

Veilig zakelijk internetten

Hoe help ik
mijn organisatie
verbeteren?

Veilig zakelijk internetten

Hoe help ik
mijn organisatie
verbeteren?

Colofon

Samenstelling en eindredactie:

Inge Aarts, ECP.NL

Jacob Boersma, ECP.NL

Joyce Martina, ECP.NL

Anke Muller-Sloos, Anthonio / Nederlof & Partners,

Management à la Anke

Alexander Overdiep, OPR / Advies

Teksten:

Diverse auteurs (zie Bijlage 6)

Ontwerp omslag en binnenwerk:

Drukkerij Sonneveld/ Programmabureau KWINT

Druk: Drukkerij Sonneveld

© Maart 2005 Programmabureau KWINT,

Leidschendam, behalve waar anders aangegeven.

KWINT is het nationaal programma van overheid en bedrijfsleven om veilig en betrouwbaar internetten te stimuleren.

Hoewel bij de samenstelling en ontwikkeling van deze publicatie *Beveiligingsbewust Management* grote zorgvuldigheid is betracht, kunnen het programma KWINT, het programmabureau (ECP.NL) en de Opdrachtgever geen aansprakelijkheid aanvaarden voor schade, van welke aard ook, die het directe of indirecte gevolg is van handelingen en/of beslissingen die (mede)gebaseerd zijn op in *Beveiligingsbewust Management* vervatte informatie.

Overname toegestaan met bronvermelding:


Programma KWINT, www.kwint.org, behalve de afbeelding op pagina 11 en 18: overname daarvan is niet toegestaan zonder voorafgaande schriftelijke toestemming van Deloitte.

ISBN : 90 - 76957 - 11 - 8

Programma:

KWINT
veilig en betrouwbaar internetten

Een initiatief van:

 Ministerie van Economische Zaken



"Internetgebruik is inmiddels heel gewoon. Zo gewoon dat in vele ondernemingen de veiligheidsroutine wat verslapt. Zorg dus met dit boekje in de hand dat uw bedrijfsinformatie niet "gratis" elders gebruikt wordt. En zorg dat u - mochten echte cybercriminelen het op uw bedrijf voorzien hebben - uzelf en uw klanten kunt verzekeren dat u het nodige hebt geregeld om schade tegen te gaan."



Jacques Schraven
Voorzitter vereniging VNO-NCW

"Internet is niet meer weg te denken. Het biedt het MKB zoveel kansen om te innoveren; bedreigingen zijn er echter ook. Denk maar aan de beveiliging van gegevens. Gelukkig staan ook op dit terrein de ontwikkelingen op de markt niet stil. Dat is te lezen in deze praktische handreiking om de beveiliging van gegevens en internet te optimaliseren. Om veilig te innoveren."



Herman Hovestad
Algemeen directeur Syntens

VNO-NCW

"ICT wordt steeds belangrijker voor ondernemingen, dus de beveiliging van ICT-systemen ook. Als ondernemer zult u het goede voorbeeld moeten geven voor uw personeel, en het belang van informatiebeveiliging moeten onderkennen."



Loek Hermans
Voorzitter
MKB Nederland



Veilig zakelijk internetten

Onlangs werd bekend dat Bill Gates vier miljoen spamberichten per dag krijgt. Microsoft heeft een speciale afdeling die ervoor zorgt dat die mails niet in zijn elektronische postbus terechtkomen. Zo kan hij toch gewoon zijn werk doen. Ik hoop dat die afdeling niet alleen bezig is met de spamberichten voor Bill Gates, maar ook met allerlei andere vormen van internetveiligheid, zoals virussen en hackers en 'denial of service attacks'.

Wat dat betreft verkeert de ondernemer in het kleinste bedrijf in dezelfde positie als Bill Gates van het grote Microsoft: als de ICT-voorzieningen niet goed zijn beveiligd, kan de schade niet te overzien zijn. Net zoals de ondernemer 's avonds nog eens controleert of alle deuren op slot zijn, zou hij of zij daarom goede controle moeten uitoefenen op de beveiliging van de elektronische toegang tot de onderneming.

De veiligheid van voorzieningen is voor mij als coördinerend ICT-Minister een speerpunt in mijn ICT-beleid. Omdat de meeste ondernemingen tot het midden- en kleinbedrijf behoren, is het juist ook voor deze groep belangrijk om de veiligheid op orde te hebben. Met het programma KWINT (KWetsbaarheid op INternet) probeer ik daarom de MKB'ers en hun branche-organisaties te ondersteunen op het gebied van veilig gebruik van ICTvoorzieningen.

In de gesprekken die ik heb met MKB'ers, merk ik gelukkig dat de beveiliging van informatie steeds meer aandacht krijgt. Steeds vaker zien niet alleen de IT-medewerkers of de systeembeheerders de noodzaak van maatregelen, maar ook het management van ondernemingen. Deze brochure helpt systeembeheerders en IT-medewerkers om nog meer aandacht te krijgen voor dit onderwerp. Ik juich deze publicatie dan ook van harte toe.

Laurens-Jan Brinkhorst,

Minister van Economische Zaken



1. Inleiding	7
2. Voor wie is deze brochure bestemd?	8
3. Wat is informatiebeveiliging en wat levert het op?	9
4. Argumenten voor beveiligingsbeleid	10
5. Hoe zorgt u voor bewustwording?	13
Introductie voor de Bijlagen	15
Bijlage 1: Checklist afhankelijkheid (elektronische) informatie	16
Bijlage 2: Model voor de Risico Management Cyclus	18
Bijlage 3: Vragen die tot nadenken stemmen	19
Bijlage 4: Hoe nu verder?	20
Bijlage 5: Programma KWINT	23
Bijlage 6: Totstandkoming publicatie	25

1. Inleiding

Voor de continuïteit van uw bedrijf is goede gegevensbeveiliging noodzakelijk. Beveiliging is echter meer dan alleen het nemen van technische maatregelen. Alleen het regelen van toegang en het eenmalig installeren van bijvoorbeeld een *firewall* (bescherming tegen ongeautoriseerde toegang tot uw bedrijfsnetwerk via een internetverbinding) en een virusscanner geeft geen veiligheid. Zeker niet als daarna niet meer naar deze beveiligingsmaatregelen wordt omgekeken. Informatie is één van de belangrijkste productiefactoren van uw bedrijf. Een goede beveiliging hiervan vereist planning en beleid.

Een goed beveiligingsbeleid en in het bijzonder beveiliging van de informatie slaagt niet zonder betrokkenheid van het management. Niet alleen omdat er budget nodig is, maar vooral omdat alle personeelsleden zich bewust moeten zijn van de risico's (de OESO¹ noemt dit een 'Veiligheidsbewuste cultuur' ('*Culture of Security*')). Beveiligingsbewustzijn is alleen te bereiken met steun van het management.

Conclusie: Bewustwording van de noodzaak tot beveiliging bij alle lagen van de organisatie is onontbeerlijk. Deze uitgave geeft handreikingen om het belang van informatiebeveiliging bij managers 'tussen de oren te krijgen'.

Deze brochure is uitgegeven door het Ministerie van Economische Zaken via het programma KWINT, voor veilig en betrouwbaar internetten, www.kwint.org.

¹ De Organisatie voor Economische Samenwerking en Ontwikkeling, een samenwerkingsverband tussen de Europese landen, de Verenigde Staten, Canada en Aziatische landen om de economische ontwikkeling van de lidstaten te bevorderen.

'MKB Europa overweldigd door virusplaag'

Bijna een kwart van het MKB in Europa moest in het eerste kwartaal van 2004 noodgedwongen zijn activiteiten tijdelijk stilleggen door virusuitbraken.

Voor de landen Frankrijk en Italië hadden erg veel last van virusuitbraken: respectievelijk 50 en 30 procent van het MKB in deze landen was tijdelijk non-actief. Hierbij gaat het om bedrijven met minder dan twintig werknemers. Ook voor Britse bedrijven geldt dat ze jaarlijks miljarden euro's kwijt zijn aan cybercriminaliteit.

De economische gevolgen van en de frequentie waarin de virussen elkaar opvolgen, zijn schadelijk voor bedrijven. Elk internetvirus kost een bedrijf in totaal vijfduizend euro door geleden schade.

De virusuitbraken kosten het MKB alleen al in West-Europa jaarlijks 22 miljard euro en het lijkt alsof het erger wordt. In het eerste kwartaal van 2004 hebben we al meer virusuitbraken gezien dan in hetzelfde kwartaal van 2003.

Vrij naar Bram Waagmeester, *Infoworld*, 29 maart 2004, met referenties naar Reuters, Jack Clark van McAfee en het Britse National Hi-Tech Crime Unit.

2. Voor wie is deze brochure bestemd?

De berichtgeving over virussen en hackers neemt toe. Toch wordt het belang van informatiebeveiliging nog door velen onderschat. Binnen of rondom organisaties zijn er gelukkig wel vaak individuen die informatiebeveiliging zien als noodzaak voor een goede bedrijfsvoering. Zij hebben echter wel hulp nodig om dit belang ook tot alle lagen van de organisatie door te laten dringen. Ze zijn 'roependen in de woestijn'. Zonder breed draagvlak zijn pogingen om de organisatie veiliger te maken gedoemd te mislukken. Omdat bijvoorbeeld het management niet het goede voorbeeld geeft en omdat medewerkers niet kunnen worden gewezen op het niet naleven van veiligheidsvoorschriften. Deze uitgave richt zich op diegenen die hun organisatie graag op alle lagen bewust willen maken van het belang van informatiebeveiliging en daarbij ondersteuning nodig hebben. Het gaat hierbij dus bijvoorbeeld om:

- systeembeheerders of IT-personeel die verantwoordelijkheid voor de beveiliging hebben gekregen, maar geen backing van het management
- IT-deskundigen die zelf overtuigd zijn van het belang van beveiliging, maar niet de juiste argumenten kunnen formuleren om ook de rest van de organisatie te overtuigen
- (middel)management van organisaties die 'iets te verliezen hebben' als de dienstverlening naar klanten en andere betrokkenen wegvalt
- het voor ICT en/of beveiliging verantwoordelijke directielid
- de beveiligingsfunctionaris (indien aanwezig)
- brancheorganisaties die iets willen doen voor de bij hen aangesloten bedrijven

De uitgave is gericht op iets grotere MKB-bedrijven, waar wordt gewerkt met computers en internet. We hebben het dan over bedrijven met meer dan 20 werknemers en bedrijven waar grote afhankelijk-

Uit de praktijk

De back-up tapes werden steeds voller en het maken van een back-up duurde steeds langer. Uit onderzoek op het netwerk kwam naar voren dat veel medewerkers afbeeldingen, videobestanden en muziekbestanden in hun persoonlijke netwerkshare geplaatst hadden. Zelfs hele CD-ROMS met software waren naar het netwerk gekopieerd. De directie van de organisatie heeft hierop een e-mailbericht naar alle medewerkers gestuurd met het verzoek om niet-werkgerelateerde bestanden te verwijderen en software op een CD-ROM te plaatsen. De hoeveelheid opgeslagen informatie op het netwerk is met 35% afgenomen.

heid is van juistheid van gegevens of beschikbaarheid van systemen. In dergelijke bedrijven zal vaak een aparte IT-afdeling of systeembeheerder bestaan (intern of extern). Om te bepalen of uw bedrijf afhankelijk is van (elektronische) gegevens kunt u de checklist in Bijlage 1 gebruiken. De uitgave is niet specifiek bedoeld voor kleinzakelijke gebruikers of particulieren. Voor hen bestaan ook andere initiatieven zoals Surf op Safe (www.surfopsafe.nl).

Als de eerste stap gezet is en het idee is doorgedrongen dat informatiebeveiliging van belang is, zal vervolgens dit belang ook moeten worden gecommuniceerd aan de werknemers. Op die manier kan worden gewerkt aan een 'veiligheidsbewuste cultuur' in de organisatie. In de latere hoofdstukken worden handreikingen en tips gegeven om samen met het management deze boodschap te communiceren binnen de organisatie. Schematisch kan dit als volgt worden weergegeven:



3. Wat is informatiebeveiliging en wat levert het op?

Informatie als bedrijfsmiddel

Informatie komt in veel vormen voor. Het kan afgedrukt of geschreven zijn op papier, elektronisch opgeslagen zijn, per post of via elektronische media worden verzonden, getoond worden in films of de gesproken vorm aannemen. Welke vorm de informatie ook heeft, of op welke manier deze ook wordt gedeeld of verzonden, informatie en gegevensverzamelingen zijn een bedrijfsmiddel. Net als andere belangrijke bedrijfsmiddelen zijn deze van belang voor een organisatie, en dienen ze voortdurend op een passende manier beschermd en beveiligd te zijn.

Bedreigingen voor bedrijfsinformatie

In toenemende mate worden organisaties en hun informatiesystemen en netwerken geconfronteerd met allerlei risico's, waaronder computerfraude, spionage, sabotage, vandalisme, brand en overstromingen. Maar ook schade veroorzaakt door virussen, hacking en het weigeren van dienstverlening (denial of service-aanvallen (DoS)) komt steeds vaker voor, en wordt steeds ambitieuzer en steeds geavanceerder.

De bedreigingen voor bedrijfsinformatie kunnen van buitenaf komen in de vorm van bijvoorbeeld hackers en virussen, maar ook van binnenuit in de vorm van fraudeerende medewerkers. Bedreigingen zijn bovendien lang niet altijd opzettelijk van aard: de meeste beveiligingsincidenten ontstaan door onzorgvuldig handelen (bijvoorbeeld het per ongeluk wissen van belangrijke gegevens of het vergeten van een wachtwoord).

Afhankelijkheid van informatiesystemen en -diensten betekent dat organisaties voortdurend kwetsbaarder worden. De onderlinge verbondenheid van openbare en particuliere netwerken en het delen van informatie-middelen maken het alsnog moeilijker om de toegang te beveiligen, omdat steeds meer mensen vanaf steeds meer plaatsen toegang moeten kunnen krijgen.

Noodzaak van informatiebeveiliging

Informatiebeveiliging beschermt gegevens tegen dit brede scala aan bedreigingen en is nodig om de continuïteit van de bedrijfsvoering te waarborgen, om de schade voor de organisatie te minimaliseren en om de kansen van de organisatie te optimaliseren. Informatiebeveiliging is gebaseerd op drie beveiligingsmerken:

1. **Exclusiviteit:** het beschermen van gevoelige informatie tegen onbevoegde, ongeautoriseerde kennisname (onbevoegden mogen vertrouwelijke documenten niet kunnen lezen).
2. **Integriteit:** het zekerstellen van de correctheid en de volledigheid van informatie en computerprogrammatuur (berichten mogen niet tijdens de verzending veranderd kunnen worden).
3. **Beschikbaarheid:** het zekerstellen dat informatie en essentiële diensten op de juiste momenten beschikbaar zijn voor gebruikers (documenten die belangrijk zijn voor de bedrijfsvoering, moeten te allen tijde toegankelijk zijn).

Als de beschikbaarheid, integriteit of vertrouwelijkheid van belangrijke informatie of de ondersteunende processen, systemen en netwerken in gevaar komt, dan kan dit negatieve gevolgen hebben voor:

- behoud van de concurrentiepositie,
- cashflow van de organisatie,
- winstgevendheid,
- naleving van wet- en regelgeving en
- imago van de organisatie naar buiten toe.

(In bijlage 1 vindt u een checklist waarmee u kunt bepalen of uw organisatie eigenaar is van gegevens die beveiliging vereisen)

Maatregelen voor informatiebeveiliging

Informatiebeveiliging kan niet worden gerealiseerd met uitsluitend technische maatregelen, maar wordt bereikt door een passende verzameling beveiligingsmaatregelen in te zetten van zowel technische als organisatorische aard. Zo kan bijvoorbeeld worden gekozen voor een virusscanner op alle computers (technische maatregel), maar dan moet ook worden afgesproken dat deze door het systeembeheer up-to-date wordt gehouden (organisatorische maatregel) en dat het personeel de virusscanner niet zomaar mag uitschakelen (organisatorische maatregel). Maatregelen kunnen verschillende vormen aannemen, bijvoorbeeld: beleid, gedragsregels, procedures, organisatiestructuren en programmatuurfuncties.

Om te bepalen welke beveiligingsmaatregelen gebruikt moeten worden is een zorgvuldige planning en aandacht voor het detail vereist. Voor het goed beheersen van informatiebeveiliging is daarom ondersteuning vanuit het management nodig en participatie van alle medewerkers van de organisatie. Bovendien kan betrokkenheid van leveranciers, klanten en aandeelhouders vereist zijn omdat ook zij een onderdeel uitmaken van de keten waarin informatie wordt uitgewisseld. Het kan nuttig zijn specialistisch advies van externe organisaties in te winnen.

De beveiligingsmaatregelen dienen te worden ontwikkeld om aan te sluiten bij de specifieke beveiligingsdoelstellingen van de organisatie. Deze doelstellingen kunnen worden bepaald door af te wegen welke processen binnen de organisatie het meest belangrijk zijn voor de continuïteit en welke informatie en informatiestromen daarbij een rol spelen.

Beveiligingsmaatregelen zijn aanzienlijk goedkoper en doeltreffender wanneer deze worden genomen tijdens het opstellen van de specificatie van eisen in de ontwerpfase van systemen en procedures. Het is daarom van belang om al in een vroeg stadium beveiligingsdoelstellingen voor de organisatie op te stellen.

4. Argumenten voor beveiligingsbeleid

Het dilemma van bedrijfscontinuïteit

Hoe goed bent u voorbereid op branden, overstromingen, virussen en andere narigheid? En tegen welke prijs? De zorgen voor bedrijfscontinuïteit houden niet op bij een back-up van een harde schijf. Deskundigen zijn eensgezind in hun analyse en menen dat het initiatief bij de directie moet liggen.

Om op hoog niveau uw organisatie te overtuigen van de noodzaak van beveiligingsbeleid zult u met goede argumenten moeten komen. Hieronder vindt u een aantal voorbeelden van hoe het mis kan gaan als informatiebeveiliging niet goed wordt aangepakt. Vervolgens wordt nader ingegaan op argumenten die u kunt gebruiken om aan te tonen dat informatiebeveiliging wenselijk of zelfs noodzakelijk is. Ten slotte worden enkele strategische vragen gegeven, die uw organisatie zal moeten beantwoorden om de gewenste investeringen in informatiebeveiliging te kunnen bepalen.

Voorbeelden

- Na een storing in de gastoevoer die dagen duurt, moet een nutsbedrijf in Zeeland zes miljoen euro schadevergoeding betalen. Oorzaak: verkeerde besturingssoftware.
- Een ziekenhuis roept alle patiënten op om gemaakte afspraken opnieuw door te bellen. Oorzaak: niet werkende harde schijf.
- Een bedrijf kampt met een defecte waterkoeling van zijn mainframe. Dat moet gerepareerd worden. De back-up tapes liggen in de kluis van een andere vestiging. Daar is net de vorige nacht ingebroken, waarbij de kluisleutels gestolen zijn.
- Een bedrijf is na een brand uitgeweken naar een andere locatie. Het uitwijksysteem is geïnstalleerd, maar wordt vanwege ruimtegebrek op de gang gezet. Veilig, want het gebouw is goed afgesloten. Tot 's ochtends de schoonmaker komt, die de stekker uit het systeem trekt om de gang te stofzuigen.
- Grolsch is een van de bedrijven die schade opliep door de vuurwerkramp in Enschede. Nadat de brandweer het gebied afzette, had het bedrijf geen toegang meer tot het systeem. Er was een back-up gemaakt, maar toen het uitwijksysteem werd opgestart, bleek dat een van de tapes ontbrak. Ze moesten 's nachts in het eigen gebouw inbreken omdat ze een tape vergeten waren.

Wet- en regelgeving stellen eisen aan beveiliging en continuïteit

De noodzaak voor risicomanagement is toegenomen. In 1990 had u drie dagen de tijd om een in de soep gelopen situatie te herstellen. Door internet (bijv. e-commerce) moeten bedrijfsgegevens 24 uur per dag beschikbaar zijn en is de hersteltijd nul geworden. Ook de wetgever stelt steeds scherpere regels. De Wet

Bescherming persoonsgegevens vraagt om een raamwerk van calamiteitprocedures rond het ICT-systeem. In het rapport van de Commissie Tabaksblatt staat de aanbeveling dat beursgenoteerde bedrijven moeten beschikken over een auditcommissie die zich bezig houdt met veiligheidsprocedures. Bedrijven zullen steeds vaker op dergelijke regels worden aangesproken.

Zorgen voor bedrijfscontinuïteit houdt niet op bij een back-up van een harde schijf. Voor iedere calamiteit die u kunt bedenken, is een scenario op te stellen. Er is niet slechts één geautomatiseerd gereedschap dat u kunt installeren om herstel van de bedrijfsvoering te garanderen. Het is veel meer een model. U moet risico's inventariseren. Waar wilt u zich wel/niet tegen beschermen?

Wet Bescherming Persoonsgegevens

De voortschrijdende automatisering en de snelle opkomst van internet maakt het steeds eenvoudiger om persoonsgegevens te verzamelen, te bewerken en te verspreiden.

Dit heeft tot gevolg dat er een spanningsveld is tussen bescherming van de persoonlijke levenssfeer van het individu en de belangen van de (semi-)overheid, het bedrijfsleven en andere organisaties.

In verband met deze ontwikkelingen is op Europees niveau in 1995 een richtlijn vastgesteld die in Nederlandse wetgeving is omgezet via de Wet Bescherming Persoonsgegevens (WBP).

De WBP is per 1 september 2001 in werking getreden en bevat regels voor het verzamelen, verwerken en verder verstrekken van persoonsgegevens. Ook kent de WBP aan de personen van wie de gegevens worden verzameld, een aantal rechten toe.

*Bron: 'Nederland gaat digitaal. Netjes volgens de regels.'
Een uitgave van Syntens en ECP.NL in opdracht van het Ministerie van Economische Zaken.*

Kostenbesparing en vermijden van (imago) schade door risicomanagement

Ondernemen betekent risico's nemen. Maar dan op weloverwogen en bewuste wijze. Een ondernemer weegt voortdurend af welke risico's hij wil lopen en welke hij denkt te kunnen dragen. Daarvoor moet hij inzicht hebben in alle relevante risico's, dus zeker ook op het gebied van informatiebeveiliging.

Hoe kan een onderneming op nu op doelmatige wijze de beveiligingsrisico's in kaart brengen? Daarvoor geven wij een handreiking aan de hand van onderstaand model. Als de directie van uw organisatie samen met de ICT-medewerker systematisch een aantal stap-

pen doorloopt, ontstaat een duidelijk beeld van de beveiligingsrisico's en de reeds getroffen maatregelen. Aan de hand daarvan is het zaak om een passende set van beveiligingsmaatregelen te kiezen en (alsnog) in te (laten) voeren. En ook om andere risico's, welbewust, te accepteren.



Model voor risicomanagement

Bij de keuzes speelt de inschatting van de ondernemer of het verantwoordelijke management een rol. De confrontatie van kosten en verwachte 'baten' van beveiligingsmaatregelen geeft daarbij een flinke steun in de rug en helpt genomen beslissingen te onderbouwen. De kosten zijn daarbij meestal redelijk in kaart te brengen, bijvoorbeeld door offertes aan te vragen voor te plegen investeringen of door de personele lasten te berekenen om bepaalde procedures op te zetten. Baten in geld uitdrukken is lastiger. Denk daarbij aan de kleinere kans op een verstoring, het veiliger gevoel en vooral ook het *niet* lijden van imago-schade.

Het afwegen van risico's, maatregelen en de kosten en opbrengsten is een voortdurend proces. Reden waarom wij spreken van een Risico Management Cyclus. Deze is goed in te passen in de reguliere planning- en beheersingscyclus van de onderneming. Als beveiliging, en het nadenken daarover, is ingebed in de reguliere bedrijfsvoering, is dit stappenplan goeddeels geslaagd. (zie ook bijlage 2)

Noodplannen en uitwijkmogelijkheden garanderen continuïteit van het bedrijf

In feite is elk onvoorziën voorval dat de ICT-processen verstoort, waardoor gegevens niet beschikbaar zijn, een calamiteit. Een grote brand of een overstroming, maar ook een gebroken kabel door graafwerk, het ont-ruimen van de omgeving vanwege een defect aan een chloortrein...

Het opstellen van een noodplan is niet voldoende. Het moet worden getest. Een back-up bewaren in een bankkluis is bijvoorbeeld veilig, maar het betekent ook dat u daar buiten kantooruren niet bij kunt. De praktijk blijkt altijd weerbarstiger dan verwacht. Variërend van

een onwaarschijnlijke opeenstapeling van voorvallen tot heel onbenullige vergissingen. Daarnaast kan continuïteit voor uw bedrijf dermate belangrijk zijn dat er een uitwijkmogelijkheid geregeld moet worden voor het geval uw normale bedrijfspand om welke reden dan ook niet (meer) toegankelijk is. Want na een calamiteit moeten de ICT-apparatuur en bedrijfsinformatie(systemen) weer snel beschikbaar zijn. Voor een groot bedrijf met verscheidene vestigingen is het wellicht een optie om de vestigingen voor elkaar als uitwijkmogelijkheid te laten fungeren. Een alternatief is het afsluiten van een contract met een leverancier van uitwijkmogelijkheden. In alle gevallen geldt dat procedures, en niet improvisatie, daarbij de basis moeten vormen van de opbouw van de uitwijk-omgeving en dat er regelmatig getest moet worden of alles wel volgens plan verloopt of dat er bijvoorbeeld sinds de laatste test zaken binnen het bedrijf veranderd zijn die niet zijn verwerkt in het uitwijkdraaiboek.

Bedrijfscontinuïteit is een verantwoordelijkheid van het management

De verantwoordelijkheid voor bedrijfscontinuïteit hoort niet op het bord van de ICT-afdeling te liggen. De verantwoordelijkheid én het initiatief moeten bij de directie liggen. U kunt niet volstaan met anti-virus soft-

'Onoverzichtelijk+complex=kwetsbaar'

In de datacentra van de grote multinationals gaat de vertrouwde leus 'hoe meer, hoe beter' allang niet meer op. Meer data-infrastructuur leidt automatisch tot meer onoverzichtelijkheid en dus tot grotere kwetsbaarheid van het netwerk. Door de ongebreidelde groei en fusies van de afgelopen jaren dijen de ooit efficiënte en geavanceerde datacentra uit tot logge, onoverzichtelijke structuren. In grote Amerikaanse bedrijven is het normaal dat er zes of meer besturingssystemen en vier hardwareplatforms zijn geïnstalleerd. Het aantal verschillende applicaties loopt al gauw in de honderden. Hackers hebben de doelen dus voor het uitkiezen, want in de applicatielaag kunnen ze de grootste schade aanrichten, bijvoorbeeld door geld naar hun eigen rekening te sluizen. En dan gaat het meestal om aanzienlijk grotere bedragen dan bij gestolen creditcardinformatie uit een database. Stroomlijning van de infrastructuur op basis van consolidatie stelt een ICT-team in staat effectiever te reageren op onbevoegd gebruik, datacorruptie, verspreiding van virussen en wormen en allerlei andere vormen van aanvallen op het netwerk. Consolidatie stelt u in staat om ook de gevoelige data en applicaties in de middelste laag en op datacentrum-niveau te beveiligen.

Vrij naar David Auslander & Ken Won, respectievelijk chief architect bij Sun Professional Services en marketingdirecteur bij Sun Datacenter Marketing. Bron: InfoWorld, 28 april 2004.

ware en een firewall. Als maatregelen en hulpmiddelen niet procedureel in een organisatie geborgd worden en zijn, zijn ze niet effectief. Het is schrikbarend hoeveel bedrijven een firewall hebben waarvan de poorten wagenwijd openstaan.

Bedrijven investeren honderdduizenden euro's in back-upoplossingen waar ze amper toegang toe hebben. Iedereen kan data kopiëren van a naar b, maar kunt u er ook bij?

Een goed beveiligingsbeleid kan uw concurrentiepositie verbeteren

Tenslotte kunnen maatregelen om de continuïteit van uw bedrijf te waarborgen ook helpen in het versterken van de concurrentiepositie van het bedrijf. Als u kunt aantonen dat uw organisatie de risico's goed kan beheersen en de juiste maatregelen heeft genomen om de continuïteit van de dienstverlening veilig te stellen, maakt dit uw bedrijf een aantrekkelijke zakenpartner. Een certificaat van een onafhankelijke auditor (bijvoorbeeld voor de Code voor Informatiebeveiliging) kan ook een belangrijke rol spelen om het beveiligingsbewustzijn van een bedrijf te profileren.

Bepaal goed de risico's en maak informatiebeveiliging niet duurder dan nodig

Als zonder planning beveiligingsmaatregelen worden ingevoerd, zullen deze vrijwel zeker niet effectief of veel te duur zijn. Alleen als de risico's die een bedrijf loopt, goed in kaart zijn gebracht en als bepaald is welke risico's moeten worden teruggedrongen en welke kunnen worden geaccepteerd, kan er zinvol worden geïnvesteerd in de juiste maatregelen. Samenvattend kunnen we stellen dat er eerst een paar vragen beantwoord moeten worden, voordat een bedrijf gaat investeren in beveiligingsoplossingen.

Strategische vragen om de noodzakelijke investeringen te bepalen:

- Hoe belangrijk zijn gegevens voor uw onderneming: wat kost een dag dataverlies? En wat kost het maken, beschermen en opslaan van back-ups?
- Welke bedrijfscontinuïteit wordt er nagestreefd? En tot welk niveau?
- Welke kosten en inspanning heeft u hiervoor over?
- Hoever moet uitwijklocatie van de eigen vestiging verwijderd staan?
- Is eigen uitwijk geregeld of wordt dit ingehuurd bij een specialist?

Informatie in dit hoofdstuk: Vrij naar Peter Steeman, Infoworld, 09 februari 2004 en de code voor informatiebeveiliging versie 2, januari 2000, NEN.

5. Hoe zorgt u voor bewustwording?

Goede informatiebeveiliging vereist beveiligingsbewustzijn bij alle medewerkers van een organisatie. Als managers eenmaal overtuigd zijn van het belang van beveiliging, is de volgende stap dus om ook bij de rest van de organisatie dit besef te laten doordringen. Overtuigen van het management kan bovendien eenvoudiger worden als u hen ook al direct kunt laten zien hoe communicatie naar de rest van de organisatie toe het beste kan worden vormgegeven. Dit hoofdstuk geeft daarom tips en informatie over het creëren van beveiligingsbewustzijn bij alle medewerkers. Maar ook als u het management van uw organisatie nog niet overtuigd hebt, kunnen sommige van deze tips nuttig zijn, hetzij om direct het management te overtuigen (bijvoorbeeld door het uitvoeren van een risicoanalyse of het inschakelen van een externe partij), hetzij om andere medewerkers meer bij te brengen over het belang van beveiliging en zo indirect het management te bereiken.

Als we het hebben over het werken aan bewustzijn op het vlak van informatiebeveiliging bij medewerkers van een organisatie, moeten we - ongeacht op welk niveau deze medewerkers opereren - onderscheid maken tussen drie categorieën, te weten: Kennis, Houding en Gedrag:

1. Kennis
De medewerker heeft geen flauwe notie van het bestaan van informatiebeveiliging en hecht ook (nog) geen enkele waarde aan het beveiligen van informatie. Er is geen bewustzijn en dus ook geen specifieke attitude t.a.v. informatiebeveiliging. Geen sympathie, maar ook geen antipathie. Het besef is (nog) in onvoldoende mate ontwikkeld.
2. Houding
De medewerker weet van het bestaan van informatiebeveiliging en heeft reeds onderkend dat informatiebeveiliging serieus moet worden genomen. In principe staat de medewerker positief tegenover informatiebeveiliging, echter het ontbreekt hem/haar nog aan de juiste zintuigen. Het is voor deze medewerker moeilijk om situaties juist in te schatten en kwetsbaarheden, bedreigingen, schade en dus risico's goed te beoordelen. Zo ook de kwaliteitseisen die moeten worden gesteld aan de informatievoorziening (beschikbaarheid, integriteit en vertrouwelijkheid). De medewerker wil wel, maar het bewustzijn - het vermogen tot inschatting - is (nog) onvoldoende ontwikkeld.
3. Gedrag
De medewerker weet van het bestaan van informatiebeveiliging, maar heeft negatief gedrag ontwikkeld. Dit kan uiteenlopende oorzaken hebben, bijvoorbeeld doordat maatregelen zijn opgelegd zonder dat de redenen voor het treffen van deze maatregelen goed duidelijk zijn gemaakt. Of omdat de maatregelen een grote belemmering vormen en het werk (bijna) onmogelijk maken. Het zal extra energie kosten om het gedrag van deze categorie te laten omslaan naar een positieve houding.

In dit hoofdstuk worden een aantal manieren aangegeeft waarmee het bewustzijn van medewerkers te prikkelen is, zowel medewerkers uit categorie 1, 2 als 3. Het is aan u om voor uw specifieke situatie te bepalen welke methoden bruikbaar zijn. Let wel, het daadwerkelijk inrichten van informatiebeveiliging, het geven van een invulling aan informatiebeveiliging, is hierbij nog niet aan de orde. Het gaat met name om het creëren van een kritische massa, ofwel voldoende toewijding (commitment), in de organisatie, om vervolgens succesvol informatiebeveiliging te kunnen lanceren, niet als project maar als proces.

Voorbeelden van te ondernemen acties zijn (in willekeurige volgorde):

Voer gezamenlijk een risicoanalyse uit

Het gezamenlijk uitvoeren van een risicoanalyse - hetzij serieus of als exercitie - kan zeer verhelderend zijn. U wordt gedwongen goed na te denken over afhankelijkheden, kwetsbaarheden, mogelijke bedreigingen en eventuele schade. Het management weet en beseft veelal niet wat de gevolgen kunnen zijn van een incident. Vooral het kwantificeren doet de ogen openen. Het gaat hierbij in hoofdzaak om de acceptatie van 'het probleem': hebben we een boze vijand of niet? Het bepalen van maatregelen hoeft nog niet aan de orde te zijn.

Span een derde partij voor uw kar

Vreemde ogen dwingen. Dit gaat niet alleen op voor kinderen, maar ook voor organisaties. Hoe jammer dat ook is, vaak wordt met meer aandacht geluisterd naar de accountant dan naar de eigen mensen. Een kritisch rapport van een in informatiebeveiliging gespecialiseerde partij kan ook helpen het management te laten beseffen dat informatie in wezen een belangrijk bedrijfsmiddel is en de betrouwbaarheid van de informatievoorziening aandacht behoeft.

Hang prikkelende posters op

Net zoals bij reclame kan door middel van gerichte uitingen een 'pull' teweeg worden gebracht. Een goede poster zet mensen aan tot nadenken, vooral als de uitgebeelde situaties zeer herkenbaar zijn. Hang ze bijvoorbeeld op bij de koffieautomaat.

Stel prikkelende vragen

'Wat als'-vragen kunnen een prikkelende werking op het bewustzijn hebben. Wat als de mailserver crasht? Of een specifieke fileserver? Vooral op terreinen waarvan we weten dat zaken niet goed geregeld zijn. Wat als de accounts van vertrokken medewerkers of inhuurkrachten blijven bestaan? Wat als een medewerker of een leverancier een laptop met een virus op het interne netwerk aansluit? Voorbeelden van prikkelende vragen zijn te vinden in Bijlage 3.

Rapporteur

Wat er mis is op het vlak van informatiebeveiliging is vaak niet zichtbaar. Pas wanneer centraal gerapporteerd wordt, ontstaat er een beter beeld van het pro-

bleem. Een incident op zich hoeft niets te betekenen, maar in een aantal incidenten tezamen kan een trend worden onderkend. Door te rapporteren - en niet alleen over incidenten, maar ook bijvoorbeeld gebeurtenissen waar het net niet fout ging - wordt informatiebeveiliging zichtbaar.

Laat incidenten gebeuren en meet ze breed uit

Organisaties en informatieleverende systemen kunnen zeer kwetsbaar zijn, zonder dat u daar erg in heeft. Ook al zijn maatregelen genomen, organisatorisch en/of technisch, toch kunnen er nog 'blinde vlekken' zijn die verdere aandacht behoeven. Door incidenten te laten gebeuren, liefst zonder daadwerkelijk schade aan te richten, kunnen kwetsbaarheden worden aangetoond. Kwetsbaarheden die door kwaadwillenden kunnen worden benut. De boodschap is: "Kijk, zo gemakkelijk is het om ...". Acties die kunnen worden ondernomen en waarvoor eventueel de hulp van een derde partij kan worden ingeroepen, zijn het onder vrijwaring laten uitvoeren van penetratietesten. Dit zijn testen waarbij wordt vastgesteld hoe eenvoudig of moeilijk het is bij een organisatie binnen te dringen, hetzij vanaf internet of het interne netwerk met de belangrijke ICT-systemen als doelobject, hetzij door een 'ongenode gast', als insluiper, met kantoren en de eigen medewerkers als doelobject.

Confronteer!

Over gegevensbeveiliging bestaan harde cijfers. Cijfers tonen aan hoe het doorgaans gesteld is met informatiebeveiliging. Cijfers die ook vertellen hoe kwetsbaar u al snel bent als u niet minimaal een aantal zaken heeft geregeld. Goede voorbeelden zijn eenvoudig te vinden, zie veel van de kaderstukjes in deze publicatie. Als u dit combineert met wat er al mis gaat (uit de rapportages) en wat er mis kan gaan (zie de vorige paragraaf), dan heeft u goed materiaal om belanghebbenden van potentiële risico's - door niets te doen - bewust te maken.

Benader het positief

Er zijn veel voorbeelden van hoe organisaties het gered hebben, konden overleven, dankzij het treffen van de juiste maatregelen. Er zijn ook voorbeelden van grote schade ten gevolge van beveiligingsincidenten. Echter met doemscenario's schiet u in het algemeen niet zo veel op. Met de combinatie van negatieve en positieve voorbeelden kunnen medewerkers worden overtuigd van het nut van gegevensbeveiliging. Zo kan worden aangetoond dat gegevensbeveiliging in belangrijke mate bijdraagt aan de continuïteit van de organisatie.

Geef een helder kosten/baten-plaatje

Gegevensbeveiliging wordt vaak gezien als kostenpost, zonder dat daar baten tegenover staan. Als een verzekering waar u jarenlang (te) veel geld aan kwijt bent, zonder verder enig profijt voor de organisatie. Maar is dat ook zo? Nee! Door informatiebeveiliging aandacht te geven is wel degelijk een betere bedrijfsvoering mogelijk met aanwijsbare baten. Denk bijvoorbeeld aan een bijdrage aan het imago, het terugdringen van kosten (geld wat u niet (meer) uitgeeft, is winst!), processen die meer of beter gestructureerd, soepeler verlopen, etc. Hoofdstuk 3 geeft ook uitleg over wat gegevensbeveiliging oplevert.

Geef een goede presentatie

Rondom gegevensbeveiliging hangt nog steeds vaak mist. Men heeft amper een beeld van wat het inhoudt en houdt er daardoor een (verkeerd) beeld op na met wellicht ook enkele achterhaalde vooroordelen. Tel daar bij op 'onbekend maakt onbemind', dan is daarmee de neutrale of negatieve houding tegenover gegevensbeveiliging verklaard. Wilt u hier wat aan doen, organiseer dan voor de (eind)verantwoordelijken - veelal het management, dus de directie met de managementlaag daaronder - een heldere presentatie over gegevensbeveiliging. Houd deze presentatie laagdrempelig en eenvoudig. Gegevensbeveiliging hoeft niet ingewikkeld te zijn.

En ten slotte: geef zelf het goede voorbeeld!

Uit de praktijk

De organisatie dacht haar IT-beveiliging goed voor elkaar te hebben. Dubbele firewalls, de laatste patches en hotfixes geïnstalleerd en een virusscanner met recente virusdefinities. Toch liet de organisatie een security audit uitvoeren. Bij de security audit hoorde ook een code review. Hieruit kwam naar voren dat de scripts op de webserver geen invoervalidatie kenden. Hierdoor kon iedere websitebezoeker met behulp van de zoekpagina op de website de webserver hacken. Door het toevoegen van een paar extra regels code werd dit probleem verholpen.

In de bijlagen vindt u een praktische verzameling stukken die u helpen uw organisatie verbeteren.

Dat betekent niet dat u begint bij Bijlage 1 en doorgaat tot het eind en dat dan uw organisatie helemaal op orde is. Deze bijlagen zijn er vooral om uw ondernemerschap te prikkelen. En om u te laten zien wat er allemaal al bedacht is waar u uw voordeel mee kunt doen.

Bijlage 1: Checklist afhankelijkheid (elektronische) informatie

Op de volgende bladzijde vindt u een checklist waarmee u kunt komen tot een classificatie van de gegevens (digitaal, maar ook op papier) die in uw organisatie worden gebruikt. Het doel van een dergelijke gegevensclassificatie is om vast te stellen of een organisatie eigenaar (of beheerder) is van gegevens die beveiliging vereisen. Het is dus een soort checklist om bewustzijn te creëren van de noodzaak van passende beveiligingsmaatregelen. Immers, niet iedere organisatie is zich bewust van het soort gegevens dat het onder beheer heeft.

Uiteindelijk is het beter om de processen te classificeren in uw organisatie, op basis van de gegevens die bij die processen verwerkt worden. Als daarbij wordt geconstateerd dat een proces kwetsbaar is (omdat er kwetsbare gegevens in worden verwerkt), kunt u tot de conclusie komen dat het nodig is het proces op een gestructureerde manier opnieuw in te richten met passende beveiligingsmaatregelen. Hierbij kunt u gebruik maken van de Code voor Informatiebeveiliging (ISO 17799, uitgegeven door NEN)

Bij processen waarbij (potentieel) gevoelige gegevens worden verwerkt, kunt u denken aan:

- Salarisbetalingen / salarisadministratie
- Uitsturen van facturen
- Betalen van leveranciers
- Rapportages opleveren (intern en extern)
- Accepteren van opdrachten
- In- en extern rapporteren
- Privacygevoelige processen

Invulinstructie

Bij de categorieën op de volgende pagina dient u steeds voor uzelf de volgende vragen te beantwoorden en het bijbehorende niveau van kwetsbaarheid aan te vinken:

Integriteit

Hoe erg is het als de betreffende gegevens ongemerkt worden veranderd gedurende verzending? Hoe erg is het als de identiteit van de afzender van de betreffende gegevens niet kan worden geverifieerd? (Laag: geen enkel gevolg voor de bedrijfsvoering, Baseline: storend, maar oplosbaar probleem, Hoog: forse schade (in tijd/geldlimago), Zeer hoog: kan leiden tot faillissement, rechtszaak e.d.)

Exclusiviteit

Hoe erg is het als de betreffende gegevens bij de verkeerde ontvanger terechtkomen? Hoe erg is het als deze gegevens publiekelijk worden verspreid? (Laag: geen enkel gevolg voor de bedrijfsvoering, Baseline: storend, maar oplosbaar probleem, Hoog: forse schade (in tijd/geldlimago), Zeer hoog: kan leiden tot faillissement, rechtszaak e.d.)

Beschikbaarheid

Hoe erg is het als de betreffende gegevens niet op korte termijn beschikbaar zijn of kunnen worden gemaakt? (Laag: het is geen probleem als de gegevens nooit meer boven water kunnen worden gehaald, Baseline: de gegevens mogen een paar dagen niet beschikbaar zijn voordat forse schade (in tijd/geldlimago) optreedt, Hoog: de gegevens mogen enige uren niet beschikbaar zijn voordat forse schade optreedt, Zeer hoog: de gegevens moeten altijd vrijwel onmiddellijk beschikbaar zijn, anders treedt schade op)

Gegevensclassificatie checklist

Persoonsgegevens

		laag / n.v.t.	baseline	hoog	zeer hoog
NAW gegevens (Naam, Adres, Woonplaats etc.)	integriteit exclusiviteit beschikbaarheid				
NAW (vertrouwelijk) (privé-adres, geheim telefoonnummer etc.)	integriteit exclusiviteit beschikbaarheid				
Persoonlijke gegevens (gegevens over burgerlijke staat, sofinummer etc.)	integriteit exclusiviteit beschikbaarheid				
BKR gegevens (Bureau Krediet Registratie)	integriteit exclusiviteit beschikbaarheid				
Justitiële gegevens (strafblad, boetes etc.)	integriteit exclusiviteit beschikbaarheid				
Fiscale gegevens (belastingaangifte, bankafschriften etc.)	integriteit exclusiviteit beschikbaarheid				
Gegevens m.b.t. sociale activiteiten (lid verenigingen etc.)	integriteit exclusiviteit beschikbaarheid				
Medische gegevens	integriteit exclusiviteit beschikbaarheid				
Gegevens m.b.t. communicatie activiteit (belgedrag, surfgedrag)	integriteit exclusiviteit beschikbaarheid				
..... (persoonspecifiek, zelf invullen)	integriteit exclusiviteit beschikbaarheid				

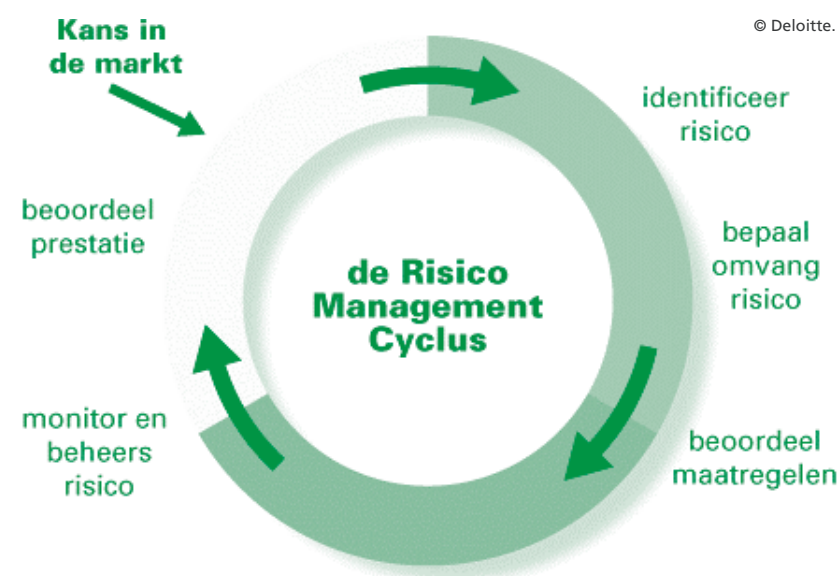
Voetnoten

- 1 Naast beveiliging als ondersteuning van het ondernemingsdoel, kan beveiliging ook een vereiste zijn vanuit wetgeving. Te denken valt aan de WBP, Telecomwet, Wet Computercriminaliteit etc.
- 2 De Wet Bescherming Persoonsgegevens stelt hogere eisen aan het verwerken en opslaan van de volgende persoonsgegevens: godsdienst, levensovertuiging, ras, gezondheid, seksuele leven, lidmaatschap vakvereniging, politieke gezindheid, strafrechtelijke persoonsgegevens en onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag

Bedrijfsgegevens (1)

		laag / n.v.t.	baseline	hoog	zeer hoog
NAW gegevens klanten (Naam, Adres, Woonplaats etc.)	integriteit exclusiviteit beschikbaarheid				
NAW klant (vertrouwelijk) (privé-adres, geheim telefoonnummer etc.)	integriteit exclusiviteit beschikbaarheid				
Bijzondere persoonsgegevens (2) (zoals bedoeld in de WBP)	integriteit exclusiviteit beschikbaarheid				
Website gegevens	integriteit exclusiviteit beschikbaarheid				
KvK gegevens (Kamer van Koophandel)	integriteit exclusiviteit beschikbaarheid				
Intellectueel eigendom (source code, recepten, nog niet uitgebrachte muziek, etc.)	integriteit exclusiviteit beschikbaarheid				
Klantgegevens, overig (ordergeschiedenis, accountmanagement gegevens etc.)	integriteit exclusiviteit beschikbaarheid				
Overige concurrentiegevoelige gegevens (offerte's e.d.)	integriteit exclusiviteit beschikbaarheid				
Financiële gegevens (niet openbaar)	integriteit exclusiviteit beschikbaarheid				
Personeelsgegevens (adresgegevens, personeelsdossiers, etc.)	integriteit exclusiviteit beschikbaarheid				
Koersgevoelige gegevens (niet openbaar en niet financieel)	integriteit exclusiviteit beschikbaarheid				
Juridische gegevens (elektronische koopovereenkomst etc.)	integriteit exclusiviteit beschikbaarheid				
..... (branchespecifiek, zelf invullen)	integriteit exclusiviteit beschikbaarheid				

Bijlage 2: Model voor de Risico Management Cyclus



Zoals bijgaande figuur al aangeeft moet Risico Management cyclisch worden uitgevoerd, bij voorkeur in samenhang met de reguliere planning- en beheersingscyclus van de onderneming. Dit betekent ook dat het beste effect wordt bereikt als deze actie wordt uitgevoerd als een gezamenlijke activiteit van het managementteam en de verantwoordelijke ICT-medewerker. De ICT-medewerker om beveiligings(aspecten van)risico's in kaart te brengen evenals reeds ingevoerde maatregelen en om, waar nodig, aanvullende maatregelen voor te stellen en/of te zorgen voor implementatie. Het management als verantwoordelijke voor de bedrijfsdoelstellingen, maar vooral ook om te beoordelen of het verantwoord is een risico te dragen of dat het juist getuigt van een gezonde bedrijfsvoering om bijtijds te investeren in maatregelen.

In de Risico Management Cyclus worden achtereenvolgens de volgende stappen gezet:

- breng de overkoepelende doelstellingen van het bedrijf of de organisatie in kaart
- identificeer de risico's die hiermee verbonden zijn
- breng de impact van deze risico's in kaart (wat zijn de kosten als het misgaat?)
- beoordeel de effectiviteit van de huidige beheersingsmaatregelen
- stel aan de hand van de eerdere stappen vast in welke mate de organisatie kwetsbaar is
- bepaal in hoeverre deze kwetsbaarheid acceptabel (te dragen) is
- tref maatregelen als de kwetsbaarheid niet acceptabel is

Bij het bepalen van de te nemen maatregelen om het verschil tussen het huidige en het gewenste niveau van informatiebeveiliging te overbruggen, dient de onderneming/organisatie steeds de te maken kosten en verwachte baten tegen elkaar af te wegen. De kosten zijn daarbij in de regel redelijk in kaart te brengen. Door bijvoorbeeld offertes aan te vragen voor te plegen investeringen of door de personele lasten te berekenen om bepaalde procedures op te zetten, kan een bruikbare raming van de te maken kosten worden gemaakt.

Bij het in geld uitdrukken van de te verwachten baten speelt de complicatie dat een hoger niveau van beveiliging of een kleinere kans op een verstoring of incident, zich niet zo eenvoudig in geld laat uitdrukken. Toch kunnen wettelijke vereisten of 'simpelweg' de behoefte aan een beter gevoel van veiligheid voor het management en de directie aanleiding zijn in informatiebeveiliging te investeren. Daarnaast kunnen ook als baten geldende schade (aan imago of daadwerkelijke bedrijfsresultaten) die niet opgelopen wordt bij een goede beveiliging.

Bron: De Code voor Informatiebeveiliging, Versie 2, Januari 2000, NEN

Bijlage 3: Vragen die tot nadenken stemmen

Onderstaande vragen zijn voorbeelden van het soort vragen dat u kunt stellen aan managers of collega's om hen te laten nadenken over kwetsbaarheid van de informatiesystemen in hun organisatie. De vragen kunnen het begin zijn van een (informele) risicoanalyse, waarbij kan worden gekeken hoe vaak een potentiële kwetsbaarheid zich voordoet en wat de gevolgen zijn als het misgaat.

- 1 Weet u precies wie uw medewerkers en collega's zijn? Dan weet u ook wie te gast is in uw bedrijfspand. Spreekt u deze bezoekers aan als ze zonder begeleiding door het pand lopen?
- 2 Sluit u de PC van een collega af als deze het kantoor verlaten heeft en u ook vertrekt? Ook als deze alleen maar een paar minuten weggaat?
- 3 Is het mogelijk uw bedrijfspand uit te lopen met een PC of laptop onder uw arm?
- 4 Houdt u de deur open voor uw collega's? Houdt u de deur open voor andermans bezoekers? Houdt u de deur open voor de loodgieter?
- 5 Zijn uw collega's op de hoogte van uw wachtwoord? Ook niet als u op vakantie gaat?
- 6 Maakt u op meerdere plaatsen gebruik van één en hetzelfde wachtwoord?
- 7 Krijgt een medewerker met een tijdelijk contract ook de beschikking over de wachtwoorden die door uw collega's en u gebruikt worden?
- 8 Synchroniseert u uw vertrouwelijke gegevens van een laptop met het netwerk? En ook met een PDA? Wat gebeurt er als u deze laptop of PDA kwijtraakt? Zijn de gegevens alleen met een Windows-wachtwoord beschermd?
- 9 Als u een website bezoekt, wordt u wel eens gevraagd om eerst iets te installeren voordat u verder kunt? Klikt u dan op 'Ok'?
- 10 Bent u wel eens voor niets naar de printer gelopen omdat uw uitgeprinte documenten er niet inlagen? Heeft u zich wel eens afgevraagd wat er met uw afgedrukte documenten gebeurd is?
- 11 Heeft uw wel eens een vreemd e-mail bericht ontvangen van iemand die u niet kent? Zat daar ook wel eens een bijlage bij? Heeft u deze bijlage ook geopend? En wat doet u als een bekende u een bijlage toezendt die u niet verwacht?
- 12 Hoe erg is het als uw PC en/of de gegevens die erop staan, blijvend onbruikbaar zijn?
- 13 Wat is uw bedrijfslaptop waard voor u? En hoeveel voor een dief? En hoeveel voor een concurrent?
- 14 Is uw internetverbinding de hele dag 'open' sinds u ook ADSL heeft? En hoort u de PC wel eens 'draaien' zonder dat u of iemand anders er achter zit?
- 15 Is het allemaal waar wat er op internet staat? Wél als het op de website van uw branchevereniging staat? Of op de website van uw bank? Hoe herkent u een betrouwbare website?

Bijlage 4: Hoe nu verder?

Als u meer wilt weten over het opzetten van een goed beveiligingsbeleid in uw organisatie, kijk dan ook eens hier:

Websites:	
antivirus.pagina.nl	Startpagina voor allerlei sites over antivirus software
windowsupdate.microsoft.com	Bedrijfsite van Microsoft - downloaden van (critical) updates met behulp waarvan uw PC (zo) veilig (mogelijk) te maken en houden is
www.antiphishing.org	Site over phishing - wat het is en hoe het te voorkomen
www.govcert.nl	Het Computer Emergency Response Team van de Nederlandse overheid. De organisatie biedt ondersteuning aan de overheid op het gebied van preventie en afhandeling van ICT-gerelateerde veiligheidsincidenten, zoals computervirussen, hacker-activiteiten en fouten in applicaties en hardware.
www.grc.com	Hier is "Shields Up" te vinden - een gratis Internet veiligheidscontrole- en informatiedienst.
www.gvib.nl	Genootschap van Informatie Beveiligers - Indien u zich beroepsmatig bezig moet houden met de vertrouwelijkheid, beschikbaarheid en integriteit van informatie, zult u zich al snel rekenen tot de groep van personen die zich bezig houdt met informatiebeveiliging. Mogelijk doet u dat als Informatie technologie manager of als auditor. Wellicht werkt u voor de overheid, bij een bank of in het bedrijfsleven.
www.hackerwhacker.com	Site met nieuws, informatie en (gratis) gereedschap om te voorkomen dat uw PC of netwerk gehackt wordt (zie ook "HackYourself")
www.informatiebeveiliging.nl	Deze website is bedoeld als informatiekanaal voor ondernemers en managers die belangstelling hebben voor het onderwerp informatiebeveiliging. U vindt hier nieuws over dit onderwerp, dossiers over deelonderwerpen van informatiebeveiliging en aankondigingen van evenementen met als thema: beveiliging.
www.isaca.nl	Site van de Information Systems and Control Association
www.kwint.org	Programma Kwint voor veilig en betrouwbaar internetten. Informatie- en communicatietechnologie in het algemeen en Internet in het bijzonder vormen een steeds belangrijkere schakel in de huidige samenleving. De mogelijkheden die Internet biedt, worden echter nog onvoldoende benut. Een belangrijke reden hiervoor is de onveiligheid die veel gebruikers van Internet ervaren.
www.ictoffice.nl	ICT-Office behartigt de economische belangen van de aangesloten organisaties richting politiek en overheid. Met een achterban die meer dan 25 miljard euro omzet en ruim 200.000 medewerkers telt, is ICT-Office dé woordvoerder van de Nederlandse ICT-sector.

www.nivra.nl	Het Koninklijk Nederlands Instituut van Registeraccountants (NIVRA) is de publiekrechtelijke beroepsorganisatie van de ruim 13.000 registeraccountants. Een profiel van het NIVRA geeft u meer informatie over de taken van de beroepsorganisatie en de positie van het NIVRA in de maatschappij.
www.norea.nl	Site van de beroepsorganisatie van IT-auditors
www.platforminformatiebeveiliging.nl	Het Platform Informatiebeveiliging, kortweg PI genoemd, is een vereniging die zich beijert voor de beveiliging van informatie en informatiesystemen. De belangrijkste pijler voor PI is het ontwikkelen en onderhouden van richtlijnen voor de praktische inrichting van informatiebeveiliging. Het organiseren van themabijeenkomsten is een tweede pijler voor de onderlinge samenwerking tussen de leden.
www.security.nl	Site is opgericht en wordt onderhouden door een groep van specialisten op het gebied van gegevensbeveiliging.
www.surfopsafe.nl	Deze website informeert u, als consument of kleine zakelijke gebruiker, over het veilig gebruik van internet. Ook biedt Surf op Safe de mogelijkheid om vragen te stellen aan een team van deskundigen.
www.uni-cert.nl	KPN-CERT ondersteunt de klant [van het KPN netwerk] pro-actief om de veiligheid van niet alleen het eigen bedrijfsnetwerk te waarborgen, maar ook de netwerken waarover KPN de dienstverlening aan haar klanten biedt. Onderdeel van het verzorgingsgebied zijn de consumenten ISP's Planet Internet en HetNet. KPN-CERT verzamelt en analyseert bovendien incidenten en geeft advies om deze in de toekomst te voorkomen. Het gaat hier om incidenten die door klanten uit het verzorgingsgebied reactief zijn aangemeld, alsmede over klanten uit het verzorgingsgebied.
www.waarschuwingsdienst.nl	Gratis ; De Waarschuwingsdienst, een initiatief van het ministerie van Economische Zaken, waarschuwt computergebruikers en kleinbedrijf tegen computervirussen en lekken in software. De Waarschuwingsdienst is een dienst van het Computer Emergency Response Team van de Nederlandse overheid.
www.zonelabs.com	Site met informatie en (gratis) producten ter bescherming van uw PC

...en kijk ook eens bij uw branchevereniging!

Publicaties:

- Nederland gaat digitaal, met een veilig gevoel - Wim Sipman e.a. (Syntens 2002, www.syntens.nl)
- Informatiebeveiliging onder controle - Paul Overbeek (Financial Times 2000, Exin 2004)
- Code voor Informatiebeveiliging - NEN-ISO/IEC 17799-2002 (NEN 2004)
- Code of Practice for Information Security Management, ISO 17799 (ISO standard, 2000)
- Fighting Computer Crime, a New Framework for Protecting Information - Donn B. Parker (John Wiley & Sons, 1998)
- Beyond Fear, Thinking Sensibly about Security in an Uncertain World - Bruce Schneier (Copernicus Books 2003)
- Secrets & Lies, Digital Security in a Networked World - Bruce Schneier (John Wiley & Sons, 2000)
- The Art of Deception: Controlling the Human Element of Security - Kevin Mitnick (John Wiley & Sons, 2002)
- ITIL Security Management - OGC (Exin 1999)

Opleidingsinstellingen:

NEN (www.nen.nl)
Infosecure (www.infosecure.nl)
Management Studiecentrum (www.studiecentrum.com)

Internet is overal

Zowel in het bedrijfsleven als binnen de overheid, de zorg, het onderwijs en ook privé maken we steeds meer gebruik van het internet. Aan dit internetgebruik kleven ook risico's die de veiligheid en de betrouwbaarheid ervan verminderen. Het Programma KWINT is voortgekomen uit het belang dat de overheid hecht aan het scheppen van randvoorwaarden die deze veiligheid en betrouwbaarheid bevorderen.

Na onderzoek naar de mogelijkheden om de kwetsbaarheid op het internet te verminderen is in 2001 de kabinetsnota 'Kwetsbaarheid op internet' opgesteld. Het programma KWINT geeft praktische uitvoer aan de actielijnen die in deze kabinetsnota zijn geschetst. Met het programma wil de overheid een bijdrage leveren aan 'het zich beter kunnen beschermen van overheid, burgers en bedrijfsleven tegen de risico's die aan het internetgebruik kleven'. Bovendien wil zij voorzien in een publiek-privaat platform waar onderwerpen gerelateerd aan internetveiligheid besproken worden.

Binnen het programma KWINT wordt hard gewerkt aan de ontwikkeling van concrete en praktisch inzetbare producten voor onder andere:

- Continuïteit van het internet
- Voorkomen van hacking
- Transparantie van het internet
- Integriteit van informatie
- Voorkomen van denial of service aanvallen
- Voorkomen van misbruik door eigen personeel
- Virusbestrijding
- Exclusiviteit van informatie

De producten worden in samenwerking met deskundigen vanuit de markt en de overheid ontwikkeld. Branche- en intermediaire organisaties kunnen de producten, eventueel met een vertaalslag voor de eigen achterban, gebruiken om zo het veiliger internetten binnen hun branche te stimuleren.

Een greep uit de resultaten...

- Computerbeveiliging voor ondernemers (met o.a. een top 10 aan beveiligingsmaatregelen)
- Stappenplan aangifte computercriminaliteit
- Voorlichtingsmateriaal ter bewustwording van (potentiële) computercriminelen van de gevolgen van cybercrime
- Transparameters voor Internetdienstverlening (kwaliteitsgegevens)
- Analyse van continuïteit van het Nederlandse deel van het internet
- Stappenplan voor het creëren van bewustzijn bij het management voor beveiligingsbeleid binnen hun organisatie

KWINT werkt verder aan...

- Analyse van de totstandkoming van (inter)nationale standaarden voor netwerk- en informatiebeveiliging

- Opstellen en uitwerken van een plan voor implementatie van kwaliteitscriteria transparantie van het internet
- Analyse van opleidingen op het gebied van informatiebeveiliging
- Gedragscode veilig internetten voor kinderen (chatten)

De resultaten komen voort uit de verschillende Projectgroepen:

- Continuïteit van het NL internet
- Transparantie voor kwaliteitsgegevens
- Beveiligingsbeleid en -maatregelen
- Opleidingen Informatiebeveiliging
- Veilig internetten voor kinderen
- Cybercrime (expertgroep)

Daarnaast beschikt KWINT over een Stuurgroep, een adviesgroep communicatie en een adviesgroep risico analyse.

Participeren?

Partijen die een bijdragen kunnen leveren aan het programma KWINT zijn van harte uitgenodigd om te participeren. Neem daarvoor contact op met ons programmabureau.

Omdat publiek-private samenwerking binnen het programma KWINT van belang is, is het programmabureau belegd bij ECP.NL, platform voor eNederland (www.ecp.nl). ECP.NL is een publiek-private non-profitorganisatie. Zij biedt een objectief en betrouwbaar platform, waar deelnemende bedrijven en instellingen kennis van de ontwikkeling en toepassing van ICT delen en bundelen.

Contact:

Programma KWINT
p/a Postbus 262
2260 AG Leidschendam
070 - 419 03 09
info@kwint.org
www.kwint.org



In kabinetsnota 'KWINT' is aangegeven dat internetgebruikers zelf ook belangrijke maatregelen kunnen nemen om de risico's van internetgebruik te beperken. Om dit te stimuleren is de overheid de voorlichtingscampagne *Surf op Safe* gestart. Deze campagne richt zich met name op de particuliere en de kleinzakelijke gebruiker van het internet. Meer informatie is te vinden op www.surfopsafe.nl.

Participanten programma Kwint

A/B/M/Adviesbureau
 ABN AMRO Bank NV
 ABN AMRO eSCS
 ABZ Nederland
 AMS-IX
 Amsterdam Internet Exchange
 Anthonio/Nederlof & Partners
 AON Risk Management
 Atos Origin BV
 BA Research NL
 BDO Accountants & Adv. CD-ITC
 Belastingdienst Autom.centrum
 Bureau Keteninformatisering Werk en Inkomen
 Capgemini
 Cisco Systems International BV
 COAX NL
 Coll.Bescherming Pers.gegevens
 Collis BV
 COMGE Ver. Van IT-Managers
 Consumentenbond
 Cosyco IT Solutions
 CSC Computer Sciences Corp.
 CSF
 Deloitte.
 DigiNotar BV
 Dirksen Opleidingen / Hogeschool Dirksen
 Duthler Associates
 ECP.NL
 ECPAT
 EDP Audit Pool
 eJure
 EPN-Platform voor de informatiesamenleving
 Fox-IT
 GAK Nederland
 Gemeente Den Haag
 Gemnet B.V.
 GOVCERT
 GWK
 Hardam Consultancy B.V.
 HCC
 High Tech Crime Initiative Schiphol
 HSB Cards & Card Systems BV
 IBM Security & Privacy Services
 ICT Forum
 ICT Office
 ICTU
 IFT Noord Ned. Arrondis.parket
 ilse media groep B.V.
 InfoSecure bv
 ING Groep
 Integral BV
 Interpay Nederland BV
 iPing Research BV
 ISP wijzer
 Izeom BV
 Kaboem Media bv
 Kampert Organisatie Advies BV
 Kaspersky Labs BV
 Kath. Universiteit Brabant
 KEMA Quality B.V.
 Kennisnet
 Koninklijk NIVRA
 Koninklijke Ahold N.V.
 Koninklijke KPN NV
 Koninklijke Notariele Beroepsorg.
 Korps Landelijke Politiedienst
 KPMG
 KPN
 Macintosh Retail Group N.V.
 Management à la Anke
 Media Plaza

Meldpunt kinderporno op Internet
 Microsoft B.V.
 Min. van Binnenlandse Zaken & Koninkrijksrelaties
 Min. van Defensie
 Min. van Economische Zaken
 Min. van Justitie
 Min. van Landbouw, Natuur & Voedselkwaliteit
 Min. van Onderwijs, Cultuur & Wetenschappen
 Min. van Volksgezondheid, Welzijn & Sport
 MKB-Nederland
 MTV Nederland
 MUADA
 National High Tech Crime Center
 NCRV
 Ned. Normalisatie-instituut
 Ned. Omroepproductie Bedr. nv
 Ned. Thuiswinkel Organisatie
 Ned. Ver. BedrijfsTelecommunicatie Grootgebruikers
 Nederlandse Vereniging van Banken
 Network Business Group
 NGI, platform voor ICT professionals
 NLIP
 NOREA
 Nortel Networks BV
 NS Stations BV
 OHRA BV
 OPR/Advies
 OPTA
 Ouders Online / Mijn Kind Online
 Pinkroccade Confideon
 PricewaterhouseCoopers Accountants NV
 Priority Telecom
 Privver Nederland B.V.
 Profit for the world's children
 Pronk Organisatie Advies
 Raad Nederlandse Detailhandel
 Raad voor Accreditatie
 Rabobank Nederland
 Sauer Quality Consulting bv
 SDU Identification BV
 Seneca Risk & Security
 Siemens Nederland N.V.
 SinfoX BV
 Sipman Consultancy/Unicate
 Smart Card Charter
 Sogeti Nederland BV
 Spamvrij
 Spill B.V.
 Stichting De Kinderconsument
 Stichting Ict op School
 Stichting Internet DN
 Stichting NICAM/Kijkwijzer
 Stichting RAND Europe
 Stichting SURF
 Stratix Consulting Group BV
 Surfkids
 SURFnet bv
 SurfPlan
 Syntens
 Technika10.nl
 Telindus BV
 The Smart Valley
 TNO
 TU Delft / Koepel ICT-Delft
 Unilever R&D Vlaardingen
 Van Dijken Raadgeving BV
 VECAI
 Verdonck, Klooster & Associates
 Vereniging van KvK's in Nederland
 Vereniging VNO-NCW
 Wiessing Advies BV

Bijlage 6: Totstandkoming publicatie

De volgende personen hebben een bijdrage geleverd aan deze publicatie:

A.J. Muller-Sloos	
F.E. van Paassen	
M. Jak	
I.M. Aarts J.R. Boersma J. Martina-Roel	
M. van der Wel	
R.M. Vermeulen	
P.W.A. Overdiep	
F. van Vonderen	
R.J.F. de Vries	

Verder heeft de projectgroep KWINT Beveiligingsbeleid en -maatregelen als klankbord gediend voor deze publicatie. De leden van deze projectgroep zijn:

