# INTERNETBEVEILIGING: EEN BEHEERPERSPECTIEF

*E.J.M. Ridderbeekx*
*J. van den Berg*

## 1. INLEIDING

Het Amerikaanse onderzoeksbureau Gartner geeft de volgende omschrijving van het Internet:

*"(...) a mass market social phenomenon that is taking the world by storm. It promises universal connectivity, linking everyone with everyone else, and interconnecting all computer devices, providing unprecedented and unparalleled access to information of every conceivable type. The Internet is owned and managed by no one and everyone, an anarchic model with which few IT-professionals are comfortable. Add to this, mass-media hype greater than that for any pop star"* [GART1996].

Het aardige van deze losse omschrijving is dat er tussen alle superlatieven een lichte toon van onrust doorklinkt. Natuurlijk, de beloftes van het Internet zijn groot en worden deels al ingelost. Voor particulieren is het een hulp bij hobby, een bron van vermaak, een wereldomspannend huis-aan-huis-blad, een communicatiemiddel; voor ondernemingen is het een uithangbord in de digitale straat, een communicatiemiddel van en naar cliënten, een nieuw distributiekanaal, een electronische toonbank en soms een virtuele kassa. Maar aan de andere kant zorgt het "anarchistische" beheermodel waarmee het Internet is opgegroeid en nu het stadium van volwassenheid lijkt te hebben bereikt voor een zekere terughoudendheid en scepsis aan gebruikerszijde.

Die voorzichtige opstelling lijkt voor een deel veroorzaakt te worden door het feit dat potentiële gebruikers beveiliging van het Internet als een belangrijke barrière bij toepassing zien [KPMG1996]. Uit het gerefereerde onderzoek komt echter ook een zonnig vooruitzicht naar voren: de onderzochte organisaties schatten in dat de gevoelde beperkingen van het Internet, waaronder die ten aanzien van beveiliging, op korte termijn in belangrijke mate zullen verdwijnen.

In dit artikel wordt een minder optimistische visie verwoord. Of, genuanceerder gesproken, er zal worden betoogd dat de beveiligingsproblematiek niet vanzelf verdwijnt. Internet beveiliging vereist een *actieve*, *consciëntieuze*, en *continue* aanwezige aandacht van de betrokken organisaties. In het navolgende zal worden besproken hoe men hieraan vorm kan geven.
Alvorens stil te staan bij de managementkant van Internetbeveiliging, zullen we eerst de ons inziens meest fundamentele aspecten van beveiliging van netwerken in het algemeen bespreken. Deze discussie levert een risicomodel op dat gebruikt kan worden als analysegereedschap voor allerlei vormen van Internet-gebruik. Daarmee wordt tevens het probleemgebied afgebakend en wordt Internetbeveiliging geplaatst binnen het kader van het beheer van informatiesystemen.

## 2. NETWERKEN

### 2.1 Betekenis van netwerken voor de organisatie

Iedere organisatie heeft te maken met (primaire en secundaire) processen, die essentieel zijn voor het halen van de bedrijfsdoelstelling. Om deze bedrijfsprocessen adequaat te kunnen beheersen wordt gebruik gemaakt van informatiesystemen, die een afbeelding vormen van de reële systemen waarmee de organisatie te maken heeft [LOOI1997]. Voor een belangrijk deel zijn deze informatiesystemen geau-

tomatiseerd. Computernetwerken[1] kunnen worden beschouwd als onderdeel van deze informatiesystemen. Het zijn onderling gekoppelde autonome computersystemen [TANE1996], die faciliterend zijn voor de gegevensverwerking en het gegevensverkeer binnen de informatiesystemen. Daarmee spelen netwerken een belangrijke rol in de kwaliteitsbeheersing van de bedrijfsprocessen.

## 2.2 Interne en externe netwerken

Voorzover een netwerk zich binnen het beheergebied van de organisatie bevindt wordt gesproken van een *intern* netwerk. De aanwezigheid binnen het beheergebied impliceert dat de organisatie zowel de mogelijkheid als de verantwoordelijkheid heeft het netwerk in stand te houden conform de kwalitatieve en kwantitatieve eisen en randvoorwaarden die binnen de organisatie gelden. De organisatie is in dat opzicht volledig *autonoom* in zijn keuze van functionaliteit en technische specificaties van het interne netwerk, net zoals de organisatie autonoom is ten aanzien van zijn processen en ondersteunende geautomatiseerde informatiesystemen.
Interne netwerken kunnen worden gekoppeld aan externe netwerken. Externe netwerken zijn netwerken die niet binnen de directe invloedssfeer en beheerverantwoordelijkheid van de organisatie liggen. De reden voor een dergelijke koppeling ligt in de mogelijkheden een kwaliteitsverbetering van de eigen primaire processen te realiseren, omdat de netwerkkoppeling zorgt voor het beschikbaar komen van additionele informatiekanalen. Daarmee maakt men echter de kwaliteit van de eigen processen mede afhankelijk van de kwaliteit van processen, informatiesystemen, en netwerken van instanties buiten de eigen invloedssfeer. Deze afhankelijkheid doorbreekt niet per definitie de genoemde autonomie, maar brengt daarvoor wel bedreigingen met zich mee. De onderneming zal dus moeten afwegen:

- de mate waarin een koppeling met een extern netwerk kan bijdragen aan de kwaliteit van eigen netwerken, informatiesystemen, en bedrijfsprocessen (*rendementscriterium*);
- de mate waarin een dergelijke koppeling afbreuk kan doen aan de beheersbaarheid van de geautomatiseerde informatiesystemen en daarmee aan de kwaliteit van de bedrijfsprocessen (*risicocriterium*).

Ons inziens dient hierbij te gelden dat een kwaliteitstoename van de eigen bedrijfsvoering een *eis* is die aan een koppeling met een extern netwerk gesteld moet worden. *Randvoorwaardelijk* hierbij is dat de koppeling niet ten koste mag gaan van de beheersbaarheid van de eigen informatiesystemen. Netwerkbeveiliging speelt daarin een zeer belangrijke rol.

Voor individuele organisaties is het Internet een extern netwerk; men heeft geen mogelijkheden het Internet te beïnvloeden, behalve dat men het Internet kan uitbreiden door er zelf deel van uit te (gaan) maken. En dat is een keuze die veel ondernemingen en instanties al gemaakt hebben, gedreven door de beloftes die het Internetconnectiviteit doet: toegang tot immense hoeveelheden informatie en informatiesystemen, aanwezigheid op markten zonder geografische barrières of tijdverschillen, efficiënte communicatie, samenwerking, en bereikbaarheid.
Gezien hetgeen hierboven is gesteld ten aanzien van externe netwerken moet een organisatie een Internetkoppeling afwegen op basis van de genoemde rendements- en risicocriteria. Essentieel in de formulering van de vragen op grond van deze criteria is dat de eigen informatiesystemen en bedrijfsprocessen centraal worden gesteld. Met name ten aanzien van Internetbeveiliging (dat, zoals nog zal worden betoogd, een uitvloeisel is van het risicocriterium) is dit een fundamenteel andere benadering dan die waarbij beveiliging in een Internetcontext wordt gezien als een probleem waarvan de aard en omvang door technische kenmerken worden bepaald. Internet zelf is niet onveilig; het wordt onveilig in combinatie met bepaalde bedrijfsprocessen, namelijk die processen die te kritisch zijn om ze van Internetfunctionaliteit afhankelijk te maken.

In kader 1 is ingegaan op de rendementskarakteristieken van Internetconnectiviteit. Daarbij is de functionaliteit die Internet kan bieden gerelateerd aan bepaalde bedrijfsprocessen.

[1] In het vervolg van dit artikel zal de term *netwerk* worden gebruikt als synoniem voor *computernetwerk*.

**Kader 1. Rendement van Internetgebruik**

***Organisatiebreed: Samenwerking***
Grote kracht van het Internet als infrastructuur is dat het kan bijdragen aan efficiënte samenwerking: geografische verschillen hebben geen invloed meer op de tijd die gemoeid is met het delen of verspreiden van kennis en informatie. E-mail, nieuwsgroepen, file transfer zijn in dat opzicht oudgedienden. Recentere ontwikkelingen maken ook het transport van geluid en beeld mogelijk, waardoor telefonie en *video conferencing* via het Internet mogelijk worden. De nieuwste generatie web-browsers biedt standaard-faciliteiten op het gebied van *workflow management* en *groupware*. Het Internet biedt, kortom, legio kansen om vorm te geven aan de communicatie die voor een goede samenwerking noodzakelijk is.

***Pre-sales processen: Voorlichting en reclame (verkoop- en marketing informatiesystemen)***
Voor veel organisaties zijn de eerste stappen op het Internet voornamelijk gericht op het geven van informatie over de produkten en diensten die men aanbiedt. Hierbij kan het gaan om het verduidelijken van organisatie- en produktkarakteristieken, maar ook om het aanzetten tot een koopbeslissing ("uithangbord- en toonbankfunctie").

***Sales processen: Marktonderzoek (marketing informatiesysteem)***
Een stap verder dan de hierboven genoemde, tamelijk "passieve", aanwezigheid op het Internet is het gebruiken van Internet als een manier om meer grip te krijgen op de wensen van de consument. Enquêtes en marktonderzoeken zijn met behulp van Internet services heel goed mogelijk.

***After Sales processen: Serviceverlening en klantenondersteuning (verkoopinformatiesysteem)***
Faciliteiten als e-mail en het World Wide Web lenen zich uitstekend voor *pre-* en *after-sales* serviceverlening die is afgestemd op de wensen en eisen van een individuele klant. Hierbij kan worden gedacht aan uitgeverijen die geïnteresseerden periodiek met een e-mail op de hoogte brengen van nieuw verschenen titels binnen bepaalde interessegebieden. Ook de aanwezigheid van *helpdesks* en *online*-consumentenservices, die individuele vragen van cliënten beantwoorden zijn een voorbeeld van deze klantenondersteuning.

***Verkoop- en administratieve processen: Electronische commercie en transactieverwerking (voorraadinformatiesysteem, financieel informatiesysteem, verkoopinformatiesysteem)***
Veel aandacht is momenteel gericht op de mogelijkheden die het Internet (en met name het World Wide Web) biedt ter ondersteuning van electronische commercie. Hierbij wordt Internettechnologie gebruikt om de totstandbrenging van commerciële transacties tussen aanbieders en afnemers te ondersteunen.

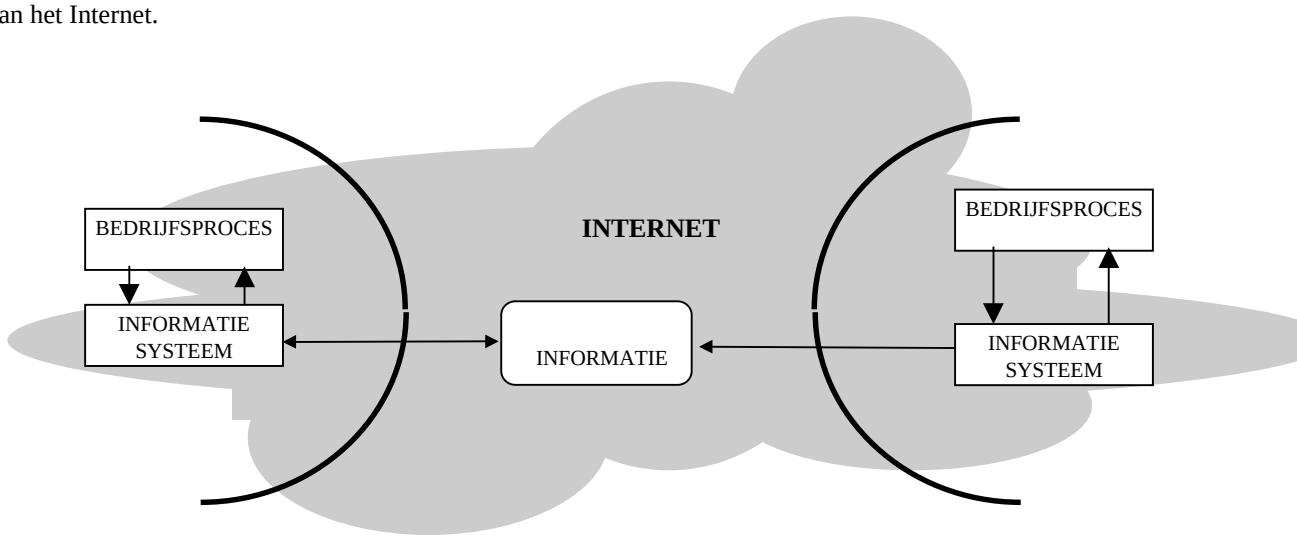
***Educatie en vermaak***
Het Internet kan een belangrijke educatieve taak vervullen. De enorme hoeveelheid informatie die met een doorsnee PC en een Internet-account voor eenieder bereikbaar wordt, maakt het Internet tot een universeel naslagwerk, alhoewel de toegankelijkheid niet door iedereen even hoog zal worden ingeschat.

Uit de voorbeelden blijkt dat koppeling van het interne netwerk aan het Internet kan bijdragen aan een doeltreffender en doelmatiger inrichting en vormgeving van interne informatiesystemen en bedrijfsprocessen. Die verbeteringen zijn, zoals gezegd, een *conditio sine qua non* voor Internetconnectiviteit. Maar hoe zit het met de randvoorwaarde van behoud van beheersbaarheid? In welke mate doet een koppeling met het Internet afbreuk aan de beheersbaarheid van de eigen informatiesystemen en bedrijfsprocessen?

## 3. RISICO'S VAN INTERNETGEBRUIK

De aard van een bedrijfsproces is bepalend voor de kwaliteitseisen die gesteld moeten worden aan het informatiesysteem dat het bedrijfsproces (mede) bestuurt. Wordt het informatiesysteem voor een gedeelte "gevoed" door externe informatie, of steunt het informatiesysteem deels op componenten die door de organisatie niet direct beïnvloedbaar zijn, dan moet gezorgd worden voor het afdwingen van de noodzakelijke kwaliteit; aan de bedrijfsprocessen kan afbreuk worden gedaan indien men hierin tekortschiet, hetgeen tot schade voor de organisatie kan leiden. Internetbeveiliging is gericht op het bijdragen aan dit kwaliteitsniveau.

In figuur 1 is dit op basis van een eenvoudig communicatiemodel weergegeven. De krommen geven de grenzen van de beheergebieden van beide communicatiepartners weer. Beide exploiteren ze informatiesystemen, die worden gebruikt ter besturing van bedrijfsprocessen, en beide maken ze daarbij gebruik van het Internet.




Figuur 1. Eenvoudig communicatiemodel

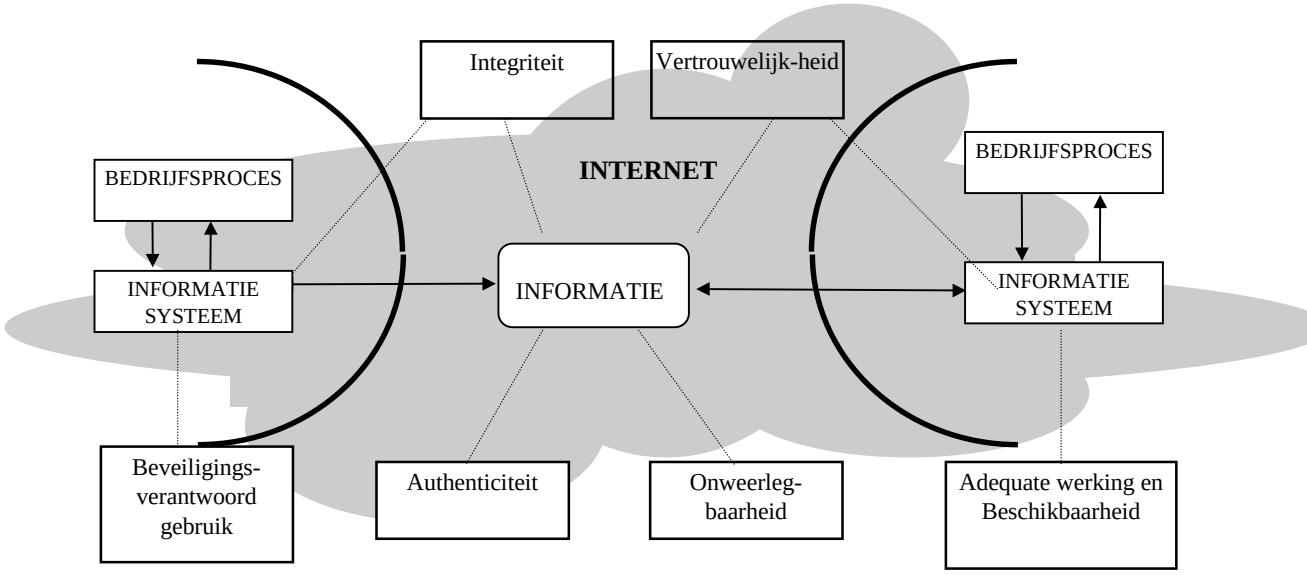
Het risico dat van gebruik van het Internet uitgaat is dat de kwaliteit van de informatiesystemen van de organisatie zodanig nadelig door de koppeling met het Internet wordt beïnvloed dat het de kwaliteit schaadt van de bedrijfsprocessen die met behulp van die informatiesystemen worden bestuurd. Dit is op twee manieren mogelijk:

a. *doordat de kwaliteit van de uitgewisselde informatie tekortschiet;*
Internet faciliteert in de eerste plaats de uitwisseling van informatie. Organisaties bewerken deze informatie verder binnen de eigen informatiesystemen. De bedrijfsprocessen die met behulp van de informatiesystemen worden bestuurd zijn bepalend voor de kwaliteitseisen die aan de informatie vanuit het Internet moeten worden gesteld. Als we de informatie-overdacht tussen communicatiepartners zoals weergegeven in figuur 1 nader analyseren komen de volgende punten naar voren:

1. *vertrouwelijkheid.* Informatie moet ontoegankelijk zijn voor derden;
2. *integriteit*. Informatie moet voor derden onveranderbaar zijn;
3. *authenticiteit*. De ontvanger moet zekerheid hebben over de herkomst van de informatie;
4. *onweerlegbaarheid.* De zender mag niet in staat zijn te ontkennen dat het verzenden van bepaalde informatie heeft plaatsgevonden.

b. *doordat (delen van) de informatiesystemen zelf in negatieve zin worden beïnvloed.*
Als onderdelen van informatiesystemen zijn -naast hardware (apparatuur en interne netwerken) en software (programmatuur en data)- ook mensen en procedures te onderscheiden. Procedures hebben tot doel aan mensen (gebruikers) aan te geven op welke wijze de functionaliteit van het informatiesysteem goed gebruikt kan worden. Ervan uitgaande dat de risico's voor informatiesystemen worden gevormd door de risico's voor de componenten van informatiesystemen, resulteren de volgende kwaliteitsaspecten in het kader van Internetbeveiliging:

1. *de adequate werking en beschikbaarheid van de hardware*;
2. *de vertrouwelijkheid en integriteit van de software*;
3. *het beveiligingsverantwoord gebruik*.




Figuur 2. Risicomodel

In figuur 2 is bovenstaand risicomodel schematisch weergegeven. Internetbeveiliging is gericht op het waarborgen van bovengenoemde kwaliteitsaspecten, teneinde de beheersbaarheid van bedrijfsprocessen te waarborgen.

De exacte afbakening van beveiligingseisen binnen het bredere gamma van kwaliteitseisen die aan informatie en informatiesystemen gesteld kunnen worden kan overigens best onderwerp van discussie zijn. Echter, het gaat er bij beveiliging in de eerste plaats om dat de belanghebbenden hetzelfde onder het begrip verstaan.

Conform het in het voorgaande beschreven risicocriterium moeten de genoemde bedreigingen worden gerelateerd aan de bedrijfsprocessen en informatiesystemen waarvoor het Internet wordt gebruikt. Dit moet een zorgvuldige afweging opleveren, waarin gedifferentieerd en genuanceerd met deze bedreigingen wordt omgegaan en waarbij feitelijk een goede risico-analyse gestalte krijgt. Ter illustratie hiervan zijn in het kader twee eerdergenoemde bedrijfsprocessen globaal afgezet tegen enkele van de genoemde bedreigingen.

**Kader 2. Risico's van Internetgebruik**

***Pre-sales processen: Voorlichting en reclame (verkoop- en marketing informatiesystemen)***
Deze vorm van communicatie is bijna per definitie gericht op een brede doelgroep. Aan vertrouwelijkheid van de informatie, noch aan authenticiteit of onweerlegbaarheid zullen derhalve doorgaans hoge eisen worden gesteld. Integriteit daarentegen is wezenlijk.

***After Sales processen: Serviceverlening en klantenondersteuning (verkoopinformatiesysteem)***
Informatie-uitwisseling in het kader van pre- of after-sales ondersteuning is ten opzichte van voorlichting en reclame veel meer toegespitst op een individuele consument. Mogelijk bevat de uitgewisselde informatie cliëntspecifieke gegevens die eisen stellen aan de vertrouwelijkheid. Authenticiteit van de informatie is van belang omdat zowel producent als consument mogelijk acties gaan ondernemen op basis van uitgewisselde informatie. In sommige gevallen zal de aanbieder bovendien zeker willen zijn van de identiteit van de klant, om bijvoorbeeld vast te stellen of deze wel recht heeft op service. Mogelijk is ook dat ten behoeve van het voorkomen van toekomstige disputen het feit dat service is verleend ondubbelzinnig moet kunnen worden aangetoond.

***Verkoop- en administratieve processen: Electronische commercie en transactieverwerking (voorraadinformatiesysteem, financieel informatiesysteem, verkoopinformatiesysteem)***
Omdat het hierbij gaat om de totstandkoming van overeenkomsten met fysieke en financiële consequenties, is authenticiteit

van de informatie van eminent belang. Dat geldt tevens meestal voor authenticatie van de "electronische handelspartner", en de onweerlegbaarheid van de specificaties van een bepaalde transactie. Vertrouwelijkheid zal doorgaans hooglijk op prijs worden gesteld.

## 4. NOODZAKELIJK BEVEILIGINGSNIVEAU VERSUS BEVEILIGINGSBELEID

Als een organisatie, die overweegt om op een of andere actieve wijze van het Internet gebruik te gaan maken, duidelijkheid heeft gecreëerd in de aard en omvang van de risico's waaraan zij door de koppeling onderhevig is, ziet zij zich geplaatst voor de uitdaging deze beveiligingsrisico's op een toereikende manier te mitigeren. Centraal hierbij staat de definitie van een *noodzakelijk beveiligingsniveau*. Het noodzakelijk beveiligingsniveau wordt hier gedefinieerd als "de mate waarin beveiligingsrisico's moeten worden afgedekt".
De term beveiligingsniveau zou kunnen suggereren dat de beveiligingsambitie van een organisatie wordt uitgedrukt in een absolute maateenheid: "we hebben een beveiligingsniveau van 40 graden op de schaal van Valente", of "we streven naar een beveiligingsniveau dat 10 punten boven het branchegemiddelde ligt". In werkelijkheid is het echter een relatief begrip dat zich moeilijk laat kwantificeren. Bovendien heeft de term alleen maar betekenis in de context van een bepaalde organisatie. De essentie van het noodzakelijk beveiligingsniveau is, dat het de schakel vormt tussen de hierboven besproken risico-analyse enerzijds en een set met afgewogen beveiligingsmaatregelen anderzijds. Afgewogen, omdat een overdaad aan beveiligingsmaatregelen niet efficiënt zou zijn; anderzijds stelt een tekort aan maatregelen de organisatie bloot aan ongewenste beveiligingsrisico's. Bij deze inschatting spelen de karakteristieken van de organisatie en de aard van haar processen een belangrijke rol; zij zijn een belangrijke bepalende factor voor de gevoeligheid van de organisatie voor beveiligingsproblemen.

Deze uitdaging is niet nieuw. Binnen het vakgebied informatiebeveiliging besteedt men van oudsher veel aandacht aan het vinden van een manier om beveiligingsmaatregelen in de organisatie te verankeren door ze zorgvuldig af te stemmen op risico's en specifieke bedrijfskenmerken. Een centrale rol daarbij speelt het *beveiligingsbeleid*, zoals bijvoorbeeld wordt beschreven in [NGI1993]. Ons inziens is de traditionele formulering van beveiligingsbeleid onvoldoende toegespitst op een situatie waarbij Internetgebruik in het spel is. In tegenstelling tot de dagen waarin *host based security* de boventoon voerde is in een Internetcontext sprake van een enorm dynamische omgeving. Het Internet verandert niet alleen zelf, maar heeft direct invloed op maatschappelijke aspecten en economische verhoudingen. Ook daardoor verandert het risicoprofiel waarmee een organisatie zich geconfronteerd ziet. De dynamiek van de relevante omgevingskenmerken en risico's noodzaakt tot een voortdurende monitoring en bijstelling van het beveiligingsbeleid. De term beveiligingsniveau zoals hierboven gedefinieerd sluit beter aan bij de turbulentie van de Internet-omgeving; inhoud geven aan *de mate waarin beveiligingsrisico's moeten worden afgedekt* kan alleen maar als men zich bij voortduring afvraagt welke de risico's en de huidige maatregelen zijn en hoe deze zich ten opzichte van elkaar verhouden.

Het management van een organisatie kan gestalte geven aan de definitie van een *gewenst* of *noodzakelijk* beveiligingsniveau door in algemene termen te formuleren welke eisen ze stelt, en welke inschatting men maakt ten aanzien van de risicogevoeligheid voor de turbulentie van de Internetontwikkelingen. Om de op die eisen afgestemde diepgang en snelheid van handelen mogelijk te maken zullen vervolgens mensen en middelen moeten worden vrijgemaakt en verantwoordelijkheden moeten worden belegd.

Belangrijk is voorts dat de organisatie zich bewust is van de mogelijk beperkte levensduur van te nemen maatregelen. De *triggers* voor het bijstellen van beveiligingsmaatregelen kunnen daarbij heel divers zijn. Deze kunnen niet alleen liggen in wijzigingen in het gevoerde beleid, maar bijvoorbeeld ook in veranderingen met betrekking tot:

- de bestaande wetgeving;
- beschikbare Internetservices;
- aanwezige kennis en expertise;
- produkten die de concurrent op een website aanbiedt;
- maatschappelijke standpunten over privacy;

- het imago van de onderneming;
- standaarden in de branche.

Beveiligingsbeleid of beveiligingsniveau: het lijkt een terminologische kwestie. Essentieel is dat de turbulentie van het Internet binnen heel korte tijd nieuwe eisen kan stellen aan de acties die een beveiligingsbewuste organisatie moet uitvoeren. Waar het om gaat is dat snel en goed op deze steeds veranderende omstandigheden kan worden ingespeeld.

## 5. BEVEILIGINGSMAATREGELEN

Maatregelen zijn nodig om op een adequate manier het hoofd te kunnen bieden aan de risico's waaraan informatie en informatiesystemen blootstaan. Of, in termen van de vorige paragraaf, maatregelen zijn noodzakelijk om het door de Internet-gebruikende organisatie noodzakelijk geachte beveiligingsniveau te realiseren.

Een sterk stelsel van maatregelen bestaat uit zowel technische als organisatorische maatregelen. De technische maatregelen liggen op het gebied van het op een bepaalde wijze toepassen en configureren van hardware en software binnen de eigen beheeromgeving. De organisatorische maatregelen zijn erop gericht de werkwijzen en acties van medewerkers te richten op de beperking van risico's, bijvoorbeeld door een goed gebruik en beheer van de technische maatregelen. Tussen technische en organisatorische maatregelen bestaat een duidelijke afhankelijkheid. De effectiviteit van technische maatregelen schiet tekort als deze onvoldoende zijn ingebed in organisatorische maatregelen. Organisatorische maatregelen alleen zijn evenmin toereikend ter realisatie van het noodzakelijke beveiligingsniveau. Slechts in combinatie kunnen beveiligingsrisico's op een doeltreffende manier worden beheerst.

Een tweede onderscheid dat kan worden gemaakt is dat tussen *preventieve* maatregelen enerzijds en *repressieve* maatregelen anderzijds. Preventieve maatregelen worden genomen om schade als gevolg van het bestaan van risico's te voorkomen. Repressieve maatregelen zijn gericht op het vaststellen van schade[2], het beperken van verdere schade, en het herstellen van de oorspronkelijke toestand[3]. Conform het gezegde "voorkomen is beter dan genezen" verdienen preventieve maatregelen de voorkeur boven repressieve maatregelen. Toch zullen repressieve maatregelen deel moeten uitmaken van het volledige maatregelenstelsel dat ontworpen en geïmplementeerd wordt om het gewenste beveiligingsniveau te bereiken. Dit heeft een aantal redenen. Op de eerste plaats is het niet altijd mogelijk om tegen alle bedreigingen effectieve en efficiënte preventieve maatregelen te treffen. Op de tweede plaats veronderstelt een preventieve maatregel kennis over de specifieke kenmerken van een bedreiging. Die kennis bestaat echter slechts voor die bedreigingen, die Neumann de *known vulnerabilities* noemt [NEUM1996]. Internet en Internet-diensten zijn voortdurend aan verandering onderhevig en leveren daarmee ook bij voortduring nieuwe bedreigingen op. De beveiligings*bugs* in populaire webbrowsers die met regelmaat aan het daglicht komen zijn hiervan een goede illustratie. Met het nemen van repressieve maatregelen wordt het bestaan van *<u>un</u>known vulnerabilities* erkend en onderkend, en verschuift het accent van het voorkomen van schade naar het kunnen vaststellen en beperken van schade.
Ten derde kunnen repressieve maatregelen worden gezien als een extra laag van beveiliging ter aanvulling op preventieve maatregelen. Het getuigt van voorzichtigheid en realisme om rekening te houden met scenario's waarin preventieve maatregelen kunnen falen of tekortschieten. Repressieve maatregelen dienen dan als een vangnet: de trapeze-act mislukt, ondanks de uitgebreide preventieve repetities, maar de acrobaat overleeft.

Over concrete voorbeelden van beveiligingsmaatregelen is veel materiaal gepubliceerd. In de kaders 3 en 4 is zeer beknopt aangegeven welke belangrijke technische en organisatorische maatregelen getroffen kunnen worden om het noodzakelijke beveiligingsniveau te realiseren. Daarbij is tevens aangegeven welke risico's door de betreffende maatregel met name worden geadresseerd, en of de betreffende maatregel met name preventief of repressief van karakter is.

---

[2] Soms wordt deze categorie maatregelen apart genoemd als *detectief*.
[3] Soms wordt deze categorie maatregelen apart genoemd als *correctief*.

**Kader 3. Technische maatregelen**

***Firewalls***
Een firewall is een verzameling van hardware- en softwarecomponenten die is geplaatst op het koppelvlak van netwerken om de risico's van die koppeling te beperken conform het gewenste beveiligingsniveau en het daarop afgestemde beveiligingsbeleid. Het gaat daarbij concreet met name om:

- het filteren van Internetservices, waarbij ongewenste services worden geblokkeerd;
- het beperken van communicatiemogelijkheden van interne systemen met het Internet en van het Internet met interne systemen;
- het verborgen houden van informatie over de structuur en samenstelling van het interne netwerk;
- het inzicht geven in netwerkgebruik en in (pogingen tot) netwerkmisbruik.

Risicogebied: de adequate werking en beschikbaarheid van de hardware;
de vertrouwelijkheid en integriteit van de software.
Preventief/repressief: voornamelijk preventief.

***Encryptie***
Encryptie is een proces waarbij gegevens in originele, leesbare en begrijpelijke vorm worden omgezet in een vorm die bedoeld is onbegrijpelijk te zijn behalve voor hen die de middelen hebben om de originele vorm te herstellen.

Risicogebied: de vertrouwelijkheid van de informatie die wordt uitgewisseld;
de integriteit van de informatie die wordt uitgewisseld.
Preventief/repressief: preventief

***Authenticatiemaatregelen en digitale handtekeningen***
Authenticatie is gericht op het vaststellen van de identiteit van een communicatiepartner of van de echtheid van uitgewisselde informatie. Authenticatie van een communicatiepartner kan plaatsvinden op basis van een eigenschap van die partner (een vingerafdruk), kennis (zoals een password), bezit (bijvoorbeeld een *smartcard*), naam en herkomst van berichten (hostnames en IP-adressen), maar ook op grond van cryptografische technieken.
De authenticiteit van een bericht kan worden aangetoond met behulp van digitale handtekeningen. Deze zijn gebaseerd op een combinatie van hashing-methodes en cryptografische technieken. Digitale handtekeningen hebben als voordeel dat ze vaak tevens kunnen dienen als middel om integriteit van de verzonden informatie vast te kunnen stellen, en om onweerlegbaarheid van informatieverzending te realiseren.

Risicogebied: de authenticiteit van de informatie die wordt uitgewisseld;
de onweerlegbaarheid van informatie-uitwisseling.
Preventief/repressief: preventief

***Autorisatiemaatregelen***
Bij autorisatie gaat het om het toekennen van rechten aan een (geauthenticeerde) communicatiepartner en het afdwingen van het feit dat de communicatiepartner zich aan die rechten houdt. Het is een belangrijk uitgangspunt dat aan gebruikers, programma's, en processen binnen een informatiesysteem die en slechts die bevoegdheden worden toegekend die de gebruiker, het programma, of het proces nodig hebben voor het uitvoeren van hun taak. De specifieke implementatie van deze regel is afhankelijk van de aard van de betreffende omgeving, maar zal in ieder geval de volgende zaken omvatten:

- een identificatie van gebruikers, programma's en processen;
- een definitie van toegangsregels voor gebruikers, programma's en processen op resources zoals bestanden, geheugen, en periferie;
- een mechanisme dat deze toegangsregels afdwingt.

In het UNIX-operating systeem bijvoorbeeld wordt deze autorisatie geregeld op basis van *user- en group identification numbers* (UID's en GID's) en *file- en directory permissions*.

Risicogebied: de adequate werking en beschikbaarheid van de hardware;
de vertrouwelijkheid en integriteit van de software.
Preventief/repressief: preventief

***Logging- en alarmeringsmaatregelen***
Logging is het vastleggen van informatie over relevante gebeurtenissen binnen een informatiesysteem. Op de eerste plaats is het op basis van gelogde gegevens mogelijk te reconstrueren welke gebeurtenissen ten grondslag hebben gelegen aan de huidige status van het systeem. Een dergelijke audit-trail is uit beveiligingsoogpunt wezenlijk om (pogingen tot) ongeoorloofde acties te kunnen traceren en de daarmee eventueel aangerichte schade te kunnen herstellen. Op de tweede plaats kunnen logbestanden, die meestal nogal omvangrijk zijn, worden gebruikt als basis voor (geautomatiseerde) detectie en analyse van

patronen op het gebied van gebruik en misbruik. Een dergelijke analyse zou ook inzicht kunnen geven in implementatiefouten ten aanzien van preventieve maatregelen.
Waar logging in essentie een betrekkelijk passieve activiteit is, is alarmering veel meer gericht op het herkennen van vooraf gedefinieerde situaties *op het moment* dat deze zich voordoen, en het ondernemen van vooraf bepaalde acties als reactie op deze situaties. Alarmering kan plaatsvinden door de firewall, maar ook op hostniveau kan de Internetgebruikende organisatie alarms in werking stellen. De condities op basis waarvan het alarmeringsmechanisme in werking moet treden moeten door de organisatie worden vastgesteld. Dat is geen eenvoudige taak; analyses van de logbestanden kunnen mogelijkerwijs als input dienen.
De acties die bij een alarm ondernomen moeten worden kunnen variëren: er kan automatisch een melding verschijnen op het firewall-console, de dienstdoend systeembeheerder kan van een e-mail worden voorzien, de Internetkoppeling kan worden dichtgezet. Belangrijk is dat scenario's voorhanden zijn waarin de te nemen acties in geval van beveiligingsalarms duidelijk zijn uitgewerkt.

Risicogebied: de adequate werking en beschikbaarheid van de hardware;
de vertrouwelijkheid en integriteit van de software.
Preventief/repressief: repressief

**Kader 4. Organisatorische maatregelen**

***Inrichten beheerorganisatie***

Een koppeling met het Internet dient beheerd te worden, zowel waar het gaat om de functionele taken om het gerealiseerde beveiligingsniveau in overeenstemming te houden met het door de organisatie noodzakelijk geachte niveau, als om operationele taken ten aanzien van de koppeling. Ook de audit-functie, die is gericht op het op een onafhankelijke wijze vaststellen van de overeenstemming tussen het noodzakelijke beveiligingsniveau enerzijds en het gerealiseerde beveiligingsniveau anderzijds, is van belang. Voor een beschrijving van de complexiteit van die functie (en tevens een goed overzicht van technische bedreigingen) wordt verwezen naar [MEEK1997].

Risicogebied: alle onderkende risico's
Preventief/repressief: beide

***Coherent stelsel van beveiliging***
Internet levert voldoende beveiligingsuitdagingen op, en het *tacklen* van die uitdagingen kan grote delen van de beschikbare aandacht van IT- en beveiligingsfunctionarissen in beslag nemen. Hierbij moet men ervoor oppassen niet zodanig gepreoccupeerd te zijn met het beveiligen van een externe netwerkkoppeling dat men andere bedreigingen uit het oog verliest. Al gauw heeft men dan een situatie van "*steel doors in grass huts*": de deur van en naar het Internet zit prima dicht, maar op andere plaatsen zijn externe koppelingen aanwezig (zoals modems van gebruikers, inbellijnen van leveranciers) die de effectiviteit van die sterke deur tot praktisch nul reduceren. De organisatie dient ervoor te zorgen dat er sprake is en blijft van een coherent organisatiebreed stelsel van informatiebeveiliging. Dit voorkomt zwakke plekken in het *overall*-beveiligingsniveau en alle mogelijke onaangename verrassingen van dien, en heeft daarmee primair een preventief karakter. Ook de interne dreiging van fraudes of fouten door personeel moet een voortdurend punt van aandacht blijven. Op geen enkel moment mag de indruk bestaan dat het risico dat daarvan uitgaat (de zogenaamde *insiders threat*) wordt gereduceerd door een goed beveiligd Internetgebruik.

Risicogebied: alle onderkende risico's
Preventief/repressief: preventief

***Afhandeling beveiligingsincidenten***
Een belangrijke repressieve organisatorische beheermaatregel is voorts het opstellen van procedures en richtlijnen die gevolgd moeten worden op het moment dat (het vermoeden bestaat dat) een beveiligingsincident ten aanzien van het Internetgebruik heeft plaatsgevonden. Het gaat daarbij zowel om het aangeven van een centraal meldpunt als om het definiëren van te ondernemen acties in termen van vastlegging, analyse, en oplossing. Doelstelling hiervan is om de schade als gevolg van beveiligingsincidenten zo snel mogelijk te ontdekken en zoveel mogelijk te beperken. Bovendien stelt een analyse van een opgetreden incident de organisatie wellicht in staat het stelsel van preventieve maatregelen structureel te uit te breiden en te verbeteren.

Risicogebied: alle onderkende risico's
Preventief/repressief: repressief

***Bevorderen beveiligingsbewustzijn***
Door het gebruik van netwerken in het algemeen en het Internet in het bijzonder zijn verantwoordelijkheden op het gebied van beveiliging verschoven [NGI1995]. Waar in een situatie van *host based security* en domme terminals de nadruk nog lag op

(informatie)beveiliging als taak van de automatiseringsafdeling, heeft de doorsnee gebruiker nu ook een voorname rol gekregen in het geheel van de beveiliging. In gedecentraliseerde en gedistribueerde systemen beheert hij zijn eigen IT-omgeving (zijn PC, software, vaste schijf, randapparaten, netwerkaansluiting), en bovendien zijn andere participanten in het netwerk afhankelijk geworden van de mate van beveiliging die hij toepast. De aansluiting van een van thuis meegebracht modem bijvoorbeeld, met welke goede bedoelingen dan ook, kan funest zijn voor de beveiliging van het interne LAN waarop de gebruiker werkt.
Dit is een behoorlijk beheerprobleem. Strakke regels en harde sancties zijn een mogelijkheid om gewenst beveiligingsgedrag af te dwingen, maar het is sterker om te proberen de gebruiker te overtuigen van het belang van een veilig Internetgebruik. Het zal in het algemeen, afhankelijk van het noodzakelijke beveiligingsniveau, nodig zijn om specifieke maatregelen te nemen om het beveiligingsbewustzijn bij individuele gebruikers te vergroten. Daarbij kan tevens een plaats worden ingeruimd voor de problematiek van *social engineering*, en voor het omgaan met programmatuur en bestanden die van het Internet worden gehaald [OTB1996]. Verschillende middelen en methoden zijn voorhanden ter verhoging van het beveiligingsbewustzijn van gebruikers; verwezen wordt naar [NGI1995].

Risicogebied: alle onderkende risico's
Preventief/repressief: beide

***Formulering standaarden en gedragsregels***
Als de organisatie op het Internet zichtbaar aanwezig is of zal zijn, is het raadzaam om standaarden te formuleren voor de wijze waarop de organisatie zich daar presenteert. Dit zorgt niet alleen voor uniformiteit maar ook voor een overweging welke gegevens wel, en welke gegevens niet voor de Internet-buitenwereld bedoeld zijn. Daarnaast verdient het aanbeveling om gedragsregels te formuleren die in acht moeten worden genomen als medewerkers van de organisatie informatie uitwisselen met anderen op het Internet, bijvoorbeeld via e-mail of nieuwsgroepen [OTB1996].

Risicogebied: alle onderkende risico's
Preventief/repressief: preventief

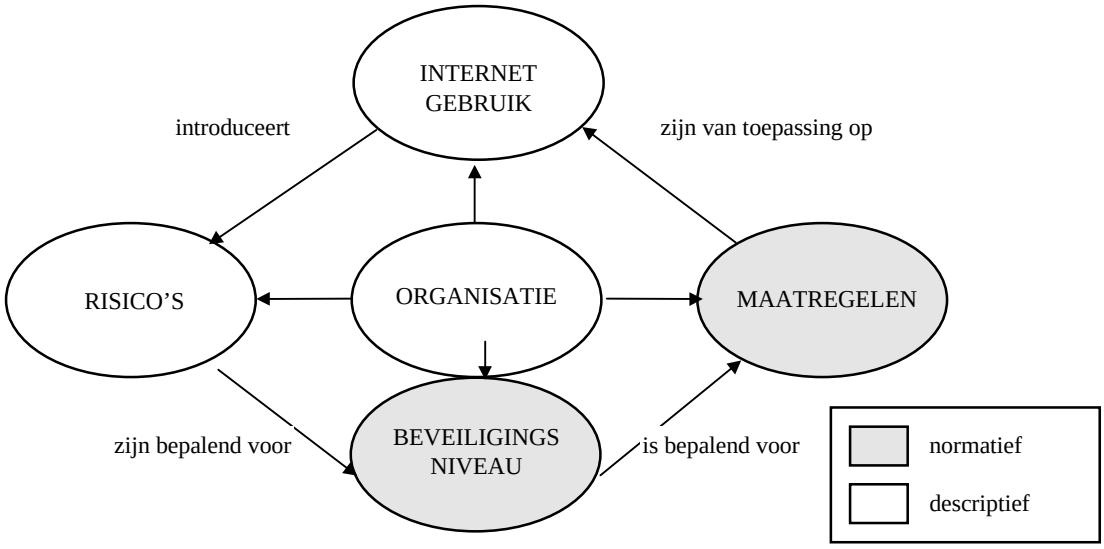
***Op peil houden van kennis***
Het realiseren van een veilig Internetgebruik vereist kennis van complexe materie. Het is dan ook niet ongebruikelijk dat organisaties hierbij steunen op expertise van specialistische dienstverleners. Hoeveel kennis men echter ook inhuurt, de eindverantwoordelijkheid voor het realiseren van het noodzakelijk geachte beveiligingsniveau blijft te allen tijde bij de organisatie zelf berusten. Om die verantwoordelijkheid te kunnen dragen moet een zekere kritische massa van kennis over Internet en beveiligingsproblematiek binnen de organisatie aanwezig zijn. Hiertoe zullen middelen (menselijke en financiële capaciteit) vrijgemaakt en gealloceerd moeten worden.
Meerdere malen al is in dit artikel de dynamiek van het Internet ter sprake gebracht. Dagelijks worden nieuwe diensten aangeboden en wordt nieuwe programmatuur ingezet en aan gebruikers ter beschikking gesteld. Hiermee zijn ook de bedreigingen voor de beveiliging van Internetgebruik zeer veranderlijk. Gerelateerd aan het gestelde over noodzakelijke kennis betekent dit, dat het op peil houden van kennis een *continue* punt van aandacht moet zijn.

Risicogebied: alle onderkende risico's
Preventief/repressief: beide

## 6. SLOTOPMERKINGEN

Ter afsluiting van dit artikel zal worden geschetst hoe het voorgaande gebruikt kan worden voor de realisatie van een permanent verantwoord Internet-gebruik. Dit zal gebeuren aan de hand van het volgende model, waarin tevens de structuur van dit artikel te herkennen is:

Centraal staat de organisatie die:
- van het Internet gebruik maakt ter ondersteuning van haar eigen informatiesystemen en bedrijfsprocessen;
- risico's onderkent die inherent zijn aan gebruik van Internet, gegeven de karakteristieken van haar bedrijfsprocessen;
- op basis hiervan een noodzakelijk beveiligingsniveau definieert, en
- op basis van dit beveiligingsniveau maatregelen neemt.




Figuur 3 Dynamisch structuurmodel

Deze abstractie is *dynamisch*; zodra in één of meerdere van de elementen een verandering optreedt wordt de cyclus opnieuw doorlopen omdat de overige elementen dan aan een heroverweging en/of herformulering onderworpen moeten worden. In het navolgende worden de samenstellende delen van dit model nogmaals kort aan de orde gesteld.

**Het Internet**

Het Internet biedt de organisatie diverse mogelijkheden een bijdrage te leveren aan de eigen informatiesystemen en bedrijfsprocessen. De communicatieservices op het Internet veranderen voortdurend. Voor een organisatie levert dit continue nieuwe mogelijkheden op voor toepassing binnen de eigen bedrijfsprocessen. Het besef dat zowel de ontwikkelingen in het Internet, als de veranderingen in het soort gebruik dat de organisatie hiervan maakt, aanleiding kunnen zijn voor nieuwe bedreigingen is zeer belangrijk[4]. Om op een veilige manier van het Internet gebruik te kunnen blijven maken is het noodzakelijk dat een dergelijke verandering wordt gevolgd door een cyclus zoals die is aangegeven in het model. Daarbij worden risico's met behulp van het gegeven risicomodel vastgesteld die voortvloeien uit de manier waarop Internetservices in informatiesystemen zijn ingepast. Vervolgens worden zodanige beveiligingsmaatregelen getroffen dat de risico's worden afgedekt conform het beveiligingsniveau dat door de organisatie is vastgesteld.

De essentie hiervan is dat de organisatie zich bewust wordt van de turbulentie en dynamiek van het probleemgebied. Het inventariseren van risico's en het treffen van beveiligingsmaatregelen is geen eenmalige actie op het moment dat Internet in de organisatie wordt geïntroduceerd. Er moet worden zorg gedragen voor cycli waarin maatregelen bij voortduring worden aangepast aan nieuwe omstandigheden.

**Risico's**

De *risico's* die voortvloeien uit het gebruik van het Internet door een organisatie zijn van divers karakter. Zij hebben betrekking op zowel de informatie die tussen communicatiepartners via het Internet wordt uitgewisseld, als op de informatiesystemen van de communicatiepartners. De aard en omvang van de risico's wordt mede bepaald door de functionaliteit het Internetgebruik. Deze risico's zijn potentieel zo groot dat het van belang is ze volledig in beeld te brengen. Belangrijk is tevens het inzicht dat de specifieke verschijningsvorm van deze risico's sterk aan verandering onderhevig is, omdat het Internet zo'n dynamische omgeving is. Voor een systematische aanpak kunnen de bedrijfsprocessen geno-

[4] Hierbij kan bijvoorbeeld gedacht worden aan de ontwikkelingen rondom *executable content* in het algemeen en Java(-applets) in het bijzonder.

men te worden waaraan het Internetgebruik bijdraagt. Het model dat in figuur 3 is gepresenteerd kan daarbij als basis dienen.

**Beveiligingsniveau**

Op grond van de risico's die de organisatie voortdurend in kaart brengt, en op basis van de karakteristieken van de bedrijfsprocessen zal de bedrijfsleiding expliciet moeten maken in welke mate de onderkende risico's moeten worden afgedekt. Dit *noodzakelijke beveiligingsniveau* is instrumenteel; formulering ervan is een middel om een afgewogen set maatregelen te kunnen treffen en om steeds te kunnen bepalen of deze set nog voldoet aan de veranderende risico's en organisatiekarakteristieken.

Het is aan te bevelen dit beveiligingsniveau expliciet gestalte te geven. Het management kan dit doen in een kort beleidsdocument, dat vervolgens gebruikt wordt om te bepalen of veranderde risico's moeten leiden tot wijzigingen in de getroffen maatregelen, en als toetssteen voor omvang en diepgang van de maatregelen. Essentieel is het "onderhoud" aan dit geformuleerde beveiligingsniveau: wijzigingen in actuele risico's, in de manier waarop de organisatie van het Internet gebruik maakt, of anderszins in de kenmerken van de organisatie zullen mogelijk moeten leiden tot een herformulering van het noodzakelijke beveiligingsniveau.

**Maatregelen**

Door uit te gaan van het noodzakelijke beveiligingsniveau kan worden bereikt dat de omvang en diepgang van beveiligingsmaatregelen zich op een goede manier verhouden tot de specifieke kenmerken van de organisatie en de risico's die ze loopt ten aanzien van Internetgebruik. Dat is belangrijk vanuit een effectiviteitsoverweging (worden de risico's afgedekt?), maar ook vanuit een efficiency-overweging (worden de risico's afgedekt conform het noodzakelijke beveiligingsniveau?).

Ook hier is het aan te bevelen een aanpak te kiezen, waarbij als uitgangspunt wordt gehanteerd dat verschillende soorten risico's verschillende soorten maatregelen vereisen. Een goede balans tussen technische en organisatorische maatregelen, waarvan sommige een preventief en andere een repressief karakter hebben is voor het bereiken van een werkzaam stelsel van beveiligingsmaatregelen noodzakelijk.

**Organisatie**

Zoals uit bovenstaande punten blijkt ligt er een forse taak voor de organisatie die op een verantwoorde manier met het Internet aan de slag wil en aan de slag wil blijven. Er is geen sprake van een eenmalige actie; er is evenmin sprake van triviale materie of van een stabiel probleemgebied. Dat leidt tot de conclusie dat gedurende de tijd dat de organisatie van Internet gebruik maakt zowel capaciteit als specifieke expertise moet worden aangewend om te waarborgen dat het noodzakelijke beveiligingsniveau kan worden gerealiseerd en gehandhaafd. De organisatie moet zich realiseren dat ze deze middelen zal moeten vrijmaken.
Overigens wordt hierbij opgemerkt, dat de organisatie dezelfde expertise moet aanwenden om de "kansen"-kant van Internetgebruik optimaal af te stemmen op de bedrijfsprocessen binnen de organisatie. Om doelmatigheidsredenen ligt het dan ook voor de hand deze specifieke Internetkennis en -capaciteit aan te sturen vanuit een coördinerende instantie of stuurgroep, die zowel verantwoordelijk is voor een goede benutting van de mogelijkheden die het Internet de organisatie biedt, als voor de instandhouding van het beveiligingsniveau dat de organisatieleiding noodzakelijk acht. In een dergelijke opzet zijn de rendementsgeoriënteerde commercie en de risico-georiënteerde beveiliging bovendien niet van elkaar geïsoleerd, en dat is in overeenstemming met hun rollen in een organisatie die op een verantwoorde manier omgaat met het Internet.

**Geraadpleegde literatuur**


[GART1996] *The Gartner Group scenario 2001: an IT Odyssey*. Strategic Analysis Report, The Gartner Group, 1996.

[KPMG1996] *Electronic Commerce: Over Internet en Intranet.* KPMG, 1996.

[LOOI1997] Looijen, M., *Beheer van Informatiesystemen.* Kluwer, 1997.

[MEEK1997] Meekeren, P. van, en M. Buijs, *Internet, EDP-auditors en deskundigheid*. In: de EDP-Auditor nr. 2, 1997

[NEUM1995] Neumann, P., *Computer related risks*. Addison Wesley 1995.

[NGI1993] *Beveiligingsbeleid en beveiligingsplan.* Rapport van het Nederlands Genootschap voor Informatica, Afdeling beveiliging. Kluwer 1993.

[NGI1995] *Beveiligingsbewustzijn bij gegevensbescherming. Hoe dit ten goede te beïnvloeden.* Rapport van de afdeling beveiliging van het Nederlands Genootschap voor Informatica. Kluwer 1995.

[OTB1996] *Internet koppelingen*. Studie van het Overlegorgaan Technische Beveiligingsstandaarden. OTB 1996.

[RIDD1997] Ridderbeekx, E., *Internet, World Wide Web en Beveiliging.* Doctoraalscriptie, Erasmus Universiteit, 1997.

[TANE1996] Tanenbaum, A., *Computer Networks*. Prentice Hall, 1996.

**Curricula vitae**

Ed Ridderbeekx is als senior EDP-auditor werkzaam bij de Interne Accountantsdienst van Generale Bank Nederland N.V.. Hij houdt zich bezig met de beoordeling van en advisering over een breed scala aan informatiebeveiligingsvraagstukken. Daarbij hebben netwerken en internetworking zijn bijzondere interesse en aandacht. Hij schrijft dit artikel op persoonlijke titel.

Jan van den Berg is als universitair docent werkzaam bij de vakgroep Informatica van de Economische Faculteit van de Erasmus Universiteit Rotterdam. Zijn onderwijs concentreert zich op de vakken computersystemen en computernetwerken. Binnen zijn onderzoek staan onderwerpen uit de kunstmatige intelligentie centraal, in het bijzonder neurale netwerken, fuzzy systems en genetische algoritmen.