Van dreiginganalyse naar beveiligingsplan

Een strategische aanpak voor security professionals

Berndt Rif MSc CPP

ISBN: 9789081604314 / NUR 800

Vormgeving & omslagontwerp: Security Press BV
Opmaak en eindredactie: Security Press BV
Drukwerk: Thieme Almere

1e druk: oktober 2010

Deze titel maakt deel uit van de Boekenreeks van het vaktijdschrift BEVEILIGING. Meer informatie over deze reeks en het maandblad is te verkrijgen via Security Press BV, www.securitypress.nl en www.beveiliging.nl.

© Copyright 2010 Security Press BV

Alle rechten voorbehouden. Alle auteursrechten en databankrechten ten aanzien van deze publicatie worden uitdrukkelijk voorbehouden. De rechten berusten bij Security Press BV. Behoudens de in of krachtens de Auteurswet gestelde uitzonderingen, mag niets uit deze uitgave worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand of openbaar gemaakt in enige vorm of op enige andere wijze, zonder voorafgaande schriftelijke toestemming van Security Press BV. Voorzover het maken van reprografische verveelvoudigingen uit deze uitgave is toegestaan op grond van de Auteurswet, dient men de daarvoor wettelijk verschuldigde vergoedingen te voldoen aan de Stichting Reprorecht (www.reprorecht.nl). Voor het overnemen van (een gedeelte van) deze uitgave voor commerciële doeleinden dient u zich te wenden tot Security Press BV (www.securitypress.nl). Hoewel aan de totstandkoming van deze publicatie de grootst mogelijke zorg is besteed, kan voor de aanwezigheid van eventuele (druk)fouten of onvolledigheden niet worden ingestaan en aanvaarden de auteur, eindredactie en uitgever geen aansprakelijkheid voor de gevolgen van eventueel voorkomende fouten en onvolledigheden.

Inhoud

Inleiding 7

Bedreigingen



De security manager als geweten van de organisatie 8
De security manager als inlichtingenmakelaar 14
De security manager als business intelligence professional 21
De security manager als wereldburger 27

Risicoanalyse



Bepalen van te beschermen bedrijfsbelangen 33
De bedreigingen van het organisatiebelang in kaart gebracht 37
De weerstand van de organisatie tegen vastgestelde dreigingen 44
Risicoanalyse: samenhang tussen belang, dreiging en weerstand 51

Beveiligingsplan



De inrichting van het proces security management 57
Organisatorische beveiligingsmaatregelen 61
Bouwkundige beveiligingsmaatregelen 66
Elektronische beveiligingsmaatregelen 71
IT-beveiligingsmaatregelen 77
Personele beveiligingsmaatregelen 81
Opzet van de beveiligingsorganisatie 86
Red teaming 92



Inleiding

Waarom vertonen mensen crimineel gedrag? Hoe en wanneer manifesteert dit zich? Welke dreigingen vormen de diverse soorten crimineel gedrag voor een organisatie? En hoe is te voorkomen dat deze dreigingen ontaarden in onaanvaardbare indidenten?
Het zijn vragen die de kern vormen van het boeiende vakgebied van de security manager. De antwoorden erop zijn echter van veel verschillende factoren afhankelijk en kunnen daarom door dit boek niet gegeven worden. Wel geven de hoofdstukken successievelijk richting aan het denkproces, dat de security manager helpt om met de kennis die hij van zijn organisatie heeft, de diverse beveiligingsvraagstukken op een structuele, constructieve en bovenal professionele manier op te lossen. Bovendien komt een aantal niet voor de hand liggende dreigingen aan de orde, die op het moment wellicht nog niet spelen, maar die in de dreiging- en risicoanalyses van een moderne organisatie niet mogen ontbreken. Denk aan economische spionage en terrorisme.
De aanpak van die risicoanalyse vormt het tweede deel van het boek. Dat begint met een beschrijving van het belang van risico's binnen een organisatie, redenerend vanuit doelstellingen als continuïteit en rendement. Vervolgens wordt gekeken naar hoe de security manager voor het opstellen van een risico-analyse aan input vanuit zijn organisatie komt en hoe zijn organisatie omgaat met de conclusies die vervolgens uit die analyse naar voren komen. Wat zou de organisatie zoal kunnen overkomen, wat zijn daarvan de gevolgen en wie zou daarbij belang kunnen hebben? In hoeverre is de organisatie tegen dreigende invloeden bestand? Waar zitten de kwetsbaarheden en met welke maatregelen zijn die kwetsbaarheden op evenwichtige wijze zodanig aan te pakken, dat de continuïteit van de organisatie op een aanvaardbaar niveau geborgd wordt? Voor de antwoorden op die vragen geven de hoofdstukken van het derde deel van dit boek de richting aan. Bekende en conventionele maatregelen worden beschreven, maar ook minder bekende, zoals beleid tegen de risico's van *social* en *human engineering* en de inzet van zogenoemde *red teams*. In alle gevallen wordt vanuit het centrale proces en de belangen van de organisatie geredeneerd en komen zowel de mogelijkheden als de onmogelijkheden van de verschillende maatregelen aan bod. Voor beginnende security managers en managers die security 'erbij' gaan doen, vormt dit boek een heldere en inspirerende introductie in het vakgebied. Ervaren security managers zal het helpen bij het vergroten van de structuur in de bestaande aanpak en het verder professionaliseren daarvan. Waar 'hij' en 'zijn' staat, mag natuurlijk ook 'zij' en 'haar' worden gelezen!

De security manager als geweten van de organisatie

De wetenschappelijke literatuur kan, als het onderwerp criminaliteit ter sprake wordt gebracht, worden samengevat in drie essentiële hoofdvragen. 'Waarom, wanneer en hoe' doet het verschijnsel van crimineel gedrag zich voor? Laten we eerst vanuit een sociologische invalshoek kijken naar de achtergrond van de vraag 'waarom' mensen crimineel gedrag vertonen. Wat maakt dat mensen op een gegeven moment de gestelde norm overtreden? En wat is die norm precies?

Crimineel gedrag is, als wij de definitie uit het boek 'Actuele Criminologie' van professor J.J.M van Dijk als uitgangspunt nemen, het menselijke gedrag dat door de wetgever strafbaar is gesteld.
Wat kan, en misschien wel moet, de hedendaagse security manager in zijn dagelijkse werk doen met de inzichten en de theorieën die afkomstig zijn uit de sociologie? Om een antwoord te geven op deze vraag dient te worden gekeken naar de invloed van sociale veranderingen op het gedrag van mensen, de gevolgen van relatieve deprivatie op het gedrag van mensen en de perceptie bij mensen dat het ontbreekt aan sociale gerechtigheid. Ook moet worden gekeken naar wat dit in de toekomst betekent voor de security manager. Misschien moet de security manager wel als geweten van de organisatie worden gezien? Immers, de security manager zou als geen ander de bedreigingen in kaart moeten kunnen brengen die het management van de organisatie zelf mede veroorzaakt.

Gevolgen sociale veranderingen

In de loop van de geschiedenis zijn mensen, als gevolg van arbeidsdeling en specialisatie, over steeds grotere afstanden van elkaar afhankelijk geworden. Het gevolg van deze ontwikkeling van arbeidsdeling en specialisatie is dat er steeds grotere 'interdependentie netwerken' zijn ontstaan waarbinnen mensen op elkaar zijn aangewezen zonder dat zij elkaar nog kennen. Het gevolg is dat mensen zijn zich steeds meer ondergeschikt zijn gaan voelen aan anonieme, onpersoonlijke en veelal ook onvoorspelbare instellingen. Ook binnen de eigen organisatie is de mens vaak niet meer dan een klein radertje geworden in een groter, vaak niet meer te overzien,



uurwerk. Dat dit verschijnsel makkelijk spanning en frustratie tot gevolg kan hebben, zeker als mensen het gevoel hebben niet meer serieus te worden genomen, is niet verwonderlijk.
Voor de hedendaagse security manager is het steeds belangrijker geworden de gevolgen van deze vergaande arbeidsdeling, specialisatie en toenemende anonimiteit van mensen ten opzichte van de maatschappij in het oog te houden. Dit maatschappelijke verschijnsel, waar sociologen voortdurend over praten, doet zich namelijk ook op kleine schaal voor binnen organisaties en bedrijven. Hoe groter en internationaler de organisatie of het bedrijf is, hoe groter ook vaak het probleem van de anonimiteit. Met name de cultuur en structuur van een organisatie of bedrijf, die anonimiteit en onbetrokkenheid van mensen bij het werk tot gevolg kunnen hebben, zijn essentieel voor het bepalen van de risico's als het gaat om de kans om slachtoffer te worden van crimineel gedrag.

Gevolgen relatieve deprivatie

Het begrip relatieve deprivatie ontstaat op het moment dat mensen de condities waarin zij leven en werken ter discussie stellen; benoemen waar zij in hun eigen ogen eigenlijk recht op zouden moeten hebben, en vervolgens zien wat het verschil is tussen wat zij zouden moeten hebben en wat zij daadwerkelijk hebben. Bij relatieve deprivatie gaat het dus niet om achterstand in absolute zin, maar om relatief en subjectief beleefde achterstand. Wie kent niet de voorbeelden van de topmanagers die, afgaand op het oordeel van de gemiddelde werknemer, bezig zijn met 'zakkenvullen'. Goede bonusregelingen en mooie lease-auto's, terwijl de gemiddelde medewerker moet vrezen om het behoud van zijn baan. Bovendien heeft deze medewerker het gevoel er aan het einde van het jaar zelf financieel op achteruit te zijn gegaan.
Onderzoek heeft laten zien dat hoe groter het verschil is tussen de verwachtingen die mensen nastreven en de daadwerkelijke situatie waarin men verkeert, des de groter de kans is dat mensen crimineel gedrag gaan vertonen. Mensen zullen dan proberen de realiteit in overeenstemming



te brengen met de eigen verwachtingen. Het gevoel om achtergesteld te zijn en niet aan eigen gestelde verwachtingen te kunnen voldoen, kan in eerste instantie tot 'afwijkend gedrag' leiden. Daar waar het gevoel van het achtergesteld zijn samengaat met zwakke bindingen met de organisatie of het bedrijf, bestaat gevaar van crimineel gedrag.

Motieven

Voor de security manager is het begrip van relatieve deprivatie goed bruikbaar bij het in kaart brengen van de motieven van mensen om crimineel gedrag te vertonen. Kennis van de ontwikkelingen in de maatschappij, en de veranderingen in de eigen organisatie, kunnen door de security manager worden gebruikt als input bij het bepalen van het risico om slachtoffer te worden van crimineel gedrag. Zowel van het eigen personeel, alsook van klanten, leveranciers en bezoekers. Het onthouden van erkenning aan mensen en het afbrokkelen van draagvlak voor (top)managers, zijn in het verleden veelvuldig reden geweest voor mensen om zelf

het gelijk te halen door een aanval op de organisatie of het bedrijf. Frustratie kan gemakkelijk crimineel gedrag tot gevolg hebben als bij mensen het gevoel bestaat dat er geen sociale gerechtigheid is.
Ook daar waar er zich sociale problemen en spanningen voordoen in de directe externe omgeving van de organisatie is het vrijwel uitgesloten dat de organisatie daarvan zelf gevrijwaard blijft. Voor de security manager is het dan ook van belang zich goed te realiseren in welke sociale omgeving zijn organisatie is gevestigd, en welke problemen zich voordoen in die omgeving. De vestigingsplaats van een organisatie, en dan in het bijzonder de sociale omgeving in enge zin, is een belangrijk aspect waar in een risicoanalyse rekening mee moet worden gehouden. De security manager dient dan wel een degelijke informatiepositie te hebben opdat de benodigde informatie tot hem komt.

Ontbreken sociale gerechtigheid

Personeel dat zich tekort gedaan voelt, geen kans meer heeft op verdere promotie, zal zich sneller schuldig maken aan 'diefstal' op kleine schaal. Onderzoek uitgevoerd door de Association of Certified Fraud Examiners, heeft dit ook daadwerkelijk aangetoond. Elementen zoals positie, salaris, de tijd dat een persoon werkzaam is bij de organisatie, leeftijd, opleiding en eerdere criminele antecedenten blijken allemaal belangrijke indicatoren van mogelijk crimineel gedrag te zijn. Zeker als er bij werknemers een vervreemding ten opzichte van de eigen organisatie of bedrijf zichtbaar wordt. Immers, goed voorbeeld doet volgen. Is het de werknemer te verwijten als hij het gedrag van (top)managers, die vanuit zijn gezichtspunt slechts uit lijken te zijn op eigen gewin, gaat kopiëren? Vanuit het strafrecht gezien wel, maar vanuit de sociologie gezien is het niet verrassend. De werknemer neemt immers de geldende waarden en normen van het management over.
Voor de hedendaagse security manager is het van belang de gevolgen van de vergaande arbeidsdeling, stratificatie, specialisatie en de toenemende anonimiteit van mensen ten opzichte van de maatschappij en de eigen organisatie goed in het oog te houden. De security manager zal zich moeten realiseren dat die anonimiteit en onbetrokkenheid van mensen bij het werk zijn weerslag zal hebben op het noodzakelijke beveiligingsregime binnen de organisatie. De invloed van de perceptie bij de gemiddelde werknemer dat het ontbreekt aan sociale gerechtigheid komt namelijk veelal ook tot uitdrukking in het gedrag van die individuele werknemer. De security manager moet er rekening mee houden dat dit

niet altijd op een positieve manier zal gebeuren, zeker niet als 'frustratie' door uitblijven van erkenning de oorzaak is. Om maar te zwijgen over het verkeerde voorbeeld dat het management, in de ogen van de gemiddelde werknemer, soms lijkt af te geven.

Geweten

De theorie van relatieve deprivatie is voor security managers goed bruikbaar bij het in kaart brengen van motieven, van zowel personeel als ook klanten, om crimineel gedrag te vertonen. Kennis van de ontwikkelingen in de maatschappij, en veranderingen in de eigen organisatie, kunnen vervolgens worden gebruikt als input bij het bepalen van het risico om daadwerkelijk slachtoffer te worden van crimineel gedrag. Ook de structuur en cultuur van de organisatie, als het gaat om de beleving van 'sociale gerechtigheid' bij werknemers, zijn belangrijke indicatoren om de kans op crimineel gedrag in de organisatie in te schatten. Het probleem is alleen wel dat de toenemende criminaliteit niet zal worden opgelost zolang de oorzaken niet worden aangepakt. Hier zal de security manager mee moeten leren omgaan.
Het uitbesteden van werkzaamheden, die niet tot de zogenaamde corebusiness van de organisatie horen, rukt ook steeds verder op. In de ogen van de gemiddelde werknemer, die mogelijk de dupe wordt van deze ontwikkeling, wordt zijn jarenlange trouw aan de organisatie niet beloond. Als in de perceptie van de werknemer het uitbestedingstraject dient om meer winst te kunnen maken, heeft deze werknemer in zijn ogen een goed argument om zich tegen de eigen organisatie te gaan keren. Naar mijn mening is het de taak van de security manager om het management voor deze mogelijke bijwerkingen van uitbesteden te waarschuwen.

Goed voorbeeld

Ook als het gaat om het aanpakken van criminaliteit binnen de organisatie moet de security manager zich bewust zijn van het signaal dat het (top)management aan werknemers afgeeft. Is er vanuit het gezichtspunt van de werknemer sprake van 'goed voorbeeld doet volgen'? Zo ja, dan zullen repressie en het op zijn tijd op staande voet ontslaan van een medewerker die de (strafrechtelijke) norm heeft overtreden, niet de oplossing zijn. Er zal dan, wil de organisatie het probleem echt aanpakken, moeten worden gekeken naar de cultuur binnen de eigen organisatie. Ook hier ligt, vanuit beveiligingsoogpunt gezien, een taak voor de security manager om het onderwerp op de agenda te zetten.

De security manager zal, wil hij deze uitdaging kunnen aangaan, wel eerst een serieuze gesprekspartner moeten worden in de 'boardroom'. Een roepende binnen het facilitaire bedrijf, die eerst zijn eigen facilitair directeur moet overtuigen, zal vrijwel nooit in de boardroom opvallen. Bovendien zal de security manager ook een goede informatiepositie moeten hebben binnen de eigen organisatie. Immers, hij dient te weten wat de motieven van de personeelsleden zijn om de norm binnen de eigen organisatie te overtreden. Pas als de security manager trends kan verklaren en een relatie weet te leggen tussen criminaliteit en de cultuur van de organisatie, kunnen problemen echt worden aangepakt. In de boardroom wil men onderbouwde verklaringen horen, geen gissingen of verwachtingen.
De andere optie is, zeker als het niet lukt om de boardroom te bereiken, het blijven blussen van brandjes en het reactief blijven reageren op incidenten. Ook leuk, maar op de lange termijn zet het geen zoden aan de dijk. Belangrijk is wel om vast te stellen dat het feit dat de security manager geen gesprekspartner is voor het (top)management, niet altijd ligt aan de security manager. Soms kiest het management bewust voor het buiten de deur houden van deze professional. Immers: wat niet weet, wat niet deert. Daar waar beveiliging al is uitbesteedt, en een organisatie ook geen eigen security manager meer in dienst heeft, zit er waarschijnlijk niets anders op dat de situatie accepteren. In dat geval is namelijk het geweten van de organisatie, en veelal de kennis die men had van de problemen in de eigen organisatie, al met het badwater weggegooid.

Literatuur

ACFE (2004) *Report to the Nation on Occupational Fraud and Abuse*, Austin: Association of Certified Fraud Examiners.
Bovenkerk, F. (2001) *Misdaadprofielen*, Amsterdam : Meulenhoff.
Broder, J.F. (2000) *Risk Analysis and the Security Survey*, Boston: Butterworth-Heinemann / member of the Reed Elsevier Group.
Claes, P.F. en Meerman, H.J.J.M. (1998) *Riskmanagement; inleiding tot het risicobeheersingsproces*, Houten: Stenfert Kroese.
Dijk, J.J.M. van, Sagel-Grande, H.I. en Toornvliet, L.G. (2002) *Actuele Criminologie*, Den Haag: SDU Uitgevers.
Otten, M.H.P., Boin, A. and Torre, J. van der (2001) *Dynamics of Disorder: lessons from two Dutch riots*, Leiden: Crisis Research Center Leiden University.
Sztompka, P. (1993) *The Sociology of Social Change*, Oxford : Blackwell.
Wilterdink, N. en Heerikhuizen, B. van (1993) *Samenlevingen; Een verkenning van het terrein van de sociologie*, Groningen: Wolters-Noordhoff.

De security manager als inlichtingenmakelaar

Naast het beantwoorden van de vraag waarom mensen crimineel gedrag vertonen, is het voor de security manager misschien nog wel belangrijker om een antwoord te vinden op de vraag wanneer mensen dit gedrag gaan vertonen. Hierbij kunnen verschillende theorieën behulpzaam zijn.

De bekende Belgische strafpleiter en criminoloog Jef Vermassen (auteur van onder meer het boek 'Moordenaars en hun motieven') heeft ooit gezegd dat criminelen en destructieve personen schuilgaan achter een masker van vriendelijkheid en hoffelijkheid. Daarnaast vertonen zij volgens hem een voorliefde voor kinderen en dieren. Ook hebben mensen die iets te verbergen hebben de mond vol van idealen en goede bedoelingen. Wie gelooft dat een slecht mens hoorns en bokkenpoten heeft zal, volgens Vermassen, nooit een slecht mens ontdekken. In het verlengde van deze uitspraak zei Pieter Baan in het verleden al eens: "misschien bestaat de echte beroepsmisdadiger inderdaad, doch ik vrees dat hij onder de 95 procent van de mensheid te vinden is en niet bij het handjevol delinquenten dat steeds maar weer in de gevangenis verdwijnt". Wat betekenen deze uitspraken nu voor de hedendaagse security manager die in de dagelijkse praktijk heeft te maken met de 95 procent van Pieter Baan? Naast het beantwoorden van de vraag waarom mensen crimineel gedrag vertonen is het voor de security manager misschien nog wel belangrijker om een antwoord te vinden op de vraag wanneer mensen dit gedrag gaan vertonen.

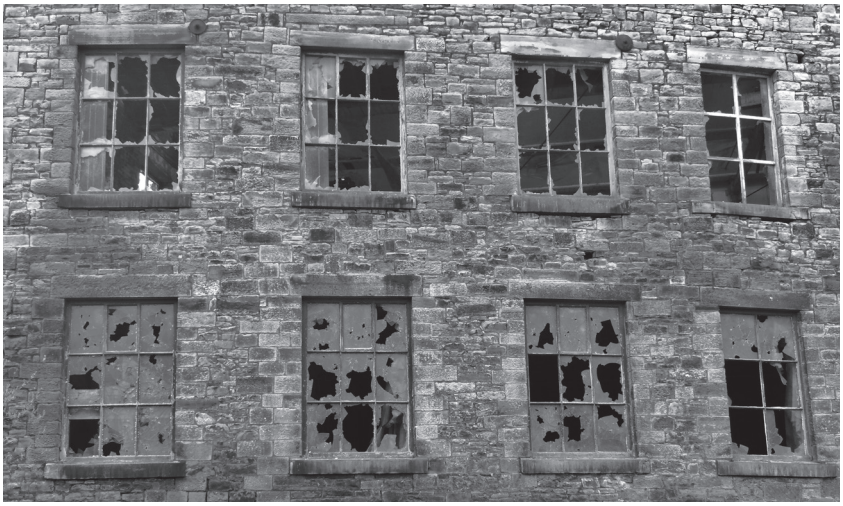
Normen, waarden en cultuur

Om het menselijke gedrag beter te kunnen begrijpen wordt vanuit verschillende invalshoeken gekeken naar de drie aspecten die mede bepalen wanneer iemand crimineel gedrag gaat vertonen: gelegenheid, druk en rationalisatie. Het is voor de security manager belangrijk, wil hij criminaliteit in enge zin kunnen bestrijden, om inzicht te hebben in de 'anomietheorie' van Merton, de 'broken-windows-theorie' van Wilson en Kelling en het 'flitspuntmodel' van Waddington.
Volgens bepaalde wetenschappers is een van de belangrijkste factoren

die bepaalt of een kind in zijn latere leven crimineel verdrag gaat vertonen het feit of de vader van het kind crimineel gedrag vertoont. De theorie die dit uitgangspunt verder uitwerkt en ingaat op het ontstaan en het voortbestaan van crimineel gedrag, gaat uit van een wisselwerking tussen omgeving en persoon. Aanhangers betogen dat noch erfelijke en biologische factoren, noch omgevingsfactoren als armoede, werkloosheid of een gebrekkige opvoeding, afzonderlijk criminaliteit kunnen veroorzaken. Het zijn juist de verschillende combinaties van deze aanwezige factoren die kunnen leiden tot verschillende soorten van criminaliteit. Mensen worden in een specifieke cultuur geboren en er door gevormd. Het gevolg is dat de verschillende groepen die in de maatschappij naast elkaar leven ook allemaal hun eigen specifieke cultuur hebben. In bedrijven en instellingen komen deze mensen, die allemaal hun eigen achtergrond meenemen, samen. Om nu een antwoord te kunnen geven op de vraag wanneer mensen crimineel gedrag gaan vertonen is het belangrijk om te kijken naar hoe de verschillende cultuurpatronen met elkaar interacteren. Voor de security manager betekent dit dat de cultuur binnen de eigen organisatie en de aanwezige subculturen een belangrijke risicoindicator zijn bij het beoordelen van de kans op crimineel gedrag. Hij zal al deze (sub)culturen en de verschillende uitingsvormen hiervan moeten herkennen, wil hij effectieve beveiligingsmaatregelen kunnen treffen.

Anomietheorie

Het begrip anomie is afkomstig van de Franse socioloog Emile Durkheim. Die stelde dat snelle en ingrijpende sociale veranderingen grote invloed hebben op allerlei groepen in de samenleving. Belangrijke waarden en normen, die tot dan toe werden geaccepteerd, vervagen of verdwijnen. Het gevolg is dat mensen zich gaan inzetten voor nieuwe doelen die strijdig met elkaar zijn, dat individuen zich onzeker gaan voelen en dat er collectief gezien een zekere normonzekerheid en zelfs normloosheid (anomie) ontstaat.
De socioloog Robert Merton, die de theorieën van Durkheim verder heeft uitgewerkt, geeft aan dat wanneer de maatschappelijke doelen en de geaccepteerde, of beste methode om deze doelen te bereiken, niet samengaan met de middelen om de doelen te bereiken, er anomie ontstaat. Volgens Merton vinden mensen die geen toegang hebben tot de maatschappelijk geaccepteerde middelen om het door hun zelf gestelde doel te bereiken, altijd wel een manier om met de spanning die dit veroorzaakt om te gaan.



Als individuen zich aanpassen door het verwerpen van de doelen en de middelen, of de doelen accepteren maar niet de middelen, wordt het gedrag dat zij vertonen bestempeld als afwijkend. Veelal is dit wat wij crimineel gedrag noemen. Volgens Merton zijn er vijf aanpassingsstrategieën die mensen kunnen gebruiken op het moment dat ze het idee van de sociale doelen geïnternaliseerd hebben, maar niet in een positie verkeren om deze op legitieme wijze te bereiken. De vijf strategieën zijn conformiteit, vernieuwing, ritualisme, terugtrekgedrag en rebellie of verzet.

Inzicht

Voor de security manager is met name de strategie van de rebellie of verzet interessant, omdat mensen zich dan actief gaan verzetten tegen de situatie waarin zij verkeren. Dit verzet kan crimineel gedrag tot gevolg hebben. Om een indicatie te hebben wanneer crimineel gedrag zich kan gaan voordoen zal de security manager inzicht moeten hebben in de verwachtingspatronen en spanningen die zich voordoen in het eigen bedrijf. Ook de spanningen in de omgeving van het bedrijf kunnen niet buiten beschouwing worden gelaten. Wassenaar als vestigingsplaats levert een ander plaatje op dan de Bijlmer. Dit betekent dat, om een goede risicoanalyse te kunnen maken, de security manager informatie moet verzamelen om de dreiging ten opzichte van het eigen bedrijf te kunnen bepalen. Alleen als de security manager adequate inlichtingen tot zijn beschikking

heeft kan hij, met de anomietheorie van Merton als uitgangspunt, een deel van de 'wanneer'-vraag beantwoorden.

Broken windows-theorie

De Amerikaanse criminologen James Wilson en George Kelling zijn bekend geworden vanwege hun onderzoek naar de sociale processen die als oorzaak kunnen worden aangewezen voor de achteruitgang van buurten en het feit dat buurten daarmee kwetsbaar worden voor criminaliteit. De stelling van Wilson en Kelling is dat verloedering en overlast op den duur ernstige vormen van criminaliteit tot gevolg zal hebben. Om het afglijden van buurten tegen te gaan dient, volgens Wilson en Kelling, allereerst de verloedering en de overlast krachtig te worden aangepakt. Naast deze eerste stap, die veelal 'zero-tolerance' benadering wordt genoemd, is uiteindelijk stap twee doorslaggevend: 'het herstel van de informele sociale controle'.
Wetenschappers hebben in het verleden al aangegeven dat, voor de gemiddelde crimineel, de beslissing om een strafbaar feit te begaan een rationeel afwegingsproces is. De daders zijn zich bewust van de kosten van hun daad, het risico om daadwerkelijk te worden aangehouden, en de verwachte opbrengst. Er zal echter altijd een gelegenheidsstructuur voor criminaliteit moeten zijn voordat er sprake kan zijn van crimineel gedrag. Voor de wetenschappers van de zogenaamde 'Chicago School' is criminaliteit een consequentie van een afname van sociale controle, die een verhoging van criminaliteit tot gevolg kan hebben.
De broken-window theorie, en inzichten van wetenschappers die zich hebben beziggehouden met vergelijkbare onderwerpen, suggereren dat een fysieke en economische achteruitgang in bepaalde gebieden kan leiden tot de situatie dat die gebieden gevoelig worden voor de ontwikkeling van criminaliteit. Dit in combinatie met een afwijkende socialisatie van de mensen die in die bepaalde omgeving wonen betekent dat de ontwikkeling en uitbreiding van crimineel gedrag geen verrassing mag zijn.

Bruikbare indicatoren

Voor de security manager kan het inzicht in het principe van de 'gelegenheidstructuur' bruikbare indicatoren opleveren voor het bepalen van de kans op crimineel gedrag in de eigen organisatie. Een organisatiecultuur die tot gevolg heeft dat mensen elkaar niet aanspreken op het niet nakomen van afspraken is mogelijk een eerste indicatie van een gebroken raam. Een organisatie met een cultuur zonder duidelijke waarden en

normen, of een cultuur waar mensen liever de andere kant op kijken als er iets onacceptabels gebeurt, is de volgende stap. De ramen beginnen barsten te vertonen. De security manager zal, om effectieve beveiligingsmaatregelen te kunnen treffen, de cultuur van zijn organisatie door en door moeten kennen. Hij zal ook de verschillende (sub)culturen binnen zijn organisatie, en de daaraan verbonden risico's, moeten herkennen. De security manager zal over een goede inlichtingenpositie moeten beschikken. Heeft de security manager geen goede inlichtingenpositie en weet hij niet wat er binnen zijn eigen organisatie speelt, dan zal hij het antwoord op de 'wanneer'-vraag moeilijk kunnen geven.

Flitspuntmodel

Als mensen zich onderdrukt voelen en geen uitweg meer zien voor hun problemen, dan is het brandbaar materiaal volgens David Waddington aanwezig. Het is dan slechts nog een kwestie van tijd voordat een vonk er voor zorgt dat mensen iets gaan doen met die onderliggende gevoelens van ontevredenheid. Volgens Waddington is de verklaring van crimineel gedrag zelden te herleiden naar één enkele factor. Om te begrijpen waarom een 'vonk' een 'vuur' tot gevolg kan hebben moeten we volgens hem het principe van 'ontbranding' bestuderen. Het is dan niet de aanwezigheid of afwezigheid van bepaalde elementen die een mens crimineel maakt, maar het is de interactie van de verschillende elementen die maakt of een mens zich crimineel gedraagt.

Niveaus

Het door Waddington ontwikkelde 'flitspuntmodel' combineert het zogenaamde brandbare materiaal met het aspect van onderlinge interactie tussen mensen. Dit betekent dat Waddington rekening houdt met psychologische en sociologische invloeden. Het daadwerkelijke flitspunt wordt veelal voorafgegaan door een serie van kleinere incidenten. Hoewel Waddington zijn model heeft ontwikkeld voor de bestudering van verstoringen in de openbare orde, is het model zeer zeker bruikbaar voor de verklaring van de 'wanneer'-vraag als het gaat om crimineel gedrag. Waddington geeft aan dat er een probleem ontstaat op het moment dat achtergestelde groepen niet in staat zijn hun positie te verbeteren en geen vertrouwen meer hebben in de bestaande organisatie. Waddington heeft een aantal bepalende factoren van crimineel gedrag gevonden en die ondergebracht in verschillende 'niveaus' waarop analyse kan plaatsvinden. Het structurele niveau refereert aan conflicten die hun oorsprong



vinden in materiële en ideologische verschillen tussen sociale groepen. Het culturele niveau gaat in op de manier waarop groepen de maatschappij zien, en waarop zij hun eigen plaats in de maatschappij beoordelen. Tevens gaat hij op dit niveau in op de normen en waarden die het gedrag bepalen, en hoe die normen en waarden door de eigen sociale groep worden gewaardeerd. Volgens Waddington zijn etnische achtergronden, jongeren culturen, bezigheden en specifieke locaties allemaal bepalende factoren voor de manier waarop situaties worden beoordeeld. Het gevolg is dat deze factoren allemaal bijdragen aan het op dat moment, door het individu, vertoonde gedrag.
De andere niveaus van analyse kunnen criminaliteit verklaren en mogelijk maken, maar uiteindelijk kan de 'wanneer'-vraag volgens Waddington alleen worden verklaard op het niveau van de interactie. De security manager zal zich, wil hij de verschillende risico-indicatoren voor crimineel gedrag binnen zijn organisatie kunnen herkennen, rekenschap moeten geven van de bijdrage die het 'flitspuntmodel' kan leveren. In het flitspuntmodel komen de eerder aangehaalde anomietheorie en 'broken-windows' theorie samen. Het centrale thema waar de security manager bij de beantwoording van de 'wanneer'-vraag rekening mee moet houden is de heersende cultuur binnen en buiten de eigen organisatie. Alle eerder genoemde aspecten die bepalen 'wanneer' er een risico ontstaat tot crimineel gedrag - gelegenheid, druk en rationalisatie - vinden altijd hun oorsprong binnen de heersende culturele normen en waarden. En dan ook vooral in de wijze waarop wordt opgetreden tegen overtredingen.

Cultuur

De besproken theorieën kunnen de security manager helpen bij het beantwoorden van de vraag 'wanneer' crimineel gedrag voorkomt. Verklaringen van crimineel gedrag kunnen worden gebruikt bij het in kaart brengen van 'risicogroepen' binnen de eigen organisatie, of in de omgeving van de organisatie. De binnen de organisatie aanwezige cul-

tuur en subculturen zijn vervolgens een belangrijke risico-indicator bij het beoordelen van de kans op crimineel gedrag. Een succesfactor voor het bieden van weerstand tegen criminaliteit en het kunnen treffen van effectieve beveiligingsmaatregelen is nu juist het kennen en herkennen van de (sub)culturen en de verschillende uitingsvormen van deze (sub)culturen. Dit vraagt echter nogal wat van de hedendaagse security manager. Daar waar de security manager in het verleden nadacht over de inzet van fysieke en elektronische beveiligingsmaatregelen, moet nu ook worden nagedacht over 'cultuur' als beveiligingsmaatregel. De security manager zal dus ook socioloog en psycholoog moeten worden. Daarnaast zal hij, wil hij de bedrijfscultuur kunnen doorgronden, moeten weten wat voor gevoelens in de eigen organisatie spelen. De security manager zal dus actief inlichtingen moet gaan verwerven. Dat dit met de nodige waarborgen moet worden omkleed spreekt voor zich, want in Nederland zijn wij nog al huiverig, gezien onze geschiedenis, voor een al te grote voortvarendheid op dit vlak. De begrippen subsidiariteit, proportionaliteit en integriteit zijn dan de te hanteren kernwaarden. Kortom, alleen maar uitdagingen voor de hedendaagse security manager.

Literatuur

Bovenkerk, F. (2001) *Misdaadprofielen*, Amsterdam: Meulenhoff.
Dijk, J.J.M. van, Sagel-Grande, H.I. en Toornvliet, L.G. (2002) *Actuele Criminologie*, Den Haag: SDU Uitgevers.
Hall, S. and Jefferson, T. (eds) (1975) *Resistance through Rituals: Youth Subcultures in Post-war Britain*, London: Routledge.
Lissenberg, E., Ruller, S. van en Swaaningen, R. van (eds) (1999) *Tegen de regels: Een inleiding in de Criminologie*, Nijmegen: Ars Aequi Libri.
Morrison, K. (1995) Marx, Durkheim, Weber; *Formations of Modern Social Thought*, London: Sage Publications.
Raine, A. (1993) The Psychopathologie of Crime; *Criminal Behavior as a Clinical Disorder*, London: Academic Press.
Scarman Centre (1998/2000) *Module Crime, Order and Society*, Leicester: University Leicester, Scarman Centre.
Vermassen, J. (2004) *Moordenaars en hun motieven*, Amsterdam: Meulenhoff.
Waddington, D., Jones, K. en Critcher, C. (1989) *Flashpoints; Studies in public disorder*, London: Routledge.
Wilterdink, N. en Heerikhuizen, B. van (1993) *Samenlevingen; Een verkenning van het terrein van de sociologie*, Groningen: Wolters-Noordhoff.

De security manager als business intelligence professional

'Wat niet weet, wat niet deert', luidt een goed Nederlands spreekwoord. Dit lijkt ook te gelden voor het onderwerp economische spionage. Zelden wordt gesproken over dit onderwerp en de daaruit voortvloeiende schade. Toch is het moeilijk te geloven dat economische spionage in Nederland niet voorkomt. Het verhogen van het beveiligingsbewustzijn voor dit onderwerp is daarom op zijn plaats.

Pierre Marion, een voormalig topman van de Franse inlichtingendienst DGSE, maakte er in het verleden geen geheim van. Als het gaat om economische belangen zijn Frankrijk en de Verenigde Staten tegenstanders, geen bondgenoten. In een rapport uit 2002, van het Amerikaanse Defense Personnel Security Research Center, wordt Frankrijk nog steeds genoemd als één van de bondgenoten van de VS die zich schuldig maken aan economische spionage tegen dat land. Opmerkelijk is dat in dit rapport staat vermeld dat, naast landen zoals Rusland en China, ook Israël en het Verenigd Koninkrijk de afgelopen jaren geheime informatie via Amerikaanse staatsburgers hebben trachten te verwerven.

Schade

Echte vrienden, die je kunt vertrouwen, lijken niet meer te bestaan als het gaat om economische belangen. Een neveneffect van het proces van globalisering. De inkomsten die het Amerikaanse bedrijfsleven misloopt als gevolg van economische spionage lopen in de miljarden. Het bureau van de National Counterintelligence Executive geeft in haar jaarverslag van 2002 aan dat de schade voor het Amerikaanse bedrijfsleven, ten gevolge van economische (bedrijfs)spionage, jaarlijks zo'n 300 miljard dollar bedraagt. Als bron wordt een onderzoek van de American Society for Industrial Security (ASIS) genoemd.
In september 2005 meldde National Counterintelligence Executive Michelle van Cleave dat momenteel zeker honderd landen - waaronder enkele zeer bevriende naties - pogingen ondernemen om op een heimelijke manier geheime economische bedrijfsinformatie in de Verenigde Staten te verwerven. Het bureau van de National Counterintelligence Executive

is een soort Nationaal Coördinator Spionagebestrijding, een in Nederland (nog) onbekend fenomeen.
Prof.dr. Marc Cools en prof.dr. Bob Hoogenboom definiëren spionage als een stelsel van clandestiene pro-actieve handelingen door individuen, particuliere bedrijven en/of overheidsinstellingen, in dienst van de overheid, die zijn gericht op de vergaring van financieel economische informatie over buitenlandse bedrijven ten behoeve van politieke doelen. Met pro-actief bedoelen Cools en Hoogenboom dat gesloten bronnen worden aangeboord en operaties worden opgezet.
Nog in september 2002 geeft Qian Qichen, de vice-premier van China, in het Volksdagblad aan dat zijn land naast het vertrouwen dat het heeft in het werven van 'lokaal personeel' in andere landen, ook actief inlichtingenactiviteiten in het buitenland zal gaan ontplooien. Het doel van dit alles is, volgens Qian Qichen, het stimuleren van de verdere economische en sociale ontwikkeling van China. De uitspraak van de vice-premier lijkt de definitie van Cools en Hoogenboom te bevestigen. Maar het gaat tegenwoordig al verder. Ook een toenemend aantal multinationals ontplooit activiteiten op het vlak van wat met een mooi woord competitive intelligence heet. Tussen de 60 en 82 procent van de multinationals in de Verenigde Staten beschikt over aparte corporate intelligence units. Tot deze groep bedrijven behoren IBM, Procter & Gamble, Xerox en Motorola. De definitie van Cools en Hoogenboom moet daarom iets worden aangepast. Economische spionage is een stelsel van clandestiene pro-actieve handelingen door individuen, particuliere bedrijven en overheidsinstellingen, die zijn gericht op de vergaring van informatie over en van buitenlandse concurrenten, teneinde de eigen economische positie te verbeteren.
Gezien de plek die Nederlandse bedrijven en instellingen in het buitenland innemen en ook omdat Nederland een 'kennisland' is waar hoogwaardige technologie kan worden gehaald, lijkt economische spionage een reële dreiging voor de security manager om rekening mee te gaan houden. Kort gezegd, waarom zou je met veel moeite iets gaan ontwikkelen of gaan maken als je het gemakkelijk in Nederland kunt stelen?

Incidenten

Al in de jaren tachtig werden Japanse geheimagenten verdacht van samenwerking met Japanse multinationals om via clandestiene operaties hightech firma's in Sillicon Valley te bespioneren. Een ander specifiek voorbeeld zijn de twee ingenieurs van het Japanse elektronicaconcern



Hitachi die uit waren op de bedrijfsgeheimen van IBM. De ingenieurs kochten - zo dachten zij - een medewerker van IBM om ten einde geheime documenten in handen te krijgen. Zij kregen echter, na onderzoek door de FBI, een arrestatiebevel onder ogen. Uiteindelijk verschenen dertien medewerkers van Hitachi voor de rechter en moest het bedrijf 300 miljoen dollar genoegdoening aan IBM betalen.
In 1987 zijn vervolgens in de pers de eerste geluiden te horen over het feit dat de Franse inlichtingendienst DGSE een grootschalig offensief zou hebben ingezet tegen Europese vestigingen van onder andere IBM en Texas Instruments. De DGSE zou deze bedrijven hebben uitgekozen omdat zij een leidende positie hadden op het vlak van computer technologie. Met succes waren er zes medewerkers van IBM door de DGSE gerekruteerd om geclassificeerde informatie te verstrekken. Als wij de verhalen moeten geloven bleek het Franse staatsbedrijf Bull commerciële, technische en financiële gegevens in handen te hebben gekregen. Ook werden in die periode Amerikaanse zakenlieden gewaarschuwd om niet met Air France te vliegen nadat was ontdekt dat de Franse inlichtingendienst afluisterapparatuur had geplaatst en agenten als passagiers en stewards liet meevliegen.

Wetenschappers

Meer recent, in 2002, kwam aan het licht dat in Zweden drie medewerkers van het Telecombedrijf Ericsson waren gearresteerd op verdenking van spionage voor Rusland. Twee Russische diplomaten, actief als inlichtingenfunctionarissen, werden uitgewezen. In 2004 en 2005 zijn in verschillende landen, waaronder de Verenigde Staten en Frankrijk, Chinese studenten en wetenschappers betrapt op het vergaren van informatie. Zo werden bij een huiszoeking van een Chinese studente twee harde schijven aangetroffen met geheime gegevens van auto-ontwerpen.
Het dagblad Washington Post maakte op 12 december 2005 melding van het feit dat Kenneth Feld, directeur van onder andere het Ringling Circus en van Disney on Ice, een voormalig CIA-agent heeft ingehuurd om dierenrechtengroeperingen in de gaten te houden. Feld zou persoonlijk



toezicht houden op de 'spy-operation'. Op 18 januari 2006 werd op de website van 'sportsnetwork' melding gemaakt van het feit dat het spionage incident tussen Ferrari en Toyota aan het escaleren is. In een Duitse rechtbank werden de namen van drie hooggeplaatste (ex) medewerkers van Toyota genoemd. Zij werden beschuldigd van het gebruik van informatie die is gestolen van Ferrari.
De New York Times gaf in dezelfde periode aan dat Yahoo een strafzaak is begonnen tegen het bedrijf (M)FORMA uit San Fransisco. Zeven voormalige medewerkers van Yahoo, die een overstap naar (M)FORMA hebben gemaakt, werden ervan beschuldigd grote hoeveelheden vertrouwelijke informatie te hebben gekopieerd en meegenomen naar het nieuwe bedrijf. Uit een Brits onderzoek uit 2004, blijkt dat 70 procent van de ondervraagde medewerkers vertrouwelijke informatie van hun vorige werkgever heeft meegenomen naar de nieuwe baan. Toch makkelijk, al die USB-sticks.

Indicatoren

Als blijkt dat concurrenten, of mensen die zich voordoen als bijvoorbeeld journalist, informeren naar projecten of producten die niet publiekelijk bekend zijn, moeten alle alarmbellen gaan rinkelen. Ook als blijkt dat buitenstaanders beschikken over strategische (bedrijfs)informatie, of als in een aanbestedingsronde een bedrijf steeds een betere offerte weet uit te brengen waardoor opdrachten worden misgelopen, is argwaan op zijn plaats. Onderhandelingen over mogelijke samenwerkingsprojecten en grootschalige wervingscampagnes van concurrenten waar ook de medewerkers van het eigen bedrijf op solliciteren kunnen soms een

andere bedoeling hebben, namelijk het verkrijgen van informatie. Ook het meewerken aan externe surveys, of het aanknopen van contacten met collega-vakgenoten naar aanleiding van bijvoorbeeld een beurs of congresbezoek, kan leiden tot compromittering van vertrouwelijke informatie. Zeker als de tegenpartij, die natuurlijk erg vriendelijk overkomt, kwade bedoelingen heeft.
Dit roept de vraag op of de security manager al dit soort mogelijke incidenten krijgt gemeld. Weet de security manager waar de kwetsbare informatie in zijn bedrijf ligt, waarin de concurrenten van het bedrijf interesse hebben en welke mogelijkheden de concurrent heeft om aan deze informatie te komen?
Als de security manager al niet weet waar de 'kroonjuwelen' van de organisatie liggen, dan weten de medewerkers binnen het bedrijf waarschijnlijk ook niet dat zij voor kwaadwillenden een interessant doelwit zijn om te benaderen. En zeg nu niet dat het bedrijf geen interessante informatie heeft voor buitenstaanders. Als dat echt zo zou zijn, heeft het tenslotte geen bestaansrecht. Er zijn zelfs voorbeelden van een pizzabezorgdienst die bijna failliet ging omdat de concurrent de klantenlijsten in handen wist te krijgen.

Naïef

In Nederland houden wij ons in het algemeen redelijk aan de geldende waarden en normen. Dit maakt ons, ook omdat wij vergeleken met andere landen minder nationalistisch zijn, soms een beetje naïef. Wij kunnen ons namelijk moeilijk voorstellen dat 'concurrenten', zeker als deze uit het buitenland komen, zich niet aan de geldende Nederlandse waarden en normen houden. Niets is, ook gezien de eerder gegeven voorbeelden, minder waar. De wereld wordt kleiner, de belangen groter en de concurrentie harder. Zoals iemand eens zei, de beste manier om de tafelmanieren te veranderen is het verkleinen van het stukje taart dat op tafel staat.
De eerste en misschien wel de belangrijkste tegenmaatregel die de weerstand tegen economische spionage kan verhogen is het besef dat het bedrijf interessante informatie heeft waarin anderen zijn geïnteresseerd en waarvoor men bereid is de afgesproken spelregels even ter zijde te leggen. Dit onderwerp zal eerst bespreekbaar moeten worden gemaakt, en zeg nu eerlijk, wie heeft er op dit moment binnen zijn bedrijf een security awareness campagne waar medewerkers structureel over het onderwerp spionage worden voorgelicht? Toch is dit de eerste stap. Pas als de security manager het onderwerp op de agenda weet te krijgen, bestaat de

kans dat pogingen om heimelijk informatie uit het bedrijf te ontvreemden worden waargenomen.
Medewerkers, en (top)managers, die zich bewust zijn van het feit dat zij over waardevolle kennis bezitten, zullen eerder geneigd zijn mogelijke incidenten te melden. Alleen dan kan de security manager daadwerkelijk onderzoeken of er iets aan de hand is. Een voorwaarde is wel dat hij zijn bedrijf of instelling en de concurrenten daarvan door en door kent. Hij moet weten waar de waardevolle informatie ligt, welke bijzondere onderzoeksprojecten er gaande zijn, waarin 'de vijand' geïnteresseerd is en wat zijn capaciteiten zijn om de informatie te verwerven. Met andere woorden: de security manager als business intelligence professional.
Als de security manager daar de meerwaarde niet van inziet, zullen het (top)management en de medewerkers dat zeker niet doen. Met als gevolg een open huis waar de vertrouwelijke informatie voor het oprapen ligt. Als wij Kevin Mitnick moeten geloven, een van de bekendste (ex)hackers allertijden, hoeft de buitenstaander veelal alleen om vertrouwelijke informatie te vragen. Vaak is dit al genoeg om deze te krijgen, gezien het feit dat wij anderen graag helpen, zeker als zij betrouwbaar overkomen. Met bovenstaand in het achterhoofd, is dit dus niet wenselijk.

Literatuur

Cleave, M. van (2005) *Hearing on Sources and Methods of Foreign Nationals Engaged in Economic and Military Espionage*, Washington: National Counterintelligence Executive
Cools, M. en Hoogenboom, B. (1996) *Kwetsbare kennis; Over bedrijfsspionage en informatiebeveiliging*, Alphen aan den Rijn: Samsom Bedrijfsinformatie
Herbig, K.L. en Wiskoff, M.F. (2002) *Espionage against the United States by American Citizens 1947-2001*, Monterey: Defense Personnel Security Research Center
Mitnick, K.D. en Simon W.L. (2003) *De kunst van het misleiden; de menselijke factor in informatiebeveiliging*, Amsterdam: Pearson Education Benelux
Neddermeijer, H. (2004) *Bedrijfsspionage, waan of werkelijkheid*, Amsterdam: Security Press
Prescott, J.E. en Miller, S.H. (2001)(Eds) *Proven Strategies in Competitive Intelligence; lessons from the trenches*, New York: John Wiley & Sons
Steward, P. (1994) *The role of the US Government in Industrial Espionage*, Washington DC: National Defense University
Whitehead, S. (2006) *Corporate Counterintelligence; Enhancing Security and Business Continuity*, Nice: ASIS European Security Conference 2006

De security manager als wereldburger

Het begint er zo langzamerhand op te lijken dat de sociale wetenschappers gelijk krijgen. De wereld is één groot sociaal systeem geworden met een toename van onderlinge afhankelijkheden tussen landen en tussen mensen. Het gevolg van het globaliseringproces. Globalisering blijkt een complex proces waarbinnen relaties tussen mensen op verschillende plaatsen op de wereld steeds sneller naar elkaar toegroeien.

Er zijn sociologen, en dit is met name interessant voor security managers, die globalisering zien als een toename van de dominantie van de westerse wereld, in het bijzonder van de Verenigde Staten, over andere economische-, politieke- en culturele systemen in de wereld. Zonder ons verder te verdiepen in de juistheid van deze discussie, kijken we naar de gevolgen van één van de verschijnselen die deze sociale wetenschappers aanstippen. Volgens deze wetenschappers wordt het namelijk steeds duidelijker dat er tegengestelde belangen bestaan tussen landen, en als gevolg daarvan ook tussen bevolkingsgroepen. In het bijzonder gaat het dan om belangen die in de ogen van de betrokken mensen zijn gebaseerd op 'het wel kunnen deelnemen' aan of 'het worden buitengesloten' van de vooruitgang. En in het verlengde daarvan de welvaart die dit met zich meebrengt.

Ongelijkheid

Een belangrijk element, die deze tegengestelde belangen tussen bevolkingsgroepen aan het licht brengt, is de verspreiding van nieuwe mediavormen over de wereld. Dit betekent dat voorheen geïsoleerde en gesloten samenlevingen in toenemende mate worden blootgesteld aan politieke en sociale ontwikkelingen die zich voordoen op andere plaatsen in de wereld. Verbeteringen in transport en communicatie hebben tot gevolg dat er steeds meer interacties tussen mensen, afkomstig uit verschillende samenlevingen, plaatsvinden. De connecties tussen samenlevingen hebben inmiddels ook laten zien welke grote verschillen en ongelijkheden er in de wereld tussen bevolkingsgroepen bestaan. Er zijn sociale wetenschappers die dan ook betogen dat het globaliseringproces uiteindelijk

meer instabiliteit dan stabiliteit in de wereld teweeg zal brengen. Juist de verspreiding van informatie over het feit dat anderen het beter hebben kan volgens deze wetenschappers, als het samengaat met het bestaan van concrete grieven als resultaat van ongelijkheid, leiden tot extreme reacties. Mensen willen ook welvaart en rijkdom vergaren en als het moet met niet legitieme middelen. De uitingsvormen van dit streven zijn niet langer gebonden aan tijd en plaats.

Spanningen

Sinds 11 september 2001 is het duidelijk geworden dat de wereld met een nieuw soort, grensoverschrijdend, openbare orde probleem wordt geconfronteerd. Dit probleem beperkt zich veelal niet meer tot de eigen nationale grenzen. George Tenet, de voormalig directeur van de CIA, heeft nog niet zo lang geleden aangegeven dat lang sluimerende frustraties in combinatie met overheden die niet in staat zijn te voldoen aan de behoefte van de eigen bevolking de deur openzetten voor verschrikkelijk alternatieve oplossingen. Waar de toenemende globalisering toe kan leiden en welke gevolgen zich daarvan manifesteren in Nederland, kan de security manager onder meer nalezen in het jaarverslag van de Algemene Inlichtingen en Veiligheidsdienst (AIVD). Regelmatig worden ook wetenschappelijke artikelen geschreven waarin wordt ingegaan op problemen en spanningen die zich in Nederland voordoen naar aanleiding van de toegenomen globalisering en de manifest wordende tegenstellingen tussen in Nederland levende bevolkingsgroepen. Radicalisering van groepen mensen is daarvan een goed voorbeeld. De gemiddelde security manager zal als gevolg van het proces van globalisering, binnen zijn eigen bedrijf - op microniveau - ook steeds meer te maken krijgen met de gevolgen van de toenemende spanningen die tussen de verschillende bevolkingsgroepen bestaan. Dit leidt tot twee belangrijke vragen. Hebt u de dreigingen, die het gevolg van deze spanningen zijn, binnen uw eigen organisatie al in kaart gebracht? Hebt u zich al in verdiept in de vraag hoe u deze dreigingen kunt herkennen, en als dat is gelukt, wat u er vervolgens aan kunt doen om deze weg te nemen?

Dreigingsbeeld

De eigen organisatie is deel van een steeds groter sociaal systeem geworden. Naast terrorisme, waarvan we de voorbeelden inmiddels kennen, is ook criminaliteit met de huidige open grenzen een steeds groter grensoverschrijdend probleem geworden. Dit is iets wat de security



manager dagelijks merkt en waarmee hij zal moeten leren omgaan. Om te weten tegen welke dreiging de organisatie zich moet wapenen zal de security manager daarom niet meer alleen moeten kijken naar de eigen buurt waar zijn organisatie is gevestigd, en met de lokale contactpersoon van het wijkteam van de politie moeten praten over trends, maar hij zal ook steeds meer moeten gaan kijken naar ontwikkelingen die vanuit omringende landen op zijn organisatie afkomen.
Het in 2004 door het Korps Landelijke Politiediensten (KLPD) opgestelde nationale dreigingsbeeld zou verplichte literatuur moeten worden voor de security manager van de 21ste eeuw. De essentiële vraag is dan ook met welke criminele dreigingen de security manager op dit moment volgens de dienst Nationale Recherche Informatie rekening moet gaan houden.

Zwakste schakel

Interessant is dat het rapport van de dienst Nationale Recherche Informatie, overigens gewoon te vinden op internet, aangeeft dat daar waar de (beveiliging)techniek er steeds beter in slaagt om de crimineel buiten de organisatie te houden, het gevolg is dat deze zelfde crimineel zich steeds vaker gaat richten op de zwakste schakel in de organisatie: de mens! Het probleem zit dus veelal verstopt in de eigen organisatie, ook al willen

wij dat met onze Nederlandse traditie vaak niet hardop uitspreken. De doorsnee medewerker, die legitiem aanwezig is en zonder problemen de toegangscontrole mag passeren, blijkt een bedreiging voor het organisatiebelang te kunnen veroorzaken. Daar waar de security manager zich in de 20ste eeuw hoofdzakelijk richtte op het inzetten van organisatorische maatregelen en techniek om criminaliteit te bestrijden, zal hij het vizier in de 21ste eeuw ook steeds vaker op de mens moeten gaan richten. Waarom? Omdat de security manager het de crimineel steeds moeilijker heeft gemaakt gemakkelijk zijn slag te slaan.

Partners in crime

De security manager wordt, om het maar meteen weer wat lastiger te maken, op dit moment ook nog eens geconfronteerd met medewerkers die verschillende culturele achtergronden hebben. Veelal zijn de medewerkers afkomstig uit verschillende landen. Dat maakt de vraag 'wat is gewoon gedrag en welk gedrag kan wijzen op mogelijke criminele intenties?', steeds lastiger te beantwoorden. Zeker als de security manager geen inzicht heeft in wat er in de wereld speelt en wat 'normaal' gedrag is voor mensen die een andere culturele achtergrond hebben. Toch is het, zeker als wij het rapport van de dienst Nationale Recherche Informatie lezen, belangrijk om inzicht te krijgen in deze materie.
De samenwerking tussen criminelen blijkt voor een groot deel af te hangen van etnische en culturele herkomst of achtergrond. Daarnaast zijn ook sociale banden en bloedverwantschap van belang. De partners in crime, zoals de dienst Nationale Recherche Informatie het noemt, worden gevonden in de kring van familie, vrienden, bekenden en vrienden van vrienden. Daarnaast blijken criminele groepen ook steeds beter in staat om hun illegale werkwijze af te schermen. Daarbij moet onder meer worden gedacht aan intimidatie van getuigen. Ook wordt melding gemaakt van een nieuwe vorm van criminaliteit: mobiel banditisme. Dit betekent dat met name Oost-Europese groeperingen zich gaan bezighouden met relatief eenvoudige criminaliteit. De groepen komen Nederland binnen om hun slag te slaan, en zo staat dat ook in het KLPD rapport beschreven, zijn vervolgens even snel weer weg als ze gekomen zijn.
Niet uitgesloten kan worden dat deze vorm van criminaliteit zal toenemen naar mate de toegang tot de oude EU vanuit de nieuwe lidstaten makkelijker wordt. Dit maakt het beeld voor de security manager complex. In de toekomst krijgen wij meer te maken met criminelen die uit het buitenland afkomstig zijn en vaak gericht op zoek gaan naar lucratieve buit. Ook kan

er een dreiging uitgaan van de eigen medewerker die bijvoorbeeld door zijn familie onder druk gezet kan worden om strafbare feiten te plegen.

Uitbesteden

Interessant is ook, zeker nu in Nederland op grote schaal diensten worden uitbesteed, dat de dienst Nationale Recherche Informatie signaleert dat werknemers in de logistieke en facilitaire keten worden gerekend tot een risicogroep. Ook ICT-personeel, dat vanuit hun functie kan beschikken over veel digitaal opgeslagen informatie, blijkt een risicogroep te zijn. Uit opsporingsonderzoeken is inmiddels een beperkt aantal gevallen bekend waarbij ICT-personeel betrokken was bij het plegen van strafbare feiten. Met name in het buitenland zijn meerdere gevallen geconstateerd van corrupt ICT-personeel.
Het is wel enigszins logisch dat criminele organisaties zich steeds vaker gaan richten op het 'rekruteren' van medewerkers in de logistieke en facilitaire keten. Daar waar bedrijfsnetwerken steeds beter worden beveiligd, en daar waar de beveiligingstechniek steeds effectiever wordt, wordt het steeds aantrekkelijker om bedrijfspersoneel te benaderen voor medewerking. Of misschien nog wel beter, meteen een eigen medewerker in een bedrijf te plaatsen. Eventueel via een leverancier. En zeg nu zelf, het is een koud kunstje om te achterhalen bij welke leverancier een willekeurig bedrijf diensten inhuurt. Zonder nu meteen overal spoken te gaan zien, is het goed om eens stil te staan bij de vraag wat u nu als security manager eigenlijk weet van het (ingehuurde) personeel dat bij uw organisatie werkzaam is, en uzelf de vraag te stellen of deze mensen kwetsbaar zijn voor chantage en afpersing? Het hoeft immers niet altijd de kwaadwillendheid van een medewerker zelf te zijn die aanleiding geeft tot het plegen van een strafbaar feit. Als een criminele organisatie weet op welk punt iemand gevoelig is en men wil in uw bedrijf kennis of technologie stelen, is het een kwestie van de druk op een personeelslid opvoeren totdat iemand gaat meewerken. Al is het alleen maar door het doen van een beroep op de loyaliteit van uw medewerkers gezien hun afkomst en familiebanden.

Human engineering

Rest het stellen van de vraag of u als security manager op dit moment al een goed inzicht heeft van wat er op dit moment voor dreiging, en dan ook met name vanuit het buitenland, op uw organisatie afkomt? Weet u of uw personeel kwetsbaar is voor chantage en afpersing en weet u waar

de loyaliteit van uw personeel ligt? Bij uw bedrijf, bij de eigen familiekring of misschien wel bij de eigen bevolkingsgroep? Zijn medewerkers in uw organisatie, gezien de spanningen in de wereld, gevoelig voor radicale denkbeelden? Bent u zich ook bewust dat waar technische en elektronische controlemiddelen steeds moeilijker te manipuleren en te omzeilen zijn, criminele groeperingen hun toevlucht steeds vaker zoeken tot het aspect van human engineering? De verwachting is dat er steeds meer gebruik zal worden gemaakt van het aanspreken van mensen op een mogelijke dubbele loyaliteit.
De uitbestedingtendens, van onder andere beveiligingspersoneel en (ICT) netwerkbeheerders, zou uw bedrijf gezien de veranderende (dreiging)situatie wel eens kunnen gaan opbreken. Wie controleert de controleur als deze aan de verkeerde kant blijkt te staan? De security manager? Dan zal deze wel moeten weten wat in de wereld om hem heen gebeurt. Kortom, hij zal een wereldburger moeten worden.

Literatuur

Akerboom, E.S.M. (2003) '*Contraterrorisme in Nederland*', het Tijdschrift voor de Politie, Nummer 6 (Jaargang 65), Doetinchem: Elsevier / Reed Business Information.
Central Intelligence Agency (2003) *Speeches and Testimony, Worldwide Threat Briefing, The worldwide Threat in 2003: Evolving Dangers in a Complex World, 2003*,
Cutter, S.L., Richardson, D.B., and Wilbanks, T.J., *The Geographical Dimensions of Terrorism*, New York: Routledge.
Dienst Nationale Recherche Informatie (2004) *Nationaal Dreigingsbeeld; Zware of georganiseerde criminaliteit*, Zoetermeer: Korps Landelijke Politie Diensten.
Giddens, A. (1991) *Modernity and Self-Identity; Self and Society in the Late Modern Age*, Cambridge: Polity Press in association with Blackwell Publishers Ltd.
Huntington, S.P. (1996) *The clash of Civilizations and the Remaking of World Order*, New York: Simon & Schuster.
Onwudiwe, I.D. (2001) *The globalization of terrorism; interdisciplinary research series in ethnic, gender and class relations*, Aldershot: Ashgate Publishing Limited.
Whittaker, D.J. (2001) *The Terrorism Reader, London and New York*: Routledge Taylor and Francis Group.
Woodward, K. (2003) *Social Sciences; The big issues*, London and New York: Routledge Taylor and Francis Group.

Bepalen van te beschermen bedrijfsbelangen

Onderzoek, uitgevoerd in 2005, heeft laten zien dat de security manager er slechts bij een klein aantal organisaties in is geslaagd om, samen met voor het primaire proces verantwoordelijke lijnmanagers, te benoemen wat precies de 'te beschermen belangen' van de organisatie zijn. Bij de meeste organisaties blijkt de zogenaamde 'belangenanalyse', die als input essentieel is voor een goede kwalitatieve risicoanalyse, afwezig.

Het gevolg is dat de security manager zelf is gaan bedenken wat de te beschermen belangen van de organisatie zijn. Omdat hij hierover vaak niet in gesprek is met het lijnmanagement dat voor het primaire proces verantwoordelijk is, doen zich uiteindelijk bij het treffen van beveiligingsmaatregelen problemen voor. Er blijkt dan veelal geen draagvlak aanwezig te zijn bij het (top)management voor het nemen van maatregelen. Beveiliging is dan weer die lastige en overbodige kostenpost, die ook nog eens hinderlijk is voor de voortgang van het primaire bedrijfsproces.

Beleggen verantwoordelijkheid

In plaats van beveiliging neer te zetten als kostenpost is het voor de security manager van belang om aan te tonen dat beveiliging een noodzakelijk onderdeel is van het reguliere bedrijfsproces. Het gaat dan vooral om het zichtbaar maken dat beveiliging op verschillende manieren kan bijdragen aan het vergroten van de winst van de onderneming of de continuïteit van de organisatie. Gezien het feit dat, behoudens enkele uitzonderingen daargelaten, het 'proces security management' niet gepositioneerd is als ondersteunend proces van het primaire proces, wordt het hoog tijd dat security managers het management daadwerkelijk gaan betrekken bij het opstellen van een risicoanalyse voor de organisatie. Het is namelijk uiteindelijk het (top)management dat, in samenspraak met de lijnmanagers, moet bepalen welke bedrijfsprocessen - lees 'te beschermen belangen' - bescherming nodig hebben. Niet de security manager. De laatste is slechts adviseur. De eerste stap is dan ook om de verantwoordelijkheid voor de keuzes, als het gaat om welke belangen bescherming behoeven, daar neer te leggen waar hij hoort te liggen: bij het management.

Risicoanalyse

Wat is nu het eigenlijk het unieke product, of die unieke dienst, die de organisatie aan de samenleving levert? Op welk moment zou, als de producten die de organisatie maakt niet meer geleverd kunnen worden, de continuïteit van de organisatie in het geding komen? Hoe groot is de schade als het primaire proces wordt onderbroken als gevolg van een incident? Hoe lang mag deze onderbreking duren? Welke incidenten tasten het 'imago' van de organisatie op een dusdanige wijze aan dat het bestaansrecht kan worden aangetast omdat afnemers weglopen?
De antwoorden op deze vragen van de security manager zullen uiteindelijk moeten worden gegeven door de verantwoordelijke bestuurders van de organisatie. Pas wanneer het (top)management zich op strategisch niveau uitspreekt over de 'te beschermen belangen' heeft de security manager een opdracht en een kapstok voor het opstellen van een risicoanalyse.
Het is, ter afronding van deze fase, belangrijk dat de uitspraken van het management over de 'te beschermen belangen' worden vastgelegd. De security manager kan dan, als hij daadwerkelijk aan de slag gaat met het opstellen van de risicoanalyse, verwijzen naar de 'belangen van de organisatie' die volgens het (top)management bescherming behoeven.

Betrokkenheid lijnmanagement

Zodra er op strategisch niveau een duidelijke uitspraak is over de 'te beschermen belangen' van de organisatie kunnen, op het tactische niveau, de lijnmanagers door de security manager met deze vaststelling worden geconfronteerd. Er dienen zich dan meteen nieuwe vragen aan waarop de security manager antwoord moet krijgen. Welke bijdrage levert de betreffende lijnmanager vanuit zijn verantwoordelijkheid aan het maken van het unieke product of die unieke dienst? Wanneer komt de continuïteit van zijn bijdrage aan dit product of aan deze dienst in het geding?
Als lijnmanagers geen antwoord op deze vragen kunnen of willen leveren, kan de security manager eigenlijk niet goed verder. Als de lijnmanagers al niet weten wat wel of niet essentieel is voor hun bijdrage aan het unieke product of de unieke dienst van de organisatie, kan ook niet van een security manager worden verwacht dat deze dat inzicht wel heeft. De praktijk laat echter vaak zien dat lijnmanagers, natuurlijk met de nodige ondersteuning en uitleg, zeer goed in staat zijn om de security manager van de benodigde antwoorden te voorzien. Ook in deze fase is het weer van belang om alle uitspraken vast te leggen en het lijnmanagement aan de verslaglegging te committeren.

Nu op strategisch en op tactisch niveau de 'te beschermen belangen' van de organisatie duidelijk zijn, is het aan de security manager om te gaan beschrijven welke (vitale) processen er binnen de organisatie zijn aan te wijzen die essentieel zijn om het unieke product of de unieke dienst waar het (top)management zich over heeft uitgesproken te kunnen blijven leveren. Veel organisaties zullen waarschijnlijk niet meer (goed) kunnen functioneren zonder bijvoorbeeld de IT-voorziening. Andere organisaties daarentegen komen misschien in de problemen als er 'knelpunten' in het logistieke proces optreden.

Voldoende draagvlak

Het is aan de security manager om, na de eerdere input die het management heeft gegeven, te bepalen wat nu die echte (vitale) processen zijn, die voor de continuïteit van de organisatie essentieel zijn. Ook zal een antwoord moeten worden gegeven op de vraag waar, en op welke momenten, 'imagoschade' kan optreden die een gevaar kan opleveren voor de continuïteit van de organisatie. In eerste instantie zal de security manager zijn bevindingen met het lijnmanagement moeten bespreken. Belangrijke vraag aan de lijnmanagers is daarbij of er processen over het hoofd zijn gezien? Pas op het moment dat de lijnmanagers zich kunnen vinden in het verhaal van de security manager en er voldoende draagvlak is, kan er een document worden opgesteld en vastgesteld waarin de (vitale) processen worden beschreven.
Nadat is vastgesteld wat de (vitale) processen zijn die voor de continuiteit van de organisatie noodzakelijk zijn, kan een verdere verdiepingsslag worden gemaakt. Wat zijn nu, binnen die (vitale) processen de echt 'kwetsbare onderdelen' die essentieel zijn voor het functioneren van het proces? Ook dit is een vraag voor de lijnmanagers die verantwoordelijk zijn voor het goede verloop van het betreffende proces. In deze fase wordt duidelijk, als het goed is, wat nu de specifieke onderdelen zijn - of locaties - waarvoor daadwerkelijk beveiliging noodzakelijk is.

Valkuil

Bij de belangenanalyse gaat het er niet om de noodzakelijke beveiliging te beschrijven. Er kan niet vaak genoeg worden gewaarschuwd om niet in deze valkuil te stappen. Waar het wel om gaat, zonder in de discussie van wel of geen beveiliging te vervallen, is het verantwoordelijke (lijn)management de vraag te laten beantwoorden wat nu de kwetsbare onderdelen binnen het primaire (bedrijfs)proces zijn. Als deze vraag goed

wordt beantwoord levert dit in de praktijk vaak de kwetsbare locaties op en soms zelfs specifieke kwetsbare ruimtes.
Nu de vitale processen en de kwetsbare onderdelen binnen deze processen duidelijk zijn, kan een antwoord worden gegeven op de vraag wat nu de echte 'te beschermen belangen' van de organisatie zijn. Hoe specifieker de onderdelen of locaties beschreven worden - en natuurlijk ook waarom zij essentieel zijn - hoe gemakkelijker het wordt om bij het opstellen van de daadwerkelijke risicoanalyse keuzes te maken.
Belangrijk is wel om in deze fase goed voor ogen te houden dat de belangenanalyse weliswaar door de security manager is geschreven, maar dat deze uiteindelijk wordt vastgesteld door het (top)management in samenspraak met het lijnmanagement. Het is dan uiteindelijk ook niet de security manager die eindverantwoordelijk is voor het treffen van beveiligingsmaatregelen, naar het lijnmanagement dat afhankelijk is van de 'te beschermen belangen' en dat bepaalt wat voor budget daarvoor beschikbaar is. Op deze manier wordt duidelijk waar, in een latere fase, de (beveiligings)verantwoordelijkheden van de lijnmanagers liggen. De security manager maakt op deze manier zijn rol als adviseur optimaal waar, zonder probleemeigenaar te worden.

Literatuur

Broder, J.F. (2000) *Risk Analysis and the Security Survey*, Boston: Butterworth-Heinemann / member of the Reed Elsevier Group.
Claes, P.F. en Meerman, H.J.J.M. (1998) *Riskmanagement; inleiding tot het risicobeheersingsproces*, Houten: Stenfert Kroese.
Coumou, C. (2003) *Risicomanagement voor security- en facilitymanagers*, Alphen aan den Rijn: Kluwer.
Haaf, W. ten, Bikker, H. en Adriaanse, D.J. (2002) *Fundamentals of business engineering and management*, Delft: Delft University Press.
Overbeek, P., Roos Lindgreen, E. en Spruit, M. (2000) *Informatiebeveiliging onder controle*, Amsterdam: Prentice Hall.
Purpura, P.P. (1998) *Security and Loss Prevention*, Boston: Butterworth-Heinemann /member of the Reed Elsevier Group.
Roper, C.A. (1999) *Riskmanagement for Security Professionals*, Boston: Butterworth-Heinemann / member of the Reed Elsevier Group.
Sennewald, C.A. (1998) *Effective Security Management*, Boston: Butterworth-Heinemann / member of the Reed Elsevier Group.
Veld, J. in 't (2002) *Analyse van Organisatieproblemen; Een toepassing van denken in systemen en processen*, Groningen: Stenfert Kroese.

De (be)dreigingen van het organisatiebelang in kaart gebracht

Een goede kwalitatieve risicoanalyse begint met het bepalen van de belangen die voor het voortbestaan van de organisatie cruciaal zijn. Na deze belangenanalyse kan worden bekeken welke (be)dreigingen de benoemde en vastgestelde organisatiebelangen kunnen aantasten. Het gaat dan om de zogenoemde dreiginganalyse.

Voor het opstellen van een goede kwalitatieve risicoanalyse is het noodzakelijk om in eerste instantie te bepalen welke organisatiebelangen uit het oogpunt van continuïteit van groot belang zijn voor het voortbestaan van de onderneming. Dit hoeft niet alleen de beschikbaarheid van bepaalde bedrijfsprocessen te zijn, maar kan ook een onderwerp als bijvoorbeeld 'het imago' van de organisatie raken of het feit dat vertrouwelijke informatie niet mag uitlekken. Zeker als door een dergelijk incident het beeld dat men van de organisatie heeft kan verschuiven van 'betrouwbaar' naar 'onbetrouwbaar'.
Nadat deze eerste stap is gezet en er een zogenaamde belangenanalyse is opgesteld en vastgesteld door het (top)management, kan worden bekeken welke (be)dreigingen de benoemde en vastgestelde organisatiebelangen kunnen aantasten. Het resultaat van deze tweede stap is een door het (top)management vastgestelde dreiginganalyse. Vervolgens kan, als in een derde stap de bestaande weerstand tegen de beschreven dreigingen in kaart is gebracht in de vorm van een weerstandsanalyse (ist-situatie), de daadwerkelijke risicoanalyse als vierde en laatste stap worden opgesteld. Door een afweging te maken tussen belang, dreiging en weerstand kan inzichtelijk worden gemaakt welke risico's de organisatie loopt en welke aanvullende (beveiligings)maatregelen eventueel noodzakelijk zijn (soll-situatie). In dit tweede hoofdstuk van het onderdeel 'risicoanalyse' wordt stilgestaan bij de tweede (deel)stap: de dreiginganalyse.

Stand van zaken

Uit recent onderzoek blijkt dat slechts een klein aantal security managers daadwerkelijk de tijd heeft, en ook de tijd neemt, om zich te verdiepen in de (be)dreigingen van de organisatiebelangen die voortkomen uit

maatschappelijke ontwikkelingen. Daarentegen zijn de meeste security managers zich wel bewust, op basis van wat men in de Verenigde Staten *hear-say* noemt, van de externe en interne criminele (be)dreigingen die de belangen van de organisatie kunnen aantasten. Helaas blijken veel van de security managers niet instaat om deze 'criminele (be)dreigingen' ten opzichte van de eigen organisatie op een gestructureerde manier te onderbouwen met beschikbare 'historische data' en trendanalyses. Dit terwijl alleen aan de hand van 'historische data' en de 'frequentie van gerelateerde incidenten' kan worden bepaald wat de kans is dat een bepaalde dreiging zich ook in de toekomst zal manifesteren, zoals ook wordt beschreven in het boek Riskmanagement for Security Professionals van Carl Roper (1999).
Een bedreiging is volgens Roper 'iedere indicatie, omstandigheid of gebeurtenis die in potentie het verlies of de aantasting' van een organisatiebelang tot gevolg kan hebben. Om deze bedreigingen te identificeren moeten 'tegenstanders in kaart worden gebracht'. Daarnaast is het van belang 'de motivatie' en 'de capaciteiten' van de tegenstanders te kennen. Met name deze laatste twee punten zijn interessant bij het opstellen van een dreiginganalyse. Zeker als het bepalen van 'de kans' dat een dreiging zich zal gaan manifesteren, door het ontbreken van trendanalyses en historische data, koffiedik kijken is. Misschien moet de security manager het inmiddels klassieke onderdeel 'kansberekening' wel overboord zetten, wil hij een goed verhaal over (be)dreigingen aan het management kunnen voorleggen?

Onderzoek

Philip Purpura stelt in zijn boek Security and Loss Prevention (1998) dat historische data moeten worden aangevuld met de resultaten van onderzoeken naar gedrag van criminelen zoals die zijn uitgevoerd door bijvoorbeeld de University of Massachusetts en de Eastern Washington University. Deze academische onderzoeken geven aan dat 'een veelheid aan beveiligingsmaatregelen veelal overbodig is' en volstaan kan worden met enkele 'weloverwogen en gecontroleerd ingezette maatregelen'. Dan moet de onderbouwde risicoanalyse wel zijn oorsprong vinden 'in het verleden, niet in de toekomst', aldus James Broder in zijn boek Risk Analysis and the Security Survey (2000).
De praktijk is echter weerbarstig. Een groot deel van een in 2005 ondervraagde groep Nederlandse security managers gaf aan geen ingericht proces 'incidentmanagement' te hebben. Het merendeel gaf ook aan



geen goed inzicht te hebben in incidenten die zich in het verleden binnen de eigen organisatie hebben voorgedaan. Dit maakt het moeilijk, zoals de security managers zich realiseerden, om het 'probleem dat de organisatie heeft, daar waar het om schade gaat ten gevolge van criminaliteit', goed inzichtelijk te maken. Voor een goede dreiginganalyse, waar met meer dan alleen criminele dreigingen rekening moet worden gehouden, is onderzoek onontbeerlijk. De werpt meteen de vraag op 'waar moet ik mij nu op richten bij het in kaart brengen van de dreigingen voor mijn organisatie'? Als diepgaand onderzoek niet mogelijk is gezien de tijd die dit vraagt en historische data niet beschikbaar zijn, is er misschien toch wel iets voor te zeggen om 'de dreiginganalyse' op een andere, meer pragmatische manier, op te stellen. Een optie is om per 'bedreiger' te gaan bepalen wat de motivatie alsook de capaciteit is om de 'te beschermen belangen' van de organisatie aan te tasten. Bij het bepalen van de capaciteit moet dan wel op hoofdlijnen ook iets over het scenario worden gezegd, echter zonder het tot in detail uit te werken.

Bedreigers

Als eerste stap is het noodzakelijk om, uitgaande van de 'te beschermen' belangen, aan te geven welke groepen bedreigers daadwerkelijk een potentieel gevaar voor de organisatie kunnen opleveren. Afhankelijk van de vastgestelde belangenanalyse kan worden gedacht aan criminelen die (fysieke) bezittingen van de organisatie willen stelen, aan actiegroepen die de continuïteit van het bedrijfsproces willen verstoren, aan concurrenten en buitenlandse inlichtingendiensten die toegang zoeken tot geheime bedrijfsinformatie en aan gefrustreerde (ex)medewerkers. Ook journalisten, die bezig zijn met het schrijven van een achtergrondartikel over de organisatie, kunnen een dreiging opleveren als zij vertrouwelijke informatie in handen krijgen. Denk aan de imagoschade die een negatief



artikel in de pers kan opleveren. Ook kunnen, afhankelijk van de situatie, leveranciers en afnemers een dreiging opleveren.
Is dit nu een compleet beeld van mogelijke (be)dreigers? Nee, zeker niet. Dit is slechts een indicatie voor wat betreft de groepen bedreigers waar aan gedacht kan worden bij het opstellen van een dreiginganalyse. Afhankelijk van de specifieke situatie van de organisatie zal de groep potentiële bedreigers toenemen of afnemen.

Motivatie

Vervolgens doet zich de vraag voor, als de groepen bedreigers zijn geïdentificeerd, of zij ook daadwerkelijk 'de wil hebben' om acties te ontplooien die de 'te beschermen belangen' van de organisatie kunnen aantasten. Het gaat bij het bepalen van de motivatie die bedreigers hebben niet in eerste instantie om een academische onderbouwing. Alleen al vanwege de tijd die dit vraagt is dit veelal een onmogelijke opgave.
Het is belangrijk dat als het onderwerp motivatie ter sprake komt er nagedacht wordt over de onderbouwing van de reden waarom een groep bedreigers de 'te beschermen belangen' van de organisatie zouden willen aantasten, bijvoorkeur door informatie over dit onderwerp te verzamelen. Waar kan dan zoal aan worden gedacht? De reden om een organisatie als doelwit te kiezen kan voortkomen uit economische motieven, maar ook uit politieke of ideële motieven. Het kan daarnaast ook gaan om basale zaken zoals diefstal omdat iemand geld nodig heeft, of om vernieling van eigendommen omdat de organisatie slachtoffer wordt van een gefrus-

treerde werknemer of van 'jongeren' die zich vervelen en niets beter te doen hebben. De motivatie kan ook gelegen zijn in het slechte imago van de onderneming bij bepaalde actiegroepen, of het goede professionele imago van de organisatie bij concurrenten, die daarom willen weten wat de 'geheimen' van het bedrijfsproces zijn.

Capaciteit

Alleen de wil om de belangen van de organisatie aan te tasten is niet genoeg. De bedreigers moeten, voordat zij als 'dreiging' serieus kunnen worden genomen, ook daadwerkelijk de mogelijkheid en de middelen hebben om de organisatiebelangen aan te tasten. Dit betekent dat de vraag zich opwerpt of de inmiddels geïdentificeerde groepen bedreigers toegang hebben tot de organisatie. En dan natuurlijk in het bijzonder tot de 'te beschermen bedrijfsbelangen'.
Mocht de toegang niet vanzelfsprekend zijn, dan is de vraag of de toegang tot het bedrijf, of beter gezegd de toegang tot de 'te beschermen' belangen, gemakkelijk te verkrijgen is. Vragen die nu beantwoord dienen te worden liggen op het vlak van de hoeveelheid tijd en geld die een potentiële bedreiger beschikbaar heeft om de 'te beschermen belangen' van de organisatie aan te tasten. Tijd en geld zijn immers bij uitstek geschikt om toegang te krijgen tot de juiste middelen die een gevaar kunnen opleveren voor de 'te beschermen belangen'.

Scenario

Daar waar een criminele organisatie of een concurrent geld kan gebruiken om medewerkers om te kopen of in een chantabele positie te brengen, zal een activist of een journalist bereid zijn veel tijd en energie in het bereiken van zijn doel te stoppen. Misschien wel door zelf bij een organisatie in dienst te treden. De gefrustreerde medewerker daarentegen loopt al rond in de organisatie en hoeft alleen maar op een onbewaakt moment een onbevoegde handeling te verrichten. Het middel in dat geval is het gereedschap en het scenario waarmee rekening



dient te worden gehouden is dan de daadwerkelijke 'handeling' waarmee de medewerker vitale apparatuur kan ontregelen. En mocht de voordeur op slot zijn, maar de informatiebeveiliging is niet op orde, dan kan ook via externe verbindingen (internet) toegang tot de organisatie worden verkregen. Vaak zonder dat iemand het merkt. De capaciteit is in dit geval de benodigde kennis. Het scenario is *hacking*. Ook kan het voorkomen dat alle nieuwe medewerkers die bij een organisatie in dienst treden een screening moeten ondergaan. Dit is echter nutteloos als uw organisatie veel diensten, zoals beveiliging en ICT, uitbesteedt en de extern ingehuurde medewerkers niet tegen het licht worden gehouden. De capaciteit is in dit geval wederom kennis, in dit geval van en over de organisatie, en het scenario is infiltratie.

Dreiging

Als zowel de verwachte wil (motivatie) alsook de middelen (capaciteit) aanwezig zijn om de organisatiebelangen aan te tasten, en er is een daadwerkelijk uitvoeringsscenario denkbaar, is er sprake van een dreiging waarmee rekening moet worden gehouden. Deze manier van benaderen laat de 'kansberekening', die vaak zijn oorsprong vindt in quasi academisch koffiedik kijken, buiten beschouwing. Zeker in een situatie waar daadwerkelijke historische data en onderzoeksresultaten ontbreken is deze manier van benaderen het meest transparant. Als de security manager zich verdiept in de criminele ontwikkelingen die het nieuws halen en voorbeelden daarvan in de dagbladen zoekt, kan al redelijk snel een beeld van 'motivatie', 'capaciteit' en gebruikte scenario's worden gevonden. Zeker als dit globale beeld wordt aangevuld met informatie afkomstig uit bijvoorbeeld het jaarverslag van de AIVD of het door de Dienst Nationale Recherche Informatie opgestelde rapport 'Nationaal Dreigingsbeeld; Zware of georganiseerde criminaliteit'. De doelstelling van de dreiginganalyse is immers niets meer en niets minder dan het (lijn)management te confronteren met een onderbouwende en aannemelijke analyse van mogelijke bedreigingen. Belangrijk is dat de geïdentificeerde groepen bedreigers en ook de opsomming van de aanwezige motivatie (wil), capaciteit (middelen) en het verwachte scenario waarmee de organisatiebelangen kunnen worden aangetast, herkenbaar en samenhangend zijn.

Valkuilen

Belangrijk is wel om in dit stadium, bij het benoemen van de mogelijke groepen die de organisatiebelangen kunnen aantasten, een zo compleet

mogelijk beeld te schetsen. Het op dit moment al uitsluiten van bepaalde groepen bedreigers kan betekenen dat er, als de laatste stap wordt gezet, een niet volledige risicoanalyse wordt opgesteld, met alle problemen van dien.
De security manager dient zich goed te realiseren dat het uiteindelijk aan het (lijn)management is om te beslissen welke groepen bedreigers wel en welke groepen bedreigers niet in de dreiginganalyse moeten worden meegenomen. Het weglaten van een groep bedreigers op voorhand kan, zeker als een dreiging manifest wordt, cruciale gevolgen hebben als deze niet in de dreiginganalyse is meegenomen. De beslissing een groep bedreigers buiten beeld te laten is, zeker gezien de mogelijke gevolgen, een management-beslissing. Niet een beslissing voor de security manager. Het is belangrijk dat de security manager zich realiseert dat een groep bedreigers die niet in de dreiginganalyse wordt meegenomen ook niet zal terugkomen op het moment dat de daadwerkelijke risicoanalyse wordt opgesteld. Een gemiste kans! Daarnaast is het belangrijk om in deze fase dreigingen niet op voorhand te prioriteren. Ook dit is een verantwoordelijkheid, mocht er al behoefte aan prioritering bestaan, van het (lijn) management.

Literatuur:

Broder, J.F. (2000) *Risk Analysis and the Security Survey*, Boston: Butterworth-Heinemann / member of the Reed Elsevier Group.
Claes, P.F. en Meerman, H.J.J.M. (1998) *Riskmanagement; inleiding tot het risicobeheersingsproces*, Houten: Stenfert Kroese.
Coumou, C. (2003) *Risicomanagement voor security- en facilitymanagers*, Alphen aan den Rijn: Kluwer.
Haaf, W. ten, Bikker, H. en Adriaanse, D.J. (2002) *Fundamentals of business engineering and management*, Delft: Delft University Press.
Overbeek, P., Roos Lindgreen, E. en Spruit, M. (2000) *Informatiebeveiliging onder controle*, Amsterdam: Prentice Hall.
Purpura, P.P. (1998) *Security and Loss Prevention*, Boston: Butterworth-Heinemann / member of the Reed Elsevier Group.
Roper, C.A. (1999) *Riskmanagement for Security Professionals*, Boston: Butterworth-Heinemann / member of the Reed Elsevier Group.
Sennewald, C.A. (1998) *Effective Security Management*, Boston: Butterworth-Heinemann / member of the Reed Elsevier Group.
Veld, J. in 't (2002) *Analyse van Organisatieproblemen*; Een toepassing van denken in systemen en processen, Groningen: Stenfert Kroese.

De weerstand van de organisatie tegen vastgestelde dreigingen

Voordat een daadwerkelijke risicoanalyse wordt opgesteld is het nodig te bepalen wat de huidige weerstand van de organisatie is. Dit is de zogenaamde weerstandanalyse. Deze beperkt zich niet tot getroffen fysieke en personele beveiligingsmaatregelen. Ook vigerende regelgeving en de organisatie van beveiligingsfuncties binnen de organisatie moeten als weerstand tegen (be)dreigingen worden gezien.

Onderzoek dat enkele jaren geleden is uitgevoerd heeft laten zien dat het 'actief managen' van beveiliging en het 'continu analyseren en vertalen van het beleid naar organisatorische en technische alternatieven, alsmede het zorgen dat de beveiligingsmaatregelen adequaat blijven in het licht van veranderende eisen en veranderende omgeving', onvoldoende aandacht krijgt. Het gevolg van deze ontbrekende schakel op tactisch niveau is dat veel geld wordt geïnvesteerd in maatregelen die niet meer relevant zijn, terwijl nieuwe, meer effectieve maatregelen niet worden genomen. Kortom, de vraag 'wat is nu eigenlijk de weerstand van de organisatie', als het gaat om de 'te beschermen belangen' ten opzichte van de vastgestelde 'dreigingen', kan veelal niet goed worden beantwoord. Daarom is het belangrijk, voordat de daadwerkelijke risicoanalyse wordt opgesteld, te bepalen wat de huidige weerstand van de organisatie is. Dit is wat binnen de Rijksoverheid de weerstandanalyse wordt genoemd. Deze beperkt zich niet tot getroffen fysieke en personele beveiligingsmaatregelen. Ook vigerende regelgeving en de organisatie van de beveiligingsfuncties binnen een instelling of bedrijf, moeten als weerstand tegen (be)dreigingen worden gezien.

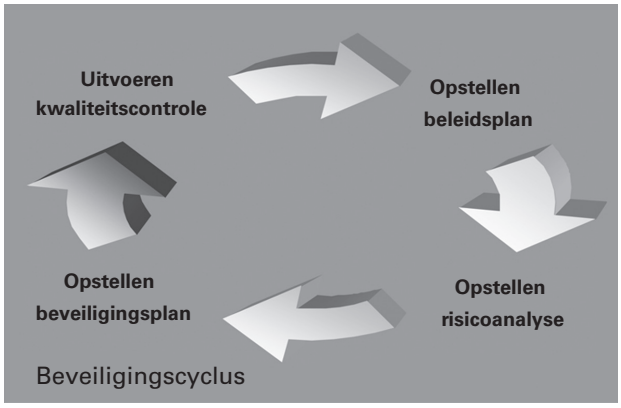
Opzet en werking

Er zijn veel instrumenten beschikbaar als het gaat om het in kaart brengen van de weerstand van een organisatie. Misschien wel teveel. Het probleem daarbij is dat voor al deze instrumenten ook een veelvoud aan termen wordt gebruikt. Het gevolg is dat eigenlijk niemand meer weet wat de betekenis van het betreffende instrument is. Kunt u uitleggen wat het verschil is tussen een security audit, security survey, security scan of

een security inspectie? En weet u dan ook zeker dat collega security managers geen andere beleving bij de gebruikte terminologie hebben? Ik niet. Tot op heden zijn wij er als security professionals helaas niet in geslaagd een eenduidige terminologie te ontwikkelen zodat iedereen meteen weet wat wij bedoelen. Toch hebben de genoemde instrumenten, die vaak te pas en te onpas worden gebruikt, wel iets gemeen. Er wordt namelijk gekeken naar de 'opzet van de beveiliging' of naar de 'werking van de beveiliging'. Soms ook naar een combinatie van beide. Nu is een veel voorkomende valkuil bij het in kaart brengen van de weerstand van een organisatie dat er vrijwel meteen wordt ingezoomd op de vraag hoe getroffen (beveiligings) maatregelen in de praktijk uitwerken. Daarbij wordt vaak uit het oog verloren dat als de (beveiligings) maatregelen niet geborgd zijn, en op papier zijn vastgelegd, de werking veelal op toeval berust. Het is daarom, hoe vervelend ook, belangrijk om eerst naar de zogenaamde 'papieren werkelijkheid' te kijken voordat in kaart wordt gebracht hoe de maatregelen in de praktijk functioneren. Met andere woorden: wat staat er in het beveiligingsbeleid en het beveiligingsplan beschreven? En wat wil de organisatie nu eigenlijk bereiken met de inzet van beveiligingsmiddelen? Dit is dan ook de eerste stap bij de weerstandanalyse. Het bekijken van de 'papieren' werkelijkheid.

Beveiligingscyclus

Om te borgen dat de goede vragen worden gesteld en ook om te verzekeren dat sprake is van 'actief managen' van beveiliging, wil ik de term beveiligingscyclus introduceren. Het hebben van een ingericht security management proces is immers ook 'weerstand' van de organisatie tegen (be) dreigingen. Het idee van de beveiligingscyclus, die zijn oorsprong vindt in de Demmingcyclus (plan-do-



Beveiligingscyclus

check-act), is dat er een logische volgorde ontstaat voor wat betreft de te nemen stappen. Daarnaast is het voortdurend doorlopen van een beveiligingscyclus ook een garantie dat beveiligingsmaatregelen adequaat blijven in het licht van veranderende eisen en veranderende omgeving.
Wat zijn nu de onderdelen van een dergelijke beveiligingscyclus? Ten eerste is het belangrijk, in het kader van de weerstandanalyse, om te bekijken welke visie voor beveiliging in de missie van de organisatie is vastgelegd. Wat is het doel dat met de inzet van het instrument beveiliging dient te worden bereikt? Immers, pas als er doelen zijn kan er een beleid worden bepaald. Vervolgens is het van belang om naar het geformuleerde beveiligingsbeleid te kijken. De beleidsmatige vraag is immers welke middelen gaan wij inzetten om de in de visie geformuleerde doelen te bereiken? De risicoanalyse speelt daarbij een cruciale factor. Het moet duidelijk zijn welke belangen de organisatie wil beschermen, welke (be) dreigingen onderkend worden ten opzichte van deze belangen en wat de weerstand van de organisatie is tegen deze (be)dreigingen.
Pas als deze vragen binnen de risicoanalyse zijn beantwoord, kan een onderbouwde keuze voor middelen worden gemaakt. Het door de organisatie opgestelde beveiligingsplan is tenslotte een logisch vervolg op de risicoanalyse. De weerstandanalyse dient om duidelijk te maken of sprake is van een ingerichte beveiligingscyclus waarbinnen alle noodzakelijke stappen zijn genomen. Is de opzet aanwezig en berust de keuze van in te zetten beveiligingsmiddelen niet op toeval, dan is het zinvol om naast de 'papieren werkelijkheid' ook de daadwerkelijke 'werking' van de beveiliging in de analyse te betrekken. Is de papieren werkelijkheid niet op orde, dan is het zinvol om eerst daar aandacht aan te besteden. Begin vooral eenvoudig.

Organisatie beveiligingsfunctie

Speciale aandacht bij de weerstandanalyse is het bekijken van de inrichting van de beveiligingsfunctie. Zijn taken en verantwoordelijkheden duidelijk belegd en ook schriftelijk vastgelegd in een beveiligingsplan? Is er sprake van een centrale beveiligingsfunctionaris, of is er als er naar aandachtsgebieden wordt gekeken sprake van versnippering? Wat veelal zichtbaar wordt, als deze vragen worden gesteld, is dat er binnen een organisatie meerdere aandachtsgebieden zijn. Fysieke beveiliging, informatiebeveiliging en personele beveiliging zijn belegd bij verschillende afdelingen. Als de verschillende leidinggevenden van afdelingen al met elkaar praten en kennis uitwisselen, is het gebruik van een gemeenschappelijk kader in die situatie toch nog vaak zeldzaam.



Mijn stelling is dat als er geen gemeenschappelijk startpunt is voor fysieke beveiliging, informatiebeveiliging en personele beveiliging, een organisatie kwetsbaar is voor (be)dreigingen die op haar afkomen. In het meest positieve scenario overlappen maatregelen elkaar. In het meest negatieve scenario werken maatregelen elkaar tegen of heffen ze elkaar zelfs op. Idealiter zou er een centrale beveiligingsfunctionaris moeten zijn, een corporate security manager, die kaderstellend is voor alle deelgebieden. Dat wil niet zeggen dat hij, of zij, vervolgens ook alles zelf gaat organiseren. Als er duidelijke kaders zijn en er een centrale functionaris is die toeziet of iedereen zijn verantwoordelijkheden nakomt, kan de uitvoering van beveiligingstaken bij verschillende afdelingen zijn belegd. Een goed voorbeeld van hoe een 'beveiligingsfunctie' binnen een organisatie kan worden ingericht is de opzet van de beveiliging binnen de Rijksoverheid. Bekijk op internet het 'Beveiligingsvoorschrift 2005', het 'Voorschrift Informatiebeveiliging Rijksdienst - Bijzondere Informatie' en de in de Staatscourant gepubliceerde 'instructie voor de Beveiligingsambtenaar (BVA)' maar eens. Al deze documenten sluiten op elkaar aan en geven een kapstok waaraan alle deelgebieden kunnen worden opgehangen. Is er binnen uw organisatie geen kapstok voor beveiliging aanwezig, dan is uw organisatie, vanuit het perspectief van de weerstandanalyse gezien, kwetsbaar.

Risicoanalyse



Traditioneel gezien, zeker voor mensen met een achtergrond binnen de manbewaking en fysieke beveiliging, is een beveiligingsplan een opsomming van beveiligingsmaatregelen. Op zich zinvol, maar als in het beveiligingsplan niet beschreven staat wat het doel van een maatregel is, kan ook niet worden bepaald of de maatregel effectief en efficiënt is. Bij de weerstandanalyse wordt daarom ook altijd gekeken of duidelijk is wat het doel van een beveiligingsmaatregel is. Pas daarna kan, als naar de werking wordt gekeken, echt een uitspraak worden gedaan over de effectiviteit van de maatregel en over de eventuele risico's die niet door de maatregel worden afgedekt. Een mooi voorbeeld, om duidelijk te maken hoe belangrijk het is om het doel van een maatregel helder voor ogen te hebben, is de discussie 'toegangsverlening of toegangscontrole'. Als in een beveiligingsplan staat dat het doel van een (fysieke)beveiligingsmaatregel is dat alleen bevoegden een organisatie mogen betreden dan is het plaatsen van een tourniquet met paslezer niet voldoende. De paslezer waar een gebruiker een pas kan aanbieden (als elektronische sleutel), om via de tourniquet toegang te krijgen, controleert immers alleen de aangeboden sleutel. Dat betekent dat er sprake is van 'toegangsverlening' op het moment dat de juiste sleutel wordt aangeboden. De doelstel-

ling was echter dat 'alleen bevoegden de organisatie' mogen betreden. Dat betekent dat gecontroleerd zal moeten worden of 'de persoon' met de sleutel bevoegd is. Gevolg daarvan is dat naast een paslezer ook gebruik gemaakt zal moeten worden van biometrie. Bij hoeveel organisaties wordt er in het beveiligingsplan gesproken over toegangscontrole, terwijl de maatregel die getroffen is niet meer is dan toegangsverlening? Een hiaat in opzet en werking. Belangrijk is daarom dat in het beveiligingsplan de daadwerkelijke 'doelen' van de maatregelen goed opgeschreven en voor wat betreft de consequenties doordacht zijn. Staan in het beveiligingsplan, per maatregel, geen duidelijke doelen omschreven, dan is er sprake van een kwetsbaarheid.

Beveiligingsinstructies

Pas als een beveiligingsbeleid voorhanden is, de beveiligingsorganisatie is ingericht, taken en verantwoordelijkheden duidelijk zijn, er effectieve beveiligingsmaatregelen staan beschreven en gekeken wordt naar doel en middel, is het zinvol om ook te kijken naar de instructies die er voor de (uitvoerende) medewerkers zijn. De werkelijkheid is immers weerbarstig en doet zich altijd anders voor dan wij verwachten. Pas als de fundering en het geraamte van het 'beveiligingsbouwwerk' staan, kan op operationeel niveau maatwerk worden geleverd. Belangrijk bij het kijken naar de instructies is het bepalen van de ruimte die er is om af te wijken van de standaard. Daarnaast is het van belang om, daar waar zich afwijkingen kunnen voordoen, te bepalen of het bouwwerk robuust genoeg is om deze afwijkingen te kunnen opvangen. Worden al deze vragen positief beantwoord, dan zegt dit iets over de weerstand van de organisatie tegen (be)dreigingen. Belangrijk is daarbij om in het achterhoofd te houden dat ook opleiding en training van medewerkers een weerstand verhogende maatregel is. Wij willen op dit aspect nog wel eens besparen en zijn dan verbaasd op het moment dat '*the shit hits the fan*', het toch even anders loopt dat verwacht, en misschien gehoopt. De weerstandanalyse neemt wel al deze aspecten mee. Het is belangrijk om, voor een goede risicoafweging, ook inzicht te hebben in opleiding en trainingseisen.

Aan de slag

Rest de vraag, hoe voer ik nu daadwerkelijk een weerstandanalyse uit? Belangrijk is dat u zelf bepaalt welke aspecten u in de analyse wilt meenemen. Mocht u de analyse voor de eerste keer uitvoeren, dan is het zinvol om u alleen tot de hoofdpunten te beperken die u inzicht geven in de

huidige stand van zaken van uw beveiligingsorganisatie. Wees daarbij vooral pragmatisch en bewaar het tot in detail uitwerken van het instrument security scan (opzet) en security survey (werking) voor een latere fase. Realiseer dat het wiel niet opnieuw hoeft te worden uitgevonden. Om inzicht te krijgen in de huidige beveiligingssituatie van de organisatie is slechts een goede vragenlijst nodig die u vervolgens gaat doorlopen. Zowel 'De Haagse Methodiek' alsook de 'code voor informatiebeveiliging' kan een prima uitgangspunt zijn voor wat betreft de te stellen vragen. Pas de vragenlijst aan uw situatie aan en wees vooral kritisch. Een vraag kan niet met 'Ja' worden beantwoord als er geen bewijs voorhanden is. En bewijs is in dit geval alleen een 'vastgesteld' en 'geldig' document. Als u de vraag 'is er een beveiligingsplan voorhanden?' positief beantwoordt, terwijl in het beveiligingsplan dat in 2004 is vastgesteld staat dat het twee jaar geldig is, neemt u alleen u zelf in de maling. Dit positieve antwoord zal vrijwel zeker niet leiden tot een ingerichte beveiligingscyclus waarbij u tegen uw algemeen directeur of voorzitter van de raad van bestuur kunt zeggen dat hij '*in control*' is.

Literatuur

Broder, J.F. (2000) *Risk Analysis and the Security Survey*, Boston: Butterworth-Heinemann / member of the Reed Elsevier Group.
Claes, P.F. en Meerman, H.J.J.M. (1998) *Riskmanagement; inleiding tot het risicobeheersingsproces*, Houten: Stenfert Kroese.
Coumou, C. (2003) *Risicomanagement voor security- en facilitymanagers*, Alphen aan den Rijn: Kluwer.
Haaf, W. ten, Bikker, H. en Adriaanse, D.J. (2002) *Fundamentals of business engineering and management*, Delft: Delft University Press.
Overbeek, P., Roos Lindgreen, E. en Spruit, M. (2000) *Informatiebeveiliging onder controle*, Amsterdam: Prentice Hall.
Pink Elephant (2001) *Syllabus ITIL Practitioner Security Management*, Utrecht: Pink Elephant Educations & Development.
Purpura, P.P. (1998) *Security and Loss Prevention*, Boston: Butterworth-Heinemann / member of the Reed Elsevier Group.
Roper, C.A. (1999) *Riskmanagement for Security Professionals*, Boston: Butterworth-Heinemann / member of the Reed Elsevier Group.
Sennewald, C.A. (1998) *Effective Security Management*, Boston: Butterworth-Heinemann / member of the Reed Elsevier Group.
Veld, J. in 't (2002) *Analyse van Organisatieproblemen; Een toepassing van denken in systemen en processen*, Groningen: Stenfert Kroese.

Risicoanalyse: samenhang tussen belang, dreiging en weerstand

Bij het uitvoeren van een bruikbare risicoanalyse is het belangrijk dat wordt gekeken naar de samenhang tussen belang, dreiging en weerstand. Hierbij zullen 'rest'-risico's moeten worden geaccepteerd. Cruciaal is dat lijnmanagers zijn geïnformeerd over deze risico's, aangezien zij verantwoordelijk zijn voor het te voeren beleid en niet de security manager.

Het succes van een risicoanalyse hangt voor een groot deel af, misschien wel voor het grootste deel, van het commitment van het (top)management. Juist omdat security management een ondersteunend proces is, en het opstellen van een risicoanalyse veelal door de security manager wordt uitgevoerd en niet door de lijnmanager, is het van belang dat het (top)management er voor zorgt dat lijnmanagers en medewerkers die niet direct bij het uitvoeren van de risicoanalyse betrokken zijn wel de benodigde informatie, ondersteuning en instemming geven. In de praktijk blijkt maar al te vaak dat de security manager niet in gesprek is met lijnmanagers en met medewerkers die een rol spelen bij de uitvoering van belangrijke handelingen binnen het bedrijfsproces. Dit terwijl het uiteindelijk de lijnmanagers zijn die verantwoordelijkheid dragen voor de voortgang van het primaire proces en de medewerkers een cruciale positie innemen als het om de uitvoering van het primaire proces gaat. Het zijn juist de medewerkers die 'handelingsperspectief hebben' als het gaat om het verstoren van het primaire proces.

Communicatie

Als er geen communicatie is tussen de security manager en de bij het primaire proces betrokken personen, ontstaan problemen op het moment dat beveiligingsmaatregelen worden getroffen. Draagvlak blijkt dan te ontbreken en alle voorbereidende activiteiten blijken verspilde energie te zijn geweest. Bovendien wordt dan ook het vaak bestaande beeld weer bevestigd dat de security manager geen serieus te nemen gesprekspartner is, omdat hij niet weet wat de belangen zijn binnen het primaire proces. Lijnmanagers en de medewerkers binnen het primaire proces die handelingsperspectief hebben, dienen te worden betrokken bij iedere

stap van de risicoanalyse. Al is het maar door (deel)producten ter instemming aan te bieden. Dit betekent ook dat, wil een lijnmanager 'voeling' krijgen met het onderwerp 'risicoanalyse', hij niet geconfronteerd moet worden met een summier schema waarin '+' en '-' staan, of niet te begrijpen getallen. Er zal door de security manager een goed en doordacht verhaal moeten worden gepresenteerd dat aansluit bij de organisatiecultuur. Geen denken meer in een vast 'format', maar denken in 'te nemen en te communiceren stappen' is dan een vereiste.

Stappen risicoanalyse

Een goede kwalitatieve risicoanalyse brengt de (deel)onderwerpen belang, dreiging en weerstand met elkaar in verband. Er kunnen immers pas effectieve beveiligingsmaatregelen worden getroffen als duidelijk is welke belangen de organisatie wil beschermen, welke (be)dreigingen deze organisatiebelangen kunnen aantasten en wat de huidige weerstand is tegen deze benoemde bedreigingen. Pas als deze vragen zijn beantwoord kan een uitspraak worden gedaan over de risico's die de organisatie eventueel loopt. Vervolgens zal ook, mocht de weerstand tegen bedreigingen onvoldoende zijn, uit de risicoanalyse voortvloeien dat er aanvullende beveiligingsmaatregelen dienen te worden genomen. Immers, als de weerstand onvoldoende is en het management heeft aangegeven dat bepaalde organisatiebelangen bescherming behoeven, kan er niet achterover worden geleund. Tenzij het (top)management aangeeft dat bij nader inzien bepaalde belangen toch niet belangrijk genoeg zijn om te worden beschermd. Ook kan het management besluiten het risico dat zich voordoet, omdat de weerstand niet voldoende is afgezet tegen de geïdentificeerde dreigingen, te accepteren. In beide gevallen kan de security manager, mocht een dreiging opportuun worden, niets verweten worden. Het valt de security manager wel te verwijten als het management, achteraf gezien, verkeerde keuzes heeft gemaakt omdat de door hem verstrekte informatie onjuist of onvolledig was. Het is cruciaal alle stappen die bij het uitvoeren van een risicoanalyse worden genomen ook daadwerkelijk te nemen en te beschrijven.

Belangen

De eerste te beantwoorden vraag is 'welke belangen van de organisatie dienen te worden beschermd'? Het middel om deze vraag te beantwoorden is het uitvoeren van een belangenanalyse. Belangrijk is dat daarbij in het achterhoofd wordt gehouden dat de security manager geen antwoord



op deze vraag kan geven. Dit kunnen alleen lijnmanagers die verantwoording dragen voor het primaire proces. Het doel van de belangenanalyse is om inzichtelijk te krijgen wat de primaire processen binnen de organisatie zijn en welke van deze processen vitaal zijn voor het voortbestaan van de organisatie. Als het uitvallen van een proces ten koste kan gaan van het vertrouwen dat de buitenwereld in de organisatie heeft, kan ook het 'aspect imago' maken dat een proces als vitaal wordt gezien. Op het moment dat duidelijk is welke processen binnen de organisatie vitaal zijn is het ook belangrijk om inzichtelijk te maken wat de zogenaamde 'vitale knooppunten' binnen deze processen zijn. Een 'vitaal knooppunt' is die plek in het proces dat, mocht het worden aangevallen en worden uitgeschakeld, het hele proces kan stilleggen. Dit 'vitale knooppunt' is dan, uit het oogpunt van de belangenanalyse, het ultieme te beschermen belang van de organisatie. Het moge duidelijk zijn dat, gezien de informatie die de belangenanalyse bevat, er ook een strikt (informatie)beveiligingsbeleid moet worden opgezet. Kort door de bocht, als de belangenanalyse op een bedrijfsnetwerk staat en het netwerk is gekoppeld aan internet, dan weet de hele buitenwereld wat de kroonjuwelen zijn van dat bedrijf. Als de belangen maar groot genoeg zijn, zullen door professionele kwaadwillenden kosten nog moeite worden gespaard om bij deze informatie te komen.

Dreiging

De tweede te beantwoorden vraag is welke bedreigingen de vastgestelde organisatiebelangen daadwerkelijk kunnen aantasten? Als het goed is heeft de security manager, juist voor de beantwoording van deze vraag, een dreiginganalyse opgesteld. Waar deze zich veelal beperkt tot het noemen van mogelijke (be)dreigers en ook aangeeft wat de motivatie en capaciteit van (be)dreigers is om de organisatiebelangen aan te tasten (scenario), gaat de risicoanalyse een stap verder. Er zal nu, om te kunnen bepalen of er sprake is van voldoende weerstand, ook moeten worden aangegeven op welke wijze een (be)dreiging zich kan manifesteren. Dit

betekent dat er een pad-analyse moet worden gemaakt. Per vitaal proces en vitaal knooppunt zal moeten worden aangegeven welke (be)dreiger de motivatie en de capaciteit heeft om het 'te beschermen organisatiebelang' aan te tasten. Vervolgens dient ook beschreven te worden hoe deze 'tegenstander' te werk zal gaan als hij besluit de organisatie aan te vallen. Bij het opstellen van deze pad-analyse is het cruciaal dat alle mogelijkheden worden meegenomen. Door het op voorhand weglaten van (be)dreigers, of het niet meenemen van scenario's en de uitwerking daarvan in een pad-analyse, kan een onjuist beeld ontstaan. Het (top)management kan dan de verkeerde keuze maken. Mocht als gevolg daarvan een (be)dreiging opportuun worden, dan is de eindverantwoordelijke manager daarop aan te spreken en niet de security manager, omdat deze de dreiging bij het opstellen van de risico-analyse achterwege heeft gelaten.

Weerstand

Pas als duidelijk is welke vitale processen en vitale knooppunten bescherming nodig hebben en inzichtelijk is welk pad eventuele (be)dreigers aflopen om de organisatiebelangen aan te vallen, is het zinvol om te kijken naar de huidige weerstand (beveiliging) van de organisatie tegen een eventuele aanval. Er zal iets gezegd moeten worden over de 'effectiviteit' van de reeds getroffen beveiligingsmaatregelen. Dit impliceert dat per getroffen (beveiligings)maatregel sprake moet zijn van een specifieke, meetbare, acceptabele, realistische en tijdsgebonden 'doeltoestand' (SMART-principe). Is niet herleidbaar wat een organisatie met de inzet van een beveiligingsmiddel wil bereiken, dan kan ook niet worden gezegd dat de weerstand tegen de benoemde (be)dreigingen voldoende is. Als per ingezet beveiligingsmiddel wel duidelijk is wat 'de doeltoestand' is, dan is het wel mogelijk om een uitspraak te doen en de vraag te beantwoorden of de weerstand van de organisatie tegen een dreiging voldoende is. Uitgaande van het feit dat er veel ontwikkelingen in de samenleving zijn en tegenstanders zich voortdurend blijven professionaliseren, is het haast onmogelijk dat de weerstand van de organisatie tegen (be)dreigingen altijd het niveau heeft wat wij graag zouden willen. Dit is echter geen enkel probleem zolang de risicoanalyse en de onderliggende pad-analyse, regelmatig tegen het licht worden gehouden. Bij het constateren van een nieuw risico kan het lijnmanagement immers besluiten om dit te accepteren. Daar is niets mis mee. Of het lijnmanagement kiest, afhankelijk van de situatie, wel voor het treffen van aanvullende beveiligingsmaatregelen. Met goede adviezen van de security manager kunnen dan juiste

keuzes worden gemaakt. Een security manager die het advies geeft een risico te accepteren op basis van een goede onderbouwing, wordt als volwaardige gesprekspartner gezien.
Onderdeel van de risicoanalyse is ook de keuze om, vanwege een te lage weerstand tegen de (be)dreigingen op basis van de in de pad-analyse inzichtelijk geworden modus operandus, aanvullende beveiligingsmaatregelen te nemen. De uitgangspunten zullen wel duidelijk vastgelegd moeten zijn, zeker bij het treffen van aanvullende beveiligingsmaatregelen die geld gaan kosten. Voor wie zeker wil weten dat alleen geautoriseerde personen de organisatie kunnen betreden voldoet het beveiligingsmiddel automatische toegangsverlening door middel van alleen een badge niet. Er zal dan ook controle van de identiteit van de aanbieder van de badge moeten plaatsvinden (biometrie). Komt ook als eis naar voren dat alleen 'bevoegde personen' toegang tot de lokatie hebben waar zich vitale processen en vitale knooppunten bevinden, dan komt ook het onderwerp zonering naar voren, waarbij weer de discussie toegangsverlening of toegangscontrole dient plaats te vinden. Vervolgens kan, als uit de pad-analyse het aspect 'infiltratie' naar voren komt, screening van personeel noodzakelijk blijken. Maatregelen hangen dus altijd samen.

Accepteren rest-risico's

Uiteindelijk zal er altijd sprake zijn van het accepteren van zogenaamde 'rest'-risico's. Er is altijd een punt waarop van de organisatie redelijkerwijs niet meer verwacht kan en mag worden dat er aanvullende beveiligingsmaatregelen worden genomen, ook al zijn de 'te beschermen belangen' nog zo groot. Bovendien kan blijken dat voor bepaalde in pad-analyses uitgewerkte scenario's geen redelijkerwijs te treffen beveiligingsmaatregelen mogelijk zijn. Dit kan liggen in het 'kostenaspect' dat niet meer in verhouding staat tot de te verwachten baten, maar kan ook voortkomen uit het feit dat een organisatie bepaalde bevoegdheden niet heeft. Zo is het uitvoeren van veiligheidsonderzoeken voorbehouden aan de AIVD. Ook zijn er in Nederland slechts een aantal bedrijven die justitie mogen bevragen uit hoofde van een toegekende bevoegdheid om zelfstandig 'antecedentenonderzoeken' te mogen uitvoeren.
De conclusie is dat altijd risico's zullen worden geaccepteerd en dat ook altijd rest-risico's blijven bestaan. Daar is niets mis mee. Het is echter wel belangrijk dat de keuzes door de juiste personen worden gemaakt op basis van juiste en volledige informatie. Daarvoor moet een goede uitvoering van de risicoanalyse garant staan. En daar schort het in de praktijk

wel eens aan. Op zich is het niet erg als een organisatie besloten heeft niet te willen weten welke risico's zij loopt. Dat maakt het leven weer iets spannender en geeft inhoud aan het begrip '*carpe diem*'.

Hoe nu verder?

Belangrijk is om, voor zo ver mogelijk, het aspect 'toeval' binnen ons vakgebied uit te bannen. Vrijwel niemand zal een risicoanalyse op de plank hebben liggen die aan alle vereisten voldoet zoals die in dit hoofdstuk zijn beschreven. Het is daarom zaak om te beginnen met het beschrijven en inrichten van een security management proces, zodat uiteindelijk alle noodzakelijke stappen worden genomen om tot een goede kwalitatieve risicoanalyse te komen. Het is logisch te beginnen op organisatieniveau, en pas daarna in te dalen tot (bedrijfs)procesniveau. Begin steeds klein, maar neem de te nemen stappen wel in de juiste volgorde. Is een organisatie nog niet klaar voor het uitvoeren van een volledige kwalitatieve risicoanalyse op organisatie of procesniveau, begin dan met het opstellen van een eenvoudiger risicoprofiel. Een gesprek met het lijnmanagement over dit risicoprofiel kan dan op termijn leiden tot voldoende draagvlak om tot een volwaardige risicoanalyse te komen.

Literatuur

Broder, J.F. (2000) *Risk Analysis and the Security Survey*, Boston: Butterworth-Heinemann / member of the Reed Elsevier Group.
Claes, P.F. en Meerman, H.J.J.M. (1998) *Riskmanagement; inleiding tot het risicobeheersingsproces*, Houten: Stenfert Kroese.
Coumou, C. (2003) *Risicomanagement voor security- en facilitymanagers*, Alphen aan den Rijn: Kluwer.
Haaf, W. ten, Bikker, H. en Adriaanse, D.J. (2002) *Fundamentals of business engineering and management*, Delft: Delft University Press.
Overbeek, P., Roos Lindgreen, E. en Spruit, M. (2000) *Informatiebeveiliging onder controle*, Amsterdam: Prentice Hall.
Purpura, P.P. (1998) *Security and Loss Prevention*, Boston: Butterworth-Heinemann / member of the Reed Elsevier Group.
Roper, C.A. (1999) *Riskmanagement for Security Professionals*, Boston: Butterworth-Heinemann / member of the Reed Elsevier Group.
Sennewald, C.A. (1998) *Effective Security Management*, Boston: Butterworth-Heinemann / member of the Reed Elsevier Group.
Veld, J. in 't (2002) *Analyse van Organisatieproblemen; Een toepassing van denken in systemen en processen*, Groningen: Stenfert Kroese.

De inrichting van het proces security management

De uitdrukking ´een aantal activiteiten is nog geen proces´ gaat natuurlijk ook op voor het werkveld van security manager. Om achteraf als security manager te kunnen verklaren waarom bepaalde (beveiligings)maatregelen zijn getroffen, en ook waarom er verschillende (beveiligings)activiteiten worden uitgevoerd, zal de security manager er voor moeten zorgen dat het proces ´security management´ waar hij voor verantwoordelijk is op een transparante manier is ingericht.

Binnen een ingericht proces 'security management' kan het niet voorkomen dat er maatregelen op het vlak van beveiliging getroffen zijn waarvan niemand binnen de organisatie meer weet waarvoor deze dienen. Dit werpt de vraag op hoe het proces 'security management' er dan precies uitziet. En welke stappen moet de security manager nemen om het proces 'security management' in te richten?

De beveiligingscyclus

In eerste instantie moet duidelijk zijn wat de missie, de visie en de ambitie van de organisatie is als het gaat om het onderwerp beveiliging. Deze uitgangspunten dienen dan ook door het (top)management te worden vastgelegd, op strategisch niveau, in een beveiligingsbeleid. Vervolgens zal het (top)management ook, als het fundament voor de te treffen beveiligingsmaatregelen op strategisch niveau duidelijk is, een uitspraak moeten doen over de af te dekken risico´s. Dit betekent dat de security manager een risicoanalyse moet opstellen en deze ter vaststelling aan het (top) management moet voorleggen. Pas als er duidelijke uitgangspunten in een strategisch beleidsplan zijn vastgelegd, en het (top)management zich heeft uitgesproken over de af te dekken risico's in de vorm van een risicoanalyse, kan de security manager een daadwerkelijk beveiligingsplan op tactisch en operationeel niveau opstellen. Om te komen tot een 'gesloten kwaliteitscirkel', ter borging van het proces 'security management' en ook als garantie dat de organisatie zich voortdurend blijft verbeteren, dient er structureel een kwaliteitscontrole plaats te vinden. Dit kan door een security scan, een security survey of een security audit uit te (laten) voeren.



Deze kwaliteitscontrole geeft dan vervolgens input die kan leiden tot bijstelling van het beveiligingsbeleid, de risicoanalyse en het beveiligingsplan. Simpel gezegd, als deze stappen achter elkaar worden genomen en er ook daadwerkelijke borging heeft plaatsgevonden, is er sprake van een ingerichte beveiligingscyclus. Veel moeilijker hoeft het niet te zijn.

Het Beveiligingsplan

De basis voor het beveiligingsplan, op tactisch niveau, wordt gelegd in het beveiligingsbeleid en in de risicoanalyse. Het kan immers niet zo zijn dat er beveiligingsmaatregelen getroffen worden die niet direct te relateren zijn aan onderkende (be)dreigingen en in de risicoanalyse genomen beslissingen door het (top)management. Op tactisch niveau dient het beveiligingsplan antwoord te geven op de vraag welke (deel)processen de security manager binnen het proces 'security management' kan inzetten om de doelstellingen, die zijn vastgesteld in het beveiligingsbeleid, te realiseren. In het beveiligingsplan op het tactische niveau wordt nog geen uitspraak gedaan over concreet in te zetten organisatorische-, bouwkundige-, elektronische-, personele- en ICT (beveiligings) maatregelen. Per (deel)proces zal duidelijk moeten worden beschreven wat de doelstelling van het (deel)proces is, hoe taken en verantwoordelijkeden belegd zijn, welke functionarissen nodig zijn om het (deel)proces uit te voeren en hoe meetbaar is of de doelstelling van het (deel)proces is gehaald. Pas als duidelijk is hoe de verschillende (deel)processsen binnen het proces

security management zijn ingevuld kan er een vertaling worden gemaakt naar een beveiligingsplan op operationeel niveau. Zowel het tactische beveiligingsplan, alsook het operationele beveiligingsplan, zijn beide organisatorische beveiligingsmaatregelen. Als over het beveiligingsplan op tactisch niveau gesproken wordt heeft men het ook wel over de grote 'O'.

Beveiligingsmaatregelen

Op operationeel niveau heeft de beveiligingsorganisatie ook de beschikking over organisatorische (beveiligings)maatregelen. Ook wel de kleine 'o' genoemd. Hierbij moet dan vooral gedacht worden aan (werk)instructies voor beveiligingsfunctionarissen. Daarnaast kunnen er op operationeel niveau ook bouwkundige, elektronische, personele en ICT maatregelen worden ingezet. Belangrijk is om, voordat een keuze gemaakt wordt voor het inzetten van specifieke (beveiligings)maatregelen, helder te hebben wat het uitgangspunt is voor de inzet van deze maatregelen. Zijn maatregelen belangrijker dan mensen of staan deze maatregelen mensen bij de uitvoering van de hen toebedeelde taak ten dienste. Vaak is het nog zo dat beveiligingsfunctionarissen geconfronteerd worden met getroffen (beveiligings) maatregelen die door een manager in een ivoren toren bedacht zijn. Zij – de beveiligingsmedewerkers – moeten dan 'maar zien' hoe er met de maatregelen omgegaan moet worden. Als de mens echter het uitgangspunt is, is het ook deze mens die zelf aangeeft welke functionaliteiten (maatregelen) hij nodig heeft om zijn taak goed uit te kunnen voeren. Daar dient dan door de organisatie wel rekening mee gehouden te worden. Vaak hoor ik collega's zeggen dat het niveau van 'de beveiligingsmedewerker' onder de maat is en dat voorkomen moet worden dat deze mensen 'zelfstandig gaan denken en beslissingen gaan nemen'. Wat mij betreft is dit een slechte basis voor de inrichting en opzet van een beveiligingsorganisatie. Doelstellingen zullen dan zeker niet worden gehaald. Ik maak mij hard voor het inzet van 'de mens' als denkend wezen. Dit betekent dat als eerste ingezet zal moeten worden op training en opleiding van deze mens. Veelal blijkt deze mens namelijk, als hij serieus genomen wordt, een 'goed gemotiveerde vakman of vakvrouw' te zijn. Het ontwikkelen van beveiligingsmedewerkers is een, helaas vaak (bewust) vergeten, beveiligingsmaatregel.

Stap voor stap

Het beveiligingsplan begint met de organisatorische beveiligingmaatregelen op tactisch niveau en op operationeel niveau, de zogenaamde

grote 'O' en kleine 'o'. Dan komen de bouwkundige beveiligingsmaatregelen. Vervolgens komen ook de elektronische beveiligingsmaatregelen, de personele beveiligingsmaatregelen en de ICT beveiligingsmaatregelen aan de orde. Tot slot zijn er twee vormen van (kwaliteits)controle. De security scan en de security survey.

Samenhang

Wat vooral belangrijk is, is om steeds de samenhang te blijven zien tussen de verschillende soorten beveiligingsmaatregelen. De risicoanalyse, waar de weerstandanalyse onderdeel van is, heeft immers laten zien dat het manifest worden van een dreiging wordt tegengegaan door het samenspel van alle te treffen (beveiligings)maatregelen. Vaak zie ik in de praktijk nog dat het bij het realiseren van beveiligingsmaatregelen lijkt of iedere maatregel op zich voldoende weerstand moet bieden tegen een dreiging. Niets is minder waar. Door juist aandacht te hebben voor synergie kan één en één drie worden. Van 'alles iets minder' geeft dan toch een optimaal resultaat. En dat willen wij als security professionals toch? Er is geen enkele reden om bij voortduring te blijven streven naar een maximaal resultaat. Kosten en baten zijn dan niet meer in verhouding.

Literatuur

Broder, J.F. (2000) *Risk Analysis and the Security Survey*, Boston: Butterworth-Heinemann / member of the Reed Elsevier Group.
Claes, P.F. en Meerman, H.J.J.M. (1998) *Riskmanagement; inleiding tot het risicobeheersingsproces*, Houten: Stenfert Kroese.
Coumou, C. (2003) *Risicomanagement voor security- en facilitymanagers*, Alphen aan den Rijn: Kluwer.
Haaf, W. ten, Bikker, H. en Adriaanse, D.J. (2002) *Fundamentals of business engineering and management*, Delft: Delft University Press.
Overbeek, P., Roos Lindgreen, E. en Spruit, M. (2000) *Informatiebeveiliging onder controle*, Amsterdam: Prentice Hall.
Purpura, P.P. (1998) *Security and Loss Prevention*, Boston: Butterworth-Heinemann / member of the Reed Elsevier Group.
Roper, C.A. (1999) *Riskmanagement for Security Professionals*, Boston: Butterworth-Heinemann / member of the Reed Elsevier Group.
Sennewald, C.A. (1998) *Effective Security Management*, Boston: Butterworth-Heinemann / member of the Reed Elsevier Group.
Veld, J. in 't (2002) *Analyse van Organisatieproblemen; Een toepassing van denken in systemen en processen*, Groningen: Stenfert Kroese.

Organisatorische beveiligingsmaatregelen

De basis voor alle 'organisatorische beveiligingsmaatregelen' is het committment van het (top)management. Voor het verkrijgen hiervan zijn twee uitgangspunten voor de security manager belangrijk om in de gaten te houden. Het eerste uitgangspunt is 'hou het simpel'. Het tweede uitgangspunt is, en dit heeft betrekking op de te treffen maatregelen en de uit te voeren activiteiten, 'net genoeg'. Uiteindelijk gaat het immers om het bereiken van een niveau van optimale beveiliging, niet van maximale beveiliging. Kosten en baten moeten altijd in verhouding staan.

Steeds vaker lopen security managers aan tegen het verschijnsel dat er geen draagvlak binnen de eigen organisatie is voor het onderwerp beveiliging. Een mogelijke oorzaak is dat het voor de organisatie niet duidelijk is waarom bepaalde beveiligingsmaatregelen worden getroffen en wat het nut is van bepaalde activiteiten die worden uitgevoerd. Bij nader onderzoek blijkt dan veelal dat er geen ´sponsor´ voor het onderwerp security management binnen het (top)management aanwezig is. En als er al wel een duidelijke toewijzing van de portefeuille binnen het (top) management heeft plaatsgevonden, is er meestal wel iets te zeggen over de transparantie waar een security manager mee te werk gaat. Als de portefeuillehouder binnen het (top)management niet weet wat er speelt en geen zicht heeft op de werkzaamheden en activiteiten van de security manager, blijft begrip en draagvlak natuurlijk ook uit. En dat lijkt mij niet wenselijk. De basis voor alle 'organisatorische beveiligingsmaatregelen' is immers uiteindelijk het committment van het (top)management. Om dit committment te krijgen zijn twee uitgangspunten belangrijk om in de gaten te houden. Het eerste uitgangspunt is 'houd het simpel'. Het tweede uitgangspunt, wat betrekking heeft op de te treffen beveiligingsmaatregelen, is 'net genoeg'. Uiteindelijk gaat het immers om het bereiken van een niveau van optimale beveiliging, niet van maximale beveiliging.

Strategisch niveau

De belangrijkste organisatorische maatregel is het door het (top)management vastgestelde en binnen de organisatie uitgedragen beveiligingsbe-



leid. In het 'strategische' beleidsdocument zal een relatie gelegd moeten worden tussen de algemene bedrijfsdoelstellingen en de doelstelling van het proces security management. De centrale vraag daarbij is 'wat is de bijdrage die van beveiliging wordt verwacht?', als het gaat om het creëren van een veilige en beveiligde (werk)omgeving. Het proces beveiliging dient immers een bijdrage te leveren aan de primaire bedrijfsprocessen. Niet andersom. Beveiliging op zich is geen doel. In het beveiligingsbeleid zal daarom ook vastgelegd moeten worden wat het ambitieniveau van de organisatie is als het gaat om het afwenden van (be)dreigingen. Met andere woorden, waar houdt het op en wanneer wordt geaccepteerd dat kosten en baten niet meer in verhouding staan als het gaat om het treffen van beveiligingsmaatregelen? Ook zal iets gezegd moeten worden over de verschillende deelprocessen die de security manager ter beschikking heeft om de aan hem toebedeelde taken te kunnen uitvoeren. Zo zullen er organisaties zijn waar het belangrijkste deelproces gericht is op toegangs-

verlening tot de organisatie, waarbij het uitgangspunt is dat onbevoegden in beginsel niet binnen mogen komen. Daar waar het gezien het (open) karakter van een organisatie niet mogelijk is onbevoegden buiten te houden, zoals bijvoorbeeld bij een ziekenhuis of een winkelcentrum, zal het belangrijkste deelproces gericht zijn op het houden van toezicht. Immers daar waar iedereen in beginsel welkom is kan pas actie worden ondernomen als duidelijk wordt dat een persoon ongewenst gedrag vertoont. Verder zal iedere organisatie, onafhankelijk van het karakter van de organisatie, deelprocessen hebben waarbinnen 'alarmverificatie' en 'incidentopvolging' plaatsvinden. Welke deelprocessen er verder ook denkbaar zijn, de basis voor de inzet van deze deelprocessen moet gelegd zijn op strategisch niveau. In het kader van de transparantie van een deelproces is het wenselijk om in het beveiligingsbeleid expliciet te stellen dat er alleen beveiligingsmaatregelen kunnen worden getroffen op operationeel niveau als deze voortkomen uit een beschreven (tactisch) deelproces en als deze een directe relatie hebben met het (strategische) proces 'risico's analyseren'. Ik zal nu niet verder ingaan op het onderwerp risicoanalyse. Wel belangrijk is het proces risicoanalyse duidelijk te positioneren. Het beste als een strategisch deelproces omdat dit proces input geeft aan al de beschreven beveiligingsprocessen op tactisch niveau.

Tactisch niveau

Op dit niveau komen wij de beschrijving van de daadwerkelijke deelprocessen tegen die de security manager ter beschikking staan voor het realiseren van de aan het proces security management gegeven opdracht. Per deelproces zal in een (tactisch)beveiligingsplan beschreven moeten worden wat de doelstelling is en op welke wijze het deelproces wordt ingezet. Ook zal nagedacht moeten worden, uitgaande van 'meten is weten', wat de benodigde normen en indicatoren zijn om achteraf een uitspraak te kunnen doen over de effectiviteit van het deelproces. Iedere organisatie zal, ook met inachtneming van de bedrijfscultuur, naar een 'eigen vorm' voor dit (tactische) beveiligingsplan moeten zoeken. De term 'maatwerk' is hier op zijn plaats. Wil er voldaan kunnen worden aan de eis van draagvlak en transparantie dan is 'plakken en knippen' geen optie. Er zal tijd vrijgemaakt moeten worden om met een groep mensen, die bij het onderwerp beveiliging betrokken zijn, stap voor stap de deelprocessen uit te werken. Alleen dan is de garantie dat er voldoende draagvlak kan worden gecreëerd en transparantie kan worden gewaarborgd, te geven. Ook belangrijk is het benoemen van de op het operationeel niveau

benodigde plannen, richtlijnen en procedures om het uiteindelijke werk wat uit een deelproces voortkomt te kunnen uitvoeren. Op tactisch niveau zullen de randvoorwaarden moeten worden gecreëerd zodat de benodigde documenten er ook daadwerkelijk komen. Benoem de documenten daarom ook meteen in het (tactische) beveiligingsplan. Als de organisatie geen tijd en middelen wil vrijmaken om de deelprocessen goed te kunnen inzetten en er voor te zorgen dat de benodigde documenten er komen, moet dat nu duidelijk worden. Het is onwenselijk als er op operationeel niveau energie verloren gaat aan het voeren van deze discussie. Vragen die nu ter beantwoording op tafel moeten komen te liggen zijn 'wie is er verantwoordelijk voor de uitvoering van de verschillende taken binnen een deelproces?' en 'wat is er nodig om een deelproces goed uit te kunnen voeren?'. Hier wordt bijvoorbeeld de basis gelegd voor het vrijmaken van geld en middelen om een goed (nieuw) sluitplan op te zetten en te implementeren, maar ook voor het feit dat activiteiten binnen deelprocessen alleen kunnen plaatsvinden op basis van – door nader gespecificeerde – door het (top)management vastgestelde richtlijnen.
De praktijk bewijst vaak uit dat deze richtlijnen er alleen komen als op voorhand duidelijk is wie verantwoordelijk is - in de uitvoering - voor de totstandkoming van de documenten. Leg dit daarom ook meteen vast in de beschrijving van het deelproces. Dat voorkomt veel discussie achteraf.

Operationeel niveau

De uitvoering. Daar gaat het immers om. Als de security manager er op strategisch niveau in geslaagd is om duidelijke uitgangspunten en ambities vast te (laten) stellen en op tactisch niveau in het beschrijven van transparante deelprocessen, kan op operationeel niveau aan de eis voldaan worden dat altijd duidelijk is waarom specifieke beveiligingsmaatregelen worden getroffen en waarom bepaalde beveiligingsactiviteiten worden uitgevoerd. Per maatregel of activiteit zal er, voor de uitvoerende beveiligingsmedewerker, een duidelijke instructie moeten zijn waarin beschreven wordt wat er wanneer van hem of haar verwacht wordt. Deze instructie zal ook een 'doelstelling' moeten hebben. Ook voor de uitvoerende medewerker moet duidelijk zijn waarom de specifieke maatregel of activiteit nodig is. Bovendien is deze transparantie een noodzakelijke voorwaarde voor de beveiligingsmedewerker om, als de maatregel wegvalt of de activiteit niet kan worden uitgevoerd, te bepalen wat de alternatief in te zetten maatregelen of activiteiten zijn. Ik durf de stelling aan dat in 98 procent van de gevallen, waarin op operationeel niveau 'fouten'

zijn gemaakt, dit direct voortkomt uit het feit dat het voor de betreffende medewerker niet duidelijk was wat de doelstelling van een maatregel of activiteit was. En waarom niet? Omdat het deelproces niet transparant is ingericht en het management heeft verzuimd om aan de betreffende medewerker het 'hoe en waarom' van maatregelen en activiteiten uit te leggen. En daar zijn we weer terug bij een eerdere stelling. De mens, en zeker de beveiligingsmedewerker op het uitvoerende niveau, blijkt vaak niet het uitgangspunt voor de security manager. Immers, deze man of vrouw moet niet teveel vrijheid krijgen om zelf afwegingen te kunnen maken. Want juist dan gaat het fout. Ik ben van mening dat het alleen fout gaat als deze mens vanuit het deelproces waarbinnen hij of zij ingezet wordt niet de benodigde kennis en vaardigheden meekrijgt. Het vak beveiligen brengt nu eenmaal met zich mee dat het uiteindelijk altijd om de mens gaat die beslissingen neemt. De techniek denkt niet, de techniek weegt opties niet af en de techniek laat het vaak afweten als het er echt op aan komt. Daar zorgt onze lieve vriend Murphy wel voor. De security manager zou wat meer vertrouwen moeten hebben in de (vak)mensen op de werkvloer. Een prachtige organisatorische beveiligingsmaatregel lijkt mij.

Literatuur

Broder, J.F. (2000) *Risk Analysis and the Security Survey*, Boston: Butterworth-Heinemann / member of the Reed Elsevier Group.
Claes, P.F. en Meerman, H.J.J.M. (1998) *Riskmanagement; inleiding tot het risicobeheersingsproces*, Houten: Stenfert Kroese.
Coumou, C. (2003) *Risicomanagement voor security- en facilitymanagers*, Alphen aan den Rijn: Kluwer.
Haaf, W. ten, Bikker, H. en Adriaanse, D.J. (2002) *Fundamentals of business engineering and management*, Delft: Delft University Press.
Overbeek, P., Roos Lindgreen, E. en Spruit, M. (2000) *Informatiebeveiliging onder controle*, Amsterdam: Prentice Hall.
Purpura, P.P. (1998) *Security and Loss Prevention*, Boston: Butterworth-Heinemann / member of the Reed Elsevier Group.
Roper, C.A. (1999) *Riskmanagement for Security Professionals*, Boston: Butterworth-Heinemann / member of the Reed Elsevier Group.
Sennewald, C.A. (1998) *Effective Security Management*, Boston: Butterworth-Heinemann / member of the Reed Elsevier Group.
Veld, J. in 't (2002) *Analyse van Organisatieproblemen; Een toepassing van denken in systemen en processen*, Groningen: Stenfert Kroese.

Bouwkundige beveiligingsmaatregelen

Als een security manager gevraagd wordt naar de onderbouwing van getroffen bouwkundige beveiligingsmaatregelen blijft het vaak stil. Dit is veelal ook het geval als, bij een budgetaanvraag, de vraag naar voren komt waarom juist ´die specifiek voorgestelde bouwkundige beveiligingsmaatregelen´ noodzakelijk zijn. Het op voorhand op basis van de risicoanalyse onderbouwen van bouwkundige beveiligingsmaatregelen kan achteraf veel tijd schelen. Juist transparantie is een noodzakelijke voorwaarde voor committment van het (top)management en kan budgetbesprekingen een stuk gemakkelijker maken.

Het treffen van bouwkundige beveiligingsmaatregelen is vaak een kostbare en tijdrovende aangelegenheid. Dan zou je mogen veronderstellen dat er, voordat bouwkundige beveiligingsmaatregelen getroffen worden, goed is nagedacht over het ´hoe´ en ´waarom´ van de maatregelen. Helaas is het tegendeel vaak het geval. Als een security manager gevraagd wordt naar de onderbouwing van de getroffen bouwkundige beveiligingsmaatregelen blijft het vaak stil. Dit is veelal ook het geval als bij een budgetaanvraag de vraag naar voren komt waarom juist die specifiek voorgestelde bouwkundige beveiligingsmaatregelen noodzakelijk zijn.

Onderbouwen

Mijn stelling is dat als de security manager op voorhand meer tijd zou besteden aan het onderbouwen van bouwkundige beveiligingsmaatregelen, dit achteraf veel tijd kan opleveren. Transparantie is een noodzakelijke voorwaarde voor committment van het (top)management en kan budgetbesprekingen een stuk gemakkelijker maken. Het niet toekennen van budget voor bouwkundige beveiligingsmaatregelen maakt dan namelijk ook meteen inzichtelijk welk risico niet afgedekt wordt. Vooral binnen organisaties die risico´s zoveel mogelijk willen mijden zal ´transparantie´ het leven van de security manager gemakkelijker maken. Een goede onderbouwing, met een directe relatie met de risicoanalyse, zal dan vaak committment opleveren voor het treffen van de noodzakelijke bouwkundige beveiligingsmaatregelen.

Belangrijk om vast te stellen is vanuit welk beveiligingsproces de te treffen bouwkundige beveiligingsmaatregelen worden ingezet. Bij veel organisaties komen de bouwkundige beveiligingsmaatregelen voort uit het proces ´toegangverlening´. Toegangverlening is dan vaak gedefinieerd als het proces dat (doelstelling) alleen bevoegden toegang tot de organisatie geeft en onbevoegden buiten de organisatie moet houden. Bij een dergelijke definitie vallen alle toegangscontrolemiddelen, gevelopeningen en muren onder dit werking van dit proces. Ook kan het zijn dat er nog een proces binnen de organisatie bestaat dat wordt ingezet om op incidenten te reageren. Als dit proces wordt gebruikt om incidenten zo snel mogelijk te beëindigen of om, mocht dat niet meteen mogelijk zijn, in ieder geval uitbreiding tegen te gaan, kan dit proces ook bouwkundige maatregelen noodzakelijk maken. Als deze twee beveiligingsprocessen daadwerkelijk onder de verantwoordelijkheid van de security manager vallen, spreek ik zelf liever van bouwkundige veiligheidsmaatregelen in plaats van bouwkundige beveiligingsmaatregelen. Een dergelijke ´woordkeuze´ kan er voor zorgen, hoe vreemd het ook mag klinken, dat het onderwerp door het (top)management serieuzer genomen wordt. Het woord beveiliging heeft op dit moment soms een wat negatieve lading en ´veiligheid´ is hot. Maak daar gebruik van zou ik zeggen.

Onderbouwing

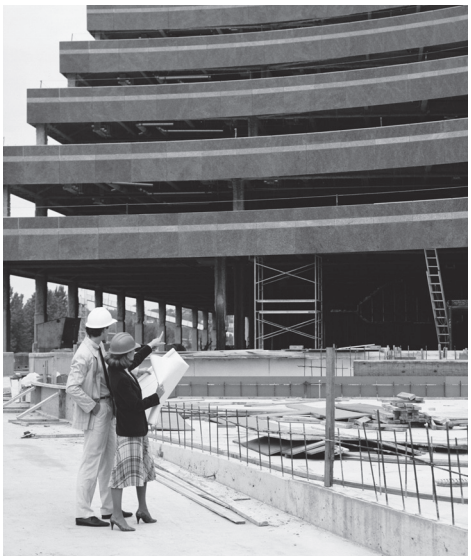
Uiteindelijk zal iedere bouwkundige beveiligingsmaatregel of liever gezegd bouwkundige veiligheidsmaatregel, als uitgegaan wordt van de eerder genoemde twee processen, verklaarbaar moeten zijn. Dit betekent dat een veiligheidsmaatregel direct te relateren moet zijn aan een in de risicoanalyse onderkende dreiging. Er zal ook duidelijk beschreven moeten zijn op welke manier een dreiging zich kan manifesteren. Pas dan kan inzichtelijk worden gemaakt welke bijdrage een bouwkundige veiligheidsmaatregel kan leveren om het risico, dat een specifieke dreiging voortkomt, te minimaliseren. Ook het veiligheidsbeleid kan, als het gaat om de ambitiebepaling, aanknopingspunten geven voor de onderbouwing van veiligheidsmaatregelen. Het vrijgeven van een fysieke barrière (toegangsverlening) door middel van het slechts aanbieden van een toegangsverleningsmiddel, zoals een toegangspas, is prima als ook onbevoegden de organisatie mogen betreden. Immers, de pas kan door een ieder worden gebruikt. Als de ambitie die in het veiligheidsbeleid staat is dat ´onbevoegden de organisatie niet mogen betreden´, kan niet volstaan worden met het gebruik van slechts een simpele toegangspas. Er zal

dan ook gezien de gestelde ambitie vastgesteld moeten worden, voordat een barrière wordt vrijgegeven, dat de persoon die de pas gebruikt ook daadwerkelijk de persoon is die bij de pas hoort. Dit vraagt om een vorm van biometrie. Immers, er zal een uniek kenmerk gecontroleerd moeten worden. Het is aan te bevelen, juist om steeds terugkerende discussie over nut een noodzaak van bouwkundige veiligheidsmaatregelen te voorkomen, eenmalig tijd te besteden aan het beschrijven en laten vaststellen van de uitgangspunten die ten grondslag liggen aan deze maatregelen.

Verlenen van toegang

De risicoanalyse kan het, gezien de tegen de organisatie gerichte dreigingen, noodzakelijk maken om beveiliging ´in de diepte´ toe te passen. In de procesbeschrijving ´toegangsverlening´ zal dan opgenomen moeten worden dat aan de inzet van bouwkundige veiligheidsmaatregelen een zoneringsmethodiek ten grondslag ligt. Deze methodiek zal dan wel beschreven moeten worden. Belangrijk is om bij de beschrijving in het oog te houden dat de algemene bedrijfsprocessen van de organisatie het uitgangspunt zijn. Het wel of niet kritische karakter van een bedrijfsproces, als gekeken wordt naar de continuïteit van de organisatie, is dan maatgevend voor het benodigde veiligheidsregime (zone). Vervolgens kan, als er sprake is van een zoneringsmethodiek, een document worden opgesteld waarin ´functionele eisen´ worden gesteld aan de toegangscontrolemid-


Foto: Boon Edam



delen, gevelopeningen en muren van de gedefinieerde zones of compartimenten. Bij toegangscontrolemiddelen kan dan gedacht worden aan de eis dat er niet meegelopen mag worden of dat een barrière pas vrijgegeven wordt als is vastgesteld dat de toegangspas en de persoon die deze gebruikt bij elkaar horen. Het heeft ook de voorkeur, voor wat betreft muren en gevelopeningen, om in het document meteen een verwijzing op te nemen naar bestaande NEN-normen. Dit kost initieel wat meer tijd, maar scheelt in de toekomst veel tijd als het proces en de eisen transparant zijn beschreven. Nieuwe vragen over de voor een bedrijfsproces benodigde veiligheidsmaatregelen kunnen dan meteen langs de opgestelde meetlat worden gelegd en snel worden beantwoord. Zodra de benodigde zone duidelijk is zijn de maatregelen dat ook. En achteraf is alles, gezien de eis van transparantie, goed uit te leggen. Wat nog belangrijk is, is dat het treffen van maatregelen ´in de diepte´ niet per definitie betekent dat er hele zware bouwkundige maatregelen worden getroffen bij hogere beveiligingszones. Als er voor het onbevoegd betreden van de eerste zone al sprake is van detectie, en er moet daarna nog toegang tot twee of drie zones worden verkregen om bij het meest kritische bedrijfsproces te komen, kan de weerstand van al deze zoneovergangen worden meegenomen om te bepalen welke ´aanvullende´ vertraging bij de hoogste zone noodzakelijk is. Logisch toch. Voorwaarde is wel een transparante beschrijving. Pas dan kan deze relatie gelegd worden.

Beheersen van incidenten

Bij het proces dat zich richt op het beheersbaar houden van incidenten moet niet alleen gedacht worden aan beveiliging. Ook safety is dan een aspect om rekening mee te houden. Vanuit de veiligheidsgedachte kunnen dan, om uitbreiding van incidenten zoals bijvoorbeeld brand tegen

te gaan, functionele eisen worden opgesteld voor te treffen bouwkundige veiligheidsmaatregelen. Sommige van deze veiligheidsmaatregelen zijn zelfs voorgeschreven door de wetgever. Deze safety-maatregelen voorkomen incidenten niet, zoals bouwkundige veiligheidsmaatregelen in het kader van toegangsverlening wel gericht zijn op het voorkomen dat onbevoegden de organisatie betreden, maar kunnen wel deel uit maken van het document waarin de ´functionele eisen´ van bouwkundige veiligheidsmaatregelen beschreven staan. Rest de vraag ´hoe ziet een dergelijk document er dan precies uit´. Helaas is deze vraag niet makkelijk te beantwoorden. Uitgaande van het specifieke karakter van een organisatie zal iedere security manager een eigen vorm moeten kiezen. Ik kom dan ook niet met een passende beschrijving van alle benodigde bouwkundige veiligheidsmaatregelen of een beschrijving van wat nu precies bouwkundige veiligheidsmaatregelen zijn. Ook zal ik geen opsomming geven van in het kader van transparantie benodigde onderbouwende documenten. Deze kennis is vaak al aanwezig bij een security manager. Het gaat om het aangeven van een mogelijke denkrichting. De uitdaging is juist dat stukje op te pakken en zelf verder uit te werken wat bruikbaar is voor uw specifieke organisatie.

Literatuur

Broder, J.F. (2000) *Risk Analysis and the Security Survey*, Boston: Butterworth-Heinemann / member of the Reed Elsevier Group.
Claes, P.F. en Meerman, H.J.J.M. (1998) *Riskmanagement; inleiding tot het risicobeheersingsproces*, Houten: Stenfert Kroese.
Coumou, C. (2003) *Risicomanagement voor security- en facilitymanagers*, Alphen aan den Rijn: Kluwer.
Haaf, W. ten, Bikker, H. en Adriaanse, D.J. (2002) *Fundamentals of business engineering and management*, Delft: Delft University Press.
Overbeek, P., Roos Lindgreen, E. en Spruit, M. (2000) *Informatiebeveiliging onder controle*, Amsterdam: Prentice Hall.
Purpura, P.P. (1998) *Security and Loss Prevention*, Boston: Butterworth-Heinemann / member of the Reed Elsevier Group.
Roper, C.A. (1999) *Riskmanagement for Security Professionals*, Boston: Butterworth-Heinemann / member of the Reed Elsevier Group.
Sennewald, C.A. (1998) *Effective Security Management*, Boston: Butterworth-Heinemann / member of the Reed Elsevier Group.
Veld, J. in 't (2002) *Analyse van Organisatieproblemen; Een toepassing van denken in systemen en processen*, Groningen: Stenfert Kroese.

Elektronische beveiligingsmaatregelen

Net zoals bij ´bouwkundige beveiligingsmaatregelen' dient de inzet van 'elektronische beveiligingsmaatregelen' voort te komen uit de beschrijving van de beveiligingsprocessen die de security manager voor de uitvoering van zijn taak ter beschikking staan. Voordat de vraag beantwoord kan worden 'welke processen dat nu eigenlijk zijn', als het gaat om de inzet van elektronische beveiligingsmaatregelen, zal eerst stilgestaan moeten worden bij de vraag 'wat bedoelen wij nu eigenlijk met het begrip elektronische beveiligingsmaatregelen'. Zelden geven security managers, die met elkaar in gesprek zijn, een zelfde antwoord op deze ogenschijnlijk simpele vraag. En dan druk ik mij nog voorzichtig uit.

De beleving bij het woord 'elektronische beveiligingsmaatregelen' was bij de invoering van de eerste beveiligingsopleidingen, begin jaren tachtig van de vorige eeuw, anders dan nu. Maar een echte bijstelling van de definitie is in de literatuur niet goed traceerbaar.
Er is natuurlijk wel wat op aan te merken, maar voor dit hoofdstuk wordt uitgegaan van de werkdefinitie dat als een security manager over elektronische beveiligingsmaatregelen spreekt, hij het over 'technische (hulp) middelen' heeft 'die de beveiligingsmedewerker bij de uitvoering van de aan hem of haar toebedeelde taak ter beschikking staan'. Met andere woorden, alle beveiligingsapparatuur die 'elektronica' bevat en van afstand bediend kan worden door beveiligingsmedewerkers, of die 'elektronische' apparatuur waarvan 'de status of het beeld' op afstand uitleesbaar is door beveiligingsmedewerkers.
Het is geen sluitende definitie, maar voor dit hoofdstuk over elektronische beveiligingsmaatregelen wel afdoende. Bij elektronische beveiligingsmaatregelen kan, uitgaande van de werkdefinitie, ondermeer gedacht worden aan op afstand bedienbare doorgangen, de inzet van verschillende soorten detectoren en de plaatsing van (observatie)camera's. Het gaat dan om de verschillende 'veldcomponenten' en niet om de complexe systemen die er aan gekoppeld kunnen zijn. Die (geautomatiseerde) systemen komen in het hoofdstuk over ICT beveiligingsmaatregelen aan de orde.

Beveiligingsplan



Belangrijk is om vast te stellen vanuit welk beveiligingsproces elektronische beveiligingsmaatregelen worden ingezet. Bij veel organisaties komt de inzet van elektronische beveiligingsmaatregelen voort uit de processen ´toegang verlenen´, 'toezicht houden', 'verifiëren van alarmen' en 'incidenten afhandelen'. Waar bouwkundige beveiligingsmaatregelen bij het proces toegang verlenen veelal gericht zijn op (fysieke) weerbaarheid van zones en compartimenten en de (on)mogelijkheid voor onbevoegden om bij barrières wel of niet te kunnen meelopen, gaat het bij elektronische beveiligingsmaatregelen veel meer om de bediening van barrières zoals bijvoorbeeld een tourniquet of tourlock. Bij het proces 'toezicht houden' gaat het bij de inzet van elektronische maatregelen om (hulp) middelen die de beveiligingsmedewerker ondersteunen om verstoringen van een vooraf gedefinieerde ´rusttoestand´, ook wel de 0-situatie genoemd, te constateren. De elektronische beveiligingsmaatregelen zijn dan vooral die (veld)componenten die afwijkingen van de gedefinieerde rusttoestand (automatisch) kunnen waarnemen. Er kan dan gedacht worden aan detectiemiddelen die signaleren dat er mogelijk personen op een lokatie zijn op een moment dat er niemand behoort te zijn, maar ook aan detectoren die waarnemen dat er sprake is van een mogelijk (beginnende) brand.

Daarnaast kunnen camera's en detectoren van een gebouwbeheersysteem de beveiligingsmedewerker behulpzaam zijn bij het waarnemen van afwijkingen die kunnen wijzen op het manifest worden van een (be)dreiging.

Alarmen verifiëren en incidenten afhandelen

Kijken wij naar het proces 'verifiëren van alarmen' dan kunnen elektronische beveiligingsmaatregelen behulpzaam zijn bij het valideren van elektronisch afgegeven (alarm)meldingen. Door een signaal, afgegeven vanuit het proces toezicht houden, kan binnen het proces verifiëren van alarmen worden vastgesteld of er echt sprake is van een incident, zoals bijvoorbeeld inbraak of brand, of dat sprake is van een onterechte melding. Door het bekijken van camerabeelden of het combineren van gegevens van verschillende detectoren kan door 'de beveiligingsmedewerker', de mens, een eerste conclusie worden getrokken. Los van het analyseren en correleren van signalen, die zijn afgegeven door elektronische beveiligingsmiddelen, kan natuurlijk ook altijd de mens worden ingezet om op lokatie de situatie te gaan bekijken. Is er sprake van een positief geverifieerd alarm, waardoor gesproken kan worden over een daadwerkelijk incident omdat de 'rust toestand' is doorbroken, komt als laatste het proces 'incidenten afhandelen' in beeld. Binnen dit proces kunnen elektronische beveiligingsmaatregelen ondersteuning bieden aan de mens, de beveiligingsmedewerker, bij de afhandeling van het incident. Gedacht kan dan worden aan de inzet van camera's om te bepalen of beveiligingsmedewerkers of externe hulpdiensten veilig een ruimte kunnen betreden, maar ook voor het volgen van medewerkers die handelend optreden. Dit laatste om de veiligheid van de medewerkers op de lokatie van het incident te bewaken of juist om hen naar de juiste lokatie te (bege)leiden. Detectoren kunnen binnen het proces incidenten afhandelen ook gebruikt worden voor het krijgen van informatie over bijvoorbeeld uitbreiding of verplaatsing van een incident.

Toezicht houden

Vooral binnen het proces 'toezicht houden' komt de inzet van elektronische beveiligingsmaatregelen veelvuldig voor. Belangrijk is echter om te bepalen, en dat wordt nog wel eens vergeten, wat de doelstelling is die aan de inzet van verschillende elektronische beveiligingsmaatregelen ten grondslag ligt. Er zullen, met andere woorden, functionele programma's van eisen moeten komen. Het gaat dan om beantwoording van vragen,

op het moment dat bijvoorbeeld camera's worden ingezet om toezicht houden te houden, zoals 'wat wil ik nu eigenlijk zien en op welk moment wil ik dat zien?'. Wil ik een mogelijke (be)dreiging pas zien als een dreiging manifest is geworden, en de inbreker door een raam naar binnenklimt, of wil ik een mogelijke (be)dreiging al kunnen waarnemen voordat er sprake is van een daadwerkelijk incident? Als de laatste vraag positief beantwoord wordt zijn de eisen die de security manager aan camera's moet stellen anders dan wanneer volstaan kan worden met het bekijken van een incident nadat dit heeft plaatsgevonden. Het gaat dan om een pro-actieve inzet versus een reactieve-inzet van een elektronisch beveiligingsmiddel. Dezelfde vragen dienen door de security manager ook beantwoord te worden voordat kan worden overgegaan tot het plaatsen van andere soorten van (elektronische) detectiemiddelen. Een cameraplan en een detectieplan dient niet alleen inzichtelijk te maken op welke locaties elektronische beveiligingsmaatregelen worden ingezet, maar ook wat de betreffende (hulp)middelen nu precies moeten zien of waarnemen. Het stilstaan bij deze vragen in de planningsfase kan veel teleurstellingen achteraf voorkomen. Daar waar elektronische beveiligingsmaatregelen in de praktijk niet blijken te voldoen is vaak niet goed nagedacht over de vraag, voordat tot aanschaf en inzet werd overgegaan, wat nu eigenlijk precies van de beveiligingsmaatregel verwacht werd.

Virtuele surveillance

Vanuit het proces 'toezicht houden' worden vaak beveiligingsmedewerkers ingezet. Het lopen van zogenaamde surveillanceronden door beveiligingsmedewerkers, om afwijkingen van de 'rust toestand' te kunnen waarnemen, is niet ongewoon. Dat is ook prima op het moment dat beveiligingsmedewerkers preventief worden ingezet als 'zichtbare beveiligingsmaatregel', zodat kwaadwillenden weten dat ze beveiligingsmedewerkers tegen het lijf kunnen lopen. Maar als het geen bewuste overweging is om beveiligingsmedewerkers preventief 'ter ontmoediging' in te zetten, kunnen surveillanceronden natuurlijk ook 'virtueel' gelopen worden. Hiervoor kunnen elektronische beveiligingsmaatregelen, zoals (intelligente) camera's, de mens prima ondersteunen. De beveiligingsmedewerker hoeft voor het 'houden van toezicht' zijn plaats niet meer te verlaten en kan vanaf een centrale positie vaak meer waarnemen dan tijdens een echte surveillanceronde. Het implementeren van deze manier van surveillance vraagt echter wel veel denkwerk vooraf voordat tot de inzet van camera's kan worden overgegaan. Vanuit het proces toezicht houden



dienen functionele eisen te worden geformuleerd met betrekking tot wat er 'gezien moet kunnen worden' en ook onder welke omstandigheden. Alles wat in deze fase niet door de security manager als functionele eis wordt geformuleerd zal de camera, die voor virtuele surveillance gebruikt wordt, ook niet kunnen. Moet het mogelijk zijn om overdag en 's nachts duidelijke beelden te hebben, is het erg als de beelden onduidelijk zijn als het sneeuwt of regent, moeten personen alleen kunnen worden waargenomen of moeten personen tot op individueel niveau te identificeren zijn, is een overzicht van de lokatie waar een mogelijk incident zich voordoet voldoende of moet een mogelijk incident als het zich verplaatst gevolgd kunnen worden, is het herkennen van de kleur van een auto voldoende, of moeten het kenteken en eventuele letters op de zijkant van de auto duidelijk leesbaar zijn, is het voldoende om een incident met één camera te kunnen bekijken of moet een incident altijd vanuit meerdere kanten bekeken kunnen worden? Allemaal vragen waar vooraf over nagedacht dient te worden.

Verifiëren van alarmen

Naast de inzet van elektronische beveiligingsmaatregelen om objecten en barrières te kunnen bedienen (proces toegang verlenen) en de inzet van elektronische beveiligingsmaatregelen om afwijkingen van een vooraf gedefinieerde rusttoestand te kunnen waarnemen (proces toezicht houden), worden elektronische beveiligingsmaatregelen ook ingezet om bij een (alarm)signaal te beoordelen of daadwerkelijk sprake is van een incident (verifiëren van alarmen). Ook hier komt de security manager vaak weer uit bij de inzet, naast natuurlijk de beveiligingsmedewerker zelf, van elek-

tronische beveiligingsmaatregelen zoals camera's en (gecombineerde) detectoren. Echt belangrijk voor de security manager om zich te realiseren is dat de functionele eisen, die het proces 'verifiëren van alarmen' aan veldcomponenten stelt, anders kunnen zijn dan de functionele eisen die het proces 'toegang verlenen' of het proces 'toezicht houden' aan de veldcomponent stelt. Met andere woorden, een camera of detector die voldoet aan de functionele eisen om toezicht te kunnen houden zou wel eens niet kunnen voldoen aan de functionele eisen om (alarm)signalen te kunnen verifiëren.
Als hier op voorhand niet bij stilgestaan wordt en de security manager zich niet realiseert dat camera's en detectoren niet allemaal gelijk zijn en afhankelijk van de specificaties ieder een eigen beperking hebben voor wat betreft inzetbaarheid, blijft hij met een 'kat in de zak' zitten. Het gevolg is teleurstelling en elektronische beveiligingsmiddelen die in de praktijk niet voldoen. Duidelijke procesbeschrijvingen en het stellen van duidelijke normen en eisen aan elektronische beveiligingsmaatregelen kunnen, net zoals dat voor bouwkundige beveiligingsmaatregelen noodzakelijk is, verkeerde investeringen ondervangen. Het valt of staat dus eigenlijk weer met goede organisatorische beveiligingsmaatregelen.

Literatuur

Broder, J.F. (2000) *Risk Analysis and the Security Survey*, Boston: Butterworth-Heinemann / member of the Reed Elsevier Group.
Claes, P.F. en Meerman, H.J.J.M. (1998) *Riskmanagement; inleiding tot het risicobeheersingsproces*, Houten: Stenfert Kroese.
Coumou, C. (2003) *Risicomanagement voor security- en facilitymanagers*, Alphen aan den Rijn: Kluwer.
Haaf, W. ten, Bikker, H. en Adriaanse, D.J. (2002) *Fundamentals of business engineering and management*, Delft: Delft University Press.
Overbeek, P., Roos Lindgreen, E. en Spruit, M. (2000) *Informatiebeveiliging onder controle*, Amsterdam: Prentice Hall.
Purpura, P.P. (1998) *Security and Loss Prevention*, Boston: Butterworth-Heinemann / member of the Reed Elsevier Group.
Roper, C.A. (1999) *Riskmanagement for Security Professionals*, Boston: Butterworth-Heinemann / member of the Reed Elsevier Group.
Sennewald, C.A. (1998) *Effective Security Management*, Boston: Butterworth-Heinemann / member of the Reed Elsevier Group.
Veld, J. in 't (2002) *Analyse van Organisatieproblemen; Een toepassing van denken in systemen en processen*, Groningen: Stenfert Kroese.

IT-beveiligingsmaatregelen

Om maar meteen met de deur in huis te vallen. Vaak is nog sprake van een groot misverstand wat veelal een Babylonische spraakverwarring tot gevolg heeft. Het laten implementeren en onderhouden van IT-beveiligingsmaatregelen door de IT-afdeling betekent niet dat een organisatie 'informatiebeveiliging' op orde heeft. Zeker niet als blijkt dat de IT-afdeling uitgaat van andere (be)dreigingen en risico's dan de afdelingen die verantwoordelijk zijn voor het implementeren en onderhouden van fysieke, elektronische en personele beveiligingsmaatregelen.

Fysieke en elektronische beveiligingsmaatregelen zijn even belangrijk als IT-beveiligingsmaatregelen. Toch spreken de vakgenoten uit deze vaak gescheiden disciplines nog wel eens met enige minachting over elkaar. Behalve dat dit geheel ten onrechte is, maakt het de organisatie ook nog nodeloos kwetsbaar. Het gevolg is dat IT-beveiligingsmaatregelen niet aansluiten op andere binnen de organisatie getroffen beveiligingsmaatregelen. Een gemiste kans.

Aanvalscenario's

De tegenstanders van de organisatie, u weet wel die van het criminele en terroristische team, kunnen op drie manieren binnenkomen. Ten eerste kunnen zij de organisatie door middel van de fysieke poort betreden. Dit wil zeggen door het doorbreken of omzeilen van een fysieke (toegangs) barrière zoals een deur of muur. Ook kunnen zij, als tweede optie, toegang krijgen tot de organisatie door het nemen van de logische (toegangs)barrière. Voor het nemen van deze logische barrière is een externe koppeling met het netwerk noodzakelijk. De derde optie voor de crimineel of de terrorist is het legitiem betreden van de organisatie als medewerker of leverancier. Hiervoor gaan de fysieke- en logische toegangsdeuren immers gewoon open. Om de belangen van de organisatie te beschermen - en informatie in één of andere vorm hoort daar tegenwoordig vaak bij - dienen de beveiligingsmaatregelen bij alle drie de (toegangs)poorten dezelfde weerstand te bieden. Dit betekent dat bij de inzet van IT-beveiligingsmaatregelen dient te worden uitgegaan van dezelfde (be)dreigingen - en naar aanleiding daarvan ook van dezelfde risicoanalyse - als die aan de inzet van de bekende organisatorische-, bouwkundige-, en elektroni-

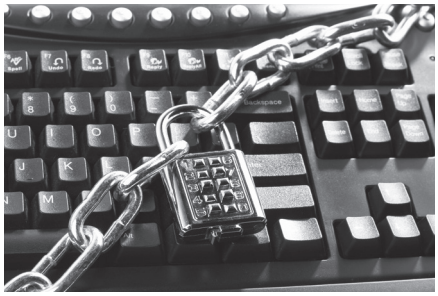
sche beveiligingsmaatregelen ten grondslag ligt. Vaak is dit niet het geval. Het gevolg is dat de voordeur van de organisatie wordt dichtgedaan, maar dat de achterdeur wagenwijd open blijft staan. Een geaccepteerd risico of een vergissing?

Logische toegang

De logische toegang tot de organisatie kan op twee manieren worden genomen. Als de IT-beveiligingsmaatregelen zoals een firewall of een virusscanner niet afdoende zijn, of misschien in zijn geheel niet aanwezig zijn, kan een crimineel of terrorist via een externe koppeling onbevoegd toegang krijgen tot de informatiesystemen van de organisatie. Dit kan gevolgen hebben voor zowel de vertrouwelijkheid, integriteit alsook beschikbaarheid van de informatie die in de informatiesystemen van de organisatie aanwezig is. In het meest positieve geval wordt waargenomen dat een persoon onbevoegd toegang heeft gekregen tot de bedrijfssystemen en kunnen er tegenmaatregelen worden genomen. In het slechtste geval blijft dit bij de security manager onopgemerkt.
De tweede manier voor een crimineel of terrorist om de logische toegang te nemen is door als medewerker bij de organisatie te komen werken. Dit betekent meestal dat er een user-id en wachtwoord voor toegang tot het informatiesysteem wordt verstrekt. Vanaf dat moment heeft een eventuele kwaadwillende legitiem toegang tot de bedrijfssystemen. En mocht de medewerker bij binnenkomst nog geheel te goeder trouw zijn, er is een trend waarneembaar dat criminele organisaties zich steeds vaker bedienen van *social engineering* en *human engineering*. Dit betekent dat zij op veilige afstand kunnen blijven en de organisatie waarschijnlijk niet eens echt te zien krijgen. Het is vervolgens de medewerker die, al dan niet onder druk, zijn gang kan gaan. Heeft de security manager IT-beveiligingsmaatregelen geïmplementeerd om dit tijdig waar te nemen of gaat hij uit van de goedheid van de mens?

Procesbenadering

Het mag geen verrassing zijn, maar de inzet van IT-beveiligingsmaatregelen is veelal gericht op toegangbeheersing. Daarom dient zich een belangrijke vraag aan. Maakt de inzet van IT-beveiligingsmaatregelen deel uit van het proces ‘verlenen van toegang’ dat de security manager heeft beschreven, of heeft de beschrijving van dit proces zich beperkt tot het opnemen van normen voor bouwkundige en elektronische beveiligingsmaatregelen? Waarschijnlijk het laatste. In dat geval is het te overwegen,



juist om te borgen dat de inzet van IT-beveiligingsmaatregelen aansluit op de in de risicoanalyse geïdentificeerde bedreigingen, de inzet van IT-beveiligingsmaatregelen op te nemen in de beschrijving van het proces 'verlenen van toegang'.
Naast het proces 'verlenen van toegang' bestaan er nog drie echte operationele processen. Dit zijn 'toezicht houden', 'alarmen verifiëren' en 'incidenten afhandelen'. Ook deze drie processen kennen specifieke IT-beveiligingsmaatregelen die kunnen worden ingezet. Misschien ook een idee om dit op te nemen in een integrale procesbeschrijving. Het resultaat is dan dat de van oudsher verschillende vakgebieden, fysieke beveiliging en IT-beveiliging, gezamenlijk gaan optrekken om ieder vanuit hun expertise op elkaar afgestemde beveiligingsmaatregelen te treffen. De voordeur en de achterdeur zitten dan beide op slot. Dit vraagt wel om een nieuw soort 'security manager' die zich de terminologie van beide terreinen eigen heeft gemaakt en boven de beide partijen binnen de organisatie kan gaan staan. Bent u die corporate informatie security manager?

Uitdaging

De security manager, die veelal een achtergrond in de fysieke beveiliging heeft gehad of in een vorig leven bij de politie heeft gewerkt, zal zich de terminologie van de IT-beveiliger eigen moeten gaan maken wil hij boven de partijen komen te staan. De IT-beveiliger zal echter op zijn beurt, wil hij dat door de inzet van IT-beveiligingsmaatregelen de doelstelling die daaraan ten grondslag ligt wordt bereikt, zich de terminologie van de klassiek opgeleide fysieke beveiligers eigen moeten gaan maken. Beide zullen vervolgens met een grote verrassing worden geconfronteerd. Zowel binnen de IT-beveiliging alsook binnen de fysieke beveiliging werken professionals die met hetzelfde bezig zijn. Wat verschilt is alleen de terminologie en de gebruikte technische oplossingen. In de academische wereld heeft men deze ontdekking al eerder gedaan. Opleidingen gaan tegenwoordig al uit van een integrale benadering waar de inzet van IT-beveiligingsmaatregelen en fysieke beveiligingsmaatregelen even belangrijk zijn. De ontdekking is echter helaas nog niet in zijn gehele omvang doorgedrongen tot alle in de praktijk werkzame beveiligers en professionals.

Beveiligingsplan

Is het erg als IT-beveiligingsmaatregelen niet aansluiten op de organisatorische-, bouwkundige-, en elektronische beveiligingsmaatregelen? En is het erg als bij het beantwoorden van de vraag 'welke IT-beveiligingsmaatregelen noodzakelijk zijn' wordt uitgegaan van een andere risicoanalyse dan die aan de inzet van organisatorische-, bouwkundige- en elektronische maatregelen ten grondslag ligt? Waarschijnlijk wel. Want het zijn niet alleen meer de criminele en terroristische groeperingen die zich toegang tot organisaties willen verschaffen. Ook buitenlandse concurrenten, die in sommige gevallen steun krijgen vanuit de inlichtingendiensten in hun land, proberen zich hiertoe heimelijk toegang te verschaffen. Stelt u zich eens voor. Uw firewall wordt geleverd door een buitenlands bedrijf. Uw grootste concurrent is gevestigd in hetzelfde land als dat van de leverancier van de firewall. En toevallig moeten in dat land de broncodes van beveiligingssoftware altijd aan de overheid ter beschikking worden gesteld. Of nog beter, u verplaatst het meest kritische bedrijfsproces of uw computercentrum naar een land waar overheidsdiensten over de schouder meekijken. Vertrouwt u de IT-beveiliging dan nog? Toch lastig als deze (be)dreigingen over het hoofd worden gezien. Helaas is dat momenteel wel de gewoonste zaak van de wereld. Sla de kranten er maar op na.

Literatuur

Broder, J.F. (2000) *Risk Analysis and the Security Survey*, Boston: Butterworth-Heinemann / member of the Reed Elsevier Group.

Claes, P.F. en Meerman, H.J.J.M. (1998) *Riskmanagement; inleiding tot het risicobeheersingsproces*, Houten: Stenfert Kroese.

Coumou, C. (2003) *Risicomanagement voor security- en facilitymanagers*, Alphen aan den Rijn: Kluwer.

Haaf, W. ten, Bikker, H. en Adriaanse, D.J. (2002) *Fundamentals of business engineering and management*, Delft: Delft University Press.

Overbeek, P., Roos Lindgreen, E. en Spruit, M. (2000) *Informatiebeveiliging onder controle*, Amsterdam: Prentice Hall.

Purpura, P.P. (1998) *Security and Loss Prevention*, Boston: Butterworth-Heinemann / member of the Reed Elsevier Group.

Roper, C.A. (1999) *Riskmanagement for Security Professionals*, Boston: Butterworth-Heinemann / member of the Reed Elsevier Group.

Sennewald, C.A. (1998) *Effective Security Management*, Boston: Butterworth-Heinemann / member of the Reed Elsevier Group.

Veld, J. in 't (2002) *Analyse van Organisatieproblemen; Een toepassing van denken in systemen en processen*, Groningen: Stenfert Kroese

Personele beveiligingsmaatregelen

Als zowel de fysieke als de logische poort van de organisatie blijkt te zijn afgesloten, blijft alleen de menselijke poort als optie voor de crimineel over. De mens als zwakste schakel. Door te gaan werken voor een organisatie, eventueel als leverancier of als (ingehuurde) adviseur, blijken de woorden 'sesam open u' vaak werkelijkheid te worden. Een pre-employment of in-employment screening kan, als laatste drempel bij deze poort, deels antwoord geven op de vraag of (nieuwe) medewerkers een risico voor de organisatie opleveren.

De security manager heeft als taak de organisatie waarvoor hij werkzaam is zoveel mogelijk te beschermen. In dit geval tegen kwaadwillenden die willens en wetens onbevoegde handelingen willen uitvoeren. Maar hoe kunnen deze personen, die de belangen van de organisatie willen aantasten, nu precies te werk gaan? De eerste optie is de organisatie wederrechtelijk te betreden. Maar als het goed is heeft de security manager effectieve bouwkundige en elektronische beveiligingsmaatregelen getroffen om dit te voorkomen. Een tweede optie is om, via externe koppelingen, te proberen het ICT-netwerk van de organisatie onbevoegd binnen te dringen. Ook dit zal lastig blijken te zijn gezien de door de security manager getroffen IT-beveiligingsmaatregelen.

Drie-poorten-benadering

Als zowel de fysieke poort als ook de logische poort blijkt te zijn afgesloten kan de crimineel ook nog besluiten te gaan werken voor de aan te vallen organisatie, eventueel als leverancier of als adviseur. Dan openen de fysieke en soms ook logische poort zich miraculeus. Door gebruik te maken van een toegangspas gaat de voordeur open en met een 'user-ID' en wachtwoord ontsluit de logische poort zich. De afgelopen jaren is veel geld uitgegeven aan fysieke, elektronische en IT beveiligingsmaatregelen. Helaas blijkt uit de statistieken steeds weer dat juist de mens problemen veroorzaakt en veelal betreft het werknemers die legitiem aanwezig zijn binnen de organisatie. Het onderwerp 'insider threat' komt internationaal steeds prominenter op de agenda te staan, met uitzondering van Nederland lijkt het wel. Immers, in de polder is iedereen even betrouwbaar. Toch? Een prima uitgangspunt, maar niet voor een security professional.

Laten wij, 'slechts voor deze discussie', eens uitgaan van het standpunt dat de Nederlandse werknemer even (on)betrouwbaar is als de gemiddelde werknemer in andere landen. Is het treffen van personele beveiligingsmaatregelen - lees: het uitvoeren van betrouwbaarheidsonderzoeken - dan een gerechtvaardigd middel om in te zetten? Het brengt immers een inbreuk op de privacy met zich mee. Naar mijn mening wel, tenminste als wij de statistieken geloven. Maar waar moet de security manager dan naar op zoek gaan bij het treffen van maatregelen om toegang van kwaadwillenden via de 'menselijke poort' tot de organisatie zo goed mogelijk af te dekken? Het antwoord op deze vraag hangt voor een groot deel af van de in de risicoanalyse onderkende dreigingen. De gemiddelde organisatie zal waarschijnlijk diefstal van eigendommen, inclusief vertrouwelijke informatie, als dreiging hebben geïdentificeerd.
De meest voorkomende reden voor personeelsleden om zich eigendommen van de organisatie onrechtmatig toe te eigenen komt voort uit een gebrek aan geld. De reguliere inkomsten komen niet meer overeen met het uitgavenpatroon. Dit kan komen door het feit dat iemand boven zijn stand leeft, een verslaving heeft of te maken krijgt met onverwachte financiële tegenvallers in de privésfeer. Ook frustratie over de carrière, interne of externe (groeps)druk of 'gewoon omdat de gelegenheid zich voordoet' kan een reden zijn om onbevoegde handelingen te verrichten. Voor de organisatie is het vooral schadelijk als personeelsleden onbevoegde handelingen uitvoeren omdat zij daartoe worden gedwongen door bijvoorbeeld criminele of terroristische organisaties. Hier komen wij op het vlak van *social* en *human engineering* terecht. Maar hoe gaat dat nu in zijn werk?

Social engineering

De medewerker die een '*target*' is geworden van een *social engineer* is zich dat veelal niet bewust. Ook niet nadat het kwaad, in dit geval meestal het verstrekken van vertrouwelijke informatie, is geschied. Dit komt omdat het bevragen van medewerkers in een voor de medewerker ogenschijnlijk ongevaarlijke omgeving plaatsvindt. De sportvereniging of de kroeg waar de medewerker komt zijn perfecte locaties waar de *social engineer* te werk kan gaan. Maar ook cursussen of congressen waaraan deelgenomen wordt kunnen een goede setting opleveren. De *social engineer* zal in eerste instantie het vertrouwen proberen te wekken van de medewerker van uw organisatie. Er zijn voorbeelden, als het belang van de informatie die men hoopt te verkrijgen maar groot genoeg is,



waar de *social engineer* er jaren voor uittrekt om een vriendschappelijke band op te bouwen. De kinderen spelen met elkaar, en de families gaan samen gezellig 'met elkaar' naar de Efteling. En dan ineens, als er geen enkele reden meer is om elkaar te wantrouwen, komt de vraag op tafel waar het om gaat. Veelal zal een dergelijke investering in tijd niet echt noodzakelijk zijn. Mensen zijn van nature graag bereid tot het delen van kennis, al is het maar om te laten zien 'een echte expert op een specifiek vakgebied te zijn'. Vleien is in een dergelijk geval genoeg om iemand aan het praten te krijgen. Achteraf, en zo werkt het menselijk geheugen nu eenmaal, weet de medewerker nog precies wat hij aan het begin en aan het einde van de avond heeft gezegd. Maar het stuk er tussenin is vaak niet meer helemaal helder. Eenmaal thuisgekomen weet het slachtoffer van de *social engineer* echt niet meer wat hij of zij allemaal heeft prijsgegeven. Er is een kleine kans bovendien dat de security manager ontdekt dat informatie op deze manier de organisatie heeft verlaten.

Human engineering

Een stap verder dan het alleen bevragen van mensen, die zich niet bewust zijn bevraagd te worden, is het daadwerkelijk aansturen of onder druk zetten van medewerkers om actief aan de slag te gaan. Dat kan betekenen dat medewerkers gericht op pad worden gestuurd om bepaalde informatie te achterhalen. Het kan ook betekenen, en iedere security manager kent de postcodegebieden waar dit gebeurt, dat medewerkers materialen bij de open en ongecontroleerde deur van de expeditie moeten neerzetten zodat het 'wat makkelijker is mee te nemen'.
Maar hoe komt het nu zover dat een medewerker zich 'laat gebruiken' door een *human engineer*? In de meeste gevallen komt dit doordat de medewerker of een zwakke plek heeft waarvan gebruik kan worden gemaakt, of omdat hij chantabel is. In beginsel is iedereen met 'een geheim' waarover in de privé- of werksituatie niet gepraat mag worden chantabel.

Zeker als er iets op het spel staat wat 'verloren' kan worden en belangrijk is voor de werknemer. Mensen blijken, om te voorkomen dat hun geheim op straat komt te liggen, vaak bereid om in opdracht onbevoegde handelingen te verrichten. Het gebruik maken van een zwakke plek, geldproblemen of een (alcohol)verslaving, is voor de *human engineer* vaak wat lastiger. Dat komt omdat de mensen, door het probleem dat zij hebben, vaak wat onvoorspelbaarder worden. En daardoor moeilijker in de hand te houden zijn. Zolang alles goed gaat en er slechts één of twee keer door een *human engineer* een medewerker wordt aangestuurd, is ook hier de kans klein dat de security manager ontdekt wat er precies is gebeurd. Als het incident al wordt waargenomen. De kans is echter groot dat diefstal van informatie, als deze niet openlijk door de ontvanger gebruikt wordt, niet eens wordt ontdekt. Dat is nog eens een voorbeeld van '*insider threat*', maar zoals eerder gezegd niet in Nederland.

Infiltratie

Een stap verder, die ook om een gedegen voorbereiding vraagt, is daadwerkelijke infiltratie van een organisatie. Kleine ondernemers zullen niet zo vaak met dit verschijnsel te maken krijgen, maar multinationals die in een 'globale' arena spelen of organisaties waar informatie te verkrijgen is die handig is om op voorhand te hebben, moeten hiermee wel rekening houden. Zeker als deze informatie kan worden omgezet in financieel gewin. Nu worden ook beleidsdossiers of plannen over een te volgen strategie van beleidsbepalende organisaties, die in eerste instantie saai lijken, ineens interessant voor buitenstaanders. Dit moet de security manager zich wel bewust zijn. Op de medewerker die een organisatie met vooropgezette plannen betreedt, zal niets aan te merken zijn. Voor wat betreft opleiding en werkervaring is het waarschijnlijk de perfecte kandidaat. De lijnmanager zal hem of haar zeker binnen willen halen. Waarschijnlijk zal hij of zij in het verleden ook nooit een misstap hebben begaan. Kortom, de perfecte schoonzoon of schoondochter. De enige kans die de security manager heeft om infiltratie in een vroegtijdig stadium te ontdekken is dan ook veelal afhankelijk van de 'organisatiecultuur'. Als er sprake is van een 'open' cultuur, waar medewerkers elkaar aanspreken op houding en gedrag, bestaat de kans dat 'vreemd' of 'afwijkend' gedrag vroeg of laat opvalt. Belangrijk is dan dat dit 'vreemde of afwijkende gedrag' bespreekbaar is. Tevens zal de security manager de organisatie indicatoren mee moeten geven waarop gelet kan worden. Handboeken over fraudeonderzoeken kunnen hierbij behulpzaam zijn.

Als social engineering, human engineering en infiltratie zo moeilijk zijn waar te nemen, wat kan de security manager dan nog doen? Het antwoord ligt bij de invoering van de preventieve maatregel 'het betrouwbaarheidsonderzoek' als zogenaamde 'last line of defense'. Met betrouwbaarheidsonderzoek wordt in dit geval zowel pre-employment screening alsook in-employment screening bedoeld.
De in-employment screening is noodzakelijk omdat een uitspraak over de (toekomstige) betrouwbaarheid van een persoon nooit meer is dan een momentopname. Morgen kunnen de omstandigheden zich al weer gewijzigd hebben. Het is belangrijk dat de diepte en omvang van een betrouwbaarheidsonderzoek zowel proportioneel alsook subsidiair zijn. De security manager maakt bij een dergelijk onderzoek immers, vanuit de organisatie gezien, een (noodzakelijke) inbreuk op de privacy van een medewerker. Dat betekent dat er een directe relatie moet zijn tussen het onderzoek en de in de risicoanalyse van de organisatie onderkende (be) dreigingen en ook dat de functie die men gaat vervullen risicofactoren kent die op voorhand in kaart zijn gebracht. Kortom, de security manager zal moeten uitleggen dat hij de goede dingen doet en de dingen goed doet. Dat klinkt gemakkelijker dan het is.
Recent hebben leden van de Vereniging Beveiligingsmanagers Nederland (VBN) in samenwerking met Nederlandse leden van de ASIS Benelux Chapter een Nationale Richtlijn (Pre-employment) Screening opgesteld. Deze kan u weer een stap verder helpen bij het bepalen van de voor uw organisatie noodzakelijk te nemen personele beveiligingsmaatregelen.

Literatuur

Broder, J.F. (2000) *Risk Analysis and the Security Survey*, Boston: Butterworth-Heinemann / member of the Reed Elsevier Group.
Claes, P.F. en Meerman, H.J.J.M. (1998) *Riskmanagement; inleiding tot het risicobeheersingsproces*, Houten: Stenfert Kroese.
Coumou, C. (2003) *Risicomanagement voor security- en facilitymanagers*, Alphen aan den Rijn: Kluwer.
Purpura, P.P. (1998) *Security and Loss Prevention*, Boston: Butterworth-Heinemann / member of the Reed Elsevier Group.
Roper, C.A. (1999) *Riskmanagement for Security Professionals*, Boston: Butterworth-Heinemann / member of the Reed Elsevier Group.
Scharrenborg, M.H.G. (2006) *Handboek Fraude & Onderzoek*, Den Haag: SDU.
Sennewald, C.A. (1998) *Effective Security Management*, Boston: Butterworth-Heinemann / member of the Reed Elsevier Group.

Opzet van de beveiligingsorganisatie

Na in de vorige zes hoofdstukken uitvoerig te hebben stil gestaan bij de vraag met welke soort maatregelen rekening moet worden gehouden bij het opstellen van een beveiligingsplan, blijft nog één vraag over waar iedere security manager graag een antwoord op wil. Hoe staat mijn organisatie er nu echt voor als wij het over het onderwerp beveiliging hebben? Want uiteindelijk geldt 'the proof is in the eating of the pudding'.

De vraag waar veel security managers zich voor gesteld zien, en die vaak lastig te beantwoorden blijkt, is hoe bepaal ik nu of mijn organisatie het op beveiligingsvlak wel of niet goed doet? En in het verlengde daarvan de vervolgvraag: zijn de juiste beveiligingsmaatregelen getroffen? Security consultants bieden 'een woud' aan instrumenten aan om antwoord te geven op deze vragen. Probleem is echter dat de namen van de verschillende instrumenten zo oogstrelend zijn dat de gemiddelde security manager door de bomen het bos niet meer ziet. Wie kan nog uitleggen wat het verschil is tussen een security audit, een security survey, een security scan of een security inspectie? En zou een collega security manager dezelfde uitleg geven aan deze begrippen? Waarschijnlijk niet. En dan gaan wij nog maar even niet in op de vraag of een security survey van de ene consultant hetzelfde is als een security scan van de andere consultant. Kortom, eenoog is koning in het land der blinden.

Licht

Tijd om eens wat licht in de duisternis te laten schijnen door het stellen van twee simpele vragen. Doet mijn organisatie op beveiligingsgebied de goede dingen en doen wij als organisatie de dingen goed? Met andere woorden: is 'de opzet' van mijn beveiligingsorganisatie juist? Een positief antwoord op deze vraag sluit het element 'toeval' bij de keuze van beveiligingsmaatregelen namelijk uit. Pas daarna is het zinvol te kijken naar 'de werking' van de gekozen beveiligingsmaatregelen. Dit om uit te sluiten dat er wordt vastgesteld dat de gekozen beveiligingsmaatregelen goed werken terwijl de initiële keuze op toeval berust. Het gevolg zou dan namelijk kunnen zijn dat de organisatie weer rustig gaat slapen terwijl

daar, gezien de toevallig juist gekozen beveiligingsmaatregelen, geen reden toe is.
In dit hoofdstuk komt een aantal handvatten aan de orde die u als security manager kunnen helpen om 'de opzet' van uw beveiligingsorganisatie te beoordelen. Pas daarna kijken wij, in het volgende en laatste hoofdstuk over 'het beveiligingsplan', naar de werking van beveiligingsmaatregelen. Belangrijk is dat u zich realiseert dat de in dit hoofdstuk beschreven stappen niet compleet zijn en dat er, om maar weer eens een spreekwoord te gebruiken, 'meerdere wegen naar Rome leiden'. Waar het om gaat is dat u als security manager kunt uitleggen waarom u bepaalde stappen wel of niet neemt? Transparantie, daar begint alles mee.

Stap 1 - Vastgestelde uitgangspunten

Waarom zijn wij op Aarde? Dat zou een goede vraag zijn om een onderzoek naar de opzet van de beveiligingsorganisatie mee te beginnen. Het fundament van iedere beveiligingsorganisatie is te vinden in het (beleidsmatige) document waarin beschreven staat wat 'het doel' is waarvoor de beveiligingsorganisatie in het leven is geroepen. Als tenslotte niet duidelijk is wat alle door de beveiligingsorganisatie getroffen beveiligingsmaatregelen tot gevolg moeten hebben, bijvoorbeeld het realiseren van 'een veilige werkomgeving', is een uitspraak of 'de goede dingen worden gedaan' en of 'de dingen goed worden gedaan' vrijwel onmogelijk. Het document waarin de uitgangspunten staan beschreven is daarom ook niet een document van de security manager, maar van het (top)management. Het document zal, naast dat het de visie en de missie van de beveiligingsorganisatie duidelijk moet maken, ook iets moeten zeggen over de door de beveiligingsorganisatie te behalen doelstellingen. De vragen die beantwoord moeten worden zijn:

- Heeft mijn organisatie een vastgesteld beveiligingsbeleid?
- Staan in het beveiligingsbeleid duidelijke doelstellingen omschreven?
- Zijn de missie en visie van de beveiligingsorganisatie helder beschreven?
- Is het beveiligingsbeleid vastgesteld door het (top)management?

Stap 2 - Taken en verantwoordelijkheden

Uiteindelijk is de directie er, als het gaat om beveiligingsvraagstukken, voor verantwoordelijk dat het juiste veiligheidsniveau wordt gerealiseerd. De directie kan zich op dit vakgebied door twee functionarissen terzijde



laten staan. Enerzijds is er op strategisch-tactisch niveau de (informatie) security manager, die de directie behulpzaam kan zijn bij het daadwerkelijk '*in control*' komen en blijven. Daarnaast is er ook het hoofd beveiliging. Deze functionaris is op tactisch-operationeel niveau verantwoordelijk voor het implementeren en uitvoeren van de zogenaamde OBE-maatregelen. Nu is het niet noodzakelijk om juist deze functionarissen binnen een organisatie te hebben. Wat wel belangrijk is, is dat ergens beschreven staat welke (beveiligings)functionarissen er binnen de organisatie zijn.
De vragen die bij deze tweede stap beantwoord moeten worden zijn:

- Is de verantwoordelijkheid van de directie op het vlak van beveiliging beschreven en zijn de taken van de portefeuillehouder beveiliging binnen de directie beschreven?
- Is er een (informatie) security manager op strategisch-tactisch niveau aangesteld en zijn daarvan de taken en verantwoordelijkheden beschreven?
- Is er een hoofd beveiliging op tactisch-operationeel niveau aangesteld en zijn daarvan de taken en verantwoordelijkheden beschreven?
- Is er een hoofd IT-beveiliging op tactisch-operationeel niveau aangesteld en zijn daarvan de taken en verantwoordelijkheden beschreven?

Stap 3 - Inrichting van de beveiligingsfunctie

De derde te beantwoorden hoofdvraag betreft de inrichting van de beveiligingsorganisatie. Immers, zoals wij eerder al zagen, kan de organisatie door middel van drie poorten worden betreden. Namelijk de fysieke poort, de logische poort en de menselijke poort. Dit betekent dat de vastgestelde uitgangspunten voor al deze poorten van toepassing zijn. Gezien vanuit dit gezichtspunt omvat 'de beveiligingsfunctie' dus fysieke beveiliging, IT-beveiliging en personele beveiliging. Het is 'oud' security management om beveiligingsvraagstukken te (blijven) benaderen vanuit de verschillende afdelingen die bij de uitvoering betrokken zijn en belangen na te streven die strijdig (kunnen) zijn met de belangen van andere betrokken afdelingen. Alleen een procesmatige benadering, waarbij ieder

specialisme een plaats krijgt binnen het proces 'security', is een waarborg voor betere samenwerking. Want uiteindelijk gaat het erom om 'samen de boef buiten de organisatie te houden'.
De vragen die bij deze stap beantwoord moeten worden zijn:

- Is beschreven welke (tactische) beveiligingsprocessen, die gebruikt worden om het beveiligingsbeleid uit te voeren, beschikbaar zijn voor de security manager?
- Is beschreven wie, van de afzonderlijke processen, de proceseigenaar is?
- Is beschreven wie, voor de afzonderlijke processen, verantwoordelijk is voor de uitvoering?

Stap 4 - Kroonjuwelen van de organisatie (belang)

Na in de eerste drie stappen te hebben gekeken naar de randvoorwaarden om het toevalsaspect te minimaliseren, gaan wij ons nu meer richten op de inhoudelijke beveiligingsaspecten. Daarbij beginnen wij met ons de vraag te stellen of wij, als verantwoordelijke security professionals, ons wel realiseren wat de 'te beschermen belangen' van de organisatie zijn. Wat zijn 'de kroonjuwelen' die het lijnmanagement wil beschermen? Is deze vraag wel eens voorgelegd aan het lijnmanagement? Grote kans dat een lijnmanager andere 'kroonjuwelen' noemt dan de security manager! Zo kan ik mijzelf een situatie herinneren waar een hoofd beveiliging veel (fysieke) maatregelen had getroffen om diefstal van computers te voorkomen, terwijl de lijnmanager, die 'eigenaar' van de computers was, het helemaal niet erg vond als computers (hardware) werden gestolen. Zolang de informatie die op de harde schijf stond maar niet gecompromitteerd werd. Als het hoofd beveiliging dit had geweten waren er andere (fysieke) beveiligingsmaatregelen ingezet en had het hoofd IT misschien wel maatregelen getroffen om de 'belangrijke informatie' te versleutelen. Toch lastig als op voorhand niet duidelijk is wat nu eigenlijk bescherming behoeft.
De vragen die bij stap vier beantwoord moeten worden zijn:

- Is er een overzicht van de kritische en/of primaire (bedrijfs)processen die beveiligd moeten worden?
- Is er een overzicht van de daadwerkelijke vitale knooppunten van waaruit deze processen onbevoegd kunnen worden beïnvloed?
- Is er een overzicht beschikbaar waarin expliciet staat beschreven wat de volgens lijnmanagers te beschermen 'kroonjuwelen' binnen hun bedrijfsproces zijn?

Stap 5 - Dreigingen ten opzichte van de organisatie (dreiging)

Pas als duidelijk is welke 'kroonjuwelen' bescherming behoeven kunnen dreigingen in kaart worden gebracht. Belangrijk is om vast te stellen wie de motivatie heeft om de organisatiebelangen aan te tasten en tevens of deze persoon (groep) daar ook daadwerkelijk de capaciteiten voor heeft. Bij een positief antwoord is het van belang om te bepalen hoe de organisatiebelangen aangetast kunnen worden. Heeft u bij stap drie vastgesteld dat u als security manager geen (tactisch) beveiligingsproces '*intelligence*' ter beschikking heeft, dan is het heel lastig om een goed antwoord op de vraag te geven welke dreigingen er zijn en welke scenario's er door de tegenstanders worden gebruikt. Het kiezen van de juiste beveiligingsmaatregelen berust dan voor een groot deel op toeval (oud security management).

De bij stap vijf te beantwoorden vragen zijn:

- Is er een dreiginganalyse beschikbaar?
- Zijn in deze analyse dreigingen gerelateerd aan (kritische) bedrijfsprocessen?
- Bevat de dreiginganalyse een beschrijving van scenario's?
- Zijn de scenario's uitgewerkt tot op het niveau van pad-analyses?

Stap 6 - Transparante beveiligingsmaatregelen (weerstand)

Nadat de te beschermen belangen duidelijk zijn gemaakt, evenals de dreigingen ten opzichte van deze belangen, is het zinvol om ook te kijken naar de (getroffen) beveiligingsmaatregelen. Het is nu immers mogelijk om de beveiligingsmaatregelen te relateren aan zowel de kroonjuwelen alsook de dreigingen ten opzichte van deze kroonjuwelen. Dit betekent dat, gezien vanuit de in stap 3 gevonden procesbeschrijvingen, alle aangetroffen beveiligingsmaatregelen verklaarbaar moeten zijn. Het is lastig om beveiligingsmaatregelen goed te verklaren als er geen procesbeschrijvingen zijn. Ook zal duidelijk moeten zijn, als er tenminste behoefte is om getroffen maatregelen te kunnen onderbouwen, wat de relatie is tussen de getroffen beveiligingsmaatregelen en de onderkende dreigingen. Waar staat de maatregel (als weerstand) in de beschreven pad-analyse en wat is de bijdrage van de maatregel aan het frustreren van de poging van de crimineel om de organisatiebelangen onbevoegd te beïnvloeden?



De bij deze laatste stap te beantwoorden vragen zijn:
- Is er een document waarin alle beveiligingsmaatregelen staan?
- Is er een relatie aangebracht, in deze beschrijving, tussen de beveiligingsmaatregel en het te beschermen belang?
- Is er een relatie aangebracht, in deze beschrijving, tussen de beveiligingsmaatregel en de onderkende dreiging?
- Is er, in deze beschrijving, een duidelijk meetbare doelstelling (SMART) aan de beveiligingsmaatregel gekoppeld?

Het mag duidelijk zijn dat de beschreven vragen indicatief zijn. Iedere security manager zal, gezien het beveiligingsniveau van zijn organisatie en de aanwezigheid van procesbeschrijvingen, moeten bepalen welke vragen zinvol zijn om te stellen. Echter, hoe minder vragen er beantwoord kunnen worden, hoe groter het toevalsaspect is mochten er toch juiste beveiligingsmaatregelen zijn getroffen. Als de conclusie is, na het kijken naar de opzet van de beveiliging, dat er nog veel gedaan moet worden, dan is het niet zinvol om al naar de werking van getroffen beveiligingsmaatregelen te gaan kijken. Als een goede onderbouwing voor de aanwezigheid van bepaalde beveiligingsmaatregelen niet te geven is, is al helemaal niet te meten of de maatregel doet wat hij moet doen.
Door alle vragen op een pagina onder elkaar te zetten en de score met kleuren (rood, geel en groen) aan te geven, hebben wij een aanzet voor een initieel meetinstrument te pakken. In dit instrument zal nog wel een vraag moeten worden opgenomen of ook een risicoanalyse op strategisch niveau is vastgesteld. Deze risicoanalyse is immers de weging van de resultaten uit stap 4 tot en met 6 (belang-dreiging-weerstand). Het is denkbaar dat de weging laat zien dat er een risico voor de organisatie bestaat, maar als dit risico geaccepteerd wordt zou het gek zijn als er wel beveiligingsmaatregelen zijn getroffen om de specifieke dreiging af te dekken.

Literatuur

Broder, J.F. (2000) *Risk Analysis and the Security Survey*, Boston: Butterworth-Heinemann / member of the Reed Elsevier Group.
Claes, P.F. en Meerman, H.J.J.M. (1998) *Riskmanagement; inleiding tot het risicobeheersingsproces*, Houten: Stenfert Kroese.
Coumou, C. (2003) *Risicomanagement voor security- en facilitymanagers*, Alphen aan den Rijn: Kluwer.
Roper, C.A. (1999) *Riskmanagement for Security Professionals*, Boston: Butterworth-Heinemann / member of the Reed Elsevier Group.

Red teaming

Na een positieve beantwoording van de vraag, is ´de opzet´ van mijn beveiligingsorganisatie goed, met als gevolg dat daarmee het element ´toeval´ bij de keuze van beveiligingsmaatregelen kan worden uitgesloten, staat dit laatste hoofdstuk in het teken van de vraag, doen wij als organisatie de dingen goed? Is met andere woorden de werking van de gekozen beveiligingsmaatregelen conform de verwachting en wordt de doelstelling die aan de specifieke beveiligingsmaatregelen ten grondslag ligt daadwerkelijk gehaald? Een *red team* kan daar uitsluitsel over geven.

Bij de beantwoording van de vraag of beveiligingsmaatregelen aan de verwachtingen voldoen, kan niet voorbij gegaan worden aan de mensen die de beveiligingstaken daadwerkelijk uitvoeren. Echter, een waarschuwing is hier op zijn plaats. Bij het kijken naar de hoe taken worden uitgevoerd is een 'afrekencultuur', als gevolg van eventueel geconstateerde tekortkomingen, funest voor de kwalitatieve ontwikkeling van de beveiligingsmedewerkers die met uitvoerende werkzaamheden zijn belast. Het gaat bij het toetsen van de werking van de beveiligingsorganisatie juist om het vinden van verbeterpunten, niet om het kunnen uitdelen van een 'zwarte piet'.

Koude oorlog

Om te beginnen met de meest voor de handliggende vraag, wat is *red teaming*? Het begrip *red teaming* stamt uit de tijd van de koude oorlog. Het rode team, in die tijd vaak het synoniem voor de russen, had als taak het uitvoeren van aanvallen op het blauwe team. Het blauwe team bestond natuurlijk uit de '*good guys*', de Amerikanen. Doelstelling van *red teaming* was enerzijds het toetsen van de paraatheid van de eigen verdediging, anderzijds het kijken of de verdediging adequaat en toereikend was. Het spreekt voor zich dat het rode team, als je dan al de taak had om de vijand te spelen, de oefening natuurlijk wel wilde winnen. Er werd daarom door het rode team zeer actief naar zwakke plekke in de verdediging van het blauwe team gezocht. Na de koude oorlog heeft, met name in Israël, het begrip *red teaming* een verdere ontwikkeling voor toepassing in het kader van (particuliere) beveiligingsdoeleinden doorgemaakt. Zo zijn er bijvoorbeeld in Tel Aviv 'hoog risico objecten' waar beveiligings-



medewerkers dagelijks met minstens acht à tien gesimuleerde aanvallen van een rood team te maken (kunnen) krijgen. Voor Nederlandse begrippen zou dit teveel van het goede zijn, wat niet wegneemt dat het principe van *red teaming* ook in Nederland universeel toepasbaar is.

Zelf aanvallen

Wat kunnen wij als security manager nu met het verschijnsel *red teaming*? Mits goed doordacht veel. Om de werking van de getroffen beveiligingsmaatregelen te toetsen en te kijken of onze beveiligingsmedewerkers de aan hun toebedeelde taken op de juiste wijze uitvoeren, kunnen wij vanuit het perspectief van de onderkende tegenstanders een 'rood team' de eigen organisatie laten aanvallen. Als het goed is en wij als security manager de juiste maatregelen hebben geïmplementeerd, kunnen criminele en terroristische scenario's die aan de grondslag liggen van getroffen beveiligingsmaatregelen niet succesvol worden uitgevoerd. Lukt het wel om een aanvalsscenario onopgemerkt te kunnen uitvoeren dan zijn er twee verklaringen, of een combinatie daarvan. De getroffen beveiligingsmaatregelen zijn, afgezet tegen de onderkende scenario's, fout of de mensen die belast zijn met de uitvoering van de beveiligingsmaatregelen voeren de aan hun toedeelde beveiligingstaken niet goed



uit. De uitdaging is, als de reden voor het falen van beveiligingsmaatregelen is vastgesteld, om ook kritische vervolgvragen te stellen. Bijvoorbeeld, 'waarom zijn de verkeerde beveiligingsmaatregelen gekozen en geïmplementeerd?' of 'waarom voeren medewerkers de aan hun toebedeelde beveiligingstaken niet goed uit'?. Veelal zal de security manager bij de beantwoording van deze vragen in de spiegel moeten kijken. Vaak zal er een '*short cut*' zijn genomen die, als het erop aankomt, noodlottig blijkt te zijn. De verklaring van een geslaagde aanval van een rood team is meestal een besparing op de kosten bij het implementeren van beveiligingsmaatregelen of het ontbreken van een goede uitleg of opleiding voor beveiligingsmedewerkers. Dit natuurlijk zonder dat de doelstellingen, die aan beveiligingsmaatregelen en uit te voeren beveiligingstaken ten grondslag liggen, zijn bijgesteld.

De menselijke factor

Organisaties waar *red teaming* inmiddels een ingeburgerd begrip is, en deze organisaties komen wij ook in Nederland tegen, zijn organisaties waar de security manager ontdekt heeft dat bouwkundige en elektronische beveiligingsmaatregelen alleen niet zaligmakend zijn. En zeker niet toereikend. Het kenmerk van deze maatregelen is immers dat zij niet kunnen nadenken. Juist voor het denkwerk zijn mensen nodig. In dit geval beveiligingsmedewerkers. Waarom? Omdat onze tegenstanders ook

voortdurend hun creativiteit gebruiken bij het aanvallen van onze organisatie. Juist daar waar het lukt om getroffen bouwkundige en elektronische beveiligingsmaatregelen te omzeilen is de mens, als het op het verdedigen van de belangen van de organisatie aankomt, onmisbaar. Deze mens, de beveiligingsmedewerker, is de '*last line of defence*' tegen creatieve criminele en terroristische tegenstanders. Dit besef is helaas in Nederland vaak ver te zoeken. Zou een organisatie die zich bewust is van het belang van de menselijke factor beveiligingswerkzaamheden nog uitbesteden of, als uitbesteding al niet te verkomen is, kiezen voor de goedkoopste aanbieder voor het leveren van geüniformeerde beveiligingsmedewerkers? Een interessante vraag. Naar mijn mening zou kwaliteit voorop moeten staan. Organisaties die zich bewust zijn van het belang van de menselijke factor investeren in medewerkers en zorgen ervoor dat deze mensen voortdurend met opleidingen worden geconfronteerd. Het gaat om het investeren in de mens en niet alleen om het implementeren van bouwkundige en elektronische beveiligingsmaatregelen. Er zijn organisaties in Nederland die dit doen, maar deze organisaties lopen er veelal niet mee te koop. Dat is ook een maatregel in het kader van informatiebeveiliging.

Dienstuitvoering

Wat is nu noodzakelijk om *red teaming* succesvol toe te passen binnen uw organisatie? Natuurlijk een rood team, maar ook, en dat is misschien wel het belangrijkste aspect, beveiligingsmedewerkers die de uitvoering van de aan hen toebedeelde taken serieus nemen. Geen vissers, die afwachten wat er voorbij komt zwemmen, maar jagers die actief opzoek gaan naar de tegenstander. Jagers zijn medewerkers die nieuwsgierig zijn en die steeds op zoek zijn naar een verklaring voor alles wat zij om zich heen waarnemen. Dit alles zonder dat de betreffende medewerker voortdurend spoken ziet. In Nederland bestaat een aantal organisaties die beveiligingsmedewerkers hebben opgeleid tot jager, of die daar mee bezig zijn. De beveiligingsmedewerkers die bij deze organisaties werken zijn iedere dag opnieuw met het vak 'beveiligen' bezig. Als er aan het einde van de dienst geen test heeft plaatsgevonden, hoe klein die test ook was, is de jager teleurgesteld. Hij heeft geen tegenstander kunnen vangen. Het oogt misschien wat overdreven om een dergelijke manier van dienstuitvoering te implementeren, maar het is wel de enige manier om ervoor te zorgen dat beveiligingsmedewerkers klaar zijn voor de aan hen toebedeelde taak op het moment dat het er op aan komt. Hoe groot is de kans dat een crimineel of terrorist wordt ontdekt als de beveili-

gingsmedewerker passief zit te vissen? Volgens mij zwemmen de meeste vissen langs de hengel, zeker als ze kunnen nadenken en weten wat het doel van 'aas' is.

Dreigingsassesment

Hoe wordt een beveiligingsmedewerker nu een goede jager? Het begint met het vertellen aan de beveiligingsmedewerkers tegen welke dreigingen de organisatie zich wil beveiligen. De security manager zal zich bewust moeten zijn dat risico's die de organisatie heeft onderkend, als uitkomst van de risicoanalyse, voor de uitvoerende beveiligingsmedewerker niet interessant zijn. Voor een beveiligingsmedewerker zijn alleen de 'dreigingen' interessant die waarneembaar zijn en waarvan hij of zij verwacht wordt ze te kunnen herkennen. De security manager zal dan ook in staat moeten zijn om door criminele en terroristische organisaties gebruikte scenario's voor de eigen beveiligingsmedewerkers inzichtelijk te maken. Tevens zal de security manager de beveiligingsmedewerkers moeten leren welke gedragingen van criminelen en terroristen hij of zij kunnen zien en welke vervolgacties van hem of haar verwacht worden als er een mogelijke dreiging wordt waargenomen. Daar waar een security manager geen inzicht heeft in scenario's die criminele en terroristische organisaties gebruiken en niet weet hoe scenario's kunnen worden herkend, kan dit ook niet van beveiligingsmedewerkers worden verwacht. Het ontbreken van dergelijke kennis maakt de organisatie kwetsbaar. Voor het op een juiste wijze kunnen toepassen van *red teaming* zal de veelal gebruikte risicobenadering van de security manager op strategisch-tactisch niveau aangevuld moeten worden met een dreigingbenadering op tactisch-operationeel niveau. Dit is een ontwikkeling die wij in Nederland nog niet veel tegenkomen. Een uitdaging. Onze tegenstanders verdiepen zich immers ook in onze beveiligingsmaatregelen, misschien dat het tijd wordt dat wij als security managers ons eens gaan verdiepen in de werkwijze van onze tegenstanders?

Literatuur

Broder, J.F. (2000) *Risk Analysis and the Security Survey*, Boston: Butterworth-Heinemann / member of the Reed Elsevier Group.
Claes, P.F. en Meerman, H.J.J.M. (1998) *Riskmanagement; inleiding tot het risicobeheersingsproces*, Houten: Stenfert Kroese.
Coumou, C. (2003) *Risicomanagement voor security- en facilitymanagers*, Alphen aan den Rijn: Kluwer.
Roper, C.A. (1999) *Riskmanagement for Security Professionals*, Boston: Butterworth-Heinemann / member of the Reed Elsevier Group.

