Informatiebeveiliging in economisch perspectief

Doelmatig investeren in de informatiebeveiliging van een webwinkel

Bachelor thesis Informatica & Economie

Begeleider: Dr. Ir. J. van den Berg

Auteur: John Zuidweg, 275827nz

Samenvatting

Het analyseren van informatiebeveiliging vanuit een economisch perspectief is niet eenvoudig: informatiebeveiliging is een onderwerp waarbij veel verschillende, interacterende factoren een rol spelen. In de literatuur zijn verschillende modellen ontworpen die theoretisch inzicht verschaffen in deze problematiek. Vaak liggen er echter onrealistische veronderstellingen aan deze modellen ten grondslag, zo worden factoren onbeïnvloedbaar verondersteld terwijl beïnvloeding in de praktijk wel mogelijk is. Modellen die de werkelijkheid beter benaderen, hebben vaak een hoog niveau van abstractie zodat ze niet direct toepasbaar zijn in de praktijk.

Omdat de verwachte kosten van beveiligingsincidenten moeilijk in te schatten zijn, wordt in veel ondernemingen volstaan met het toekennen van een beveiligingsbudget. Om dit budget zo effectief mogelijk te benutten, moeten beveiligingsmaatregelen geprioriteerd worden. In deze scriptie wordt een nieuwe methode gepresenteerd die resulteert in een rangschikking van beveiligingsmaatregelen op basis van effectiviteit. Ook het financiële aspect wordt meegenomen in de analyse zodat uiteindelijk een rangschikking naar doelmatigheid gemaakt kan worden. Managers kunnen uit de methode afleiden welke beveiligingsmaatregelen het meest doelmatig zijn, ook verschaft de methode inzicht in de financiële consequenties van verschillende soorten bedreigingen. Om de praktische werking van deze methode te illustreren wordt er in deze scriptie een case uitgewerkt waarin de methode wordt toegepast op de situatie van een webwinkel.

Inhoud

Dankwoord

Dankzij de inspirerende begeleiding van Dr. Ir. Jan van den Berg heb ik met veel plezier aan deze scriptie gewerkt. Zonder de scherpe analyse van Steven Debets, een praktijkexpert die werkzaam is bij VKA, was deze scriptie beperkt gebleven tot een theoretische analyse. Dankzij zijn opbouwende kritiek kon ik de gepresenteerde theorie beter plaatsen in een praktisch kader. Ten slotte nog een woord van dank aan dhr. G. van der Pijl, die als meelezend docent kennis wilde nemen van de inhoud van deze scriptie.

1. Introductie

Informatiebeveiliging is een belangrijk punt van zorg voor veel bedrijven. Het beveiligen van een informatiesysteem is kostbaar, maar noodzakelijk. Als er een serieus beveiligingsincident optreedt, kan dat resulteren in grote financiële schade voor de onderneming. Beveiligingsmanagers willen systemen zo veilig mogelijk krijgen, maar tegen welke prijs? In deze scriptie wordt een methode gepresenteerd waarmee beveiligingsmaatregelen geprioriteerd worden, zodat er op een doelmatige wijze geïnvesteerd kan worden in informatiebeveiliging.

1.1 Domein

Het onderwerp van deze scriptie is informatiebeveiliging. In de BS 7799 / IEC ISO 17799 standaard [2] wordt gesteld dat informatie een bedrijfsmiddel is, dat een bepaalde waarde heeft voor een onderneming. Vanuit dat oogpunt moet informatie op een correcte manier beveiligd worden. Informatiebeveiliging beschermt informatie, zodat bedrijfscontinuïteit gegarandeerd wordt. In deze scriptie wordt het doel van informatiebeveiliging gedefinieerd volgens de kenmerken zoals die geschetst worden in de BS 7799 / IEC ISO 17799 standaard [2], informatiebeveiliging is dan het garanderen van:

1. geheimhouding (confidentiality),
2. integriteit (integrity) en
3. beschikbaarheid (availability) van informatie.

Aan deze drie criteria kan alleen voldaan worden als er voldoende geïnvesteerd wordt in beveiligingsmaatregelen. De opbrengst van investeringen in deze maatregelen kan vaak niet goed in geldeenheden uitgedrukt worden, omdat kosten van beveiligingsrisico's moeilijk in te schatten zijn. Een methode die resulteert in een prioritering van beveiligingsmaatregelen is dan een goed alternatief. Ook bij allocatie van een vast budget kan volstaan worden met een rangschikking van maatregelen. In deze scriptie wordt een methode gepresenteerd die resulteert in een dergelijke prioritering.

1.2 Doelstelling

In dit onderzoek wordt een methode gepresenteerd die managers kan helpen bij het nemen van investeringsbeslissingen in informatiebeveiliging. Doel van het onderzoek is het ontwikkelen van een methode waarmee de relatieve doelmatigheid van investeringen in de informatiebeveiliging vastgesteld kan worden.

1.3 Methodologie

Eerst wordt een literatuurstudie uitgevoerd. De bestudeerde literatuur vormt de basis voor een theoretisch kader, van waaruit een nieuwe methode is ontwikkeld. Deze methode verenigt een aantal kernelementen uit de beschikbare theoretische modellen die betrekking hebben op informatiebeveiliging. De methode wordt getoetst door de uitwerking van een voorbeeld en door het voorleggen ervan aan een expert uit de praktijk.

1.4 Structuur

Eerst wordt er in hoofdstuk twee een theoretisch kader geschetst. Een aantal bestaande modellen die betrekking hebben op de economische analyse van informatiebeveiliging worden met elkaar vergeleken. Ook wordt er een overzicht gegeven van de inhoud van de BS 7799 / IEC ISO 17799 standaard. In hoofdstuk drie wordt een nieuwe methode uitgewerkt, deze methode wordt toegepast in hoofdstuk vier. Hoofdstuk vijf bestaat uit een overzicht van discussieonderwerpen die betrekking hebben op dit onderwerp. De conclusies van deze thesis worden in hoofdstuk zes samengevat. In het laatste hoofdstuk worden aanbevelingen gedaan voor praktische toepassingen en verder onderzoek.

2. Beveiligingsinvesteringen in de theorie

Nadat in 1993 de eerste webbrowser wordt gepubliceerd, komt de ontwikkeling van het Internet in een stroomversnelling. Veel ondernemingen worden verbonden met het Internet, dit brengt nieuwe beveiligingsrisico's met zich mee: bleef het domein van informatiebeveiliging eerst beperkt tot de eigen onderneming en het lokale netwerk, nu moet rekening gehouden worden met een globale dreiging van beveiligingsincidenten. Om de veiligheid van informatie te kunnen blijven garanderen moet geïnvesteerd worden in informatiebeveiliging. Er zijn inmiddels vele artikelen gepubliceerd over dit onderwerp, slechts een klein aantal van deze studies gaat in op de economische aspecten van informatiebeveiliging. In dit hoofdstuk wordt een selectie van deze artikelen besproken. De literatuurstudie dient als basis voor de relatieve indexeringsmethode (hoofdstuk drie).

Eerst wordt de aard en de complexiteit van het onderwerp duidelijk gemaakt, vervolgens worden een aantal bestaande modellen geanalyseerd. Deze modellen hebben betrekking op investeringsbeslissingen in de informatiebeveiliging. Ten slotte wordt een BS / IEC / ISO specificatie gepresenteerd.

2.1 Informatiebeveiliging is complex

Ross Anderson (2001) maakt in zijn artikel [1] duidelijk waarom beveiliging van informatie zo complex is. Hij laat zien dat informatiebeveiliging veel verder gaat dan technische implementatie van maatregelen. Hiervoor past hij elementen uit de micro-economie toe op de problematiek van informatiebeveiliging.

Uit zijn artikel blijkt dat, voor bedrijven in de informaticasector, het snel vermarkten van producten belangrijker is dan het garanderen van de veiligheid en robuustheid van het product. In de ICT-markt is er namelijk vaak sprake van hoge ontwikkelingskosten (vaste kosten) en lage marginale kosten. De ontwikkeling van een nieuw besturingssysteem heeft bijvoorbeeld miljoenen dollars gekost, terwijl het produceren van één enkele cd-rom, die de software bevat, hooguit enkele dollars kost. Als er binnen de markt veel concurrentie is, zullen bedrijven de ontwikkelde producten zo snel mogelijk op de markt willen zetten. Op die manier kan concurrentievoordeel behaald worden. Bedrijven kunnen het ontwikkelingstraject verkorten of minder tijd besteden aan het testen, zodat sneller kan worden overgegaan tot de productie. Het gevolg hiervan kan zijn, dat er producten op de markt komen die nog veel fouten, onvolkomenheden en beveiligingslekken bevatten.

Omdat bedrijven winstmaximalisatie nastreven, zullen ze kiezen voor de oplossing die het meeste oplevert, ongeacht de kwaliteit of de veiligheid van die oplossing. Zo worden er soms ondoorzichtige en onnodig complexe structuren gebruikt die het concurrenten moeten bemoeilijken de software na te maken. Op die manier wordt gestreefd naar het bereiken of het behouden van een monopoliepositie. Extra klantenbinding wordt bereikt door het verzorgen van een slechte aansluiting op producten waarvoor de leverancier zelf een alternatief levert. Klanten worden zo gestimuleerd om ook deze producten bij deze leverancier te betrekken. Deze manier van werken kan echter wel beveiligingsrisico's met zich meebrengen als producten van andere leveranciers toch moeten samenwerken met dit product.

Het garanderen van de veiligheid van een systeem kost veel meer inspanning dan het vinden van één beveiligingslek in een systeem. Anderson laat dit zien aan de hand van een voorbeeld: Als er 10,000 kritieke beveiligingslekken in de programmacode van Windows 2000 aanwezig zijn, dan kost het voor Microsoft veel tijd om al die 10,000 lekken op te sporen en te verhelpen. Voor een hacker is het relatief gemakkelijk om één beveiligingslek te vinden wat op dat moment nog niet gedicht is. Wat Anderson niet noemt, is het feit dat informatie over ontdekte beveiligingslekken zich razendsnel verspreidt: als één hacker een beveiligingslek ontdekt, zal hij direct via Internet andere hackers op de hoogte stellen. Voordat de softwarefabrikant het lek gedicht heeft, is de informatie over het beveiligingslek al verspreid over de hele wereld en zijn er al kwaadaardige computerprogramma's in omloop die het beveiligingslek uitbuiten.

Verder is er in de ICT-markt sprake van imperfecte informatie. Managers kunnen niet precies inschatten hoe het gesteld is met de kwaliteit en de veiligheid van een product. Hierdoor weten ze producten niet op hun waarde te schatten. Omdat ze denken dat de aanschaf van dure producten net zo veel risico met zich meebrengt als de aanschaf van goedkope producten, zijn ze niet bereid tot het betalen van een hoge prijs. Vaak blijkt echter dat in de lagere prijsklassen geen kwalitatief goede en veilige producten aanwezig zijn, waardoor uiteindelijk een relatief slecht en onveilig product aangeschaft wordt.

Anderson laat dus zien dat de problematiek van de informatiebeveiliging ernstig bemoeilijkt wordt door de aanwezigheid van 'perverse economische motieven'. Hij stelt dat wegruiming van deze motieven informatiebeveiliging zou reduceren tot rationeel risico management. In deze thesis worden informatiesystemen en beveiligingsmaatregelen op een rationele manier geanalyseerd.

2.2 Een economische benadering

Investeringen in informatiebeveiliging moeten op economische wijze geëvalueerd worden, zodat kosten en risico's van een beveiligingsincident vermeden worden [10], dat stellen Tsiakis en Stephanides (2005). Ze geven aan dat informatiebeveiliging vier doelen heeft:

1. Het garanderen van geheimhouding van vertrouwelijke informatie.
2. Het garanderen van de betrouwbaarheid van de informatie.
3. Het garanderen van de authenticiteit van informatie.
4. Het voorkomen van het verdwijnen van informatie.

Tsiakis en Stephanides laten zien hoe de evaluatie van investeringen in informatiebeveiliging zich ontwikkeld heeft in de loop van de tijd: Eerst lieten managers zich leiden door angsten, onzekerheden en twijfel; leveranciers speelden hier handig op in. Na verloop van tijd gingen veel bedrijven vaste budgetten toekennen aan investeringen in informatiebeveiliging, deze budgetten moesten zo efficiënt mogelijk ingezet worden. De laatste paar jaar is deze benadering steeds meer verdrongen door een nieuwe aanpak: het vaste budget wordt losgelaten en bij de inzet van beveiligingsmaatregelen wordt gekeken naar de mogelijke kosten die optreden als er niet beveiligd wordt. Nog een stap verder gaat de methode waarbij niet alleen naar de mogelijke kosten gekeken wordt, maar waarbij een structuur ontworpen wordt waarmee kosten en risico's geanalyseerd worden. Op die manier kan daar geïnvesteerd worden, waar beveiligingsmaatregelen het meeste opleveren. In de praktijk wordt echter nog steeds veel gewerkt met vaste budgetten, omdat het precies inschatten van kosten en baten van informatiebeveiliging erg complex is.

2.3 Kwetsbaarheidanalyse

Gordon en Loeb (2004) benadrukken in het door hen geschreven artikel [6] het belang van een kwetsbaarheidanalyse. Beveiligingsmaatregelen moeten daar ingezet worden, waar ze het meeste nut doen. Zij stellen dat informatiebeveiliging van een geautomatiseerd systeem moet bestaan uit het garanderen van de betrouwbaarheid en beschikbaarheid van het systeem en de geheimhouding van informatie.

Hoe meer er geïnvesteerd wordt in informatiebeveiliging, des te kleiner de kans op een beveiligingsincident. Als er maar genoeg geïnvesteerd wordt, is de kans op een beveiligingsincident op den duur verwaarloosbaar klein. Een perfecte beveiliging van kwetsbare informatie kan echter nooit worden gerealiseerd. Omdat informatiebeveiliging volgens Gordon en Loeb geen vaste kosten met zich meebrengt, wordt door een kleine investering de kans op een beveiligingsincident al gereduceerd.

Gorden en Loeb stellen een model op waarin de kwetsbaarheidanalyse een grote rol speelt. Zij beweren namelijk dat alleen de mate van kwetsbaarheid van een gegeven informatieset beïnvloed kan worden. De kans op een aanval en de mogelijke impact hiervan worden constant verondersteld. Gorden en Loeb gaan er vanuit dat, voor een gegeven informatieset en een gegeven aanval, de waarde van drie grootheden bepaald kan worden:

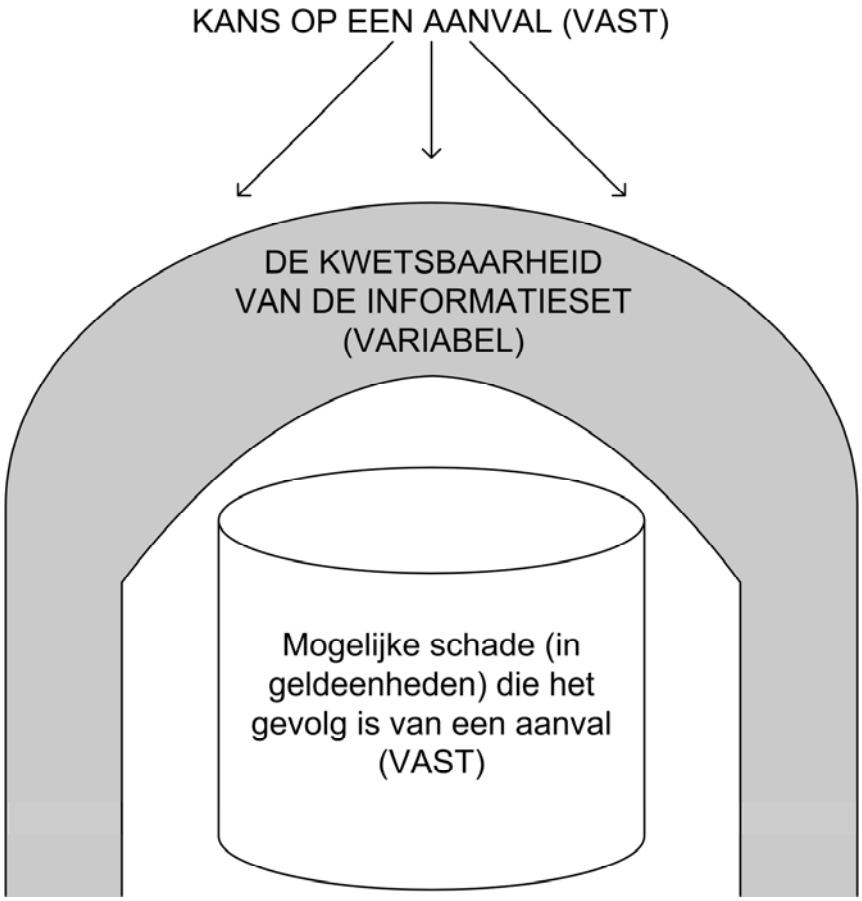
1. de kans op een aanval in een bepaalde periode,
2. de kwetsbaarheid van de betreffende informatieset en
3. de mogelijke schade in een bepaalde periode (uitgedrukt in geldeenheden) die het gevolg kan zijn van een aanval.

Het model van Gorden en Loeb is gebaseerd op deze drie variabelen, waarbij wordt gesteld dat de mogelijke schade kleiner is dan een bepaald groot bedrag. Het model doet dus geen uitspraken over systemen die zulke waardevolle publieke informatie bevatten dat de impact van een beveiligingsincident catastrofaal kan zijn. Verder wordt aangenomen dat een investering in beveiligingsmaatregelen alleen gevolgen heeft voor de kwetsbaarheid van een informatiesysteem: de kwetsbaarheid vermindert naarmate er meer geïnvesteerd wordt in informatiebeveiliging.

Er wordt een functie opgesteld, waarin de kans op een beveiligingsincident afhankelijk is van de kwetsbaarheid van het systeem en de investeringen in de beveiliging van de betreffende informatieset: $P(\text{incident}) = f(\text{kwetsbaarheid, beveiligingsinvestering})$.

In het model wordt risiconeutraliteit verondersteld, daarom zal de verwachte opbrengst van een investering steeds vergeleken worden met de kosten van die investering. De opbrengst bestaat uit de afname van de kans op een beveiligingsincident en dus een afname van de verwachte schade. Onder de aanname van risiconeutraliteit zal er geïnvesteerd worden totdat de marginale kosten gelijk zijn aan de marginale opbrengsten. Dit houdt in dat een onkwetsbaar systeem niet beveiligd wordt. Hoe kwetsbaarder een systeem, des te duurder het goed beveiligen ervan. Gorden en Loeb laten zien dat het doen van grote investeringen in de beveiliging van een zeer kwetsbaar systeem vaak suboptimaal is: de kosten van dergelijke grote investeringen zijn doorgaans hoger dan de ‘baten’. Om een zeer kwetsbaar systeem toch redelijk veilig te krijgen moet er zoveel geïnvesteerd worden in informatiebeveiliging, dat de kosten van de investering niet meer in verhouding staan tot de opbrengsten ervan in de vorm van een afname van de verwachte schade.

De kwetsbaarheidanalyse van Gordon en Loeb is schematisch weergegeven in Figuur 1: van een gegeven informatieset kan alleen de kwetsbaarheid beïnvloed worden, de kans op een aanval en de mogelijke schade die daar het gevolg van is wordt gezien als een externe variabele, ofwel als een constante. In de figuur is duidelijk te zien dat het effect van beveiliging van een informatieset tot uitdrukking komt in de kwetsbaarheid. De 'dikte' van de 'schil' die de gevolgen van een aanval beperkt, geeft uitdrukking aan de mate van kwetsbaarheid van de informatieset. Een kleinere kwetsbaarheid betekent een dikkere 'schil' en resulteert in een afname van de negatieve consequenties die het gevolg zijn van een aanval.

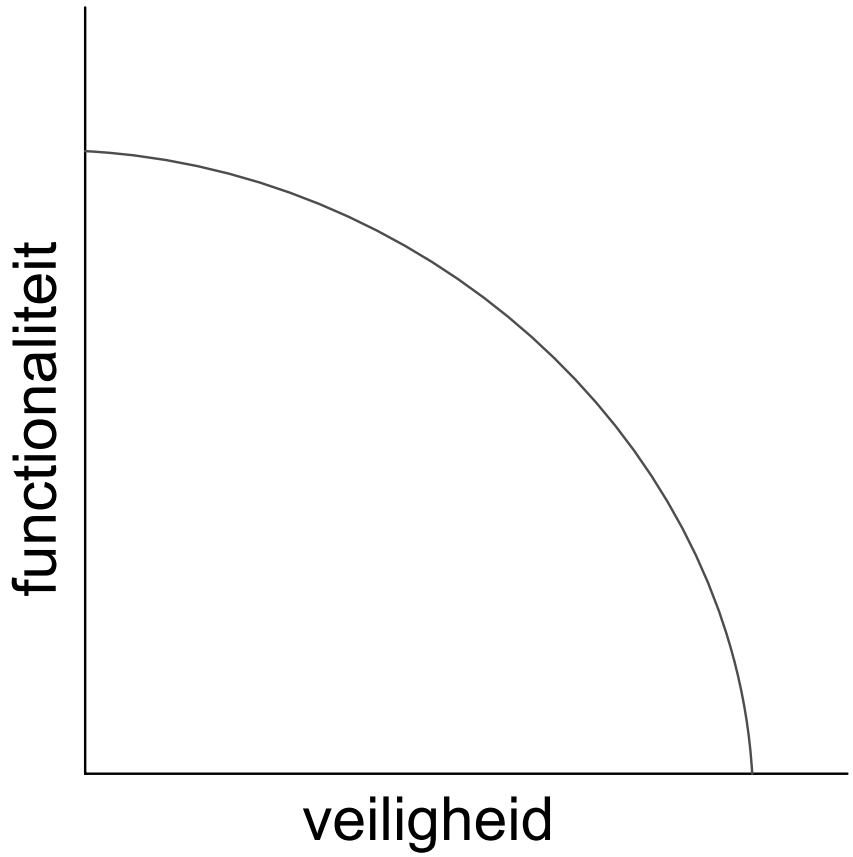


Figuur 1, standaard kwetsbaarheidanalyse

Tanaka, Matsuura en Sudoh (2005) toetsen de theoretische veronderstellingen uit de studie van Gordon en Gloeb aan de praktijk [9]. Hiervoor wordt data gebruikt van plaatselijke overheden in Japan. Bij het onderzoek ligt de focus op het verifiëren van de relatie tussen de kwetsbaarheid van een informatieset en de grootte van het te investeren bedrag in informatiebeveiliging. In dit artikel wordt ook ingegaan op de problematiek die speelt als meerdere bedrijven gebruik maken van een zelfde informatieset. Tanaka, Matsuura en Sudoh concluderen dat in de praktijk investeringen in informatiebeveiliging voor een groot deel afhankelijk zijn van de kwetsbaarheid van de betreffende informatieset.

2.4 Veiligheid versus functionaliteit

In het artikel “Towards a Model of the Costs of Security” [8] laten Larochelle en Rosasco (2003) zien dat er sprake is van een uitruil tussen beveiliging en functionaliteit. Ze veronderstellen dat alle ontwikkelingresources, zoals het beschikbare budget, vast staan. Als onder die condities software ontwikkeld wordt, zal er sprake zijn van een uitruil tussen veiligheid en functionaliteit. Deze uitruil houdt in dat, bij een vast budget, een keuze gemaakt moet worden tussen veiligheid en functionaliteit. Meer functionaliteit voor dezelfde prijs betekent minder veiligheid, terwijl een hogere mate van veiligheid alleen bereikt kan worden door de implementatie van minder functionaliteit. Een voorbeeld van deze uitruil is in de vorm van een grafiek weergegeven in Figuur 2.



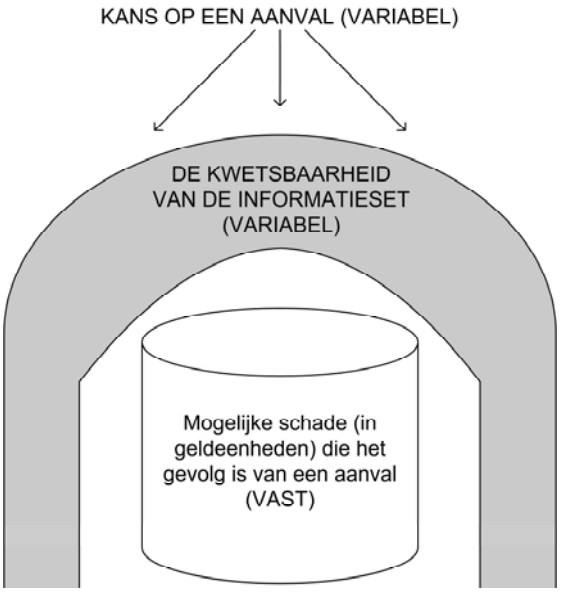
Figuur 2, voorbeeldgrafiek uitruil veiligheid en functionaliteit

Alleen de punten die op de kromme liggen zijn optimaal. Alle punten in deze grafiek die onder deze kromme liggen zijn suboptimaal: met hetzelfde budget kan een systeem ontwikkeld worden wat veiliger is, of wat meer functionaliteit biedt. Alle punten in deze grafiek die boven deze kromme liggen zijn onbereikbaar binnen het huidige budget. Alleen een verhoging van het budget of nieuwe technische ontwikkelingen kunnen deze punten binnen het bereik brengen.

2.5 Speltheorie en informatiebeveiliging

Dat ook speltheorie een rol speelt bij het nemen van investeringsbeslissingen in de informatiebeveiliging blijkt uit het artikel van Cavusoglu, Mishra en Raghunathan (2004). Zij tonen aan dat de kans op het optreden van een aanval op een systeem ook afhankelijk is van de pakkans die de betreffende hacker verwacht te lopen [4]. Een onderneming kan de gepercipieerde pakkans vergroten door implementatie van detectiesystemen en controleprocedures. De hacker zal alleen bereid zijn tot het lopen van een zekere pakkans als de verwachte opbrengst van een aanval hoog genoeg is. Deze opbrengst is zeker niet altijd financieel van aard, binnen het 'hackerswereldje' is status heel belangrijk. Om een hogere status te bereiken moeten spraakmakende aanvallen uitgevoerd worden. Daarom kan ook het bedrijfsimago van invloed zijn op de beslissing van een hacker om het informatiesysteem van dit bedrijf al dan niet aan te vallen: een bedrijf met een vriendelijk bedrijfsimago wordt over het algemeen minder aangevallen door hackers dan een bedrijf met een onvriendelijk imago. Ook de kwetsbaarheid van het systeem speelt een rol: het is gemakkelijker om in te breken in een kwetsbaar systeem, dan in een solide beveiligd systeem. Hackers zullen dus vaak een voorkeur hebben voor het aanvallen van een minder goed beveiligd systeem, al levert een succesvolle aanval op een goed beveiligd systeem voor de hackers een hogere status op. Belangrijk is om hierbij op te merken dat niet de absolute, maar de door de hackers gepercipieerde kwetsbaarheid hier doorslaggevend is. De kans op een aanval wordt in dit artikel dus niet als een constante, maar juist als een belangrijke variabele gezien (Figuur 3):

$$P(\text{aanval}) = f\left(\begin{array}{l}\text{gepercipieerde pakkans, bedrijfsimago,verwachte opbrengst aanval,}\\ \text{gepercipieerde kwetsbaarheid}\end{array}\right)$$



Figuur 3, standaard kwetsbaarheidanalyse met variabele kans op een aanval

2.6 Optimaliseren over meerdere gevolgen van beveiligingsrisico's

Als er sprake is van een restrictie op tijd of geld, zullen beveiligingsmaatregelen geprioriteerd moeten worden [3]. Butler en Fischbeck (2001) laten zien hoe een dergelijke prioritering tot stand kan komen. Hiervoor gebruiken zij een model waarin de beveiliging van een informatieset wordt geanalyseerd. Om deze analyse te kunnen uitvoeren, wordt gebruik gemaakt van optimalisatie over meerdere attributen, een techniek uit de beslissingstheorie. In dit model staat elk attribuut voor een bepaalde soort van schade die het gevolg is van een beveiligingsincident. De schade wordt uitgedrukt in geldeenheden, voorbeelden van soorten schade zijn: een verstoring van het productieproces, winstderving en een verslechterde publieke reputatie.

In dit onderzoek wordt de swing-weight methode geïntroduceerd: voor elk geanalyseerd beveiligingsincident wordt een gewicht toegekend aan elke soort impact waar mogelijk sprake van is. De gewichten worden gerelateerd aan het gewicht van de belangrijkste soort impact, vervolgens worden de gewichten genormaliseerd zodat ze sommeren tot 1. In Tabel 1 is een voorbeeld van de toepassing van de swing-weight methode weergegeven.

Tabel 1, voorbeeld toekenning gewichten via de swing-weight methode

Impact	Volgorde	Toegekende waardering	Gewicht
Afname productiviteit	1	100	.42
Verslechterde reputatie	2	80	.33
Juridische gevolgen (boetes)	3	40	.17
Winstderving	4	20	.08

Vervolgens worden verschillende bedreigingen in kaart gebracht. Per bedreiging wordt geanalyseerd in welke mate er sprake is van de verschillende soorten impact. Voor iedere bedreiging kan de som genomen worden van het product van het gewicht en de grootte van de impact. Als deze producten voor alle soorten impact bij elkaar opgeteld worden, kan de totale verwachte schade uitgerekend worden. Als per bedreiging een jaarlijkse verwachte frequentie wordt vastgesteld, kan de totaal verwachte schade per jaar (TI) uitgerekend worden. Een voorbeeld van een dergelijke berekening is weergegeven in Tabel 2.

Tabel 2, voorbeeld berekening bedreigingsindex TI

		Impact								
Bedreigingen	**Frequentie/jaar**	**Winstderving**		**Verslechterde reputatie**		**Afname productiviteit**		**Juridische gevolgen**		**TI**
		$w = .08$		$w = .33$		$w = .42$		$w = .17$		
Afwijken van procedures	4380	€2,-	.0002	1	.25	2 uur	.0083	0	0	376.69
Diefstal	24	€182	.0152	2	.5	1 uur	.0042	2	.67	6.75
Computer virussen	912	€0	0	0	0	3 uur	.0125	0	0	80.03

Butler en Fischbeck controleren de correctheid van de schatting van dit jaarlijkse schadebedrag. Hiervoor vragen ze managers om een inschatting van drie factoren van het betreffende beveiligrisico:

1. De minimale schade
2. De verwachte schade
3. De maximale schade

Vervolgens wordt een normale kansverdeling opgesteld waarin de verwachte schade als gemiddelde wordt genomen. Deze kansverdeling wordt gebruikt voor het uitvoeren van een simulatie-experiment. Als dit experiment een groot aantal keer herhaald wordt, kan op die manier ook een verwacht schadebedrag op jaarbasis bepaald worden. Op deze manier kan de eerste inschatting van de verwachte schade gecontroleerd worden. Het gaat hierbij niet om het schadebedrag op zichzelf, maar om de relatieve schade ten opzichte van andere beveiligingsrisico's. Uit een kleinschalig onderzoek blijkt dat managers goed in staat zijn beveiligingsrisico's te prioriteren door per attribuut een wegingsfactor toe te kennen.

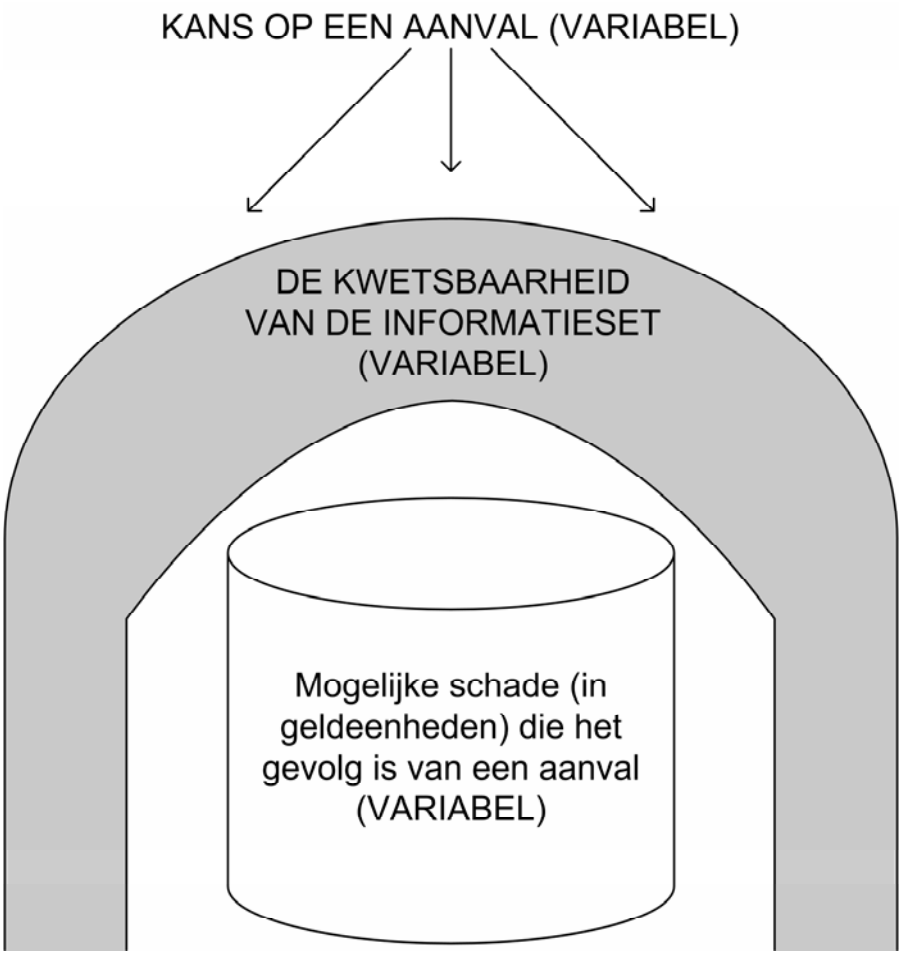
2.7 Beveiligen versus verzekeren

C. Lambrinoudakis e.a. [7] laten in een nog niet officieel gepubliceerd artikel zien dat de implementatie van beveiligingsmaatregelen aangevuld kan worden met het afsluiten van een verzekeringspolis. Beveiligingsmaatregelen sluiten het risico op beveiligingsincidenten nooit helemaal uit, een verzekeringspolis kan het resterende risico (deels) afdekken. Er wordt gesteld dat het inschatten van de financiële schade ten gevolge van beveiligingsincidenten erg moeilijk is, omdat er dagelijks nieuwe bedreigingen verschijnen.

Het uiteindelijke effect van de implementatie van beveiligingsmaatregelen is moeilijk meetbaar, omdat het al dan niet optreden van een beveiligingsincident niet direct toe te rekenen is aan één bepaalde beveiligingsmaatregel. Voor beveiligingsmanagers is het dus erg moeilijk om de optimale investering in informatiebeveiliging vast te stellen. Deze managers kunnen dit probleem, in elk geval voor een deel, van zich afschuiven door een verzekeringsmaatschappij in de arm te nemen. Deze verzekeringsmaatschappij vergoedt dan (een deel van) de schade die het gevolg is van een beveiligingsincident. Het verzekerde bedrijf betaalt hiervoor een periodieke premie. Bij de vaststelling van de hoogte van de te betalen premie moet, door de verzekeringsmaatschappij, een inschatting van de verwachte schade ten gevolge van beveiligingsincidenten gemaakt worden. In [7] wordt een methode gepresenteerd waarmee ondernemingen en verzekerings-maatschappijen de verwachte schade kunnen vaststellen. Nadat de verwachte schade in kaart gebracht is, kunnen er gerichte maatregelen genomen worden. De methode bestaat uit vier stappen:

1. Identificeer en waardeer de activa van het informatiesysteem.
2. Beng mogelijke bedreigingen en kwetsbaarheden in kaart en maak een inschatting van de mate van kwetsbaarheid en de grootte van de gevolgen van de mogelijke bedreigingen.
3. Geef met behulp van de geschatte kwetsbaarheden en bedreigingen een indicatie van de mogelijke impact van een bepaalde bedreiging en stel op die manier een risiconiveau vast.
4. Neem maatregelen op basis van het risiconiveau.

Er wordt een Markov model gebruikt om een wiskundige analyse te geven van de gevolgen van een beveiligingsincident. Volgens het model bevindt het systeem zich altijd in een bepaalde status. Als er een beveiligingsincident optreedt dat impact heeft, verandert de neutrale status van het systeem in een status die de gevolgen van het incident modelleert. Door de toepassing van dit model kunnen de verwachte kosten van een beveiligingsrisico in kaart gebracht worden. Bedrijven kunnen dit model gebruiken bij het nemen van een investeringsbeslissing in de informatiebeveiligingen en verzekerings-maatschappijen kunnen dit model gebruiken voor de vaststelling van de hoogte van de premie. Eigenlijk stellen Lambrinoudakis e.a. dat niet alleen de kwetsbaarheid van de informatieset en de kans op een aanval beïnvloed kunnen worden, maar dat ook de mogelijke schade beperkt kan worden door het afsluiten van een verzekeringspolis die (een deel van) de schade dekt die het gevolg is van een beveiligingsincident. Dit is schematisch weergegeven in Figuur 4: zowel de kans op een aanval als de kwetsbaarheid en de hoeveelheid schade worden nu gezien als beïnvloedbare variabelen.



Figuur 4, standaard kwetsbaarheidanalyse met variabele schade

2.8 Standaardspecificatie informatiebeveiliging

In februari 1995 werd de eerste versie van de 'BRITISH STANDARD Information security management' gepubliceerd. In 1998 en in 1999 is een nieuwe versie van deze standaard uitgebracht waarvan laatstgenoemde in 2000 de status van IEC / ISO standaard bereikte. Nu is deze specificatie bekend als BS 7799 / IEC ISO 17799. Deze specificatie [2] bestaat uit twee delen: in deel één worden aanbevelingen voor het van beveiligingsmanagement van informatie. In deel twee staan systemen voor beveiligingsmanagement centraal. Binnen deze standaard wordt informatiebeveiliging gekarakteriseerd als het garanderen van:

1. Geheimhouding (confidentiality): alleen geautoriseerde gebruikers hebben toegang tot informatie.
2. Integriteit (integrity): correctheid en compleetheid van informatie en van gebruikte verwerkingsmethoden.
3. Beschikbaarheid (availability): geautoriseerde gebruikers hebben toegang tot de informatie als dat nodig is.

Binnen de beveiligingsmaatregelen worden vijf verschillende categorieën onderscheiden:

1. Gedragsregels (policies)
2. Praktische toepassingen (practices)
3. Procedures
4. Organisatorische structuur
5. Beveiligingsfunctionaliteit binnen software

In het eerste deel van de specificatie wordt geanalyseerd waar implementatie van deze beveiligingsmaatregelen nodig is: er worden tien verschillende 'gebieden' onderscheiden die elk afzonderlijk beveiligingsmaatregelen vergen:

1. Beveiligingsbeleid op bedrijfsniveau
2. Organisatorische beveiligingsstructuren
3. Bedrijfsactiva
4. Personeel
5. Fysieke veiligheid en omgevingsfactoren
6. Communicatie en werkwijzen
7. Toegangscontrole
8. Systeemontwikkeling en –onderhoud
9. Bedrijfscontinuïteit
10. Wettelijke regelingen

2.9 Samenvatting literatuurstudie

Informatiebeveiliging is een moeilijk onderwerp, zeker als het benaderd wordt vanuit een economisch perspectief. Bij de beoordeling van de beveiliging van een informatiesysteem is er sprake van een wisselwerking tussen een groot aantal factoren, zoals de kwetsbaarheid van de informatieset, de verwachte schade van een beveiligingsincident en de kans op een aanval. Deze factoren zijn niet constant, ze zijn weer afhankelijk van andere variabelen.

In de literatuur zijn er verschillende modellen ontworpen. Voor deze modellen geldt dat ze vaak alleen bruikbaar zijn als er bepaalde aannames worden gedaan met betrekking tot de factoren waar de mate van informatiebeveiliging van afhankelijk is: vaak wordt één factor variabel verondersteld, terwijl alle andere elementen als constante gezien worden. Beveiligingsmaatregelen worden beoordeeld door te meten hoe groot het effect van de maatregel is op de variabele factor.

Uit de theorie kan geleerd worden dat de kwetsbaarheidanalyse belangrijk is, omdat de kwetsbaarheid het eenvoudigst te beïnvloeden is. Verder wordt ook duidelijk dat, wanneer er sprake is van vaste ontwikkelingsresources, er een keuze gemaakt moet worden tussen veiligheid en functionaliteit.

De analyse van Butler en Fischbeck [3] (paragraaf 2.6) geeft een goede aanzet voor een praktisch bruikbare methode. De swing-weight methode blijkt managers aan te spreken en levert goede resultaten op. De beschrijving van het onderzoek is echter vrij abstract, zodat managers niet goed concreet aan de slag kunnen met deze analyse.

Het model van Lambrinoudakis e.a. [7], zoals dat besproken is in paragraaf 2.7, legt geen beperkingen op aan factoren die het beveiligingsniveau van een informatiesysteem beïnvloeden. Uit het gepresenteerde model is echter niet op een eenvoudige manier een methode te destilleren die in de praktijk bruikbaar is bij het waarderen van beveiligingsmaatregelen.

Vroeger lieten beveiligingsmanagers zich leiden door angsten, onzekerheid en twijfel, nu willen ze beveiligingsmaatregelen beoordelen op doelmatigheid, zodat het beschikbare budget optimaal wordt benut. Een model waarin factoren die variabel zijn als contante gezien worden kan hierbij verhelderend werken, maar geeft nooit een compleet beeld. Er moet een methode ontworpen worden die, op een praktische manier, beveiligingsmaatregelen op waarde weet te schatten. Om dit te kunnen doen moet de theorie geoperationaliseerd worden naar een concreet niveau.

De BS 7799 / IEC ISO 17799 standaard biedt een overzicht van gebieden waarop beveiligingsmaatregelen vereist zijn, verder verdeelt deze standaard beveiligingsmaatregelen in een aantal hoofdcategorieën. Dit document biedt een goed uitgangspunt voor een concrete methode: per gebied kunnen bedreigingen, mogelijke incidenten en de impact van deze incidenten in kaart gebracht worden. Door vervolgens per maatregel het effect op deze factoren te schatten kan de effectiviteit van beveiligingsmaatregelen geanalyseerd worden.

Het is van groot belang dat alle belangrijke aspecten meegenomen worden in deze analyse. Dit houdt in, dat er bijvoorbeeld rekening gehouden moet worden met een uitruil tussen veiligheid en functionaliteit. In sommige gevallen kan een verzekering afgesloten worden die schade dekt die het gevolg is van een beveiligingsincident. Deze mogelijkheid moet ook opgenomen worden in de analyse van beveiligingsmaatregelen. In de praktijk spelen factoren als het bedrijfsimago en de beveiligingsperceptie een rol bij de bepaling van de kans op een aanval. De speltheorie biedt mogelijkheden om de relaties tussen verschillende factoren op dit gebied in kaart te brengen. Voor managers kan zulke informatie belangrijk zijn bij het inschatten van de kans op een aanval.

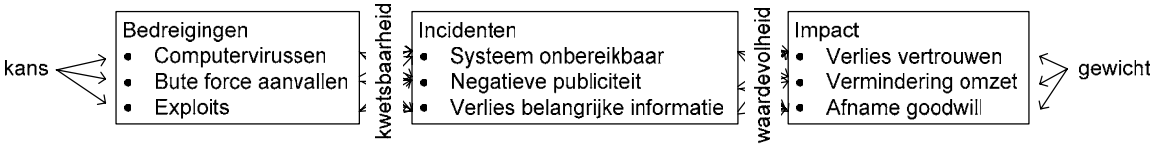
Een concrete methode, die recht doet aan al deze complexe factoren, is niet beschikbaar in de theorie, terwijl deze aanpak in de praktijk juist van grote waarde kan zijn. In het volgende hoofdstuk wordt een methode gepresenteerd, die op een praktische manier een oordeel geeft over de effectiviteit en de doelmatigheid van investeringen in informatiebeveiliging, zodat een beveiligingsbudget optimaal benut kan worden.

3. De relatieve indexeringsmethode

In dit hoofdstuk wordt een nieuwe methode gepresenteerd die inzicht verschaft in de relatieve doelmatigheid van investeringen in informatiebeveiliging. Op deze manier worden beveiligingsmaatregelen op economische wijze geprioriteerd, dit is waardevol wanneer er een vast budget gereserveerd is voor investeringen in informatiebeveiliging. In veel praktijksituaties kunnen de verwachte kosten van beveiligingsincidenten niet goed in geldeenheden uitgedrukt worden, de relatieve indexeringsmethode vormt dan een goed alternatief.

3.1 Structuur

De methode start met het in kaart brengen van mogelijke bedreigingen. Per bedreiging wordt eerst de kans van optreden ingeschat. Vervolgens wordt geanalyseerd welke incidenten het gevolg kunnen zijn van deze bedreiging. Het verband tussen een bedreiging en een incident is de kwetsbaarheid. De mate van kwetsbaarheid wordt per bedreiging, per incident bepaald. Elk incident kan, in een bepaalde mate, impact hebben op de bedrijfsvoering. Deze relatie geeft aan hoe waardevol het betreffende systeem(onderdeel) is. Aan elke soort impact wordt een gewicht toegekend, dit gewicht geeft de relatieve financiële impact weer, zodat de financiële consequenties van de verschillende soorten impact vergeleken kunnen worden. In Figuur 5 is dit schematisch weergegeven:

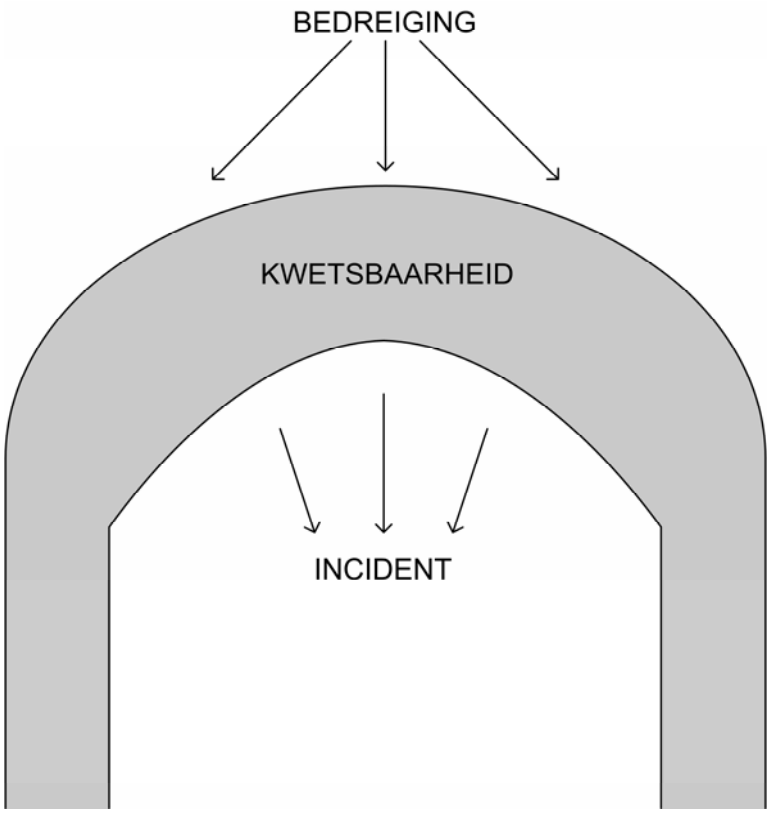


Figuur 5, voorbeeld structuur relatieve indexeringsmethode

Het proces dat moet worden gevolgd om de methode toe te passen, start met het vaststellen van kwaliteitscriteria. Er worden door de manager eisen gesteld aan de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie binnen het systeem. Op basis van deze criteria worden bedreigingen geïdentificeerd die inbreuk maken op de vastgestelde kwaliteitscriteria. Samen met de manager wordt een inschatting gemaakt van de kans op deze bedreigingen, tevens worden mogelijke maatregelen geïnventariseerd. De BS 7799 / IEC ISO 17799 standaard (zie paragraaf 2.8) kan hierbij een handig hulpmiddel zijn. De manager geeft vervolgens aan welke impact de verschillende incidenten tot gevolg kunnen hebben, tevens wordt geanalyseerd in welke mate er sprake is van deze impact. Aan de verschillende soorten impact kan een gewicht worden toegekend die uitdrukking geeft aan de economische consequenties ervan. Op deze manier kunnen de bedreigingen en beveiligingsmaatregelen gerangschikt worden op hun economische gevolgen.

3.2 Kwetsbaarheid

Elk bedrijf dat gebruik maakt van een informatiesysteem, heeft te maken met bedreigingen van beveiligingsincidenten. Deze bedreigingen komen niet alleen van buitenaf, maar zijn ook afkomstig uit de organisatie zelf. In paragraaf 2.8 van de literatuurstudie wordt de BS 7799 / IEC ISO 17799 standaard [2] besproken. Deze standaard biedt een overzicht van 'gebieden' in organisaties waarbinnen het onderwerp informatiebeveiliging aandacht vraagt. Deze standaard kan gebruikt worden om mogelijke bedreigingen van beveiligingsincidenten in kaart te brengen. Elke bedreiging kan één of meer incidenten tot gevolg hebben, de BS 7799 / IEC ISO 17799 standaard noemt per bedreiging een aantal mogelijke incidenten. De mogelijke incidenten variëren per bedreiging en zijn afhankelijk van de bedrijfsvoering van de onderneming. Per incident kan voor iedere bedreiging geanalyseerd worden hoe waarschijnlijk het optreden ervan is, gegeven dat er sprake is van de betreffende bedreiging. Deze kans is dan een uitdrukking van de kwetsbaarheid van de betreffende informatieset. De kwetsbaarheid geeft dus aan hoe sterk het verband is tussen een bedreiging en een incident: hoe sterker de relatie tussen bedreiging en incident, des te groter de kwetsbaarheid, hoe zwakker de relatie tussen bedreiging en incident, des te kleiner de kwetsbaarheid.



Figuur 6, kwetsbaarheid: relatie tussen bedreiging en incident

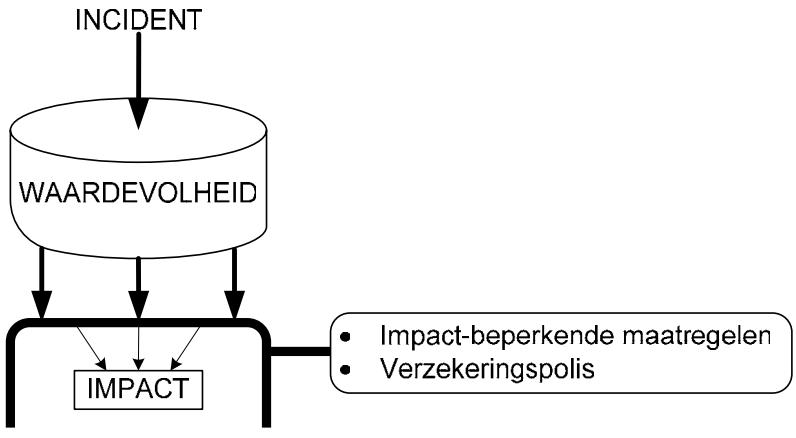
3.3 Impact

Managers zijn uiteindelijk alleen geïnteresseerd in de economische impact van beveiligingsrisico's, daarom wordt per incident geanalyseerd wat de impact is. Er zijn verschillende soorten impact denkbaar, in deze scriptie worden drie typen impact gebruikt zoals Cisco die onderscheidt [5]:

Tabel 3, economische impact volgens Cisco [5]

Type van economische impact op één organisatie	Mogelijke gevolgen van deze impact
Directe economische impact	• Schade aan systemen zodat menselijk ingrijpen vereist is (repareren of vervangen). • Onderbreking van bedrijfsvoering • Vertragingen in transacties en kasstroom
Impact op korte termijn	• Verlies van samenwerkingsverbanden met andere organisaties in waardeketen • Daling omzet • Verslechtering reputatie • Vertraging in ontwikkeling van nieuwe projecten
Impact op lange termijn	• Afname marktwaarde • Afname van vertrouwen investeerders • Afname aandelenprijs • Afname goodwill

De mate van impact die het gevolg is van een beveiligingsincident hangt sterk samen met de waardevolheid van het betreffende systeemonderdeel. Hoe meer waarde het onderdeel voor de onderneming heeft, des te groter de impact van een beveiligingsincident. Er kunnen impact-beperkende maatregelen (bijvoorbeeld implementatie van back-up procedures) genomen worden, tevens kan de impact (deels) geneutraliseerd worden door het afsluiten van een verzekeringspolis. Zie Figuur 7 voor een schematische weergave:



Figuur 7, waardevolheid: relatie tussen incident en impact

3.4 Maatregelen

Om de kans op beveiligingsincidenten te verminderen kunnen verschillende maatregelen genomen worden die resulteren in een minder kwetsbaar systeem. Ook de kans op een bepaalde bedreiging kan verminderd worden, bijvoorbeeld door toepassing van elementen uit de speltheorie (zie paragraaf 2.5). Er ook manieren om de impact van beveiligingsincidenten te verminderen. De beschikbaarheid en bruikbaarheid van de verschillende soorten maatregelen varieert per onderneming en is afhankelijk van de bedreigingen, de mogelijke incidenten en de (financiële) impact van de beveiligingsincidenten. Het is een uitdaging om creatieve oplossingen te zoeken buiten de bestaande kaders. Het is een goed idee om met een aantal betrokkenen een brainstormsessie te houden waarbij eerst zoveel mogelijk maatregelen bedacht worden, de meest aansprekende maatgelen kunnen vervolgens op waarde geschat worden door toepassing van de relatieve indexeringsmethode.

3.5 Toepassing van de relatieve indexeringsmethode

Uiteindelijk rangschikt het model de beschikbare maatregelen naar doelmatigheid. Om tot deze ordening te komen moet een aantal stappen uitgevoerd worden:

3.5.1 Inschatten bedreigingskansen

Nadat de kwaliteitscriteria voor de beschikbaarheid, integriteit en vertrouwelijkheid van informatie zijn vastgesteld, wordt voor iedere bedreiging die inbreuk maakt op deze criteria geanalyseerd in welke mate deze aanwezig is. Er kan gekozen worden uit drie opties:

1. De bedreiging is aanwezig in hoge mate
2. De bedreiging is aanwezig in zekere mate
3. De bedreiging is niet aanwezig

De manager geeft voor elke soort bedreiging aan hoe groot de verwachte mate van aanwezigheid is. In de methode worden hier linguïstische variabelen gebruikt, omdat het inschatten van een precieze kans erg moeilijk is en deze benadering goed aansluit bij de belevingswereld van de managers. De bedreigingskansen hangen af van verschillende factoren. De hoogte van bedreigingsrisico's op het gebied van virussen zijn bijvoorbeeld sterk afhankelijk van het gebruikte besturingssysteem, terwijl de kans om doelwit te worden van een hacker weer afhankelijk is van heel andere factoren: de gepercipieerde beveiliging, het imago en de bekendheid en het bedrijf spelen dan een rol. Het in kaart brengen van al deze factoren vergt een studie op zich en houdt ondermeer verband met de speltheorie.

Als alternatief voor een keuze uit die opties zou de swing-weight methode [3] (zie paragraaf 2.6) toegepast kunnen worden. Omdat risico's echter moeilijk onderling te vergelijken zijn wordt volstaan met een keuze uit drie opties.

3.5.2 Bepalen gevolgen van bedreigingen

Als een bedreiging bewaarheid wordt, kunnen er beveiligingsincidenten optreden. In de methode geeft de manager per bedreiging aan in welke mate bepaalde incidenten het gevolg zijn van deze bedreiging, gegeven dat deze bedreiging bewaarheid wordt. De verwachte kans van optreden van een incident, gegeven het optreden van een bepaalde bedreiging, wordt opnieuw uitgedrukt middels een linguïstische variabele:

1. Het incident treedt zeker op (grote kwetsbaarheid)
2. Het incident treedt waarschijnlijk op (vrij grote kwetsbaarheid)
3. Het incident treedt misschien op (gemiddelde kwetsbaarheid)
4. Het incident treedt waarschijnlijk niet op (kleine kwetsbaarheid)
5. Het incident treedt nooit op (onkwetsbaar)

Op deze manier wordt per bedreiging duidelijk wat de kans is op een bepaald incident.

3.5.3 Analyseren impact

Per mogelijk incident kan de impact geanalyseerd worden. Niet alleen de soort impact kan per incident verschillend zijn, ook de grote van de impact kan variëren. Daarom wordt de mate van impact per incident uitgedrukt middels een linguïstische variabele:

1. Er is sprake van een grote impact
2. Er is sprake van een bovengemiddelde impact
3. Er is sprake van een gemiddelde impact
4. Er is sprake van een kleine impact
5. Er is geen sprake van impact

Uiteindelijk moet de impact vertaald worden naar een financiële maatstaf. De manager is namelijk geïnteresseerd in de financiële consequenties van beveiligingsrisico's en –maatregelen. Daarom wordt de swing-weight methode [3] (zie paragraaf 2.6) toegepast op de impact: de manager geeft aan welke soort impact de grootste financiële gevolgen heeft. Deze soort impact krijgt een gewicht van 100. Vervolgens krijgen de andere soorten impact ook een gewicht. De gewichten kunnen variëren van 0 tot 100 en worden gerelateerd aan de impact met het gewicht van 100. Iedere gewicht wordt gedeeld door de som van alle gewichten, zodat deze samen sommeren tot 1. Bij de toekenning van de gewichten moeten toekomstige kosten contant gemaakt worden, verder moeten ook de kosten van functionaliteitverlies meegenomen worden in de analyse.

3.5.4 Bepalen bedreigingsindex

Per bedreiging kan een 'bedreigingsindex' vastgesteld worden. Om deze index te kunnen berekenen moeten de linguïstische variabelen omgezet worden naar numerieke waarden. Voor wat betreft de mate van aanwezigheid van een bedreiging:

1. De bedreiging is aanwezig in hoge mate → numerieke waarde 1
2. De bedreiging is aanwezig in zekere mate → numerieke waarde 0.5
3. De bedreiging is niet aanwezig → numerieke waarde 0

Voor wat betreft de verwachte mate van optreden van een incident, gegeven het optreden van een bepaalde bedreiging:

1. Het incident treedt zeker op → numerieke waarde 1
2. Het incident treedt waarschijnlijk op → numerieke waarde 0.75
3. Het incident treedt misschien op → numerieke waarde 0.5
4. Het incident treedt waarschijnlijk niet op → numerieke waarde 0.25
5. Het incident treedt nooit op → numerieke waarde 0

Voor wat betreft de mate van impact per incident:

1. Er is sprake van een grote impact → numerieke waarde 1
2. Er is sprake van een bovengemiddelde impact → numerieke waarde 0.75
3. Er is sprake van een gemiddelde impact → numerieke waarde 0.5
4. Er is sprake van een kleine impact → numerieke waarde 0.25
5. Er is geen sprake van impact → numerieke waarde 0

Alle bovengenoemde numerieke waarden bevatten op zichzelf weinig informatie. Eerst moeten alle waarden geaggregeerd worden, deze geaggregeerde grootheid krijgt pas betekenis als deze vergeleken kan worden met een andere grootheid die op dezelfde manier tot stand gekomen is. Deze geaggregeerde grootheid wordt 'bedreigingsindex' genoemd.

Gesteld wordt dat er sprake is van n bedreigingen, m mogelijke incidenten en q soorten impact. Om duidelijk te maken hoe de bepaling van de bedreigingsindex tot stand komt, worden eerst een aantal variabelen geïntroduceerd:

$\alpha_i =$ mate van aanwezigheid van bedreiging i
$a_i \in \{1, 0.5, 0\}, 1 \le i \le n$

$\beta_{ij} =$ kans op incident j ten gevolge van bedreiging i
$\beta_{ij} \in \{1, 0.75, 0.5, 0.25, 0\}, 1 \le j \le m$

$\gamma_{jk} =$ mate van aanwezigheid van impact k ten gevolge van incident j
$\gamma_{jk} \in \{1, 0.75, 0.5, 0.25, 0\}, 1 \le k \le q$

$w_k =$ gewicht impact γ_k,
$0 \le w_k \le 1$
$\sum_{k=1}^{q} w_k = 1$

Nu kan de bedreigingsindex eenvoudig berekend worden:

$TI_i =$ bedreigingsindex bedreiging i
$TI_i = \alpha_i \sum_{j=1}^{m} \beta_{ij} \sum_{k=1}^{p} w_k \gamma_{jk}$

De waarde van deze bedreigingsindex zegt op zichzelf niet veel, de kracht van de bedreigingsindex schuilt in de relatieve waarde ervan. Een waarde van 0 geeft echter wel aan dat de betreffende bedreiging geen enkel verwacht nadelig effect tot gevolg heeft, een waarde groter dan 0 geeft aan de bedreiging een zeker nadelig gevolg met zich meebrengt. Naast de bedreigingsindex per bedreiging, kan ook een totale bedreigingsindex over alle bedreigingen berekend worden:

$TTI =$ totale bedreigingsindex alle bedreigingen
$TTI = \sum_{i=1}^{n} TI_i$

Een TTI van 0 betekent dat er geen enkel nadelig effect verwacht wordt van bedreigingincidenten, een waarde die groter is dan 0 een geeft aan dat er een zekere schade verwacht wordt. De totale bedreigingsindex geeft op zichzelf weinig of geen informatie, maar als verschillende totale bedreigingsindices vergeleken worden ontstaat er een krachtig instrument voor het beoordelen van beveiligingsmaatregelen.

3.5.5 Beoordelen beveiligingsmaatregelen

De effectiviteit van beveiligingsmaatregelen kan eenvoudig beoordeeld worden: als eerst de totale bedreigingsindex zonder beveiligingsmaatregelen berekend wordt, dan kan vervolgens per beveiligingsmaatregel gekeken worden wat het effect is op de variabelen α_i, β_{ij} en γ_{jk}.

Als nu, voor elke beveiligingsmaatregel afzonderlijk, de bedreigingsindex weer berekend wordt met de nieuwe waardes voor α_i, β_{ij} en γ_{jk}, dan kunnen de beveiligingsmaatregelen gerangschikt worden op effectiviteit. De maatregel die de grootste afname van de totale bedreigingsindex *TTI* tot gevolg heeft is het meest efficiënt, terwijl de maatregel die de kleinste afname van de totale bedreigingsindex *TTI* tot gevolg heeft het minst efficiënt is.

Als ook de kosten van de implementatie en het gebruik van de beveiligingsmaatregelen meegenomen worden in de analyse, kunnen de beveiligingsmaatregelen gerangschikt worden op doelmatigheid.

Deze methode is beperkt tot de rangschikking van beveiligingsmaatregelen, daarom kan de swing-weight methode opnieuw toegepast worden: de manager geeft aan welke beveiligingsmaatregel de meeste kosten met zich meebrengt. Deze soort beveiligingsmaatregel krijgt een gewicht van 100. Vervolgens wordt aan de andere beveiligingsmaatregelen ook een gewicht toegekend. De gewichten kunnen variëren van 0 tot 100 en worden gerelateerd aan de beveiligingsmaatregel met het gewicht van 100. Iedere gewicht wordt gedeeld door de som van alle gewichten, zodat deze samen sommeren tot 1.

Door voor elke maatregel te analyseren wat het effect is op de bedreigingsindex kunnen de verschillende beveiligingsmaatregelen beoordeeld worden op effectiviteit. Door via de swing-weight methode de kosten van beveiligingsmaatregelen als prijsindex *p* mee te nemen in de analyse kunnen de beveiligingsmaatregelen gerangschikt worden op doelmatigheid. Eerst wordt gesteld dat er *r* maatregelen zijn:

$\delta_b = \text{effect beveiligingsmaatregel } b$
$\delta_b = TTI_{\text{voor implementatie maatregel}} - TTI_{\text{na implementatie maatregel}}$
$1 \le b \le r$

$p_b = \text{prijsindex beveiligingsmaatregel } b$
$0 \le p_b \le 1$
$\sum_{b=1}^{r} p_b = 1$

$\varepsilon_b = \text{doelmatigheid beveiligingsmaatregel } b$
$\varepsilon_b = \delta_b(1 - p_b)$

Wat betreft het prijspijl van de beveiligingsmaatregelen, dient opgemerkt te worden dat een eventueel functionaliteitsverlies een kostenpost is, die meegenomen moet worden in de analyse. Ook moeten toekomstige kosten verdisconteerd worden naar de netto contante waarde. Omdat de precieze kosten zeer moeilijk in te schatten zijn en er vaak sprake is van een vast budget, wordt in de relatieve indexeringsmethode volstaan met een rangschikking.

De doelmatigheidswaarde ε_b van een maatregel geeft op zichzelf geen informatie. Deze variabele is ordinaal van aard: pas in vergelijking met andere doelmatigheidswaarden kan informatie ontleend worden aan deze grootheid.

Als mogelijke beveiligingsmaatregelen gerangschikt zijn, kan dat een manager helpen bij het nemen van een investeringsbeslissing: als er een budget toegewezen is moeten de meest doelmatige beveiligingsmaatregelen in overweging genomen worden. Verder is deze methode is een handig hulpmiddel voor managers die uit verschillende maatregelen moeten kiezen welke maatregel(en) er daadwerkelijk doorgevoerd moeten worden. De methode maakt voor managers inzichtelijk wat binnen het systeem het effect is van een bepaalde maatregel.

4. Casestudie: webwinkel

In dit hoofdstuk wordt de relatieve indexeringsmethode, zoals die is gepresenteerd in hoofdstuk 3, inzichtelijk gemaakt door uitwerking van een casestudie. Het onderwerp van de casestudie is een webshop: een winkel die via Internet producten verkoopt aan consumenten. In deze casestudie is de analyse beperkt tot het risico van kwaadaardige software. Eerst worden gevolgen van dit risico in kaart gebracht, vervolgens wordt de impact van deze gevolgen ingeschat. Ten slotte worden twee maatregelen beoordeeld op doelmatigheid. In werkelijkheid spelen natuurlijk veel meer risico's een rol, waardoor de analyse complexer en uitgebreider wordt, toch geeft deze casestudie een praktisch beeld van de werking van de relatieve indexeringsmethode.

4.1 Risico: kwaadaardige software

Bij het identificeren van de beveiligingsrisico's die van toepassing zijn op deze case wordt de BS 7799 / IEC ISO 17799 standaard [2] als uitgangspunt gebruikt. In deze scriptie wordt volstaan met het analyseren van het risico van het optreden van kwaadaardige software (malicious software). De dreiging van kwaadaardige software wordt besproken in paragraaf 8.3 van het eerste deel van de BS 7799 standaard [2] en in paragraaf 4.6.3 van het tweede deel. Deze kwaadaardige software heeft verschillende verschijningsvormen:

1. Computervirussen: deze vorm van kwaadaardige software is het bekendst en veroorzaakt schade aan software en/of bestanden. Virussen kunnen ook complete netwerken platleggen en verzorgen vaak overlast door verspreiding via e-mail.
2. Netwerk wormen: zichzelf replicerende programma's die zorgen voor overlast doordat ze zich massaal via het netwerk verspreiden en vermenigvuldigen, WORM staat voor Write Once, Read Many (Times).
3. Trojaanse paarden: deze programma's zorgen ervoor dat een kwaadwillende persoon, of kwaadaardige software, toegang verkrijgt tot de het geïnfecteerde systeem en de daarop aanwezige data.
4. Spyware: niet genoemd in BS 7799, deze software verzamelt en verstuurt informatie over het computergebruik of op de computer aanwezige data.
5. Logische bommen: deze programma's leggen computersystemen lam en maken ze tijdelijk onbruikbaar.

4.2 Gevolgen

Per verschijningsvorm van kwaadaardige software kunnen diverse mogelijke gevolgen onderscheiden worden:

1. Belangrijke data gaat verloren.
2. Bestellingen kunnen niet op tijd worden geleverd.
3. Klanten worden bestookt met virusmail.
4. Het systeem is onbereikbaar (klanten kunnen website niet raadplegen en geen contact leggen via e-mail).
5. Vertrouwelijke informatie komt beschikbaar voor derden.

4.3 Impact

De impact van deze gevolgen kan per gevolg geanalyseerd worden, bij elk van bovengenoemde vijf gevolgen is in meer of mindere mate sprake van de volgende impact:

1. Direct: Schade aan systemen zodat menselijk ingrijpen vereist is (repareren of vervangen van systeemonderdelen), onderbreking van bedrijfsvoering, vertragingen in transacties en kasstroom.
2. Korte termijn: daling omzet, verslechtering reputatie.
3. Lange termijn: afname marktwaarde, afname van vertrouwen investeerders en afname van goodwill.

4.4 Bedreigingsindex

Om de bedreigingsindex uit te rekenen, moeten de stappen gevolgd worden zoals die beschreven staan in paragraaf 3.5. Er wordt van uitgegaan dat alle kwaadaardige software inbreuk maakt op de vastgestelde kwaliteitscriteria. Eerst wordt de mate van aanwezigheid van de verschillende soorten bedreigingen van kwaadaardige software in kaart gebracht:

Tabel 4, case webwinkel: aanwezigheid bedreigingen

Bedreiging	Verwachte mate van aanwezigheid	α
1. Computer virussen	hoge mate	$\alpha_1 = 1$
2. Netwerk wormen	zekere mate	$\alpha_2 = .5$
3. Trojaanse paarden	zekere mate	$\alpha_3 = 1$
4. Spyware	hoge mate	$\alpha_4 = 1$
5. Logische bommen	zekere mate	$\alpha_5 = .5$

Nu wordt voor elk incident de verwachte mate van optreden bepaald, gegeven het optreden van een bepaalde bedreiging. Aangenomen wordt:

Tabel 5, case webwinkel: gevolgen computervirussen

Bedreiging: 1. Computervirussen		
Gevolg	**Verwachte mate van optreden**	***β***
1. Belangrijke data gaan verloren	Misschien	$\beta_{1,1} = .5$
2. Bestellingen worden niet op tijd geleverd	Misschien	$\beta_{1,2} = .5$
3. Klanten worden bestookt met virusmail	Waarschijnlijk	$\beta_{1,3} = .75$
4. Systeem onbereikbaar	Misschien	$\beta_{1,4} = .5$
5. Vertrouwelijke informatie komt beschikbaar voor derden.	Nooit	$\beta_{1,5} = 0$

Een tabel als Tabel 5 kan voor elk van de bedreigingen opgesteld worden, in dit voorbeeld is de analyse beperkt tot de bedreiging van computervirussen.

Nu moet per gevolg (incident) gekeken worden hoe groot de impact is, de linguïstische variabelen zijn hier direct vertaald in numerieke waardes:

Tabel 6, case webwinkel: impact gevolgen

Gevolg	**Verachte mate van impact**		
	direct	**korte termijn**	**lange termijn**
1. Belangrijke data gaan verloren	$\gamma_{1,1} = 1$	$\gamma_{1,2} = .75$	$\gamma_{1,3} = .5$
2. Bestellingen worden niet op tijd geleverd	$\gamma_{2,1} = .75$	$\gamma_{2,2} = .5$	$\gamma_{2,3} = 0$
3. Klanten worden bestookt met virusmail	$\gamma_{3,1} = .5$	$\gamma_{3,2} = .75$	$\gamma_{3,3} = .5$
4. Systeem onbereikbaar	$\gamma_{4,1} = 1$	$\gamma_{4,2} = .5$	$\gamma_{4,3} = 0$
5. Vertrouwelijke informatie komt beschikbaar voor derden.	$\gamma_{5,1} = .5$	$\gamma_{5,2} = 1$	$\gamma_{5,3} = 1$

Stel dat impact op de lange termijn de meeste financiële gevolgen heeft (100), vervolgens impact op de korte termijn (80) en ten slotte directe impact (60). De gewichten w krijgen dan de volgende waardes: $w_1 = .25$, $w_2 = .33$, $w_3 = .42$.

Nu kan de bedreigingsindex voor de bedreiging ‘computervirussen’ uitgerekend worden: de gewichten worden vermenigvuldigd met de numerieke waarden van de impact, vervolgens worden deze getallen vermenigvuldigd met de numerieke waarde van de verwachte mate van optreden. Omdat aan computervirussen een hoge mate van aanwezigheid (numerieke waarde 1) is toegekend, mogen deze numerieke waarden direct gesommeerd worden, het resultaat van deze sommatie, 1.174375, is de waarde voor de bedreigingsindex voor de bedreiging door computervirussen. Dit getal zegt op zichzelf helemaal niets, maar als ook van alle andere bedreigingen, waaronder die van overige kwaadaardige software, een bedreigingsindex bepaald wordt, kan op die manier geanalyseerd worden welke bedreiging de grootste verwachte financiële impact heeft. De bedreigingsindex is ook nuttig bij het beoordelen van beveiligingsmaatregelen, dit is het hoofddoel van de relatieve indexeringsmethode en hierop wordt dieper ingegaan in de volgende paragraaf.

4.5 Maatregelen

Er zijn in de praktijk veel manieren bekend om de bedreiging van kwaadaardige software te bestrijden. De BS 7799 / IEC ISO 17799 standaard [2] geeft een overzicht van mogelijke maatregelen. Om te illustreren hoe beveiligingsmaatregelen beoordeeld en gerangschikt worden met behulp van de relatieve indexeringsmethode is de analyse beperkt tot twee voorbeelden van maatregelen:

1. Speciale software ter voorkoming van optreden ongewenste, kwaadaardige software: Deze programmatuur spoort kwaadaardige software op en maakt deze onschadelijk. De meeste virusscanners zijn in staat deze taak uit te voeren, mits ze regelmatig worden voorzien van de nieuwste virusdefinities.

2. Een andere mogelijkheid ter vermindering van de dreiging van kwaadaardige software is de migratie naar een ander besturingssysteem: Als de eigenaar van de webwinkel nu op de meeste van zijn computers het Microsoft Windows besturingssysteem heeft geïnstalleerd, dan kan deze ondernemer het risico van het optreden van ongewenste, kwaadaardige software verminderen door te migreren naar een besturingssysteem wat bijvoorbeeld gebaseerd is op Unix. Microsoft Windows is de defacto standaard, het gevolg hiervan is dat de schrijvers van ongewenste, kwaadaardige software zich in de meeste gevallen richten op dit besturingssysteem en niet op Unix-gebaseerde platformen.

Per maatregel moet het effect geschat worden op de bedreigingen, de gevolgen en de impact. Per maatregel wordt de complete analyse, zoals geïllustreerd in paragraaf 4.4, opnieuw uitgevoerd. Nu wordt bij de beoordeling van de verschillende effecten rekening gehouden met het verwachte effect van implementatie van de betreffende maatregel.

In dit voorbeeld heeft de eerste maatregel, speciale software ter voorkoming van optreden ongewenste, kwaadaardige software, alleen effect op de kwetsbaarheid. De berekening van de bedreigingsindex is in het voorbeeld beperkt tot de dreiging van computervirussen, vandaar dat hier volstaan wordt met het illustreren van het effect van een implementatie van een virusscanner op de kwetsbaarheid van de webwinkel:

Tabel 7, effect implementatie virusscanner op gevolgen computervirussen

Bedreiging: 1. Computervirussen		
Gevolg	**Voor implementatie virusscanner**	**Na implementatie virusscanner**
1. Belangrijke data gaan verloren	$\beta_{1,1} = .5$	$\beta_{1,1} = .25$
2. Bestellingen worden niet op tijd geleverd	$\beta_{1,2} = .5$	$\beta_{1,2} = .25$
3. Klanten worden bestookt met virusmail	$\beta_{1,3} = .75$	$\beta_{1,3} = .25$
4. Systeem onbereikbaar	$\beta_{1,4} = .5$	$\beta_{1,4} = .25$
5. Vertrouwelijke informatie komt beschikbaar voor derden.	$\beta_{1,5} = 0$	$\beta_{1,5} = 0$

Na implementatie van een virusscanner is de bedreigingsindex voor de dreiging van computervirussen 0.514375, een vermindering van 0.66 indexpunten dus.

De tweede maatregel (migratie naar een ander besturingssysteem) heeft voor wat betreft de bedreiging van computervirussen alleen effect op de aanwezigheid van bedreigingen. Stel dat de maatregel inhoudt dat er gemigreerd wordt van een Windows platform naar een op Unix gebaseerd besturingssysteem: er zijn veel minder virussen in omloop voor het Unix platform dan voor Windows, dus de bedreigingskansen nemen af:

Tabel 8, effect migratie naar Unix-platform op aanwezigheid bedreigingen

Bedreiging	**Voor migratie naar Unix-platform**	**Na migratie naar Unix-platform**
1. Computer virussen	$\alpha_1 = 1$	$\alpha_1 = .5$
2. Netwerk wormen	$\alpha_2 = .5$	$\alpha_2 = .5$
3. Trojaanse paarden	$\alpha_3 = 1$	$\alpha_3 = .5$
4. Spyware	$\alpha_4 = 1$	$\alpha_4 = .5$
5. Logische bommen	$\alpha_5 = .5$	$\alpha_5 = .5$

Opnieuw blijft de analyse beperkt tot de bedreigingsindex voor wat betreft de bedreiging van computervirussen: na implementatie van deze maatregel gaat de bedreigingsindex van 1.174375 naar 0.5871875, een halvering dus, met een afname van 0.5871875 indexpunten.

De maatregel die de bedreigingsindex het meest omlaag brengt, is de meest effectieve: $\delta_1 = 0.66$, $\delta_2 = 0.5871875$. Implementatie van een virusscanner is dus effectiever dan migratie naar een Unix-gebaseerd platform.

Stel dat de migratie naar dit op Unix gebaseerde besturingssysteem vier keer zo veel kost dan implementatie en onderhoud van virusscanners: $p_1 = .2$, $p_2 = .8$. Nu kan de doelmatigheid van beide maatregelen uitgerekend worden:

$$\varepsilon_1 = 0.66(1-.2) = 0.528$$
$$\varepsilon_2 = 0.5871875(1-.8) = 0.1174375.$$

Hieruit kan geconcludeerd worden dat, in deze casestudie, voor wat betreft de bedreiging door virussen, de implementatie van virusscanners doelmatiger is dan migratie naar een ander besturingssysteem.

Er moet wel bedacht worden dat hier maar een klein gedeelte van het systeem in ogenschouw genomen wordt: de analyse van kwaadaardige software is de case hier alleen uitgewerkt voor de bedreiging van computervirussen. Als ook de andere types kwaadaardige software meegenomen worden in de analyse, kan de doelmatigheidsanalyse heel anders uitpakken.

De werking van de relatieve indexeringsmethode is geïllustreerd in deze case. Bij toepassing in de praktijk levert de uitvoering van deze methode veel rekenwerk op: voor elke maatregel moet het effect op de bedreigingsindex worden uitgerekend. Ook het in kaart brengen van alle relevante bedreigingen, incidenten en kwetsbaarheden is geen sinecure. Deze manier van analyseren verschaft wel een nauwkeurig inzicht in de knelpunten in de beveiliging van het systeem. Verder garandeert een nauwkeurige uitvoering van de methode de totstandkoming van een rangschikking van beveiligingsmaatregelen naar doelmatigheid. Als er beveiligingsmaatregelen genomen moeten worden, verdienen de meest doelmatige maatregelen de voorkeur.

5. Discussie

De relatieve indexeringsmethode is bruikbaar op een operationeel niveau zonder dat er onrealistische veronderstellingen aan de methode ten grondslag liggen. Uitvoering van de methode stelt echter hoge eisen aan de managers: een goede werking van de methode staat of valt met de correcte inschatting van een breed scala aan factoren. Verder is de toepassing van de methode erg arbeidsintensief: voor elke relevante bedreiging moeten alle mogelijke incidenten in kaart gebracht worden. Deze incidenten worden uiteindelijk vertaald naar financiële consequenties. Ook moet per maatregel gekeken worden wat het effect ervan is op de bedreigingsindex.

Door het relatief hoge black-box gehalte is de relatieve indexeringsmethode moeilijk uit te leggen aan managers. Door, eventueel aan de hand van een voorbeeld, de methode stap voor stap te doorlopen kan de praktische bruikbaarheid duidelijk gemaakt worden.

6. Conclusie

In de literatuur zijn er verschillende modellen ontworpen die theoretisch inzicht verschaffen in de problematiek van informatiebeveiliging, vaak liggen er echter aan deze modellen onrealistische veronderstellingen ten grondslag. Zo worden bijvoorbeeld factoren constant verondersteld terwijl beïnvloeding in de praktijk wel degelijk mogelijk is. Modellen die de werkelijkheid beter benaderen hebben vaak een hoog niveau van abstractie zodat ze niet direct toepasbaar zijn in de praktijk. De relatieve indexeringsmethode komt tegemoet aan deze kritiek en biedt een praktische methode waaraan geen onrealistische veronderstellingen ten grondslag liggen. De methode brengt niet alleen in kaart hoe groot de relatieve financiële consequenties zijn van verschillende bedreigingen, maar is ook in staat om beveiligingsmaatregelen te ordenen naar effectiviteit en doelmatigheid. De methode biedt managers een krachtig stuk gereedschap in de economische analyse van investeringen in informatiebeveiliging.

7. Aanbevelingen

In de praktijk blijkt dat het inschatten van risico's erg moeilijk is. Om eindeloze discussies te voorkomen, kan het model uitgebreid worden met meetbare criteria. Aan de hand van een aantal indicatoren kan dan een risicoprofiel vastgesteld worden op basis van beschikbare gegevens over bedreigingskansen en impact daarvan.

De relatieve indexeringsmethode zou in een vervolgonderzoek aangepast kunnen worden naar een ratio indexeringsmethode waarbij bedreigingsindices van verschillende analyseobjecten en van verschillende ondernemingen onderling vergeleken kunnen worden. Dit zou mogelijkheden scheppen tot het stellen van normen aan bedreigingsindices, zodat een bepaalde mate van informatiebeveiliging gegarandeerd kan worden. De methode zou dan ook bruikbaar zijn in situaties waarbij niet volstaan kan worden met een prioritering van maatregelen.

Binnen de impactanalyse van de relatieve indexeringsmethode wordt er nu gewerkt met de drie verschillende soorten impact zoals Cisco die onderscheidt in [5]. Een meer geavanceerde uitwerking van de verschillende soorten impact maakt het model complexer, maar kan ook resulteren in een analyse die nauwkeuriger is en meer recht doet aan de praktijk.

Gebruik van de beslistheorie op basis van vage verzamelingen (fuzzy sets) zou de kracht van de methode kunnen vergroten. Bedreigingsindices komen dan tot stand op basis van lidmaatschapsfuncties waarin de verschillende bedreigingen tot uitdrukking komen.

Omdat er dagelijks nieuwe bedreigingen de kop opsteken, is de analyse van informatiebeveiliging geen statisch gegeven, maar een dynamisch proces. Het is daarom erg belangrijk dat er methodes voorhanden zijn die managers helpen bij het snel en adequaat uitvoeren van deze analyse. Daarom verdient het aanbeveling om een praktisch bruikbare methode te vertalen naar een computerprogramma. Beveiligingsmanagers kunnen dit programma dan configureren, zodat het afgestemd wordt op het specifieke te beveiligen informatiesysteem. Door herzieningen binnen het informatiesysteem door te voeren in het programma, kan steeds een actueel beeld geschetst worden van het bedreigingsniveau. Een dergelijk programma zou over een centrale database met actieve bedreigingen kunnen beschikken, zodat deze informatie direct gebuikt kan worden in het programma. Als het programma ook in staat is om de kosten en baten van beveiligingsmaatregelen te analyseren, dan kan dit ervoor zorgen dat het proces van doelmatig investeren in informatiebeveiliging minder arbeidsintensief wordt.

Referenties

[1] Anderson, R.J. 2001. Why Information Security is Hard -- An Economic Perspective. *Proceedings of the 17th Annual Computer Security Applications Conference*, 358-366.

[2] BS 7799. 1999. Information security management.
Part 1: Code of practice for information security management.
Part 2: Specification for information security management systems.

[3] Butler, S.A. Fischbeck, P. 2001. Multi-Attribute Risk Assessment. *Technical Report CMU-CS-01-169.*

[4] Cavusoglu, H. Mishra, B. Raghunathan, S. 2004.
A Model for Evaluating IT Security Investments.
Communications of the ACM, Vol. 47, No. 7, 87-92.

[5] Cisco Systems Inc. 2001. The Return on Investment for Network Security. White Paper.

[6] Gordon, L.A. Loeb, M.P. 2002. The Economics of Information Security Investment. *ACM Transactions on Information and System Security*, Vol. 5, No. 4, 438-457.

[7] Lambrinoudakisa, C. Gritzalisa, S. Hatzopoulosb, P. Yannacopoulosb, A.N. Katsikasa, S. A formal model for pricing information systems insurance contracts. *Computer Standards & Interfaces*, proefdruk, toegankelijk via ScienceDirect.

[8] Larochelle, D. Rosasco, N. 2003. Towards a Model of the Costs of Security. *Technical Report CS-2003-13*.

[9] Tanaka, H. Matsuura, K. Sudoh, O. 2005. Vulnerability and information security investment: An empirical analysis of e-local government in Japan. *Journal of Accounting and Public Policy*, No. 24, 37–59.

[10] Tsiakis, T. Stephanides, G. 2005. The economic approach of information security. *Computers & Security*, No. 24, 105-108.