaronder internetverkeer). Hierbij dienen op reeds aanwezige netwerkcomponenten de filterregels van de firewalls te worden overgenomen, waardoor zeer zuinig de beveiliging wordt versterkt.
  7. Veilig ontwerpen en implementeren van systemen (applicaties, IT-infrastructuur, IT-beheer, evenals administratieve organisatie en interne controle) door tijdens het ontwikkelen direct relevante beveiligingseisen vast te stellen en toe te passen ([Korn98], [Korn01]).
  8. Beschermen van pc's met behulp van zogenaamde harddiskversleuteling, antivirusprogrammatuur en 'personal firewalls'.
  9. Beveiligen van de werkplekken en servers van beheerders, bij voorkeur gebruikmakend van security baselines of hardening documenten voor bijvoorbeeld Windows en Unix.
  10. Implementeren van zware authenticatie en sessiebeveiliging voor beheerders, alsmede voor toegang tot vertrouwelijke informatie zoals wachtwoorden en (hoog)gevoelige gegevens.
  11. Implementeren van netwerkcomponenten op een dusdanige wijze dat de zogenaamde denial-of-service (DoS)-aanvallen minder kans van slagen hebben.

Fase 2 – Versterken monitoring van beveiliging

* *Kanaliseren van verantwoordingsinformatie betreffende de gerealiseerde kwaliteit van informatiebeveiliging*
  12. Adequaat opvolgen van beveiligingsincidenten. Dit houdt zowel het treffen van repressieve maatregelen in als het wegnemen van de oorzaak waardoor het bewuste beveiligingsincident kon optreden.
  13. Periodiek uitdraaien van bevoegdhedenoverzichten en nemen van maatregelen in geval van ongewenste geïmplementeerde bevoegdheden.
  14. Opvolgen van alarmmeldingen en analyseren van 'logging'.
* *Testen van de effectiviteit van de getroffen maatregelen*
  15. Periodiek uitvoeren van interne en externe penetratietests.

Kader 2. Essentiële beveiligingsmaatregelen.

Tot slot

Zuinig beveiligen betekent dat alleen de essentiële beveiligingsmaatregelen worden gerealiseerd. Het *aantoonbaar in control* geraken op het punt van informatiebeveiliging vraagt echter om meer dan zuinig beveiligen alleen. Op basis van zuinig beveiligen kan namelijk maximaal het niveau van 'Basic security & control measures' worden bereikt. Een organisatie dient zich af te vragen of dat niveau wel voldoende is!

Toch mag worden verwacht dat het risico van het doorbreken van functiescheidingen wezenlijk wordt gereduceerd en dat bedrijfsmatige doelstellingen wezenlijk worden ondersteund door alvast zuinig te beveiligen.

Denk echter ook aan vervolgstappen zoals het opstellen en toepassen van beveiligingsstandaarden voor de gebruikte Windows- en Unix-servers en het realiseren van een sturings- en verantwoordingscyclus betreffende alle onderwerpen uit de Code voor Informatiebeveiliging. Daarnaast doemen ook nieuwe IT-ontwikkelingen op waarop de security manager een antwoord dient te formuleren. Wat te denken van draadloze netwerken en het gebruik van USB-geheugens waarop bedrijfsgevoelige informatie in grote hoeveelheden onversleuteld wordt opgeslagen.

Literatuur

[Korn98]
Ir. P. Kornelisse RE, *Beheer en beveiliging van Unix-omgevingen*, Compact 1998/1.

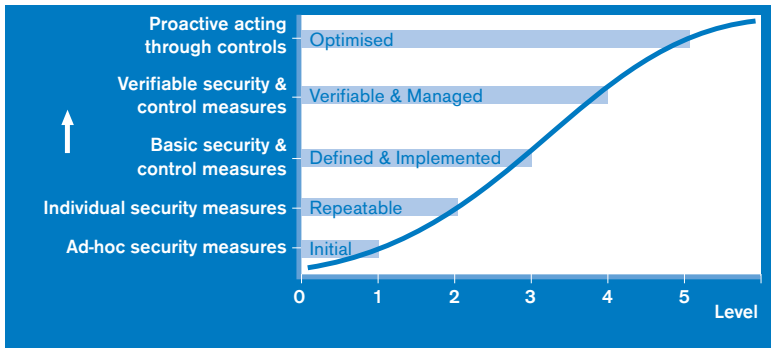
[Korn01]
Ir. P. Kornelisse RE, *De ICT-auditor en e-Business Security*, Compact 2001/5.

[KPMG02]
KPMG, *Security Survey 2002*, 2002.

[SANS03]
SANS, *Top 20 Windows and Unix*, 2003.

Ir. P. Kornelisse RE
is director bij KPMG Information Risk Management in Amstelveen, alwaar hij verantwoordelijk is voor de groep Technical Security Services. Deze groep richt zich, in de vorm van zowel advies als audit, op de beveiliging en beheersing van ICT-infrastructuren. Dit betreft onder andere ethical hacking, QA-ondersteuning en certificering betreffende transactionele websites, beveiligingsarchitecturen, platformbeveiliging (security baselines) zoals voor Windows 2000, evenals forensische onderzoeken.

kornelisse.peter@kpmg.nl



Figuur 5. Niveaus van beveiliging.