Risicoanalyse gemakkelijk gemaakt

Drs. E.P. Rutkens RE, ir. H. Bouthoorn en drs. L.P.F. Tushuizen

Formele risicoanalysetechnieken zijn zeer gebruikelijk in bijvoorbeeld de farmaceutische en financiële wereld, maar worden ook steeds vaker toegepast om de risico's die samenhangen met informatie en ondersteunende processen, systemen en netwerken, te identificeren. De complexiteit van bedrijfsprocessen, informatiesystemen en infrastructuren maakt het uitvoeren van een risicoanalyse niet eenvoudig. Er moet een gezonde, verstandige afweging worden gemaakt tussen de risico's, de maatregelen om de kans van optreden en/of het gevolg van deze risico's te beperken en het bedrijfsbelang. Dit artikel geeft een algemeen inzicht in bedreigingen en risico's alsmede in risicoanalyses die worden toegepast om de risico's die samenhangen met informatie en ondersteunende systemen te identificeren en te controleren. Daarnaast behandelt het artikel de door KPMG ontwikkelde risicoanalyse-methode SPARK.

Inleiding

Ondernemen is risico's nemen. Een organisatie dient daarom een gezonde, verstandige afweging te maken tussen risico's, maatregelen en het bedrijfsbelang. Dit geldt ook als het gaat om de beschikbaarheid, integriteit en vertrouwelijkheid van informatie. Om deze aspecten van informatie en de ondersteunende processen, systemen en netwerken te kunnen waarborgen, dienen organisaties diverse maatregelen te treffen. Aan het treffen van deze maatregelen kan een risicoanalyse voorafgaan. Hierdoor kunnen risico's die van invloed zijn op genoemde aspecten op een evenwichtige wijze worden geïnventariseerd, beheerst en gereduceerd tot een voor de organisatie aanvaardbaar niveau.

Formele risicoanalysetechnieken zijn zeer gebruikelijk in bijvoorbeeld de farmaceutische en financiële wereld, maar worden ook steeds vaker toegepast om de risico's die samenhangen met informatie en ondersteunende processen, systemen en netwerken, te identificeren. De complexiteit van bedrijfsprocessen, informatiesystemen en infrastructuren maakt het uitvoeren van een risicoanalyse niet eenvoudig. Er moet een gezonde, verstandige afweging worden gemaakt tussen de risico's, de maatregelen om de kans van optreden en/of het gevolg van deze risico's te beperken en het bedrijfsbelang.

Dit artikel geeft een algemeen inzicht in bedreigingen en risico's alsmede in risicoanalyses die worden toegepast om de risico's die samenhangen met informatie en ondersteunende systemen te identificeren en te contro-

Drs. E.P. Rutkens RE
is werkzaam als consultant bij KPMG Information Risk Management. Hij houdt zich bezig met de dienstverlening van KPMG met betrekking tot Information Security. Verder is hij betrokken bij de ontwikkeling van producten op dit gebied, waaronder beveiligingsarchitecturen en risicoanalyse.

rutkens.erik@kpmg.nl

Ir. H. Bouthoorn
is werkzaam als junior consultant bij KPMG Information Risk Management. Hij houdt zich bezig met zowel technische als organisatorische opdrachten op het gebied van informatiebeveiliging. Tevens is hij betrokken bij het projectmanagement van complexe IT-projecten.

bouthoorn.huibert@kpmg.nl

Drs. L.P.F. Tushuizen
is werkzaam als adviseur bij KPMG Business Advisory Services. Hij houdt zich onder andere bezig met risicomanagement en certificering van organisaties tegen onder andere BS7799-2.

tushuizen.lars@kpmg.nl

leren. Daarnaast behandelt het artikel de door KPMG ontwikkelde risicoanalyse SPARK. Deze methode biedt niet alleen inzicht in risico's met betrekking tot informatie en bedrijfsprocessen, maar kan eveneens als ondersteuning worden gebruikt bij het ontwikkelen van informatiebeveiligingsbeleid en beveiligingsmaatregelen, aangezien de methode maatregelen aanreikt gebaseerd op de de-factostandaard Code voor Informatiebeveiliging (BS7799, ISO 17799).

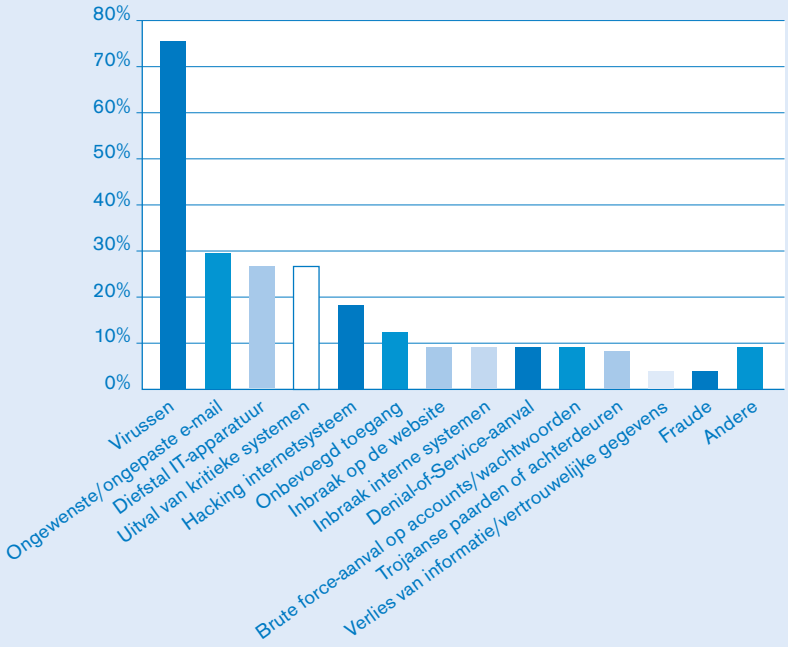
Bedreigingen en risico's

Informatie en de ondersteunende processen, systemen en netwerken zijn belangrijke bedrijfsmiddelen voor veel organisaties. Deze bedrijfsmiddelen staan vaak bloot aan tal van bedreigingen, waardoor organisaties bepaalde risico's lopen. Een organisatie kan namelijk bij het optreden van een bedreiging nadelige gevolgen ondervinden. Denk hierbij bijvoorbeeld aan omzetderving, verslechterde concurrentiepositie of imagoschade. Het begrip risico wordt vaak op verschillende wijze geïnterpreteerd en uitgelegd. Toch gaat het steeds om onzekere situaties waarbij verschillende uitkomsten mogelijk zijn. Anders gezegd, het risico wordt bepaald door de kans ('onzekere situatie') maal het gevolg ('uitkomst').

Bedreigingen met betrekking tot informatie en de ondersteunende processen, systemen en netwerken vallen uiteen in bedreigingen in relatie tot de gegevens zelf en bedreigingen in relatie tot de gegevensverwerking. Bedreigingen in relatie tot gegevens zijn bijvoorbeeld het ongeautoriseerd (zonder toestemming) wijzigen en/of verwerken van gegevens of het ongeoorloofd openbaar maken van gegevens. Bedreigingen in relatie tot het verwerken van gegevens zijn bijvoorbeeld het verstoren van de voortgang of het onderbreken van gegevensverwerkingsprocessen of het niet ter beschikking hebben van randapparatuur en overige computerfaciliteiten.

Verder zorgt het toenemend gebruik van internet ervoor dat de aard van de bedreigingen verandert en dat het aantal bedreigingen toeneemt. De oorzaak hiervan kan worden gezocht in de voortschrijdende technologische ontwikkelingen en de onbegrensde omgeving waarin de bedreigingen zich kunnen manifesteren. Bedreigingen die samenhangen met het gebruik van internet zijn bijvoorbeeld virusaanvallen[1] en zogenaamde Denial-of-Service-aanvallen[2]. Om een indruk te geven van dergelijke bedreigingen en de mogelijke (schadelijke) gevolgen, wordt in kader 1 een voorbeeld van een recent beveiligingsincident beschreven.

1) Virussen zijn programma's die zich onopgemerkt op verschillende wijze verspreiden en schadelijke handelingen kunnen verrichten.
2) Bij een Denial-of-Service-aanval wordt een computersysteem overladen met verzoeken tot informatie waardoor deze buiten werking wordt gesteld, aangezien het systeem deze grote hoeveelheid verzoeken niet kan verwerken.



Bron: Ministerie van Economische Zaken/KPMG, *Monitor Internetbeveiliging 2003.*

Figuur 1. Oorzaken van ernstige beveiligingsincidenten.

Voorbeeld: Blaster-virus

In augustus 2003 zorgt het Blaster-virus wereldwijd voor problemen. Blaster maakt gebruik van een kwetsbaarheid in het besturingssysteem Windows XP. Microsoft heeft deze kwetsbaarheid op 16 juli 2003 bekendgemaakt. Blaster zorgt ervoor dat een geïnfecteerd systeem instabiel wordt en tracht opnieuw op te starten. Daarnaast wordt vanaf het besmette systeem op verschillende systeemdata een gemeenschappelijke DoS-aanval uitgevoerd op windowsupdate.microsoft.com. Blaster is een worm die zich niet verspreidt via e-mail maar via een kwetsbare systeempoort en ftp.

Eén van de organisaties die getroffen werd door Blaster is CSX, dat het grootste spoornet in Oost-Amerika beheert. Blaster infecteerde het computersysteem in het hoofdkantoor en sloot seinen en andere systemen. Door de storing van het systeem werden zowel goederen- als passagierstreinen direct stopgezet, waardoor het treinverkeer in Oost-Amerika ernstig werd ontregeld. De seinstoring had kort invloed op het hele CSX-systeem dat 23 staten ten oosten van de Mississippi-rivier dekt.

Bronnen: www.microsoft.com en www.cbsnes.com

Kader 1. Beveiligingsincidenten.

Onderzoek in Nederland wijst uit dat virussen de belangrijkste oorzaak zijn van ernstige beveiligingsincidenten, zoals ook is weergegeven in figuur 1.

Risicoanalyse

Zoals gezegd lopen bedrijven bepaalde risico's omdat bedreigingen kunnen optreden. Daardoor zullen bedrijven maatregelen willen nemen om enerzijds de kans van het optreden en anderzijds het gevolg van deze bedreiging te doen afnemen. Om te bepalen welke maatregelen ingevoerd dienen te worden, kan een risicoanalyse worden uitgevoerd.

Risicoanalyse is het systematisch beoordelen van de schade voor de organisatie als gevolg van het optreden van een bedreiging voor de organisatie en de waarschijnlijkheid dat een dergelijk risico zich voordoet. Hierbij dient rekening te worden gehouden met de gevolgen voor de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie en andere bedrijfsmiddelen in het licht van de aanwezige bedreigingen. Met andere woorden, risicoanalyse is het proces van het begrijpen van de risico's die samenhangen met bedrijfsprocessen en de ondersteunende informatiesystemen. Het belangrijkste doel van een risicoanalyse is, na het inventariseren van de risico's, het definiëren van beveiligingsmaatregelen waarmee een voor de organisatie aanvaardbaar beveiligingsniveau wordt gerealiseerd. Bij de definitie van de maatregelen wordt rekening gehouden met de kosten en baten van de invoering van deze maatregelen.

Er worden twee vormen van risicoanalyse onderscheiden, namelijk de kwalitatieve en de kwantitatieve risicoanalyse. Bij een kwalitatieve risicoanalyse worden voor de te analyseren objecten schattingen van de gelopen risico's gemaakt. Dit is de lichtste vorm van risicoanalyse waarbij daadwerkelijk sprake is van het analyseren van risico's. Bij de kwantitatieve risicoanalyse worden de risico's waar mogelijk gekwantificeerd in meetbare criteria, meestal uitgedrukt in de financiële gevolgen voor een organisatie. Dit is de meest uitgebreide en gedetailleerde vorm van risicoanalyse.

Aangezien een kwantitatieve risicoanalyse zeer complex en kostbaar is en meetbare criteria niet in alle gevallen bekend zijn, wordt tegenwoordig ook wel een tussenvorm van beide typen risicoanalyses uitgevoerd. Hierbij wordt allereerst een kwalitatieve risicoanalyse uitgevoerd voor een breed en algemeen inzicht in bedrijfsprocessen en risico's. Een kwantitatieve risicoanalyse wordt vervolgens gebruikt om een aantal specifieke aandachtsgebieden nader te analyseren. Dit is bijvoorbeeld het geval wanneer zowel de kans op als het gevolg van een bedreiging groot is.

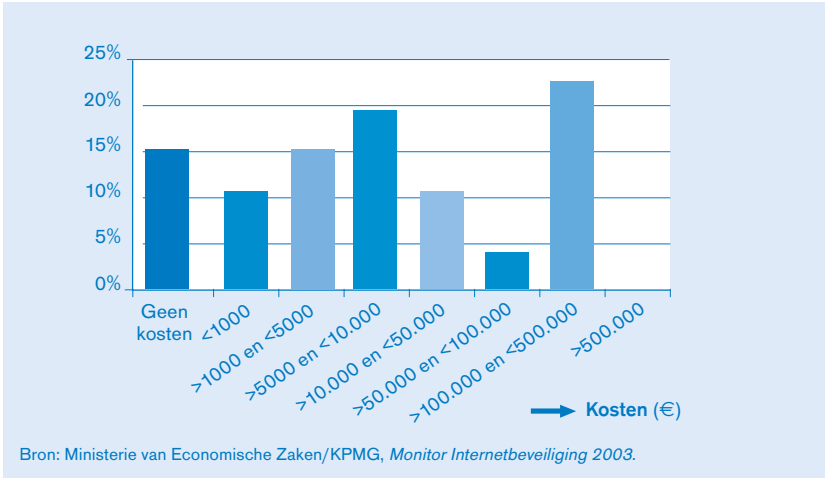
Voor de kwantificering van risico's in meetbare criteria dient zoveel mogelijk gebruik te worden gemaakt van ervaringscijfers betreffende het optreden van bepaalde gebeurtenissen in het verleden of schattingen op basis van ervaringscijfers van vergelijkbare omgevingen. Dit is niet eenvoudig. Onderzoek in Nederland wijst uit dat een groot aantal organisaties niet weet hoeveel de totale herstelkosten als gevolg van het optreden van een beveiligingsincident waren (figuur 2; hieruit blijkt dat er geen incidenten met meer dan € 500.000 schade zijn aangetroffen).

Het uitvoeren van een risicoanalyse heeft zowel voordelen als nadelen. Voordelen van een risicoanalyse zijn onder meer het verkrijgen van inzicht in de bedreigingen ten aanzien van informatie, de gevolgen daarvan voor de organisatie en de mogelijk te treffen en te verbeteren maatregelen. Daarnaast maakt een risicoanalyse een bewuste afweging (kosten versus baten) van de te treffen en te verbeteren maatregelen mogelijk. Daartegenover staat dat het uitvoeren van een risicoanalyse een tijdrovende klus is, die bovendien vaak de nodige expertise vereist. Door de complexiteit van risicoanalyses is het uitvoeren ervan bovendien relatief duur, voornamelijk in het geval van een kwantitatieve risicoanalyse.

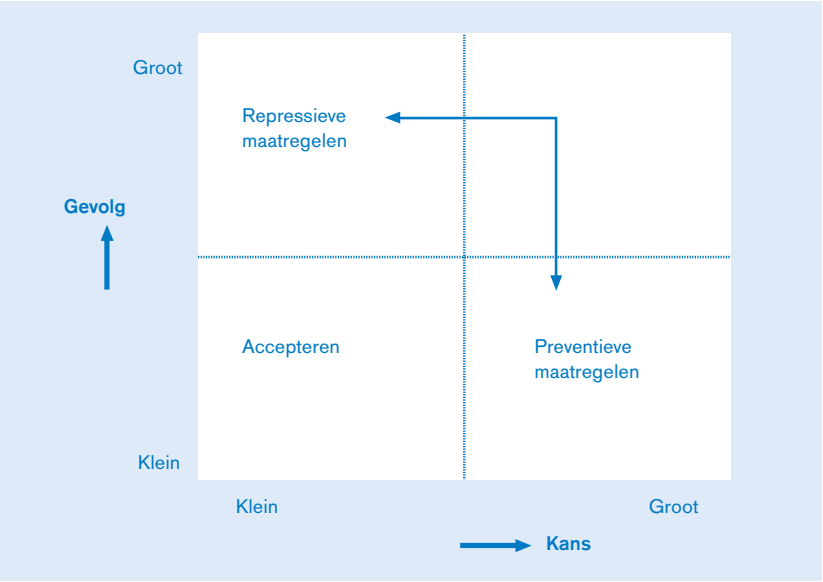
Vanwege deze complexiteit en de vaak lange doorlooptijd van gedetailleerde risicoanalyses heeft de laatste jaren de zogenaamde baselinebenadering terrein gewonnen. Baselines kunnen worden gezien in het licht van een bottom-up benadering, waarbij een stelsel algemeen geldende beveiligingsmaatregelen wordt gedefinieerd voor de 'gemiddelde' organisatie of het 'gemiddelde' bedrijfsonderdeel, onder normale omstandigheden. Door het implementeren van deze baselines kan een organisatie er zeker van zijn dat de meest voorkomende en ernstigste risico's onder normale, algemeen geldende omstandigheden voldoende zijn afgedekt.

Om meer bescherming te bieden aan bepaalde onderdelen met een hoog risico of om zich ervan te verzekeren dat sommige unieke situaties worden gedekt, zal een organisatie alsnog een risicoanalyse dienen uit te voeren teneinde dekking te bieden aan buitengewone situaties die niet door baselinebeveiligingsmaatregelen worden afgedekt.

Figuur 2. Totale (directe en indirecte) herstelkosten.



Bron: Ministerie van Economische Zaken/KPMG, *Monitor Internetbeveiliging 2003.*

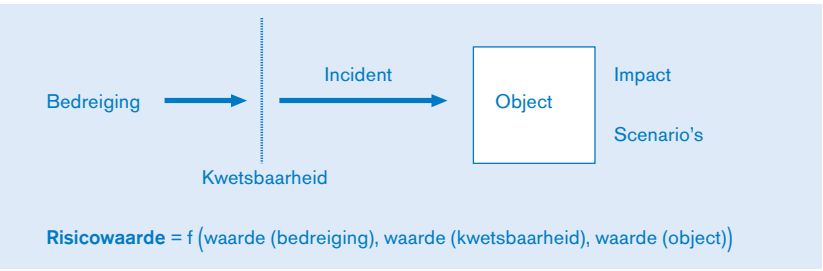


Figuur 3. Risicomatrix.

Toekomstverwachting omtrent risicoanalyse

De druk vanuit het maatschappelijk verkeer op organisaties om meer en structureel aan risicomanagement (en dus risicoanalyse) te doen, neemt toe. Zo bepaalt het zogenaamde Basel II-kapitaalakkoord dat bancaire instellingen operationele risico's dienen te bepalen en daarvoor (boven een bepaalde grens) reserves aan te houden. Een andere reden om aandacht te geven aan risico's is de invoering van 'Corporate Governance'. De commissie-Peters heeft in 1997 'Aanbevelingen inzake Corporate Governance in Nederland' gepubliceerd. De commissie heeft veertig aanbevelingen voor goed bestuur, adequaat toezicht en het afleggen van verantwoording opgesteld. Twee van deze veertig aanbevelingen hebben betrekking op risico's ofwel risicomanagement. Een andere stimulans voor het invoeren van risicomanagement zijn de recente boekhoudschandalen (Enron, Ahold, Parmalat). Met behulp van risicomanagement kan een organisatie naar buiten inzichtelijk maken wat zij heeft gedaan om de (gepercipieerde) risico's te beperken. Het tonen van 'goed huisvaderschap' kan veel negatieve publiciteit voorkomen. De verwachting is dat steeds meer organisaties ertoe over zullen gaan risicomanagement structureel in te voeren. Het beheersen van risico's die samenhangen met informatie(systemen) is hiervan een belangrijk onderdeel.

3) Naast de in dit artikel genoemde voorbeelden zijn er tal van andere risicoanalysemethoden, zoals OCTAVE (CERT), SARA (ISF), RiskMetriX (Le Platane Management) en de Risk Control Method (KPMG).



Figuur 4. CRAMM.

Maatregelen

Naar aanleiding van de door de risicoanalyse onderkende risico's zullen maatregelen om deze risico's te reduceren tot een (voor de organisatie) aanvaardbaar niveau, moeten worden verbeterd, geselecteerd of ontworpen. Per relevante bedreiging zullen al naargelang het gepercipieerde risico één of meer maatregelen getroffen moeten worden. Hierbij is het van belang dat uiteindelijk een consistente en coherente set maatregelen wordt geïmplementeerd.

Maatregelen kunnen preventief of repressief zijn. Preventieve maatregelen zijn gericht op het voorkomen van schade door de kans op het optreden van de bedreiging te verminderen, terwijl repressieve maatregelen gericht zijn op het beperken van de schade als gevolg van het optreden van de bedreiging. Of een maatregel preventief of repressief is, hangt af van de relatie tussen kans en gevolg van de bijbehorende risico's. In de risicomatrix (figuur 3) wordt dit verduidelijkt.

SPARK

Voor de inventarisatie van risico's en de afweging van de invoering van beveiligingsmaatregelen met betrekking tot kosten en baten van deze maatregelen, zijn verschillende risicoanalysemethoden beschikbaar. Figuur 4 geeft het risicomodel weer zoals dat in de aanpak CRAMM wordt gehanteerd. CRAMM staat voor CCTA Risk Analysis Management Method en is door CCTA (Central Computer and Telecommunications Agency) in Engeland ontwikkeld. CRAMM wordt ondersteund door een softwarepakket dat ook in het Nederlands verkrijgbaar is.
Een ander voorbeeld is de Afhankelijkheids- en Kwetsbaarheidsanalyse, zoals deze door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties is uitgewerkt op basis van het Voorschrift Informatiebeveiliging Rijksdienst (VIR). In de afhankelijkheidsanalyse worden betrouwbaarheidseisen aan een te onderzoeken informatiesysteem of -systemen vastgesteld. In de kwetsbaarheidsanalyse wordt de impact van de relevante bedreigingen (voor het betreffende informatiesysteem of -systemen) vastgesteld. Op basis van de kwetsbaarheidsanalyse wordt een pakket maatregelen geselecteerd dat voldoet aan de gestelde betrouwbaarheidseisen.

Een belangrijke valkuil van de genoemde methoden[3] is de mate van detaillering. De complexiteit en de hoeveelheid werk neemt explosief toe naarmate een hogere detaillering wordt gehanteerd bij de keuze van het object en de opsplitsing van het object in deelobjecten. Daarom behandelen we in dit artikel de methode SPARK.

SPRINT (Simplified Process for Risk Identification) is een kwalitatieve risicoanalysemethode ontwikkeld door het Information Security Forum (ISF)[4], voorheen het European Security Forum (ESF). SPRINT is door KPMG Information Risk Management verder ontwikkeld en geïntegreerd met de Code voor Informatiebeveiliging tot de methode SPARK (Simplified Process for Analyzing Risks by KPMG).

SPARK is een gestructureerde en relatief eenvoudige methode om de risico's met betrekking tot informatie en de ondersteunende processen, systemen en netwerken te onderzoeken. De methode is eveneens een hulpmiddel bij het selecteren van passende beveiligingsmaatregelen om de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie en bedrijfsvoering te garanderen. De methode bestaat uit drie fasen.

In fase 1 wordt de impact op bedrijfsprocessen en hieraan gerelateerde informatiesystemen van de consequentie van het verliezen van informatie (in termen van beschikbaarheid, integriteit en vertrouwelijkheid) bepaald. Op basis van deze inventarisatie wordt het informatiesysteem geclassificeerd. Voor systemen met een middelhoog en hoog gepercipieerd risico wordt verdergegaan met fase 2 van SPARK. In deze fase worden de bedreigingen, kwetsbaarheden en reeds getroffen beveiligingsmaatregelen in detail geïnventariseerd en onderzocht. Op basis van de relevante bedreigingen worden in fase 3 van SPARK, in overleg met het management, beveiligingsmaatregelen geselecteerd. Bij deze selectie kan gebruik worden gemaakt van gestructureerde vragenlijsten en referentiemaatregelen gebaseerd op de Code voor Informatiebeveiliging. Hierdoor zijn concrete aanknopingspunten voorhanden voor het treffen van maatregelen.

De methode wordt schematisch weergegeven in figuur 5. De ononderbroken pijlen geven de vereiste vervolgstappen aan en de onderbroken pijlen de mogelijke vervolgstappen. Een organisatie kan bijvoorbeeld besluiten geen verdere risicoanalyse uit te voeren voor laag-risicosystemen en haar eigen beveiligingsbeleid te hanteren in plaats van de Code voor Informatiebeveiliging.

In tabel 1 is een overzicht gegeven van alle fasen met onder andere de bijbehorende activiteiten, resultaten en door SPARK aangereikte hulpmiddelen.

SPARK kenmerkt zich door een organisatiegerichte benadering: de beslissingen over risico's en beveiligingsmaatregelen worden door het management genomen in samenspraak met specialisten en niet alleen door technische medewerkers.

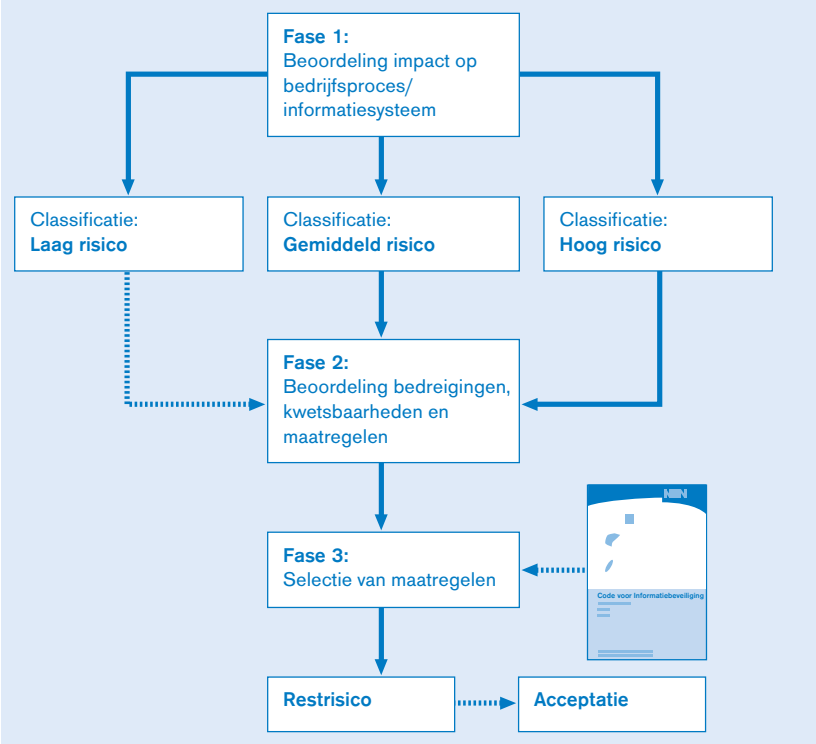
Verder is de methode zeer gestructureerd. Door gebruik te maken van de (standaard)vragenformulieren wordt op systematische wijze een oordeel gevormd over de belangrijkste beveiligingsonderwerpen. Om deze gestructureerdheid ook bij de selectie van maatregelen tot uitdrukking te brengen, maakt SPARK gebruik van de Code voor Informatiebeveiliging. Omdat echter ook andere standaarden aan de methode gekoppeld kunnen worden, zoals bijvoorbeeld CobIT of (klant)specifieke normenkaders, is SPARK zeer flexibel.

Ten slotte is de methode eenvoudig te begrijpen en toe te passen. Hierdoor is het mogelijk in een relatief korte doorlooptijd een goed resultaat te bereiken, waardoor de investering met betrekking tot tijd en geld beperkt blijft.

De eenvoudige toepassing van SPARK wordt eveneens bereikt door de geautomatiseerde ondersteuning van de methode met behulp van een in Qubus ontwikkelde applicatie. Qubus is een applicatie voor het ontwerp en de implementatie van vragenlijsten, benchmarks en rapporten. De SPARK-applicatie biedt ondersteuning bij de classificatie van informatiesystemen, de analyse van risico's en de keuze van te implementeren maatregelen door middel van geautomatiseerde vragenformulieren en een automatische koppeling van maatregelen aan risico's. Tevens biedt de applicatie verschillende rapportagemogelijkheden aan, zoals actielijsten voor de implementatie van geselecteerde maatregelen. Een onderdeel van de applicatie is weergegeven in figuur 6.

4) ISF is een internationale vereniging van meer dan 250 vooraanstaande organisaties die praktisch onderzoek verricht naar informatiebeveiliging.

Figuur 5. Schematische weergave van SPARK.



Tabel 1. Samenvatting van de fasen van SPARK.

	Fase 1. Bedrijfsimpact	2. Bedreigingen, kwetsbaarheden en getroffen maatregelen	3. Maatregelen en actieplan
Doel	Het beoordelen van de impact op bedrijfsprocessen en gerelateerde informatiesystemen.	Het beoordelen van de bedreigingen, kwetsbaarheden en getroffen beveiligings-maatregelen van het informatie-systeem en gerelateerde bedrijfsprocessen.	Het selecteren van beveiligings-maatregelen om de in fase 2 geïdentificeerde (relevante) bedreigingen en kwetsbaarheden te reduceren tot een voor de organisatie acceptabel niveau.
Belangrijkste activiteiten	Het samen met de proceseigenaar inschatten van de impact op bedrijfsprocessen en gerelateerde informatiesystemen door de gevolgen van het verlies van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie te beoordelen.	Het samen met de betrokken functionarissen inventariseren van bedreigingen en kwetsbaarheden op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid van het informatiesysteem, alsmede het in kaart brengen van de getroffen beveiligingsmaatregelen.	Het koppelen van beveiligings-maatregelen uit de maatregelensets aan de (rest)risico's uit fase 2.
Resultaat	Een overzicht van de bedrijfs-processen en informatiesystemen en de impact, inclusief een classificatie van het bedrijfs-proces in termen van beschikbaarheid, integriteit en vertrouwelijkheid.	Overzicht van de bedreigingen en kwetsbaarheden naar aard en schade en de getroffen maatregelen.	Overzicht van de (nog) te verbeteren of te treffen maatregelen.
Hulpmiddelen	Vragenformulieren bedrijfsimpact.	Vragenformulieren bedreigingen en kwetsbaarheden.	Maatregelensets en actielijsten.
Deelstappen	• Inventariseren bedrijfsprocessen en informatiesystemen; • beoordelen bedrijfsimpact; • classificatie van bedrijfsprocessen en gerelateerde informatiesystemen.	• Bepalen van de betrokken functionarissen; • verzamelen en vastleggen van gegevens; • inventariseren van bedreigingen, kwetsbaarheden en getroffen beveiligingsmaatregelen; • inschatten van (rest)risico.	• Bepalen niet-acceptabele (rest)risico's; • selecteren beveiligingsmaatregelen; • invullen actielijsten.

Figuur 6. Overzicht van Qubus-applicatie ter ondersteuning van SPARK.

Voorbeeld: Malaysian Airline System

De luchtvaartsector wordt – zeker de afgelopen jaren – gekenmerkt door een intense dynamiek. Bijvoorbeeld op het gebied van regulering. Om deze dynamiek te beheersen heeft Malaysian Airline System (MAS) Enterprise Risk Management geïntroduceerd. Het risicomanagement van informatie en informatiesystemen is hier een essentieel onderdeel van. KPMG heeft daarom SPARK bij MAS geïntroduceerd.

Met behulp van SPARK is voor alle divisies van MAS in kaart gebracht welke processen ondersteund worden door welke informatiesystemen. Vervolgens zijn de processen en ondersteunende informatiesystemen geclassificeerd in termen van beschikbaarheid, integriteit en vertrouwelijkheid. In vier maanden tijd zijn 21 processen en 64 ondersteunende informatiesystemen geanalyseerd. Hierdoor is een overzicht verkregen van de meest kritische processen per divisie, de relatie met de ondersteunende informatiesystemen en de prioriteiten met betrekking tot risicomanagement. SPARK stelde het management in staat op een snelle, consistente, gebalanceerde manier keuzen te maken om een goede, werkbare verhouding te vinden tussen beheersing van risico's en operationele bedrijfsprocessen. Doordat met behulp van SPARK tevens de bestaande maatregelen in kaart zijn gebracht, heeft het management een overzicht gekregen van de effectiviteit van de bestaande maatregelen. Voor die processen en systemen waarvan het risico (na maatregelen) te hoog werd geacht, zijn op eenvoudige wijze extra maatregelen (op basis van de Code voor Informatiebeveiliging) ontworpen en geïmplementeerd.

MAS is door KPMG getraind in het gebruik van SPARK. Hierdoor is MAS in staat in de toekomst op een regelmatige basis (bijvoorbeeld jaarlijks) de risicoanalyse zelfstandig uit te voeren.

Kader 2. SPARK in de praktijk: Malaysian Airline System.

Voorbeeld: VROM-Inspectie (onderdeel Ministerie van VROM)

Bij de rijksoverheid is sinds 1995 het Voorschrift Informatiebeveiliging Rijksdienst (VIR) van kracht. Dit voorschrift geeft onder andere aan dat er risicoanalyses uitgevoerd dienen te worden om in kaart te brengen welke risico's er gelopen worden door het gebruik van informatiesystemen. Ook door de VROM-Inspectie moest in korte tijd inzicht verkregen worden van welke informatiesystemen de primaire bedrijfsprocessen in hoge mate afhankelijk waren, zodat aangegeven kon worden welke risico's deze informatiesystemen met zich meebrachten en welke maatregelen nodig waren om deze risico's te mitigeren.

Met behulp van de SPARK-methode werd samen met KPMG eerst een 'mapping' gemaakt van de primaire bedrijfsprocessen en de informatiesystemen. Belangrijk is dat het lijnmanagement zijn verantwoordelijkheid neemt als het gaat om de beveiliging van de gegevensverwerking binnen zijn verantwoordelijkheidsgebied. Doordat met SPARK in korte tijd en met weinig moeite op hoofdlijnen inzichtelijk gemaakt kan worden welke informatiesystemen echt relevant zijn, kon de VROM-Inspectie zich richten op het verder analyseren van de medium-risk en high-risk systemen. Het kaf was van het koren gescheiden.

Een valkuil bij het uitvoeren van risicoanalyses is dat zij resulteren in enorme lijsten met maatregelen die onbeheersbaar zijn. SPARK relateert direct risico's aan maatregelen (aandachtsgebieden) uit de subparagrafen van de Code voor Informatiebeveiliging. Hierdoor was enerzijds voor het management transparant waarom bepaalde maatregelen nodig waren, anderzijds blijft de lijst overzichtelijk en beheersbaar.

Omdat de analyse werd ondersteund met de geautomatiseerde versie van SPARK kon al tijdens de interviewsessies inzicht verkregen worden in het resultaat. Een voordeel hiervan was dat er bijvoorbeeld in de interviewsessie van de kwetsbaarheden al een start gemaakt kon worden met het in kaart brengen van de huidige situatie.

Door de pragmatische aanpak van SPARK was in een doorlooptijd van ongeveer twee maanden duidelijk geworden welke systemen van belang waren voor de bedrijfsvoering van de VROM-Inspectie, welke risico's de organisatie liep in het gebruik van deze informatiesystemen en welke maatregelen geïmplementeerd moesten worden om die genoemde risico's te mitigeren.

Kader 3. SPARK in de praktijk: VROM-Inspectie.

Conclusie

Informatie en de ondersteunende processen, systemen en netwerken zijn belangrijke bedrijfsmiddelen voor veel organisaties. De beschikbaarheid, integriteit en vertrouwelijkheid ervan kunnen van essentieel belang zijn voor het behoud van de concurrentiepositie, cashflow, winstgevendheid, naleving van de wet en het imago van de organisatie. Deze bedrijfsmiddelen staan echter vaak bloot aan tal van bedreigingen, waardoor organisaties risico's lopen.

Het inzichtelijk maken en houden van de risico's verbonden aan de informatie en de ondersteunende processen zijn van wezenlijk belang om de beschikbaarheid, integriteit en continuïteit van de informatie en de systemen te borgen. Risicoanalyse is een belangrijk hulpmiddel om dit te doen.

Inzicht in de risico's maakt het namelijk mogelijk maatregelen te treffen om een voor de organisatie acceptabel beveiligingsniveau te realiseren. Afhankelijk van de gekozen benadering voor de risicoanalyse kan een dergelijke analyse maatregelen aanreiken om tot een reductie van het (rest)risico te komen.

SPARK is een kwalitatieve risicoanalysemethode die, naast classificatie van systemen en inventarisatie van de risico's, ook maatregelen aanreikt om het gepercipieerde (rest)risico te reduceren. Voor het aanreiken van deze maatregelen maakt SPARK gebruik van een normenkader gebaseerd op de Code voor Informatiebeveiliging.

De verwachting is dat steeds meer organisaties ertoe over zullen gaan risicomanagement structureel in te voeren

Literatuur

[Bure00] A.M. Buren, *New Security*, Compact 2000/4.

[Coum97a] C.J. Coumou, *Risico's en verzekeren. Wat doen we met informatiebeveiliging?*, Handboek Risico's en Verzekeren, 1997.

[Coum97b] C.J. Coumou, *Risico's waar gaat het over?*, Magazine Genootschap voor Risicomanagement, juli 1997.

[Coum00] C.J. Coumou, *Risicoanalyse als onderdeel van de Risk Control Method (RCM), een methode voor risicomanagement*, A.I.V. Control, juni 2000.

[Coum03] C.J. Coumou, *Risicomanagement voor security- en facilitymanagers*, Kluwer, 2003.

[ISF95] Information Security Forum (ISF), *Simplified Process for Risk Identification (SPRINT)*, 1995.

[Jaar02] J. Jaarsma, *Aan de slag met succesvolle risicoanalyses*, IT-beheer, nr. 7, september 2002.

[KPMG02] KPMG, *Understanding enterprise risk management*, white paper by KPMG's Assurance and Advisory Services, 2002.

[KPMG03] KPMG, *Monitor Internetbeveiliging 2003*, Ministerie van Economische Zaken, 2003.

[NGI90] Nederlands Genootschap voor de Informatica (NGI), Werkgroep Beveiligingssystemen van de sectie EDP-Auditing, *Beveiligingssystemen: een visie op toegang tot een visie*, Amsterdam, 1990.

[NNI00] Nederlands Normalisatie Instituut (NNI), *Code voor Informatiebeveiliging*, 2000.

[Over00] P. Overbeek, M. Spruit en E. Roos Lindgreen, *Informatiebeveiliging onder controle*, Prentice Hall, 2000.

[Russ91] D. Russel en G.T. Gangemi Sr., *Computer Security Basics*, O'Reilly & Associates, United States of America, 1991.

[Solm00] R. von Solms, *Risicoanalyse of security baselines?*, Compact 2000/4.

[Stel00] M. Stellinga en B. de Koning, *Een hacker is een goede wekker*, Financieel Economisch Magazine, nr. 8, 2000.