Het managen van ICT-risico's; over de onderhandelbaarheid van risico's en maatregelen

Drs. C.J. Coumou en drs. J.W.R. Schoemaker

Risicobeheersing is geen alles-of-nietszaak. En met de toenemende complexiteit van de ICT en de inbedding ervan in organisaties worden risico's en tegenmaatregelen ten aanzien van informatiebeveiliging nog meer dan voorheen een kwestie van afwegen en managen. Met een gedegen aanpak komen de overleg- en beslispunten duidelijk naar voren.

Inleiding

In dit artikel wordt aandacht besteed aan de kans op rampspoed en onheil en wat daartegen te doen valt. Vele ongewenste gebeurtenissen kunnen de informatie- en communicatietechnologie (ICT) treffen. Al in de oudheid was informatiebeveiliging van belang, bijvoorbeeld bij het geheim houden van strijdplannen voor oorlogsvoering. In die tijd werd nog geen gebruik gemaakt van geautomatiseerde gegevensverwerking en werd de boodschapper in sommige gevallen gedood teneinde de inhoud van een bericht te verwijderen. De afweging van het risico dat een geheim bij ongeautoriseerden terecht zou kunnen komen, tegen het nadeel dat de vernietiging van een middel altijd meebrengt, viel dan voor het betrokken middel slecht uit.

De ongewenste gebeurtenissen die de moderne informatieverwerking kunnen treffen komen in dit artikel uitgebreid aan bod, waarbij ook aandacht wordt besteed aan de te treffen tegenmaatregelen. Hierbij zal aandacht worden besteed aan de continue spanning tussen het optreden van dreigingen en de noodzaak van het treffen van maatregelen ter voorkoming van deze dreigingen.

De toepassing van ICT heeft zich ontwikkeld van het gebruik van centraal opgestelde en beheerde mainframes naar de toepassing van gedistribueerde informatiesystemen. Bovendien is er sprake van verregaande integratie van enerzijds informatie- en anderzijds communicatietechnologie. De aandacht die het Jaar 2000-probleem en de invoering van de euro krijgen en de kosten die gemoeid zijn met het oplossen van deze problemen tonen aan dat ICT een niet meer weg te denken onderdeel van onze samenleving vormt.

In de tijd van de traditionele mainframeomgeving vond de besluitvorming over informatiebeveiliging veelal plaats binnen en door de specialistische afdeling Automatisering. Het management van de afdeling Automatisering had duidelijk zicht op de toepassing van ICT en was verantwoordelijk voor de bijbehorende beveiligingsmaatregelen. Met de komst van gedistribueerde ICT is het er wat betreft informatiebeveiliging niet eenvoudiger op geworden. De toepassing van ICT is buitengewoon complex geworden. Overzicht over de aard en de locatie van de verschillende componenten en het gebruik ervan is niet eenvoudig. Het aantal betrokkenen neemt toe en het 'eigenaarschap' van hard- en software is niet altijd eenduidig vastgesteld.

Integratie van ICT in de bedrijfsprocessen maakt dat de besluitvorming over informatiebeveiliging geen exclusieve zaak meer kan zijn van één enkele afdeling, maar door onderhandeling tussen alle betrokkenen totstandkomt. Bij dit onderhandelingsproces worden risico's en de mogelijke maatregelen tegen elkaar afgewogen.

Begrippenkader

Alvorens in te gaan op het managen van ICT-risico's en de onderhandelbaarheid van risico's en maatregelen is het zinvol enkele begrippen te introduceren die in dit kader relevant zijn.

Het eerste begrip betreft de term *risico*. De 'dikke Van Dale' omschrijft risico als 'gevaar voor schade of verlies' en als 'de gevaarlijke kans' ([Dale84]). Het gaat dus om een mogelijke gebeurtenis die bovendien negatief wordt opgevat. Een risico omvat twee elementen, het kanselement en het element van de negatieve gevolgen.

In de literatuur wordt ook wel gesproken van *zuivere (of statische) risico's* om aan te geven dat de uitkomsten van de bedreiging altijd negatief zijn. Indien de uitkomsten ook positief kunnen zijn, wordt gesproken van *speculatieve (of dynamische) risico's* ([Clae91]). Hierin wordt iets zichtbaar van de twee kanten van de medaille van het ondernemen. De ondernemer concentreert zich veelal op de kansen die de markt hem biedt en de winsten die hierbij te behalen zijn. Naast kansen op succes zijn er ook dreigingen. Deze 'gevaarlijke kansen' kunnen de continuïteit van de bedrijfsvoering in gevaar brengen. De afweging die wordt gemaakt van de mogelijke positieve en negatieve uitkomsten bepaalt uiteindelijk of en zo ja, hoe de onderneming wordt voortgezet. Door het treffen van maatregelen kunnen bepaalde risico's immers zodanig worden beperkt dat ze voor de betreffende onderneming acceptabel worden.

Het managen van risico's is dus samen te vatten als beslissen onder onzekerheid. Om de onzekerheid te beperken wordt informatie verzameld. Om tot een besluit te komen worden zoveel mogelijk de verschillende voor- en nadelen tegen elkaar afgewogen. Het is vanzelfsprekend dat complexe situaties van besluitvorming leiden tot complexe afwegingsprocessen. Grote maatschappelijke onderwerpen met veelsoortige risico's zijn hiervan bekende voorbeelden. De (wel of niet) groei van luchthaven Schiphol, de Betuwelijn, het optreden van defensiepersoneel in internationale vredesoperaties, het zijn allemaal voorbeelden van hetzelfde proces. Een beslissingsproces waarin verschillende partijen proberen het eindresultaat te beïnvloeden in de richting van een hun welgevallige mix van risico's en maatregelen. De uitkomst van dit proces is afhankelijk van de kracht van de partijen die deelnemen aan het onderhandelingsproces over risico's en maatregelen. Daarmee is duidelijk dat risico's in sterke mate een subjectieve grootheid zijn. De

individuele beleving van risico's leidt tot een houding en beoordeling van mogelijke gedragsmogelijkheden die van persoon tot persoon sterk kunnen verschillen.

Risico's die samenhangen met de toepassing van ICT, in dit artikel omschreven als *ICT-risico's*, kunnen negatieve gevolgen hebben voor de beschikbaarheid, integriteit en/of vertrouwelijkheid van de informatie, de verwerking of het transport van deze informatie. De Code voor Informatiebeveiliging geeft de volgende toelichting op deze drie aspecten ([Code94]):
* vertrouwelijkheid: het beschermen van gevoelige informatie tegen onbevoegde kennisname;
* integriteit: het waarborgen van de correctheid en volledigheid van informatie en computerprogrammatuur;
* beschikbaarheid: het zeker stellen dat informatie en essentiële diensten op de juiste momenten beschikbaar zijn voor gebruikers.

Risicomanagement wordt gedefinieerd als de activiteiten die erop gericht zijn de risico's die een organisatie loopt bij het bereiken van haar doelstellingen, te beheersen ([Coum96]). Tot die activiteiten behoren:
* verkrijgen van inzicht in de risico's;
* vaststellen van doelen, beleid en strategie met betrekking tot het beperken van deze risico's;
* realiseren van maatregelen;
* toezicht houden op de status van de maatregelen door controle;
* actueel houden en bijsturen van inzicht, beleid en maatregelen.

Risicoanalyse omvat het analyseren van de mogelijke gevolgen van bedreigingen waaraan een organisatie of een gedeelte daarvan blootstaat. Deze gevolgen kunnen worden uitgedrukt in kwalitatieve of in kwantitatieve termen. Risicoanalyse levert het inzicht dat nodig is om de beveiliging van de ICT te integreren in het risicomanagement van de organisatie.

Beveiligingsmaatregelen zijn erop gericht mensen en middelen te beschermen met als doel een ongestoorde voortgang van de bedrijfsprocessen. Om dat goed te kunnen doen moet bekend zijn welke waarden bescherming verdienen en hoe ver de leiding van de organisatie daarmee wil gaan. Aan beveiliging hangt een prijskaartje en het vinden van argumenten om de prijs te bepalen is dan ook een onderdeel van het onderhandelingsproces dat als risicomanagement wordt omschreven. Het gaat dus om inzicht en vervolgens het doen van keuzen. Deze keuzen zijn niet altijd eenvoudig te maken omdat de relatie tussen kosten en opbrengst niet steeds duidelijk is. Brandblussers tegen brand en sloten tegen inbrekers zijn maatregelen die makkelijk kunnen worden overzien. Maar hoe verhouden de kosten van maatregelen ter vermijding van computeruitval, fraude, hackers en ander ongemak dat is verbonden aan het gebruik van ICT, zich tot de kans en de omvang van dat ongemak?

Het onderhandelingsproces

Het bereiken van evenwicht tussen risico's en maatregelen komt tot stand door middel van een onderhandelingsproces. Welke partijen zijn bij dit onderhandelingsproces betrokken en waar gaat het over? Onderhandelen over risico's en maatregelen op het gebied van ICT gaat om een afweging tussen de kosten en baten van het treffen van beveiligingsmaatregelen. Beveiligingsmaatregelen kosten geld en vragen om aandacht van het management en van de overige medewerkers binnen de organisatie. Dus niet alleen moeten investeringen worden gedaan, er zal tijd en aandacht moeten worden besteed aan controle en instandhouding van de getroffen maatregelen. De motivatie hiervoor moet komen uit de baten van de maatregelen. Deze baten bestaan uit een verminderde kans in het optreden van bedreigingen en een vermindering van de schade die deze bedreigingen kunnen veroorzaken.

Voor het ondersteunen van de besluitvorming zal informatie over de risico's en maatregelen een belangrijke rol kunnen spelen. Daarbij moet bedacht worden dat deze informatie voor een deel weinig hard kan zijn. Het gaat immers om risico's en kansen. Vergelijkingen met gebeurtenissen uit het verleden kunnen weliswaar de besluitvorming ondersteunen, maar aan de kant van de risico's blijft vooraf veel ongewis. De kosten voor te treffen maatregelen daarentegen zijn meestal goed calculeerbaar.

Eén mogelijke onderhandelingssituatie voor risico's en maatregelen treedt op als het management besluiten moet nemen over informatiebeveiliging. In een beveiligingsplan worden dan maatregelen voorgesteld die de risico's kunnen beperken. Informatie die aan het beveiligingsplan ten grondslag ligt, zoals risicoanalyse, sterkte-zwakteanalyse, 'wat als'-analyse en kostencalculaties, kan doorslaggevend zijn voor de uitkomst van de besluitvorming. Het is opvallend dat veel functionarissen die werkzaam zijn op het gebied van risicobeheer zichzelf vooral de rol van adviseur geven, zoals blijkt uit een recentelijk uitgevoerd onderzoek naar de rol van de risicobeheerder binnen de organisatie ([Boks98]). Opvallend is in dit onderzoek dat de betrokkenheid van de risicobeheerder bij het onderwerp 'beleid van het risicobeheer' heel groot is. Deze situatie legt op deze functionaris een grote verantwoordelijkheid. Meestal zijn risicobeheerders deskundiger op het gebied van de beveiliging van ICT dan de eigenaar van het bedrijfsproces of het management dat zij adviseren. Zij zullen hun advies op goede en betrouwbare informatie moeten baseren.

Een tweede situatie waarin wordt onderhandeld over risico's en maatregelen is die waarbij de aanbieder en de afnemer van ICT-diensten elkaar ontmoeten. Voor deze twee partijen is het van belang helderheid te krijgen in de verdeling van verantwoordelijkheden die samenhangen met de beveiliging van de dienst die wordt verleend. Zodra hierover duidelijkheid is verkregen, kunnen onderlinge afspraken schriftelijk worden vastgelegd in een service level agreement. De naleving van de afspraken door de aanbieder van de ICT-dienst kan worden gecontroleerd door een onafhankelijke derde in de vorm van een Third Party Mededeling (TPM). Een andere mogelijkheid is dat de aanbieder van de ICT-dienst zich laat certificeren tegen de Code voor Informatiebeveiliging. Door middel van dit certificaat, eveneens afgegeven en gecontroleerd door een onafhankelijke derde, bewijst de aanbieder van de ICT-dienst dat het onderwerp informatiebeveiliging serieus wordt genomen.

jubileumuitgave

ICT-risico's

Er zijn in relatie met ICT vele dreigingen die de voortgang en de uitkomsten van de bedrijfsprocessen negatief kunnen beïnvloeden. Het netwerk kan uitvallen, een computervirus kan de organisatie binnendringen, er kan computerfraude worden gepleegd, fouten worden gemaakt, de ruimte waar de fileservers staan opgesteld kan uitbranden, kortom, veel onheil hangt de organisatie boven het hoofd. Een voorbeeld:
In het najaar van 1998 werd een financiële instelling in Rotterdam getroffen door een computervirus. De medewerkers kregen bij binnenkomst in het kantoor via de intercom te horen dat zij hun werkstation niet mochten opstarten vanwege de aanwezigheid van een computervirus. Het heeft een hele werkdag geduurd voordat het virus op een effectieve manier was verwijderd. Hierdoor hebben honderden personeelsleden hun werk niet of slechts in beperkte mate kunnen verrichten.

Voor het nemen van beslissingen is het nodig een gestructureerd inzicht te hebben in de mogelijke bedreigingen voor de verschillende bedrijfsprocessen. In 1992 heeft het bureau Find/SVP in de Verenigde Staten geanalyseerd hoe groot het gemiddelde omzetverlies is door het uitvallen van computers. De onderzoekers kwamen toen aan een bedrag van US$ 1.300 per minuut. Per gebeurtenis kostte een uitval gemiddeld US$ 330.000, dus duurde die gemiddelde uitval ruim zes uren.

Om dit inzicht te verkrijgen kan gebruik worden gemaakt van hulpmiddelen om de vele bedreigingen te rubriceren. Neisingh gebruikt de indeling naar de aard van de inbreuk van het risico (beschikbaarheid, integriteit en vertrouwelijkheid) en maakt daarnaast onderscheid naar ongewenste gebeurtenissen van opzettelijke en van onopzettelijke aard ([Neis98]). In tabel 1 wordt deze indeling gehanteerd en worden voor iedere combinatie een of meer voorbeelden gegeven.
Een andere mogelijke indeling is die naar de bron van de bedreiging:
* de omgeving, waaronder de natuur;
* de mens (onopzettelijk of opzettelijk);
* de techniek (apparatuur, programmatuur e.d.).

Dergelijke indelingen helpen bij het structureren van het inzicht en bieden een eerste basis voor het bepalen van de risico's. Dat de werkelijkheid veel gecompliceerder is, kan worden geïllustreerd met het volgende voorbeeld waarin blijkt dat ook als duidelijke afwegingen zijn gemaakt er risico's overblijven.

Tabel 1. Rubricering bedreigingen.

	Opzettelijk	Onopzettelijk
Inbreuk op de beschikbaarheid	Sabotage, vandalisme, diefstal van gegevens	Brand, wateroverlast Computeruitval
Inbreuk op de integriteit	Fraude	Fouten Storingen
Inbreuk op de vertrouwelijkheid	Spionage, diefstal van gegevens	Regelovertreding

De AT&T-case

Een voorbeeld van een omvangrijke verstoring van de beschikbaarheid van telecommunicatie trad op in september 1991. AT&T beheerde in New York een centrale voor telecommunicatie waarmee een groot gebied werd bediend waaronder een aantal luchthavens. In verband met de grote afhankelijkheid van een ononderbroken stroomvoorziening kon AT&T beschikken over een eigen stroomvoorziening. Deze werd beschouwd als een noodzakelijke reservecapaciteit.

Met de leverancier van elektriciteit was de volgende afspraak gemaakt: Als de vraag naar elektriciteit in de regio een bepaalde omvang zou krijgen, dan mocht de telefooncentrale van AT&T van het net worden afgekoppeld. De beloning hiervoor was een laag tarief voor de geleverde elektriciteit. Het risico voor AT&T was beperkt door de mogelijkheid van een eigen stroomvoorziening alsmede de beschikbaarheid van reservebatterijen met een capaciteit voor maximaal zes uur. Een duidelijke afweging op basis van een kosten-batenanalyse.

In september 1991 deed zich een situatie voor waarin de vraag naar elektriciteit zo groot was (hitte, dus veel werkende airco's) dat AT&T volgens afspraak van het net werd afgekoppeld. Bij het overnemen van de stroomvoorziening door de eigen stroomvoorziening van AT&T begaf de omvormer het. Daarmee zou de levering van telecommunicatie beëindigd worden, ware het niet dat AT&T beschikte over de reservebatterijen. De normale procedure was dat een storing werd aangegeven door middel van zowel een visueel als een akoestisch signaal. Helaas werden beide niet opgemerkt. Naar later bleek, waren de betreffende monteurs met lunchpauze of op cursus.

Door de batterijen was het probleem de eerste zes uur niet zichtbaar. Daarna viel het gehele communicatienetwerk uit hetgeen onder meer consequenties had voor het vliegverkeer in New York. Uiteindelijk duurde de uitval van de voorzieningen negen uur, hetgeen leidde tot een schade die werd geschat op US$ 60-75 miljoen (ruim US$ 100.000 per minuut).

Beveiligingsmaatregelen

Indien niet vooraf gestructureerd over maatregelen is nagedacht, is de neiging groot om bij het optreden van een bedreiging ad-hocmaatregelen te treffen. In een acute noodsituatie is het natuurlijk van belang om handelend op te treden, bijvoorbeeld om mensenlevens te redden. Als het logistieke systeem fouten vertoont, is er geen tijd om over een beveiligingsbeleid na te denken of over de vraag hoe op een structurele wijze testprocedures kunnen worden opgezet. Er moet dan ingegrepen worden en gewerkt worden om de schade zoveel mogelijk te beperken. Is er echter wel tijd voor bezinning, dan verdient het toepassen van een structurele aanpak de voorkeur boven het treffen van ad-hocmaatregelen.

Code voor Informatiebeveiliging

Welke maatregelen kunnen nu worden getroffen om de ICT-risico's het hoofd te bieden en welke indelingen

kunnen hierbij worden gehanteerd? Een eerste indeling is te vinden in de Code voor Informatiebeveiliging ([Code94]). De Code maakt onderscheid naar de volgende beveiligingsonderwerpen:

1 Beveiligingsbeleid;
2 Beveiligingsorganisatie;
3 Classificatie en beheer van bedrijfsmiddelen;
4 Beveiligingseisen ten aanzien van personeel;
5 Fysieke beveiliging en beveiliging van de omgeving;
6 Computer- en netwerkbeheer;
7 Toegangsbeveiliging voor systemen;
8 Ontwikkeling en onderhoud van systemen;
9 Continuïteitsplanning;
10 Toezicht.

De Code voor informatiebeveiliging is gebaseerd op een verzameling van de beste praktijkmethoden ('best practices') van informatiebeveiliging en heeft als doelstellingen ([Code94]):

* het verschaffen van een gemeenschappelijke basis voor bedrijven van waaruit deze effectieve codes voor informatiebeveiliging kunnen ontwikkelen, implementeren en meten;
* het bevorderen van het vertrouwen van handelsverkeer tussen bedrijven.

CobIT

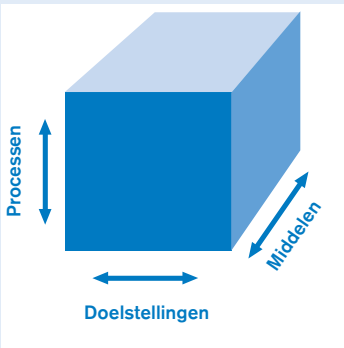
Een tweede indeling is te vinden in de Control Objectives for Information and Related Technology (CobIT). Deze set van maatregelen is ontwikkeld door de Information Systems AudiT and Control Association ([Isac98]). CobIT heeft tot doel bij een toenemende afhankelijkheid van IT op een gestructureerde wijze een overzicht te bieden van de mogelijke maatregelen voor de beveiliging van IT. Ook CobIT baseert zich op zogenaamde 'good practices'. CobIT hanteert bij de indeling van beveiligingsmaatregelen de volgende drie invalshoeken:

* doelstellingen ('Business Requirements');
* middelen ('IT-resources');
* processen ('IT-processes').

Op basis van deze drie invalshoeken ontstaat de in figuur 1 weergegeven kubus, gevuld met mogelijke beveiligingsmaatregelen.

CobIT onderscheidt de volgende doelstellingen:

* effectiveness;
* efficiency;
* confidentiality;
* integration;
* availability;
* compliance;
* reliability of information.



Figuur 1. Drie invalshoeken voor beveiligingsmaatregelen.

Zoals blijkt uit bovenstaande opsomming, gaat CobIT bij het bepalen van de doelstellingen verder dan de Code voor Informatiebeveiliging, die zich beperkt tot beschikbaarheid, integriteit en vertrouwelijkheid. Deze drie aspecten worden ook door CobIT aangegeven als doelstellingen die samenhangen met informatiebeveiliging.

Met betrekking tot de toepassing van ICT worden in CobIT de volgende middelen genoemd:

* data;
* application systems;
* technology;
* facilities;
* people.

CobIT deelt de processen in in de volgende vier domeinen:

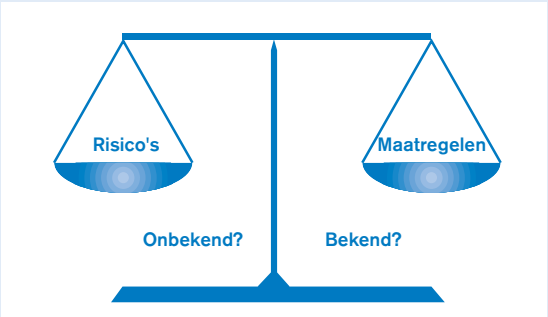
* planning and organisation;
* acquisition and implementation;
* delivery and support;
* monitoring.

Op strategisch niveau bijvoorbeeld wordt de informatiearchitectuur bepaald als onderdeel van het proces Planning en Organisatie. Dit proces richt zich met name op de middelen applicatiesystemen en gegevens. Bij de vaststelling van de informatiearchitectuur zijn volgens CobIT dan vooral de doelstellingen effectiviteit, efficiency, vertrouwelijkheid en integriteit van belang.

Welke indeling ook wordt gehanteerd, van belang is dat een volledig en geïntegreerd geheel van beveiligingsmaatregelen ontstaat waarmee alle relevante ICT-risico's op een effectieve wijze worden afgedekt.

Risicomanagement

Risicomanagement is erop gericht de risico's die een organisatie loopt bij het bereiken van haar doelstellingen, te beheersen. Hierbij is het van belang een evenwicht te bereiken tussen risico's en maatregelen. Figuur 2 geeft dit proces weer.



Figuur 2. Evenwicht.

Zoals reeds vermeld, omvat het proces van risicomanagement de volgende stappen:

1 verkrijgen van inzicht in de risico's;
2 vaststellen van doelen, beleid en strategie met betrekking tot het beperken van deze risico's;
3 realiseren van maatregelen;

4 toezicht houden op status van de maatregelen door controle;
5 actueel houden en bijsturen van inzicht, beleid en maatregelen.

1 Inzicht

Risicomanagement start met het verkrijgen van *inzicht in de risico's* die de organisatie loopt met de toepassing van ICT. Het is bij de leiding van de organisatie vaak niet bekend welke risico's de organisatie loopt met het gebruik van deze technologie. Een gestructureerd inzicht kan worden verkregen door het uitvoeren van een risicoanalyse of een zogenaamde afhankelijkheids- of kwetsbaarheidsanalyse. De laatste methode wordt voorgeschreven binnen de rijksoverheid in het Voorschrift Informatiebeveiliging Rijksdienst ([VIR94]).

De Code voor Informatiebeveiliging wijst ook op het nut van het uitvoeren van een risicoanalyse voor het bepalen van de te nemen maatregelen en het stellen van prioriteiten ten aanzien van het beheer van risico's en het implementeren van de maatregelen die in de Code zijn beschreven ([Code94]). Het uitvoeren van een kwantitatieve risicoanalyse biedt hierbij de mogelijkheid om het inzicht in de risico's en in de kwaliteit van de getroffen maatregelen meetbaar te maken ([Coum93]). Met name de objectieve wijze waarop in een kwantitatieve risicoanalyse de risico's onderling vergelijkbaar worden gemaakt, maakt deze analyse geschikt voor het onderhandelen over risico's en maatregelen. Door de mogelijkheid van 'wat als'-vragen wordt het besluitvormingsproces dynamisch ondersteund.

2 Beleid

Wanneer inzicht in de risico's is verkregen, kan het *beleid met betrekking tot de beveiliging van ICT* worden vastgesteld. De doelstellingen, uitgangspunten, prioriteiten en randvoorwaarden voor informatiebeveiliging gelden als kernpunten in het informatiebeveiligingsbeleid. Daarnaast verdient het aanbeveling aandacht te besteden aan de beveiligingsorganisatie in de vorm van de verdeling van taken, verantwoordelijkheden en bevoegdheden, aan de normen en eisen die gelden ten aanzien van de beveiliging van informatiesystemen en aan de wijze van evaluatie en beoordeling van de realisatie van het informatiebeveiligingsbeleid.

Als onderdeel van de bepaling van het beleid kan een keuze worden gemaakt uit de toe te passen risicostrategieën. Hierbij staan het management de volgende mogelijkheden ter beschikking ([Clae91]):
* vermijden;
* verminderen;
* overdragen;
* accepteren.

		Kans	
		Laag	Hoog
Gevolgen	Hoog	Repressieve maatregelen	Eerste prioriteit
	Laag	Geen prioriteit	Preventieve maatregelen

Figuur 3. Risicomatrix.

Bij *vermijden* gaat het om het kiezen van andere oplossingen of varianten zodat het risico niet meer kan optreden. De organisatie probeert de risico's te vermijden of op te heffen door zichzelf *immuun* te maken voor bepaalde bedreigingen. Een voorbeeld buiten de ICT is het afzien van het gebruik van asbest. Daardoor wordt de dreiging van het ziek worden en overlijden als gevolg van het inademen van deeltjes van deze stof vermeden. Dat ook hier sprake is van 'onderhandelen' blijkt als bedacht wordt dat asbest werd toegepast met een zeker doel. In dit geval brandwerendheid. Het is dus de vraag of met een ander materiaal een even goede brandbescherming kan worden bereikt zonder de schadelijke bijwerking van asbest.

Een voorbeeld van de toepassing van deze strategie bij ICT zou het vermijden kunnen zijn van het gebruik van netwerken om de dreiging van hackers te ontlopen.

Het *verminderen* van risico's omvat het treffen van maatregelen, hetzij van preventieve, hetzij van repressieve aard. Preventieve maatregelen zijn erop gericht de kans van optreden van de bedreiging te beïnvloeden. Repressieve maatregelen daarentegen richten zich op de gevolgen van een bedreiging.

Bij de keuze van preventieve en/of repressieve maatregelen kan de risicomatrix ([Coum96]) een goed hulpmiddel vormen. Deze matrix (zie figuur 3) kan tijdens de risicoanalyse worden gevuld waardoor de bedreigingen ten opzichte van elkaar worden geordend naar kans van optreden en potentieel gevolg.

Zoals uit de matrix blijkt, verdienen bedreigingen die zowel een hoge kans van optreden hebben en omvangrijke negatieve gevolgen kunnen veroorzaken de eerste prioriteit. Deze bedreigingen zullen door hun optreden en hun gevolgen ook binnen de organisatie herkenbaar zijn als problemen die de eerste aandacht verdienen.

Voorbeelden van repressieve maatregelen zijn continuïteitsplannen en regelingen die worden opgesteld om het hoofd te bieden aan situaties die kunnen ontstaan als gevolg van een opgetreden negatieve gebeurtenis. Back-up (reserve-exemplaren) en herstelprocedures zijn voorbeelden uit de dagelijkse praktijk. Vooraf nadenken over dergelijke voorzieningen en plannen heeft als voordeel dat crises kunnen worden voorkomen en de schade kan worden beperkt.
Voorbeelden van preventieve maatregelen zijn procedures en regels ter voorkoming van fouten. Zoals het rookverbod in sommige ruimten de kans op brand moet verminderen, zo zullen waarschuwingen voor virussen de kans op het binnendringen van vreemde en ongewenste programmatuur moeten verkleinen.

Het *overdragen* van een risico kan worden gerealiseerd door de gevolgen van het optreden van bedreigingen naar derden te leiden. De bekendste vorm hiervan is verzekeren, het overdragen van de financiële gevolgen van omschreven gebeurtenissen. Let wel: de financiële gevolgen vormen steeds een deel van de schade. Met geld is een deuk in het imago slechts beperkt te herstellen.

Tegenwoordig wordt wel het outsourcen van bepaalde activiteiten gezien als een vorm van 'overdragen van risico's'. Weliswaar is de outsourcende organisatie bevrijd van de zorg om de maatregelen rondom de uitbestede activiteiten, maar wel moet worden beseft dat de negatieve gevolgen in de vorm van vertraging van de bedrijfsprocessen, onbetrouwbare output of schade aan het imago van de organisatie blijven bestaan. In gevallen van uitbesteding zal contractueel moeten worden vastgelegd welke risico's acceptabel zijn en welke maatregelen door beide partijen zullen worden getroffen.

De laatste strategische optie bestaat uit het *accepteren* van het risico. Op grond van de resultaten van een risicoanalyse kan besloten worden dat de balans uitslaat naar de risico's. De gevolgen van het optreden van bedreigingen worden dan geringer beoordeeld dan de kosten en inspanning gemoeid met het treffen van maatregelen.

3 Maatregelen

Zodra het beleid is vastgesteld en de gewenste risicostrategieën zijn bepaald, kan worden gestart met het *realiseren van de beveiligingsmaatregelen*. Een projectmatige aanpak verdient hierbij aanbeveling. Het opstellen van een beveiligingsplan is daarvoor een eerste vereiste. Overige aandachtspunten in deze fase zijn voorlichting en training van gebruikers en het verhogen van het bewustzijn voor de noodzaak van beveiliging bij alle betrokkenen. Awareness campagnes kunnen helpen om de betrokkenen het belang van beveiliging en het bepaalde beleid ter zake onder ogen te brengen.

Omdat gebruikers nogal eens de neiging hebben om beveiligingsmaatregelen te ontduiken omdat deze als 'lastig' worden ervaren, is voorlichting en training noodzakelijk. Hierbij is het een uitdaging om niet betuttelend over te komen maar een positieve houding voor beveiliging bij het personeel te bewerkstelligen. Het verduidelijken van het beveiligingsbeleid door de balans te tonen van risico's en maatregelen kan helpen de noodzakelijke betrokkenheid en participatie te verkrijgen.

4 Toezicht

In de periode dat beveiligingsmaatregelen operationeel zijn mogen *toezicht en controle* niet ontbreken. Ook de Code voor Informatiebeveiliging is zich bewust van deze noodzaak en besteedt een apart hoofdstuk aan het onderwerp Toezicht ([Code94]). Controle van beveiligingsmaatregelen kan betrekking hebben op:

* de samenhang van de maatregel met het beleid;
* de inhoudelijke juistheid van de maatregel;
* de naleving van de maatregel door het personeel.

De fase van toezicht houden geeft de mogelijkheid de beoordeling van de balans tussen risico's en maatregelen permanent door te voeren. Maatregelen die niet worden nageleefd, hebben al snel de neiging de balans in negatieve richting te laten doorslaan. Tegenover de kosten kunnen immers geen baten staan als de maatregelen niet worden nageleefd. Zo had een organisatie een groot probleem toen moest worden teruggevallen op een backupversie van de programmatuur. Op dat moment bleek dat enige maanden daarvoor een nieuw onderdeel van de programmatuur niet in de back-upprocedure was opgenomen. Daarmee was de bruikbaarheid van de backupversie vrijwel nihil.

5 Actualiseren

Een sluitend risicomanagementproces besteedt ook aandacht aan *het actueel houden en het bijsturen* van het inzicht, het beleid en de maatregelen. Organisatieveranderingen, nieuwe bedreigingen en veranderende inzichten in de beveiliging van ICT kunnen aanleiding zijn om het beleid aan te passen en de getroffen maatregelen te herzien. De spanning tussen risico's en maatregelen blijft ook na het doorlopen van het risicomanagementproces bestaan. Het proces van risicomanagement is dus als een cyclische activiteit te beschouwen.

Toekomst

De verwachting is dat de afhankelijkheid van de toepassing van ICT in de toekomst nog verder zal toenemen. De Information Systems Audit and Control Association ([Isac98]) noemt hierbij de volgende factoren:

* een toenemende afhankelijkheid van informatie en de systemen die deze informatie leveren;
* een toename van kwetsbaarheden en bedreigingen, zoals risico's samenhangend met het gebruik van Internet en Information Warfare;
* de schaalgrootte en kosten van ICT-investeringen;
* de potentie van ICT om organisaties en bedrijfsprocessen te beïnvloeden met het creëren van nieuwe mogelijkheden en het reduceren van kosten.

Koppeling van informatiesystemen, mobiele telefonie, voice mail, electronic commerce, Internet, e-mail, elektronische belastingaangifte en elektronisch bankieren, het zijn allemaal voorbeelden van het nog steeds toenemende ICT-gebruik.

De afhankelijkheid van ICT en de daarbij behorende toename van risico's die samenhangen met het gebruik van deze technologie vragen dus om een blijvende aandacht voor informatiebeveiliging. Risicomanagement biedt de mogelijkheid om de onderhandelingen tussen risico's en maatregelen aan te gaan. Daardoor zijn bevredigende oplossingen mogelijk voor de natuurlijke spanning tussen de kosten van maatregelen en de baten van verminderde risico's.

Conclusie

Veel aandacht voor de kansen die de markt biedt en de winsten die hierbij te behalen zijn, kan leiden tot onvoldoende aandacht voor ongewenste gebeurtenissen. Vooral als die de continuïteit van de bedrijfsvoering in gevaar kunnen brengen, is het verstandig deze risico's in de besluitvorming te betrekken. Daarbij gaat het om een afweging van de kosten verbonden aan risico's en het treffen van maatregelen. Dit onderhandelingsproces moet leiden tot een acceptabele mix van maatregelen en resterende risico's. Bij het doen van voorstellen ter zake van te treffen maatregelen is het van belang rekening te

houden met de individuele beleving van risico's, zowel bij de beslisser als bij de medewerkers binnen de organisatie die belast zijn met de uitvoering van de bedrijfsprocessen.

In de praktijk blijkt het management vaak aandacht te willen besteden aan informatiebeveiliging na het optreden van een beveiligingsincident. Hierbij bestaat de neiging om de aandacht te concentreren op het incident en hiervoor ad-hocmaatregelen te treffen. Een structurele aanpak op grond van een geaccepteerde indeling van risico's en maatregelen biedt echter de beste basis voor een effectieve en efficiënte informatiebeveiliging. Hierdoor kan men voorkomen dat op één plek te veel maatregelen worden getroffen, terwijl op een ander deelterrein ontoelaatbare risico's blijven bestaan. Beheersbaarheid kan worden bereikt door de besluitvorming volgens het proces van risicomanagement te laten verlopen.

Welke indeling bij het treffen van beveiligingsmaatregelen ook wordt gehanteerd, van belang is dat een volledig en geïntegreerd geheel van beveiligingsmaatregelen ontstaat waarmee alle relevante ICT-risico's op een effectieve wijze worden afgedekt.

Het uitvoeren van een risicoanalyse of een A&K-analyse kan als hulpmiddel dienen om het management te helpen de besluiten over informatiebeveiliging te nemen. Tevens biedt een dergelijke methode de mogelijkheid om prioriteiten te stellen. De beperkte middelen voor informatiebeveiliging kunnen hierdoor worden ingezet op de bestrijding van de risico's die om de meeste aandacht vragen.

Risicomanagement is een continu en cyclisch proces. Veranderende omstandigheden, zoals de introductie van nieuwe technologieën (Internet, electronic commerce e.d.) en het ontstaan van nieuwe bedreigingen, vragen om blijvende aandacht van het management voor het afwegen van risico's en maatregelen.

Samenvatting

In dit artikel is aangegeven op welke manier risico's die samenhangen met het gebruik van ICT, de zogenaamde ICT-risico's, kunnen worden beheerst. Hierbij is aandacht besteed aan de onderhandelbaarheid van risico's en maatregelen met als uitdaging het bereiken van evenwicht tussen deze twee elementen.

ICT-risico's hebben te maken met ongewenste gebeurtenissen die negatieve gevolgen kunnen hebben voor de beschikbaarheid, integriteit en/of vertrouwelijkheid van de informatie of de verwerking van deze informatie. Hierbij kan onderscheid worden gemaakt naar opzettelijke en onopzettelijke gebeurtenissen.

Bij het treffen van beveiligingsmaatregelen kunnen verschillende indelingen als basis worden gehanteerd. Zinvolle structuren hiervoor worden aangeboden door de Code voor Informatiebeveiliging en de Control Objectives for Information and Related Technology (CobIT).

Een mogelijke aanpak voor het beheersen van ICT-risico's onderscheidt uitgaande van een procesmatige invalshoek de volgende stappen:
1 het verkrijgen van inzicht;
2 het formuleren van beleid;
3 het realiseren van maatregelen;
4 toezicht en controle;
5 het bijsturen en actualiseren van het inzicht, het beleid en de maatregelen.

Deze stappen omvatten het verkrijgen van inzicht in risico's en maatregelen, het opstellen van een informatiebeveiligingsbeleid, het uitwerken van beleidsprincipes in een beveiligingsplan en het voorbereiden, implementeren en verbeteren van concrete beveiligingsmaatregelen. Aangezien het een continu proces betreft, kan de cyclus weer opnieuw beginnen met het bewust worden van nieuwe risico's en het evalueren van bestaande maatregelen.

Tussen risico's en maatregelen bestaat een continue spanning. Het bereiken van een evenwicht tussen deze twee grootheden is te beschouwen als een onderhandelingsproces. Hierbij gaat het om een afweging tussen de kosten en baten van het treffen van beveiligingsmaatregelen. Zodra dit evenwicht is bereikt, is er sprake van een optimale beveiligingssituatie.

Literatuur

[Boks98]
K. Boks en drs. C.J. Coumou, *Functieprofiel: de risicobeheerder, Een overzicht van taken uit de dagelijkse praktijk*, KPMG EDP Auditors, 1998.

[Clae91]
P.F. Claes en H.J.J.M. Meerman, *Risk management, inleiding tot het risicobeheersproces*, Stenfert Kroese, 1991.

[Code94]
Nederlands Normalisatie Instituut, *Code voor Informatiebeveiliging*, 1994.

[Coum93]
Drs. C.J. Coumou, *Ondersteuning van risicobeheer door risicoanalyse*, A.I.V., september 1993.

[Coum96]
Drs. C.J. Coumou, *RISAN, een methode voor risicoanalyse*, in: Handboek Informatiebeveiliging, afl. 11, april 1996.

[Dale84]
Van Dale, *Nieuw Handwoordenboek der Nederlandse Taal*, negende druk, 1984.

[Isac98]
Control Objectives for Information and Related Technology, Information Systems Audit and Control Association, 1998.

[Neis98]
Prof. A.W. Neisingh RE RA, *Informatie- en communicatietechnologie en accountants: een verstandshuwelijk?*, Compact 1998/3.

[VIR94]
Ministerie van Binnenlandse Zaken, *Voorschrift Informatiebeveiliging Rijksdienst*, 1994.