IT'ERS, REGELS EN SECURITY AWARENESS

Afstudeerthesis in het kader van de
Masteropleiding Security in Information Technology
aan de Technische Universiteit Eindhoven

Drs. Caroline Neys

Versie 1.1 (open) April 2003

VOORWOORD

Deze thesis is uitgevoerd in het kader de Masteropleiding Security in Information Technology aan de Technische Universiteit Eindhoven.

Ik verwacht met dit werk een bijdrage geleverd te hebben aan de beeldvorming over beveiligingsbewustzijn binnen mijn organisatie. Omdat ik overtuigd ben van het succes er van zou ik graag de voorgestelde oplossing voor het awareness-probleem bij IT'ers in mijn organisatie toepassen om zo ook een praktische bijdrage te leveren aan het niveau van informatiebeveiliging.

Verder wil ik de volgende mensen hartelijk danken:

- Allereerst mijn twee begeleiders: Dr. T.W. v.d. Schaaf en Prof. dr. ir. H.C.A. van Tilborg. Henk voor het reviewen van de literatuurstudie en de thesis. Tjerk voor de inzet en het enthousiasme waarmee hij me door de afstudeerfase geloodst heeft.

- Evelien van der Meijs voor haar aanmoedigingen en organisatorische ondersteuning gedurende het hele opleidingstraject.

- Vervolgens mijn collega-Security Managers bij Rabobank ICT. Gijs v. Slooten en Dirk Vijver voor het aanleveren van de achtergrondinformatie bij de incidentbeschrijvingen. Martin Kimenai en Thomas Coppens voor het uitvoeren van de contratest en dezelfde Martin en Paul Samwel voor het bijzonder snel, maar toch kritisch reviewen van de eerste versies.

- Rabobank ICT voor het feit dat ze mij in de gelegenheid heeft gesteld de opleiding te volgen.

- Mijn ouders Charles en Ine Neys voor het liefdevol overnemen van mijn oppasdag.

- In het bijzonder tenslotte mijn man Arthur Rottier voor het begrip en alle ondersteuning en mijn dochtertje Claire voor het opvrolijken van de lange studiedagen en -nachten.

INHOUDSOPGAVE

HOOFDSTUK 1: AANLEIDING

INTRODUCTIE

Informatiebeveiliging krijgt in een toenemend aantal organisaties een vaste positie. Beveiligingsstandaarden als COBIT[1], BS 7799[2] en de Code voor Informatiebeveiliging[3] hebben een grote bijdrage geleverd aan de structurele wijze waarop organisaties de afgelopen jaren hun informatiebeveiliging hebben ingericht. Veel organisaties worden zich bewust van het feit dat technische en organisatorische maatregelen niet garant staan voor een voldoende mate van beveiliging. Het is belangrijk hoe mensen omgaan met deze technische middelen en procedures en of ze ontworpen en vastgesteld zijn met 'mensen' in het achterhoofd.

In de Code voor Informatiebeveiliging wordt security awareness onder de kop 'Personeel', één van de 10 belangrijkste aandachtsgebieden voor informatiebeveiliging, genoemd als belangrijk aspect waarvoor doelstellingen en activiteiten geformuleerd dienen te worden. Er wordt echter niet vermeld hoe een gewenste status van beveiligingsbewustzijn te bereiken is.

Ter voorbereiding op deze thesis is bestudeerd hoe er in de literatuur aangekeken wordt tegen het bereiken van gedrag- en cultuurverandering in organisaties[4] . Ook is gezocht naar bestaande methodes om de bijdrage van mensen aan informatiebeveiliging zo positief mogelijk te maken. Uit deze literatuurstudie is de volgende definitie voor security awareness overgenomen[5]:

> Security awareness is de mate waarin elke medewerker de volgende punten begrijpt
> - het belang van informatiebeveiliging voor de organisatie
> - het niveau van informatiebeveiliging dat voor de organisatie noodzakelijk is

> en er ook naar handelt.

De termen security awareness en beveiligingsbewustzijn duiden in deze thesis beiden op deze definitie en zullen dan ook door elkaar gebruikt worden.

---

[1] CobiT (Control Objectives for Information and Related Technologies) is een open industriestandaard die goede praktijken in het beheer, controle en beveiliging van informatietechnologie beschrijft, georganiseerd rond een logisch raamwerk van 34 IT processen. CobiT werd ontwikkeld door ISACA (Information Systems Audit and Control Association), een internationale beroepsvereniging met meer dan 30.000 leden wereldwijd.

[2] BS(British Standard) 7799 is ontwikkeld door het Department of Trade and Industry en wordt uigegeven door het British Standards Institute. Inmiddels is er een ISO standaard die volledig gebaseerd is op deze BS: ISO/IEC 17799-1.

[3] De Code voor Informatiebeveiliging dateert uit 1994 en is de vertaling van de Engelse Code of Practice for Information Security Management (BS 7799). De Code biedt het management principes ter bescherming van informatie binnen bedrijven. Niet alleen de beveiliging van computers en netwerken komt daarbij aan bod, maar ook de informatie die is opgeslagen in papieren documenten, op video, in antwoordapparaten en organizers. De kern van de Code bestaat uit 8 essentiële maatregelen, 10 hoofdcategorieën, 36 doelstellingen en 125 maatregelen

[4] Zie Rapport Literatuuronderzoek Security Awareness, C. Neys, maart 2003

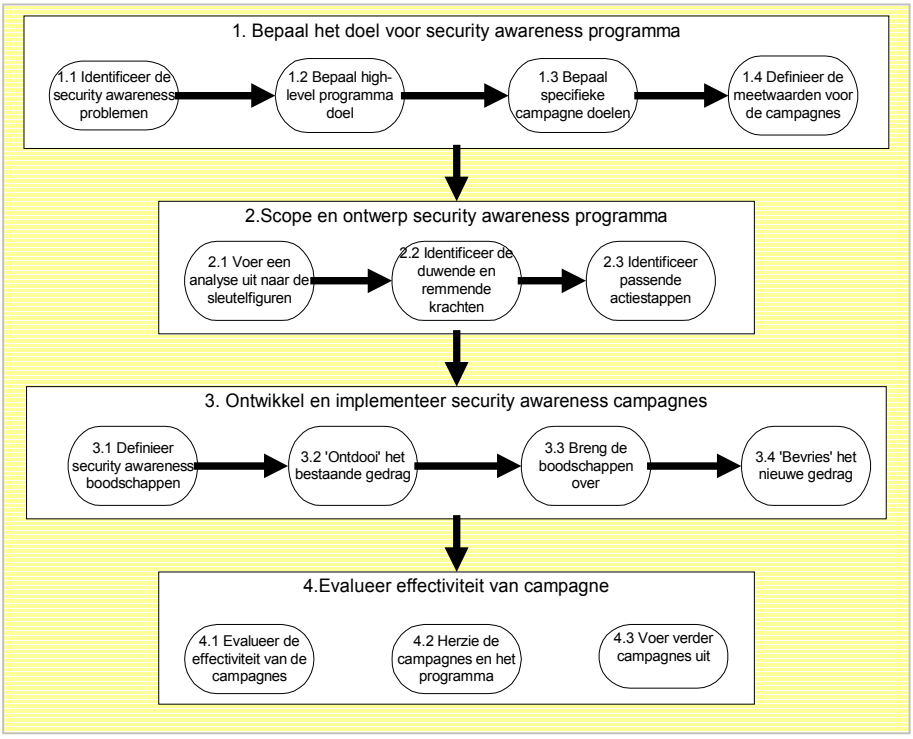
[5] Deze definitie is vrijwel gelijk aan de ISF definitie uit [ISF-1]. Alleen het begrijpen van 'de eigen verantwoordelijkheid' als derde punt is weggelaten. Dit omdat dit punt verwoord is in het Informatiebeveiligingsbeleid, welke het belang van informatiebeveiliging voor de organisatie en het minimaal vereiste niveau weergeeft.

Veel organisaties hebben zelf initiatieven ontplooid om het beveiligingsbewustzijn te verbeteren. Deze initiatieven zijn grofweg in twee groepen te verdelen, te weten de eerste en de tweede generatie.

De eerste generatie organisaties die iets aan security awareness wilde doen, zocht met veel goede wil hun heil in éénmalige acties zoals het verspreiden van foldermateriaal, postercampagnes of een lezingencyclus. Het bleek dat deze activiteiten vaak wel het gewenste effect hadden, maar dat de gedragsverandering slechts van korte duur was[6].

Bij de tweede generatie security awareness programma's is men gaan nadenken over een effectievere wijze van het overbrengen van de boodschap voor een blijvend effect. Dit heeft geresulteerd in een nog steeds groeiend aantal publicaties[7] over dit onderwerp.

Uit de literatuurstudie blijkt dat de meeste 'tweede generatie' methodieken min of meer dezelfde kenmerken in zich hebben. In vergelijking met de eerste generatie betreft het hier continue processen, waarbij een duidelijke rol van het management of andere sleutelfiguren in het bedrijf is weggelegd en waarbij zowel het doel als het resultaat meetbaar worden gemaakt. Het ISF Framework heeft alle kenmerken in zich en is daardoor een goed voorbeeld.



Figuur 1: Process for Effective Security Awareness. ISF, april 2002

Oorspronkelijk was het idee om voor de afstudeerthesis te onderzoeken of deze ISF methode ook effectief is ter verbetering van het beveiligingsbewustzijn bij de eigen werkgever, Rabobank ICT. Om verschillende redenen is dit uiteindelijk niet de probleemstelling geworden. De verklaring hiervoor moet gezocht worden in de actuele status van informatiebeveiliging bij Rabobank ICT en de bruikbaarheid van methodes zoals die van ISF. Deze aspecten zullen hierna

[6] o.a. [WU], [CO] en [HE]

[7] o.a. [BA], [ISF-1], [OU], [NOO] en [SI]

besproken worden. Alvorens te komen tot de definitieve probleemstelling zal ook ingegaan worden op het belang dat binnen de organisatie gehecht wordt aan het beveiligingsbewustzijn van medewerkers.

SITUATIESCHETS RABOBANK ICT

Ook bij de Rabobank Groep[8] is eind jaren '90 begonnen om informatiebeveiliging structureel in te bedden in de organisatie. Na een periode van uitgebreide beeldvorming over informatiebeveiliging en het opbouwen van een Information Security Framework, werd midden 2000 een nieuw Informatiebeveiligingsbeleid[9] van kracht. Deze was gestoeld op de BS 7799.

Met dit beleid als leidraad werd binnen Rabobank ICT[10] in 2000 gestart met het effectueren van de strategie en de tactische standaarden. Hierbij werd zoveel mogelijk geprobeerd om op overeenkomstige wijze als de andere groepsonderdelen invulling te geven aan de standaarden. Daarnaast werden gemeenschappelijk initiatieven ontplooid ter verbetering van de informatiebeveiliging. Consequentie van deze lijn is dat het soms lang duurt voordat zichtbare vooruitgang geboekt wordt.

Toen alle facetten van het framework ingevuld waren en het beleid, inclusief afgeleide operationele standaarden en gedragsregels, een vaste plek ingenomen hadden binnen de ontwikkel- en beheer activiteiten van Rabobank ICT, kon voorzichtig de balans worden opgemaakt:

- De beveiligingsnormen zijn vastgelegd in een groepsbreed geaccordeerd[11] beleid. Op een groeiend aantal vlakken zijn deze tactische standaarden vertaald naar operationele beheerstandaarden en blauwdrukken.

- Er is een gedragscode voor het gebruik van informatie- en communicatiemiddelen

- Er wordt samen met de andere groepsonderdelen overlegd over informatiebeveiliging in een beleidsvoorbereidend orgaan.

- Van de meeste componenten in de IT infrastructuur alsook van IT diensten en producten is vastgesteld wat de ' commerciële beveiligingswaarde' is.

---

[8] Voor een overzicht van de Rabobank Groep, zie het organisatie-organigram op www.rabobankgroep.nl.

[9] Informatiebeveiliging Rabobank Groep, Strategie en tactische standaarden. Versie 3.0, augustus 2000

[10] Rabobank ICT is een onderdeel van Rabofacet. De activiteiten van de Rabobank Groep worden ondersteund door ICT en facilitaire diensten. Rabofacet houdt zich bezig met de ontwikkeling en het beheer van businessapplicaties, internet- en intranettoepassingen, de centrale verwerking van bancaire transacties, de ICT infrastructuur voor circa 2.900 geldautomaten en circa 1.600 vestigingen. Daarnaast verzorgt Rabofacet de werkplekondersteuning voor 40.000 medewerkers van de Rabobank Groep, de post, de logistiek en het centraal afsluiten van inkoopovereenkomsten.

[11] De Rabobankorganisatie heeft een traditie in het midden- en kleinbedrijf en met name in de agrarische sector. Door op coöperatieve basis samen te werken is een financiële instelling ontstaan die het klanten mogelijk maakt hun financiële ambities in te vullen. Dit vormt het kompas van de Rabobank Groep: zij wil het mensen en ondernemingen mogelijk maken onafhankelijk en volwaardig deel te nemen aan het economische verkeer. De leden van Rabobank Nederland zijn de Rabobanken. Een regelmatige overlegstructuur zorgt ervoor dat de leden gezamenlijk en volgens een democratisch principe beslissen over het beleid van Rabobank Nederland. In een coöperatieve organisatie als de Rabobank Groep is het feit dat er een gemeenschappelijk informatiebeveiligingsbeleid is, dat door de moederorganisatie en alle gelieerde instellingen onderschreven is, een belangrijke mijlpaal op weg naar een betere informatiebeveiliging.

- Bijvoorbeeld met behulp van een risicoanalyse, kan bepaald worden op welk niveau deze waardevolle informatie-items beschermd moet worden. Dit is vervolgens te koppelen aan beveiligingsstandaarden.

- Het beheer is ingericht gebruik makende van de ITIL methodiek. Zo is het Change Management proces ingericht en wordt er een configuratiedatabase bijgehouden.

- Er is een EDP-audit afdeling die controle houdt op belangrijke, door de Raad van Bestuur te bepalen, IT trajecten.

- Incidenten worden geregistreerd en er zijn escalatieprocedures voor die gevallen waarin het incident niet direct verholpen kan worden.

- In geval van nood treedt er een calamiteitenplan in werking.

In het algemeen luidt de conclusie dat het niveau van informatiebeveiliging de afgelopen 5 jaar een sprong vooruit heeft gemaakt. Deze constatering werd gedaan na de eerste evaluatie van de effecten van de invoering van het beleid in 2001. Er werden ook enkele verbeteringen noodzakelijk geacht. De aanbevelingen[12] uit de evaluatie leidde tot de start van het Programma Informatiebeveiliging Rabobank Groep, waarbinnen een aantal projecten valt die gericht zijn op het verbeteren van het niveau van informatiebeveiliging. Rabobank ICT participeert in alle programma onderdelen.

Eén van de geconstateerde zwakke punten is het gebrek aan security awareness. De evaluatienota maakt melding van een negatieve afwijking van de door het ISF aangegeven benchmark Security Awareness. In [ISF-4] en [ISF-5] wordt uitgelegd hoe deze benchmark (SM24) tot stand gekomen is en wordt aangetoond dat organisaties die het benchmarkniveau op alle fronten bereikt hebben de kans op incidenten met 79 % zien afnemen.

Het gebrek aan beveiligingsbewustzijn lijkt enerzijds te komen doordat er onvoldoende gecommuniceerd wordt over de beveiligingsregels. Anderzijds leeft onder informatiebeveiligers sterk het idee dat al zouden de regels dagelijks onder de aandacht worden gebracht, het aantal overtredingen onverminderd hoog zou zijn. Security awareness is voor Rabobank ICT een sleutelbegrip geworden: zonder een grotere mate van bewustzijn van mogelijke risico's en inzicht in het gewenste gedrag, lukt het niet om het gewenste niveau van informatiebeveiliging te bereiken binnen de organisatie. In de volgende paragraaf wordt verder ingegaan op het belang van een hoge mate van beveiligingsbewustzijn van medewerkers binnen Rabobank ICT.

[12] Aanbevelingen zijn terug te vinden in de nota "Status Informatiebeveiliging Rabobank Groep" zoals goedgekeurd door de Hoofddirectie d.d. 10 juli 2001.

HET BELANG VAN BEVEILIGINGSBEWUSTE MEDEWERKERS

Aan de hand van een beschrijving van de rol van informatiebeveiliging binnen de organisatie en de bijdrage die daarbij van medewerkers verwacht wordt volgt hier een uitleg waarom security awareness van IT'ers zo belangrijk is voor Rabobank ICT

In de introductie is aangegeven welke definitie van security awareness in deze thesis gehanteerd wordt. De woorden "begrijpen" én "ernaar handelen" vormen essentiële punten in deze definitie. Kennis, inzicht (begrijpen) en gedrag conform kennis en inzicht (ernaar handelen) worden beschouwd als de drie kernaspecten van security awareness. Er bestaan verschillende modellen waarin deze begrippen, samen met termen als houding, emoties, omgeving, motivatie en intenties op diverse wijze in relatie tot elkaar worden gebracht. Het is niet de bedoeling hier verder in te gaan op deze gedragsmodellen[13].

Het is wel belangrijk voor het verdere onderzoek om te bepalen hoe beveiligingsbewustzijn zich verhoudt tot informatiebeveiliging. Hiervoor wordt de volgende denklijn gehanteerd[14] :

- Het niveau van informatiebeveiliging wordt bepaald door de technische en organisatorische maatregelen[15] die genomen zijn ter bescherming van waardevolle informatie. Daarnaast wordt steeds duidelijker dat het niveau van beveiliging in belangrijke mate afhankelijk is van de bijdrage die mensen leveren om deze maatregelen tot een succes te maken. Dit blijkt uit de problemen die organisaties ondervinden om met louter technische en organisatorische middelen hun informatiebeveiliging op het gewenste niveau te krijgen en te houden.

- De bijdrage van medewerkers is daarmee één van de factoren die van invloed is op het niveau van informatiebeveiliging van een organisatie. Het niveau van beveiliging is bepalend voor de mate waarin een organisatie beveiligingsrisico's loopt.

- Dit risico wordt bepaald door de kans op verstoring (bedreiging), de mate van kwetsbaarheid van objecten van informatievoorziening en de potentiële schade die gelopen wordt indien de verstoring zich daadwerkelijk voordoet.

- Omgekeerd geldt dat bepaalde type organisaties intrinsiek een hoger risico lopen door de aard van hun dienstverlening. Voor een financiële instelling zoals de Rabobank Groep geldt dat verwacht wordt dat deze een hoger niveau van beveiliging kent dan

[13] In [WO] worden een aantal gedragsmodellen die toegepast worden op security awareness behandeld.

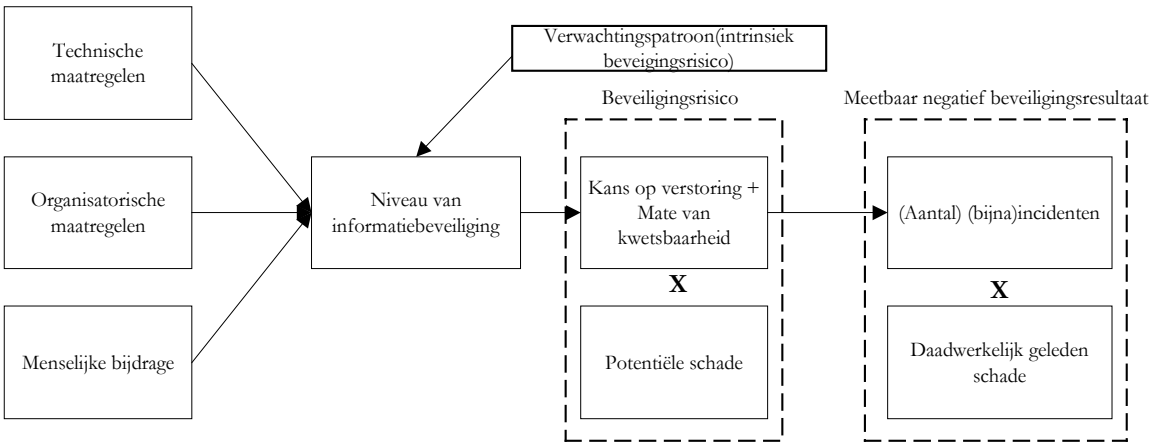
[14] De gebruikte definities van risico, bedreiging, kwetsbaarheid zijn ontleend aan [OV]. De relatieschema's niet.

[15] In [OV] wordt uitgegaan van fysieke, logische en organisatorische maatregelen. Deze indeling komt voort uit een gelaagd model van de structuur voor informatievoorziening. De onderste twee lagen zijn de basisinfrastuctuur (kabels, gebouwen) en de IT-infrastuctuur. De fysieke maatregelen richten zich hierop. Daarna volgen de gegevensinfrastructuur en de applicaties. Hierop zijn de logische maatregelen gericht. Tenslotte richten de organisatorische maatregelen zich op procedures en de bewustwording en het gedrag van gebruikers. De keuze voor de indeling in technische en organisatorische maatregelen en de bijdrage van de mens komt de gedachte dat de mens niet alleen passieve gebruiker is maar ook degene die de maatregelen bedenkt, regisseert en manipuleert. De mens is daardoor de bepalende factor bij het slagen of falen van technische en organisatorische maatregelen. Daarnaast wordt uitgegaan van een keuzemogelijkheid bij elk informatiebeveiligingsprobleem, ongeacht zijn plaats in de gelaagde werkingsgebieden uit het model van [OV]. Deze keuzemogelijkheid bestaat uit óf een technische óf een organisatorische oplossing óf een combinatie van beide. Er zijn ook andere indelingen mogelijk. Bijvoorbeeld naar aangrijpingspunt in de ontwikkeling van een incident zijn er achtereenvolgens, preventieve, detectieve, repressieve en correctieve maatregelen.

bijvoorbeeld een bakker, omdat een belangrijk deel van de dienstverlening van een bank gebaseerd is op het vertrouwen dat een klant in hem stelt. De kans dat er bij een incident imagoschade gelopen wordt is daarom veel groter dan bij de bakker. Ook de mate waarin financiële schade gelopen kan worden is veel hoger. De bank zal daarom verwacht worden meer aandacht te bestenden aan het verminderen van risico's, wat weer tot uitdrukking komt in het noodzakelijke niveau van informatiebeveiliging.

- Hoe groter de kans op verstoring en mate van kwetsbaarheid hoe groter het aantal (bijna)incidenten dat zich in werkelijkheid voordoet. Bijna-incidenten zijn die gevallen waarbij door in te grijpen een verstoring voorkomen wordt voordat een echt incident ontstaat.

- De daadwerkelijke schade die geleden is door de (bijna-)incidenten bepaalt het meetbare negatieve beveiligingsresultaat van een organisatie.



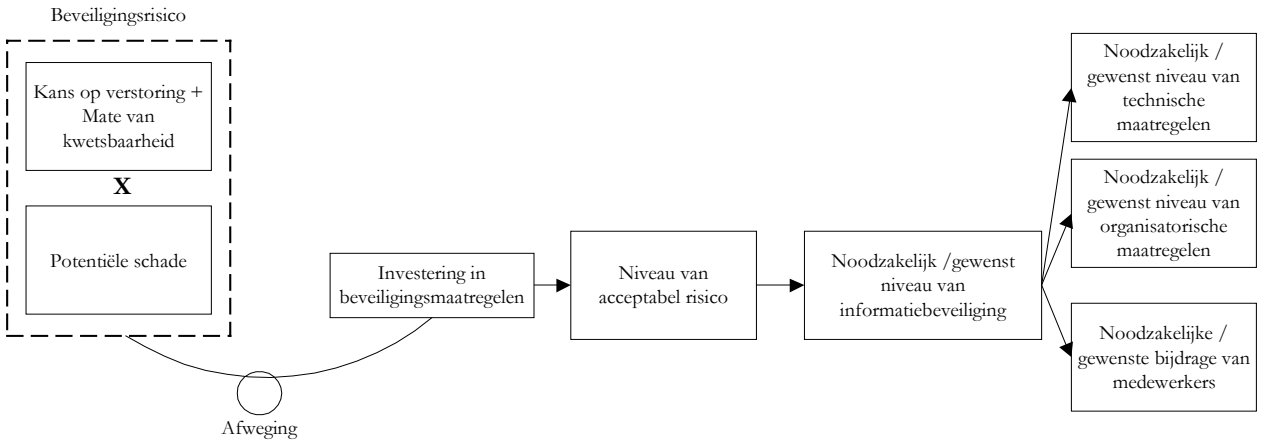
Figuur 2: Menselijke bijdrage aan informatiebeveiliging

- Het gewenste niveau van de menselijke bijdrage wordt, samen met het gewenst niveau van technische en organisatorische maatregelen, bepaald door het gewenste niveau van informatiebeveiliging.

- Er is een verschil tussen het niveau dat gewenst is en het vereiste niveau. Voor een goede informatiebeveiliging dient het gewenste niveau minstens het vereiste niveau te zijn, maar het kan ook hoger liggen. Er wordt hier verder van uitgegaan dat binnen Rabobank ICT het gewenste niveau van informatiebeveiliging gelijk is aan dit minimale niveau van informatiebeveiliging, en dus het vereiste (noodzakelijke)niveau.

- Het noodzakelijke (gewenste) niveau wordt bepaald door het belang dat een organisatie heeft bij een goede informatiebeveiliging.

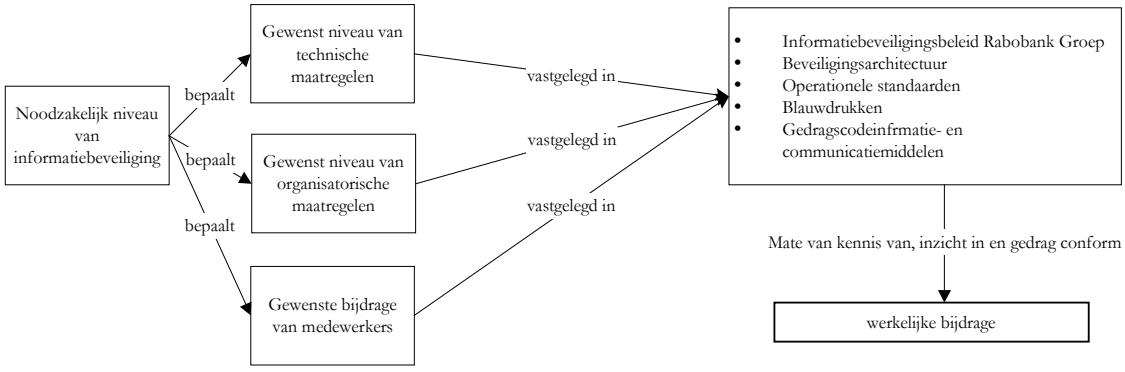
- Dit belang wordt bepaald door het tegen elkaar afwegen van het beveiligingsrisico (vgl. figuur 2) en de noodzakelijke investeringen in beveiliging om het risico weg te nemen of te verminderen. Deze afweging leidt tot het vaststellen van een niveau tot waar risico's acceptabel zijn.



Figuur 3: Gewenste bijdrage van medewerkers in verhouding tot het belang van informatiebeveiliging

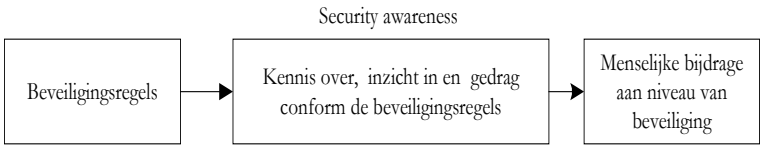
- Het gewenste niveau van maatregelen en menselijke bijdrage komt binnen Rabobank ICT tot uitdrukking in standaarden en -richtlijnen. In de eerste plaats is dat het Informatiebeveiligingsbeleid, waarin strategie en tactische standaarden zijn beschreven. De strategie biedt ook inzicht in het belang van informatiebeveiliging voor de organisatie doordat het spel van afweging van risico versus investering, zoals weergegeven in figuur 3 beschreven wordt. Daarnaast kent de organisatie ook een beveiligingsarchitectuur, operationele standaarden, blauwdrukken en een gedragscode voor de omgang met informatie- en communicatiemiddelen. Hierna zal de term 'beveiligingsregels' gebruikt worden om te refereren aan deze strategie, standaarden en richtlijnen.

- Binnen Rabobank ICT wordt de werkelijke menselijke bijdrage bepaald door de mate van kennis van, inzicht in en gedrag conform de standaarden en richtlijnen. Refererend aan de definitie van security awareness, is beveiligingsbewustzijn dus de bepalende factor in de bijdrage die een medewerker levert aan het niveau van informatiebeveiliging.



Figuur 4: Betekenis van security awareness voor een organisatie

- Een grote mate van beveiligingsbewustzijn resulteert in een belangrijke positieve bijdrage. Indien het beveiligingsbewustzijn laag is, is de bijdrage minder groot. Dit kan zelfs een negatief effect hebben op het niveau van beveiliging.



Figuur 5: security awareness als schakel tussen beveiligingsregels en de menselijke bijdrage aan het niveau van beveiliging

Het probleem waar Rabobank ICT, net als vele andere organisaties overigens, mee kampt is dat de werkelijke bijdrage niet in overeenstemming is met de gewenste bijdrage. Het streven is om een positievere bijdrage van medewerkers te bewerkstelligen. Het verbeteren van security awareness moet dus in dienst staan van het streven naar een positievere bijdrage van de medewerker aan het niveau van informatiebeveiliging. Het moet geen doel op zich zijn.

In het kader van het Programma Informatiebeveiliging is daarom in 2001 een Security Awareness Framework opgesteld. Daarbij is gebruik gemaakt van de kennis en ervaring van het ISF. Het Framework vertoont dan ook veel gelijkenis met het ISF Process for Effective Security Awareness (figuur 1). Het doel werd als volgt omschreven[16]:

> Het Security Awareness Framework beoogt diverse hulpmiddelen op te leveren voor een zo effectief en efficiënt mogelijke communicatie over (informatie)beveiliging binnen alle groepsonderdelen van de Rabobank Groep. Deze communicatie dient een beveiligingsbewust gedrag te bewerkstelligen onder andere via de verhoging van het kennisniveau over (informatie)beveiliging. Bij de realisatie van de hulpmiddelen wordt voor zover opportuun standaardisatie nagestreefd.

Het Awareness Framework is nadrukkelijk bedoeld om invulling te geven aan de vereisten uit het informatiebeveiligingsbeleid met betrekking tot het opleiden en informeren van gebruikers over informatiebeveiliging en gaat uit van een gedragsmodel waarbij onderscheid gemaakt wordt tussen drie doelgroepen te weten 'medewerkers algemeen, '(lijn)managers' en 'IT'ers'.

Binnen het Awareness Framework project is besloten voorlopig de aandacht te richten op de doelgroep 'medewerkers algemeen en prioriteit te geven aan het ontwikkelen van één hulpmiddel namelijk een E-learning module. De inhoud van de module is gericht op die aspecten van informatiebeveiliging die de gewone medewerker van de Rabobank Groep als gemiddelde gebruiker tegen komt tijdens een normale werkdag. Dit betekent dat ervan uitgegaan wordt dat de medewerker een standaard ingerichte werkplek ter beschikking heeft en ondersteund wordt door een IT beheerafdeling. Op dit moment wordt er een pilot uitgevoerd met de module.

Het beeld van de huidige situatie en de opgedane kennis uit het literatuuronderzoek hebben geleid tot het inzicht dat de door het Awareness Framework project gevolgde lijn niet de meest effectieve manier is voor het bereiken van een hogere mate van security awareness bij Rabobank ICT. Een ruime meerderheid van de medewerkers van Rabobank ICT oefent immers een functie uit die sterk IT gerelateerd is en daarom aangeduid kan worden met de term IT'er[17].

Wegens de, overigens begrijpelijke, keuze om voorlopig slechts één hulpmiddel te ontwikkelen en daarbij de aandacht niet te richten op IT'ers is dit initiatief niet bijzonder geschikt voor Rabobank ICT.

Voor de niet-IT'ers binnen Rabobank ICT wordt het initiatief van het Security Framework overigens van harte aanbevolen.

Belangrijker is echter de overtuiging dat de effectiviteit van het ISF Process for Effective Security Awareness ('Process'), dat als voorbeeld geldt voor het Rabobank Security Awareness Framework, binnen Rabobank ICT niet groot zal zijn. Deze overtuiging komt voort uit de volgende overwegingen:

Ten eerste wordt een langdurige en bijzondere inspanning verwacht van gedreven individuen. Ten tweede wordt nadrukkelijk gesteld dat zonder committment van belangrijke sleutelfiguren

[16] Uit: Programmamanagement informatiebeveiliging Awareness Framework, 7 juni 2001, A.J.M. Janssen Steenberg

[17] Binnen de classificatie 'IT'er' wordt bij Rabobank ICT het volgende onderscheid gemaakt Operator A/B/C, Beheerder A/B/C, Systeemanalist-programmeur A/B/C, IT-specialist B/C/D en Systeemontwerper A/B/C.

maar vooral ook van managers in allerlei lagen het 'Process' een kleine kans op succes heeft. Stel dat er enkele individuen de tijd en ruimte krijgen om zich te wijden aan het verbeteren van security awareness, dan vormt de coöperatieve overlegcultuur die binnen Rabobank ICT gebruikelijk is een probleem bij het aanwijzen van sleutelfiguren en het verkrijgen van het juiste committment. Rabobank ICT kent immers een organisatiestructuur waarbij nauwelijks sprake is van strakke hiërarchische beslislijnen. Committment van het hoogste management garandeert daarom niet dat de lagen daaronder ook meedoen. Bovendien zullen de krachtenvelden (stap 2.2 in het 'Process') lastig te identificeren blijken te zijn en hun invloed groter dan in qua doelstelling vergelijkbare organisaties. Ook bij eenvoudigere taken blijkt dat de invloed van belangengroepen of zelfs individuen die anders willen erg groot kan zijn.

Daarnaast heeft ook Rabobank ICT te kampen met bezuinigen en ontslagen door reorganisatie. Het is daarom niet het meest geschikte moment voor de start van grote, lees kostbare, campagnes.

Deze feiten geven aanleiding om aan te nemen dat de belangrijkste initiatieven van dit moment, ISF-achtige methodes in het algemeen en de e-learning module binnen het Rabobank Security Awareness Framework in het bijzonder niet doeltreffend zullen zijn bij Rabobank ICT.

De wens en de noodzaak om de bijdrage van medewerkers aan het niveau van beveiliging te verbeteren blijven echter onverminderd groot. Dit vormt de aanleiding om verder onderzoek te willen doen naar een effectieve wijze van het verbeteren van security awareness binnen Rabobank ICT.

HOOFDSTUK 2: PROBLEEMSTELLING, WERKWIJZE EN AFBAKENING

PROBLEEMSTELLING

In hoofdstuk 1 is de aanleiding voor verder onderzoek beschreven. In het kort komt het erop neer dat geconstateerd is dat mensen een belangrijke bijdrage kunnen leveren aan het niveau van informatiebeveiliging. Daarnaast is geconstateerd dat de bekende initiatieven om een positievere bijdrage te verkrijgen niet effectief zijn voor het onderzoeksgebied. Het probleem waar Rabobank ICT mee kampt, namelijk dat de bijdrage van IT'ers aan het beveiligingsniveau van de organisatie niet zo positief is als men zou wensen, is dus onverminderd groot. Vanuit deze aanleiding is de volgende probleemstelling ontstaan waar deze thesis een oplossing voor wil bieden:

> Het gedrag van IT'ers binnen Rabobank ICT draagt onvoldoende bij aan het vereiste niveau van informatiebeveiliging

De ernst van het probleem blijkt uit de lage benchmarkscore zoals vermeld in hoofdstuk 1 en uit de regelmaat waarmee de afdeling security management geconfronteerd wordt met meldingen van incidenten waarbij de oorzaak kan worden gezocht in gebrek aan inzicht in of sensibiliteit voor het beveiligingsrisico dat de organisatie loopt. De meldingen die binnenkomen bij Security Management zijn waarschijnlijk slechts het topje van de ijsberg[18].

Het recept voor een positieve bijdrage van IT'ers aan informatiebeveiliging lijkt eenvoudig: laat hen de beveiligingsregels van buiten leren. Vertel ze ook waarom die regels zijn zoals ze zijn en, uitgaande van de welwillendheid van de gemiddelde werknemer, zal in toenemende mate conform de regels gehandeld worden.

Dat dit een te simpele voorstelling is komt doordat er meer factoren blijken te zijn die van invloed zijn op het beveiligingsgedrag van medewerkers. Om welke factoren het gaat blijkt als geanalyseerd wordt hoe het komt dat medewerkers regels overtreden.

De oplossing voor het probleem wordt gezocht in een methode die door de organisatie gebruikt kan worden om een positievere bijdrage van IT'ers aan het niveau van beveiliging te bereiken. Bijkomend voordeel zou zijn dat de effectiviteit van de methode gemeten zou kunnen worden.

WERKWIJZE

Na geconstateerd te hebben dat er een probleem is in mijn organisatie ben ik op zoek gegaan naar een model waardoor ik beter inzicht zou krijgen in de situatie bij Rabobank ICT. Dit model heb ik gevonden in een model van Sharon Clarke[19], dat in hoofdstuk 3 besproken wordt..

De inzichten uit haar model, samen met de inzichten uit hoofdstuk 1 met betrekking tot het belang van de bijdrage van medewerkers voor het niveau van beveiliging, heb ik

[18] Tijdens een informele inventarisatieronde langs twee beheerafdelingen en een beheer-helpdesk bleek dat medewerkers en managers in staat waren veel meer voorbeelden van conflicten met de geldende beveiligingsregels uit hun dagelijkse praktijk konden noemen dan het aantal dat uit de officiële meldingen naar voren kwam.

[19] In [CL] wordt dit model beschreven. Het is deels gebaseerd op een gedragsmodel van J.Rasmussen.

toegepast op het onderzoeksterrein, Rabobank ICT. Dit leidde tot een mogelijke oplossingsrichting voor het geschetste probleem. Om de waarde van deze oplossing te toetsen zijn een drietal onderzoeksvragen opgesteld.

Vervolgens ben ik de onderzoeksvragen gaan beantwoorden. Daarbij heb ik gebruik gemaakt van de PRISMA-methode die in hoofdstuk 3 besproken wordt. Omdat deze methode niet eerder op het onderzoeksterrein van de IT is toegepast moest ook gekeken worden of de keuze voor deze methode legitiem was. De uitkomsten van het onderzoek en mijn eigen beoordeling daarvan heb ik verwoord in de sectie 'resultaten en interpretatie'. Tenslotte volgt een conclusie en een aantal aanbevelingen voor Rabobank ICT.

AFBAKENING ONDERZOEKSTERREIN

Het onderzoek naar een oplossing voor de onvoldoende bijdrage aan het niveau van beveiliging richt zich uitsluitend op IT'ers binnen de organisatie. Deze keuze is gemaakt omdat enerzijds de meerderheid van de medewerkers van Rabobank ICT onder deze categorie valt, en anderzijds omdat IT'ers door hun specifieke kenmerken een andere verhouding hebben met de informatiebeveiligingsregels dan medewerkers die slechts een gebruikersrelatie met de IT infrastructuur hebben[20].

IT'ers onderscheiden zich van gewone medewerkers door hun vaak specialistische kennis over en inzicht in bepaalde facetten van de IT infrastructuur. De boodschap die gedragscodes en awareness campagnes aan 'gewone medewerkers' richten vinden IT'ers te triviaal en ze voelen zich daarom niet aangesproken.

Het hoort bij specialisten om zich te bekwamen in hun vakgebied. Het vakgebied van de IT ontwikkelt zich snel. Om deze innovatie bij te houden dienen IT'ers vernieuwingen uit te proberen. Soms moeten daarvoor de begane paden overtreden worden. Daarmee kunnen ze echter de werking van de infrastructuur behoorlijk verstoren. Gewoon personeel heeft niet dezelfde mogelijkheden tot verstoring en heeft meestal ook niet dezelfde interesse in het uitproberen van nieuwe dingen.

Omdat ook IT adviseurs en projectleiders bij het uitoefenen van hun functie geconfronteerd worden met de grenzen van de regels, is gekozen om naast de in hoofdstuk 1, voetnoot 13 genoemde categorieën IT'ers ook de IT-adviseurs en IT-projectleiders te rekenen tot de groep medewerkers van Rabobank ICT waar deze thesis zich op richt.

[20] Voor deze stelling zijn geen harde bewijzen gevonden in de literatuur. Wel worden IT'ers in bijna alle 'tweede generatie'modellen voor effectieve security awareness, om de hier aangegeven redenen aangewezen als aparte doelgroep of als sleutelfiguren.

HOOFDSTUK 3: MODEL VAN 'NORMALE OVERTREDINGEN'

BESCHRIJVING VAN MODEL

In hoofdstuk 1 is reeds vermeld dat er verschillende modellen bestaan die beschrijven hoe gedrag ontstaat en te beïnvloeden is. Een model dat goed aansluit bij de situatie van Rabobank ICT is het model dat S. Clarke beschrijft in een artikel[21] over risicobeheersing in projecten[CL]. Dit model wordt hier gebruikt om het beveiligingsgedrag van IT'ers in de werksituatie binnen Rabobank ICT te analyseren. De basis wordt gevormd door een model van Rasmussen uit 1991[22] waarbij beschreven wordt hoe gedrag op het werk binnen bepaalde grenzen plaatsvindt.

De eerste grens die het gedrag beïnvloedt is de grens van het economisch falen. Managers eisen van medewerkers dat binnen bepaalde tijds- en budgetgrenzen geopereerd wordt. Deze druk van het management duwt de medewerker weg van de grens van economisch falen richting meer efficiency. Indien de grens overschreden wordt betekent dit de kans groot is dat wegens het overschrijden van deadlines of budgetten, er een streep gehaald wordt door de werkzaamheden.

De tweede grens wordt bepaald door het principe van de minste inspanning. Omdat een medewerker niet graag opgezadeld wordt met een overschot aan werk zal hij de neiging hebben om weg te gaan van de grens van de onacceptabele werkdruk.

In een poging weg te blijven van beide grenzen verplaatst de medewerker zich in zijn werkgedrag richting de buitenste grens die de beveiligingsregels representeert. Het management zal druk uitoefenen op de medewerker om ook deze grens niet te overschrijden, maar in de praktijk wijken de uitgevoerde processen af van de officieel voorgeschreven regels. Dit komt omdat medewerkers hun manier van werken aanpassen om tegemoet te komen aan de functionele werkdruk vanuit de omgeving.

Deze functionele werkdruk ontstaat doordat een medewerker constant de psychische en sociale omgeving toetst en deze informatie gebruikt om een mentaal model van zijn werkomgeving en activiteiten te maken. Ook zijn collega's zullen een dergelijk mentaal model ontwikkelen. Zowel persoonlijke als gezamenlijke ervaringen van bijvoorbeeld het team of de afdeling, maken deel uit van het model. Een deel van het mentale model wordt gevormd door 'improvisaties' en andere 'kort door de bocht'-regels, die succesvol bleken bij het oplossen van problemen, of een taak meer efficiënt maakten. Het feit dat dergelijke alternatieve regels beschikbaar zijn betekent dat de formele beveiligingregels niet noodzakelijkerwijs de uiterste grens zijn die het gedrag van een individu onder controle houdt. Gedragingen die, op een reguliere basis, afwijken van beveiligingsregels worden 'normale beveiligingsovertredingen' genoemd.

De buitenste grens voor 'normaal' gedrag wordt dus bepaald door de organisatiecultuur. Deze cultuur omvat een aantal ongeschreven regels die bepalen wat 'acceptabel gedrag' is. De afdelingscultuur is hier een afgeleidde van. Een positieve cultuur zal 'good practices' aanmoedigen onder medewerkers.

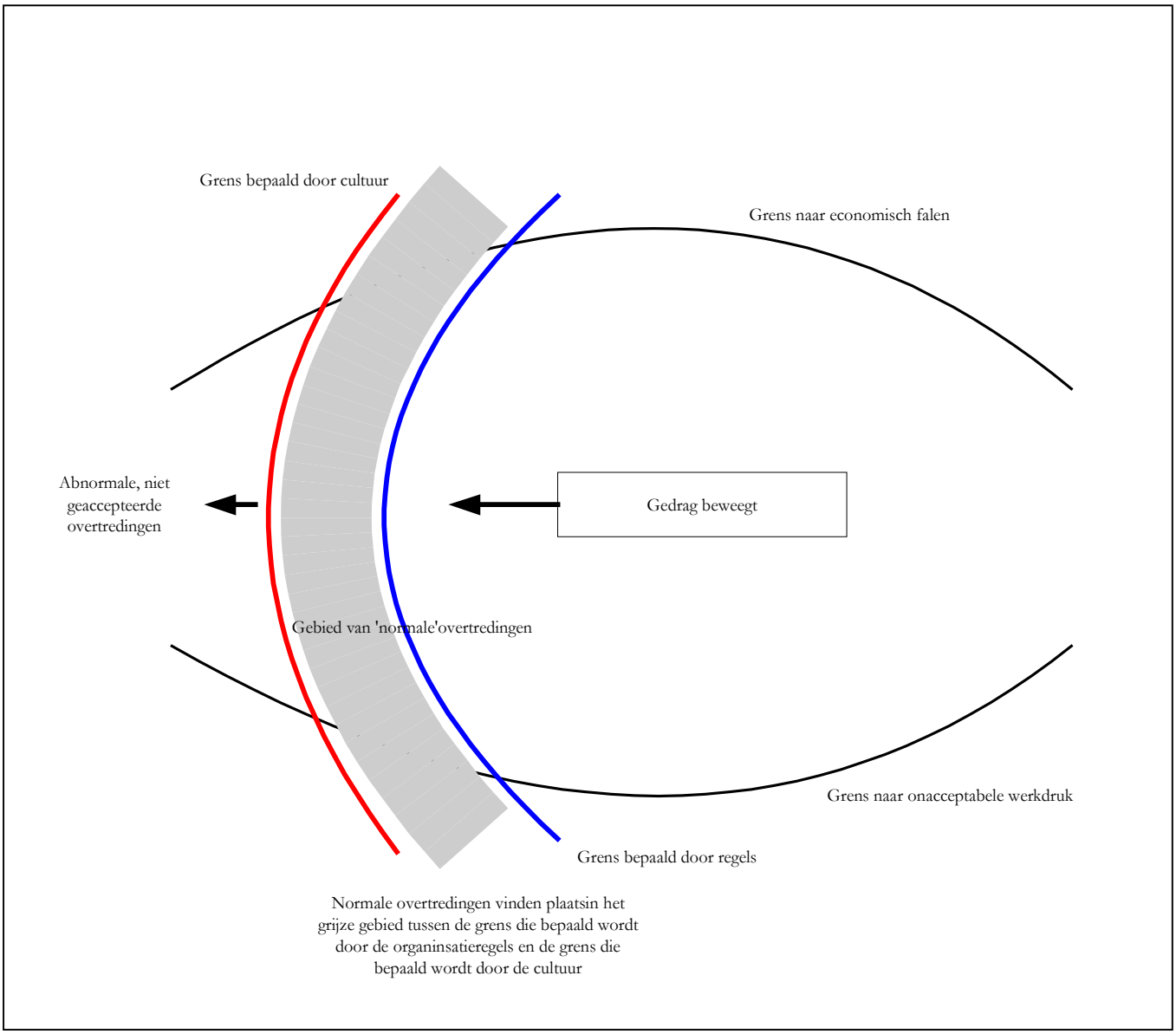
Het verschil tussen de grens die bepaald wordt door formele beveiligingsregels en de grens die bepaald wordt door de heersende cultuur vormt een grijs gebied, waarbinnen de 'normale

[21] In [CL] :'Violations as a Source of Project Risk', *The International Journal of Project & Business Risk Management*, Vol 1. Issue 2, 155-167.

[22] Clarke [CL] verwijst hier naar Rasmussen, J., Safety Control: Some basic distinctions and research issues in high hazard low risk operation. Paper als bijdrage aan Workshop on Risk Management, Bad Homburg, mei 1991

overtredingen' plaatsvinden. Dat wil zeggen handelingen die gedoogd worden, maar als normaal en acceptabel gedrag beschouwd worden door de medewerker en zijn omgeving.

Een voorbeeld is het inzetten van handige, maar niet toegestane hacktools om testen uit te voeren. Vaak gebeurt dit omdat het op dat moment de weg van de minste weerstand is. De tools zijn voorhanden en het doel van de test kan er mee bereikt worden. Binnen de afdeling is dit gedrag ook volledig geaccepteerd, waardoor er niet snel melding van zal worden gemaakt door een collega. Figuur 6 toont het hier beschreven model.



Figuur 6: Model van Clarke over 'normale overtredingen'

Dit model sluit goed aan bij de het onderzoeksterrein omdat juist mensen met meer dan gemiddelde kennis en mogelijkheden op een bepaald terrein de neiging hebben om af te wijken van de uitgezette paden. IT'ers worden beschouwd als specialisten op een bepaald gebied van de infrastructuur, die graag nieuwe ontwikkelingen binnen hun vakgebied uitproberen en zich 'te

goed' voelen voor gedragsregels die voor de gewone gebruikers gelden[23]. De kans dat IT'ers om wat voor reden dan ook afwijken van de geldende normen is groter dan de kans dat een gemiddelde gebruiker dat doet. Het inzicht dat er een grijs gebied is, waarbinnen overtredingen geaccepteerd worden, wordt daarmee extra relevant voor deze doelgroep.

Het model laat zien dat het gedrag van een medewerker richting de grens van formele regels wordt geduwd door krachten die hem van de grens van economisch falen en die van onacceptabele werkdruk afhouden.

Overtredingen ontstaan meestal omdat geprobeerd wordt een oplossing te vinden voor doelen die niet met elkaar in overeenstemming zijn. De druk vanuit deze verschillende doelen kan zo groot worden dat het overtreden van een beveiligingsregel de beste optie biedt. Als bijvoorbeeld de druk vanuit een opdrachtgever voor het op tijd in de lucht gaan van een nieuwe e-commerce toepassing erg groot is kan dit aanleiding zijn om een belangrijke testfase over te slaan. Hierdoor kan een essentiële fout niet of niet op tijd geconstateerd worden.

Ook toont het model dat er zoiets bestaat als een schermergebied waarbinnen gedrag plaatsvindt dat niet volgens de regels is maar toch geaccepteerd wordt.

Helemaal buiten de cultuurgrens valt gedrag dat echt onacceptabel gevonden wordt door de organisatie. Het gaat hier om forse overtredingen die onder geen beding door de organisatie worden toegestaan. Bij Rabobank ICT gaat het dan vrijwel altijd om forse overtredingen of overtredingen waarbij de Nederlandse Wet geschonden wordt. In het eerste geval moet gedacht worden aan opzettelijke hackpogingen vanaf een werkplek, in het tweede geval aan het verzamelen van illegaal beeldmateriaal op Rabobank systemen.

TOEPASSING VAN MODEL OP ONDERZOEKSGEBIED

In hoofdstuk 1 bleek dat er een causaal verband is tussen de bijdrage van medewerkers aan het niveau van beveiliging, de mate waarin medewerkers handelen naar de beveiligingsregels en het aantal incidenten. Indien de bijdrage van medewerkers onvoldoende positief is (negatief gaat een beetje te ver) dan zijn er relatief veel incidenten te vinden waarbij sprake is van de overtreding van een beveiligingsregel. Uit Clarke's model blijkt dat medewerkers die door de eisen van de manager of een te hoge werkbelasting onder druk staan, gedwongen zijn de grens van de geldende regels te overschrijden, wat tot incidenten leidt.

Indien zou blijken dat bij Rabobank ICT een groot aantal incidenten plaatsvinden die veroorzaakt worden door het overtreden van regels, terwijl bij slechts een klein aantal sprake is van boze opzet, dan zouden de meeste overtredingen dus in het door Clarke beschreven grijze gebied vallen en past het model van Clarke bij de situatie van Rabobank ICT. Het aantal incidenten veroorzaakt door overtredingen zou bovendien een indicatie geven van de ernst van het probleem. Indien er beveiligingsregels overtreden worden, betekende dit dat het risico dat de organisatie loopt verhoogd wordt. De beveiligingsregels weerspiegelden immers het minimale niveau van beveiliging. Een groter risico kan leiden tot meer en ernstigere incidenten.

Het grijze gebied zou binnen Rabobank ICT best wel eens relatief groot kunnen zijn. Dit zou verklaren waarom het zo moeilijk is om het beveiligingsbewustzijn van medewerkers te adresseren. Indien niet duidelijk is wat van de medewerker verwacht wordt zal hij zelf in zijn

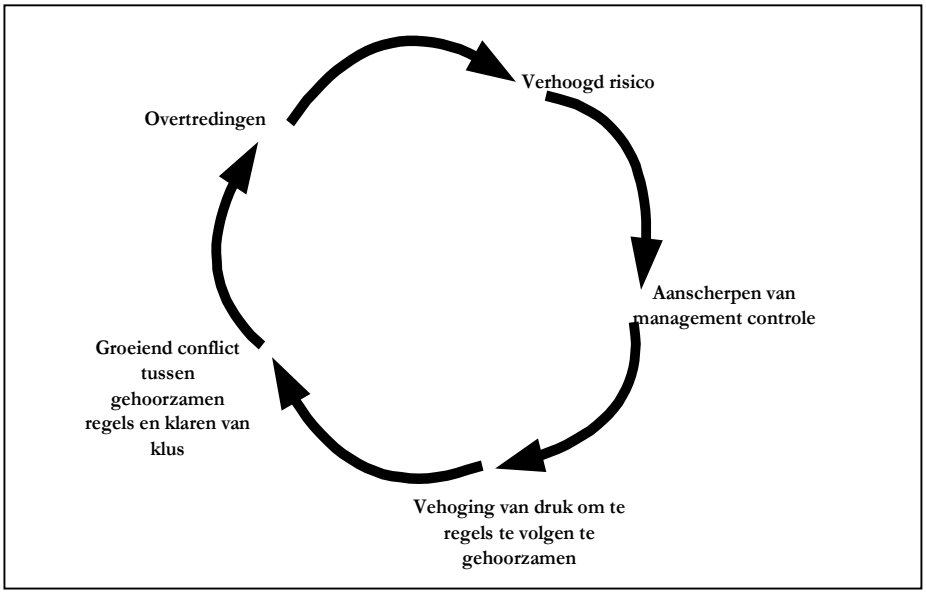
[23] Vooruitlopend op het onderzoek kan gemeld worden dat slechts 2 van de 86 geanalyseerde beveiligingsincidenten veroorzaakt werd door een niet-IT'er. In beide gevallen betrof het een verkeerde autorisatie-actie van een administratieve medewerker. Hierbij moet opgemerkt worden dat er nog 6 incidenten waren waarbij sprake was van boze opzet, maar niet bekend is of dit door een IT'er of een niet-IT'er is veroorzaakt.

omgeving zoeken naar 'best practices' en die kunnen best anders zijn dan de officiële beveiligingsregels. Het is voor een medewerker hierdoor niet eenvoudig om te bepalen wat nu eigenlijk van hem verwacht wordt. Wat is het gewenste gedrag en wanneer handelt hij conform de 'regels', indien die 'regels' deels uit ongeschreven en door de organisatiecultuur bepaalde, ongeschreven normen bestaan. Het bepalen van de eigen verantwoordelijkheid wordt op deze manier bijzonder lastig. De medewerker heeft niet zwart op wit wat hij moet doen in een bepaalde situatie.

Vaak wordt ook het risico dat de organisatie loopt door deze gedoogde overtredingen onderschat. Het is dus in het belang van de organisatie om deze overtredingen terug te dringen.

Stel dat er voldoende incidenten gevonden kunnen worden om het model van Clarke toe te passen op Rabobank ICT, dan rijst de vraag wat binnen Rabobank ICT de oorzaken zijn van deze overtredingen en wat de mogelijkheden zijn om er wat aan te doen. Voor het beantwoorden van deze vraag wordt eerst weer teruggegaan naar Clarke [CL].

Er van uitgaande dat een groot aantal beveiligingsincidenten in het grijze gebied valt, en dus in eerste instantie veroorzaakt worden door overtredingen van de beveiligingsregels, zou de meest logische reactie[24] zijn om de oplossing voor deze overtredingen te zoeken in het aanscherpen van de regels zelf en de controle op de naleving ervan door het management. Clarke[CL] laat echter zien dat dit juist geen goede oplossing is en een verlammend effect heeft op de bijdrage van medewerkers waardoor een negatieve spiraal ontstaat waarin een strakkere controle leidt tot meer overtredingen, een groter beveiligingsrisico en dus ook meer incidenten. Meer regels en strakkere controle leidt namelijk tot meer druk op de medewerkers om binnen de vereiste normen te opereren. Dit leidt vervolgens tot conflicten tussen het (moeten) volgen van de regels en het 'klaren van de klus'. Het gevolg is dat er weer regels overtreden moeten worden, wat leidt tot nog meer regels of scherpere controle.



Figuur 7: Clarke's model van de negatieve spiraal waarbij strengere controle op regels leidt tot meer overtredingen en hoger risico

[24] Uit onderzoek van Ho en Pike [CL] blijkt dat dit de meest voorkomende managementreactie is en geldt als 'best practice'.

Om te voorkomen dat uit het feit dat er zoveel incidenten in het grijze gebied vallen, onmiddellijk de conclusie getrokken wordt dat regels en de controle erop moeten worden aangeschept of de sancties verhoogd, moeten deze overtredingen geanalyseerd worden op de achterliggende oorzaken.

Het is immers goed mogelijk dat de regels zelf niet kloppen of dat een ontwerpfout in een systeem de beheerder dwingt tot bepaald gedrag. Het heeft in die gevallen geen zin om als organisatie de aandacht te richten op de overtreding van de medewerker.

Die energie kan beter gestopt worden in maatregelen die de diepere oorzaken wegnemen. Door de diepere oorzaken weg te nemen is de medewerker beter in staat zich aan de regels te houden. Hij levert dan een positievere bijdrage aan het niveau van beveiliging. Dit zou tot uitdrukking moeten komen in een vermindering van het aantal overtredingen.

Dit zou betekenen dat een organisatie de bijdrage van medewerkers in positieve zin kan beïnvloeden door incidenten -met als directe oorzaak het overtreden van beveiligingsregels- te analyseren op achterliggende oorzaken[25]. Door het wegnemen van deze diepere oorzaken door het treffen van gerichte maatregelen kan ervoor gezorgd worden dat de medewerker minder vaak in een situatie terecht komt waar hij gedwongen wordt regels te overtreden. Zo wordt zijn bijdrage aan het niveau van beveiliging verbeterd.

Het zoeken naar achterliggende oorzaken is dus essentieel. Daarna komt pas de stap van het zoeken naar passende tegenmaatregelen.

De hier gepresenteerde mogelijke oplossingsrichting is een hypothese die gebaseerd is op een aantal veronderstellingen. Om de waarde van dit concept te bepalen is het noodzakelijk deze te toetsen. Dit gebeurt aan de hand een drietal onderzoeksvragen die in het volgende hoofdstuk geformuleerd worden.

[25] De in hoofdstuk 4 beschreven PRISMA methode heeft model gestaan voor deze methode ter verbetering van de medewerkersbjidrage aan het beveiligingsniveau.

HOOFDSTUK 4: TOETSING VAN CONCEPT

ONDERZOEKSVRAGEN

Uit veronderstellingen in hoofdstuk 3 kunnen de volgende onderzoeksvragen worden gedestilleerd om te toetsen of de hypothese klopt dat het probleem bij Rabobank ICT op te lossen is door het analyseren van de incidenten:

Hoofdvraag:
Kun je de bijdrage van IT'ers aan het niveau van beveiliging inderdaad verbeteren door diepere oorzaken te analyseren van incidenten waarbij sprake is van het overtreden van een beveiligingsregel.

Subvragen:
1. Hoe vaak komen incidenten voor waarbij (zonder boze opzet) beveiligingsregels overtreden worden ?
2. Waarom worden de regels overtreden ?
3. Wat kan eraan gedaan worden ?

De beantwoording van de subvragen moet uitwijzen of de hypothese klopt..

VERWACHTTE RESULTATEN

Hoewel ingezet ter beantwoording van een hypothese moeten de onderzoeksvragen als exploratief beschouwd worden. Harde verwachtingen over de uitkomst worden daarom niet gegeven. Hieronder volgt slechts een indicatie van de verwachtte onderzoeksresultaten.

1. Voor vraag 1 geldt dat moeilijk te bepalen is wat het verwachtte aantal is. Wel wordt verondersteld dat het gaat om een significant aantal. Een te laag aantal zou betekenen dat het aantal overtredingen meevalt en dat het niet zo slecht is gesteld met de bijdrage van IT'ers aan het niveau van beveiliging als werd gedacht. Dat de bijdrage altijd beter kan vormt onvoldoende aanleiding voor verder onderzoek.

2. Bij vraag 2 wordt verwacht dat het mogelijk is om dieper liggende oorzaken te bepalen en dat de gevonden oorzaken een patroon zullen laten zien.

3. Indien een bepaalde oorzaak vaker terugkomt zou dit aanleiding kunnen zijn om bij het bepalen van tegenmaatregelen de prioriteit bij dit probleem te leggen. Hoe ongelijkmatiger de verdeling, des te beter de prioriteitsstelling kan plaatsvinden.

ONDERZOEKSMETHODEN

ONDERZOEKSVRAAG 1

De vraag hoe vaak het binnen Rabobank ICT voorkomt dat er een incident plaatsvindt dat als directe oorzaak het overtreden van een regel heeft, is getoetst aan de hand van de bestaande database van incidentbeschrijvingen van de afdeling Security Management.

Het betreft hier de geëscaleerde incidenten van de afgelopen 24 maanden (maart 2001 t/m februari 2003). Deze database is gekozen omdat er duidelijke beschrijvingen worden gegeven over de incidenten, omdat het allemaal incidenten waren die beveiligingsgerelateerde waren door de aard van het bestand, en omdat in de directe omgeving van de onderzoeker (dwz binnen de afdeling Security Management) voldoende aanvullende informatie te verkrijgen zou zijn voor uitgebreide oorzaken analyse.

Security management verzamelt beveiligingsincidenten die veroorzaakt zijn door het ontbreken of het niet effectief zijn van getroffen maatregelen. Ook wordt aangegeven wat de schade en de potentiële schade is. De rapportage is bedoeld voor het bespreekbaar maken van de incidenten bij de directie van Rabobank ICT en de verantwoordelijke lijnmanagers. Security Managers zijn op de hoogte van de beveiligingsincidenten doordat ze direct betrokken zijn of doordat ze navraag doen bij de verschillende incident- en problem managers.

Om te bepalen hoe vaak er incidenten plaats vinden die binnen Clarke's grijze gebied vallen zijn vier criteria opgesteld waaraan een incident moet voldoen. De criteria op grond waarvan er incidenten uit de database geselecteerd zijn, zijn de volgende:

1. Het incident moet zich binnen het werkgebied van Rabobank ICT afspelen.

2. Er moet een medewerker, die binnen de classificatie IT'er zoals omschreven in de afbakening valt, direct betrokken zijn bij het incident.

3. Er moet sprake zijn van het overtreden van een of meer beveiligingsregel(s) volgens de in hoofdstuk 1 beschreven definitie

4. Er mag geen sprake zijn van boze opzet

Daarnaast is het aantal incidenten geteld waarbij wél sprake was van boze opzet.

ONDERZOEKSVRAGEN 2 EN 3

Voor het beantwoorden van vraag 2 en 3 is gekozen voor een bestaande methode voor incident reporting: de PRISMA-methode[26].

BESCHRIJVING PRISMA METHODE

PRISMA (Prevention and Recovery Information System for Monitoring and Analysis) biedt een volledige methode voor het rapporteren, analyseren en evalueren van incidenten met als uiteindelijk doel om risico's te verminderen. Oorspronkelijk is deze methode ontwikkeld voor de petrochemische industrie, maar is inmiddels ook succesvol toegepast op de medische wereld, de luchtvaart en telecommunicatie en kerncentrales.

Omdat de PRISMA-methode niet eerder op het onderzoeksterrein van de IT is toegepast moet ook bekeken worden of de keuze voor deze methode legitiem is. Dit vormt onderzoekssubvraag 4.

> Subvraag 4:
> Kan de PRISMA –methode toegepast worden op een IT omgeving ?

[26] De PRISMA-methode is ontwikkeld binnen de Safetry Management Group van de Technische Universiteit Eindhoven. Voor een uitgebreide beschrijving zie [SCH-2].

De PRISMA-methode bestaat uit zeven stappen:

1) Detectie van incidenten. In deze stap worden de incidenten die waargenomen worden gerapporteerd. Belangrijk is dat er enige mate van consistentie is in de manier waarop dit gebeurt. Dit is eenvoudig te bewerkstelligen door het opstellen van een sjabloon met de onderwerpen die in ieder geval aan bod moeten komen in de incidentbeschrijving.

2) Selectie. Uit de database van incidentenbeschrijvingen worden die incidenten geselecteerd waarbij de mogelijkheid voor de organisatie om er wat van te leren het grootst is.

3) Beschrijving. De incidentbeschrijvingen die geselecteerd zijn worden opnieuw bekeken en weergegeven in een oorzakenboom-diagram. Er zijn een aantal criteria waaraan een goede oorzakenboom moet voldoen. Zo moet men zich bij het beschrijven weerhouden van het geven van meningen: alleen feiten mogen in de boom worden opgenomen. Ook het gebruik van 'of'-poorten moet zoveel mogelijk vermeden worden aangezien dit onzekerheid aangeeft in de weg van gebeurtenissen naar een incident. Het einde van een vertakking is het punt waarop verder analyse geen zin heeft omdat er bijvoorbeeld geen directe relatie meer gevonden kan worden of omdat er geen verdere feiten beschikbaar zijn. Dit einde van een vertakking wordt een basisoorzaak. Het is onwaarschijnlijk dat een incident minder dan twee basisvertakkingen heeft. Ook een al te brede basisvertakking duidt vaak op beschrijvingsproblemen. Een voorbeeld van een uitgebreide oorzakenboom is opgenomen als bijlage 1.

4) Classificatie. De classificatie van de oorzaken leidt tot inzicht in de aard van de basisoorzaken. Het EMC[27] (Eindhoven Classification Model) is ontwikkeld om de oorzaken op effectieve wijze te classificeren. Het EMC model deelt de oorzaken in drie hoofdcategorieën, te weten technisch falen, organisatorisch falen en menselijk falen. Deze indeling is gebaseerd op een model voor het ontstaan van incidenten van der Schaaf[28]. Voor de verdere onderverdeling van menselijk falen wordt gebruik gemaakt van het model van Rasmussen[29] die menselijke fouten indeelt in de categorieën Knowledge-Based, Rule-Based en Skill-Based. De classificatieschaal is opgedeeld tot een totaal van 21 subcategorieën. Voor een overzicht van de classificatiecodes en hun betekenis, zie bijlage 2.

5) Statistische verwerking. Na de classificatiestap kan uit de verzameling incidentbeschrijvingen een set van ECM geclassificeerde basisoorzaken worden gegenereerd. Indien het aantal incidenten groot genoeg is zijn hier patronen uit af te leiden.

6) Interpretatie en Implementatie. Om de methode in te kunnen zetten als tool voor risicovermindering moet het inzicht uit de classificatie leiden tot het doen van aanbeveiligen voor te nemen maatregelen. Om dit te vergemakkelijken is een classificatie/actie matrix ontworpen die bij elke hoofdcategorie uit het ECM model

[27] Voor een flowchart waarin het Eindhoven Classification Model is weergegeven wordt verwezen naar [DY]

[28] Het Classificatiemodel wordt uitgebreid besproken in [SCH-1]

[29] [DY] verwijst hier naar J. Rasmussen , Human errors: a taxonomy for describing human malfunction in industrial installations. J Occup Accid 1982; 4: 311-35

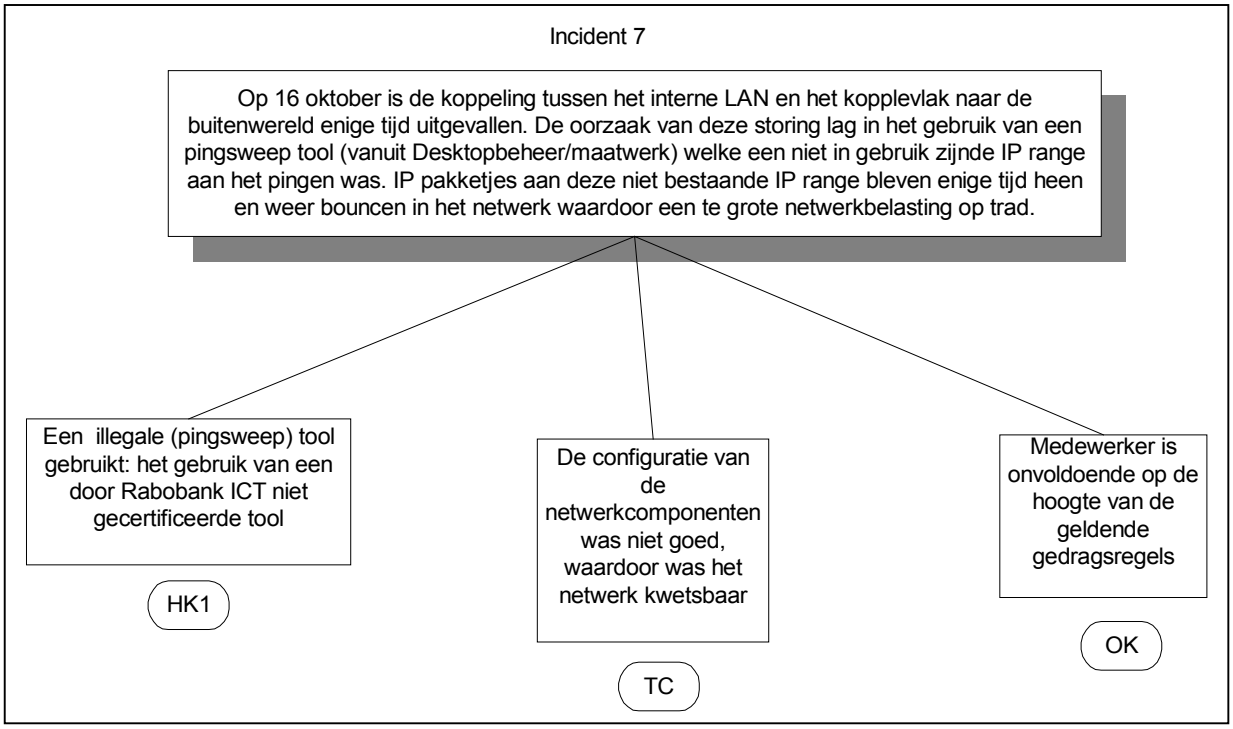
aangeeft wat de meest effectieve correctieve actie is (zie figuur 8 in het volgende hoofdstuk). Na bepaling van effectieve acties volgt implementatie van de maatregelen.

7) Evaluatie. Tenslotte zal de effectiviteit van de aanbevolen maatregel getoetst moeten worden om te zien of het risico daadwerkelijk verminderd is en het doel van het systeem dus bereikt is.

INZET VAN PRISMA METHODE

Hoewel de kennis over PRISMA-methode als geheel aanleiding gaf om de oplossing voor het probleem van de te kleine bijdrage van IT'ers aan het beveiligingsniveau te zoeken in de richting van uitgebreide oorzakenanalyses van incidenten, is de methode een systeem ter verkleining van risico's en geen methode om gedrag te beïnvloeden. Daarom wordt de PRISMA-methode hier in eerste instantie niet integraal toegepast, maar worden alleen die stappen gebruikt die antwoord geven op onderzoeksvraag 2 en 3. Dit zijn de PRISMA-stappen 3, 4, 5 en een gedeelte van 6. Hieronder wordt aangegeven wat in deze PRISMA-stappen gedaan is.

Stap 3: Van alle incidentbeschrijvingen is een oorzakenster gemaakt. Deze variant op de uitgebreide oorzakenboom slaat enkele beschrijvingsstappen over en geeft alleen de gevonden diepere oorzaken weer. Deze worden basisoorzaken genoemd. Een voorbeeld van zo'n ster staat hieronder.



Figuur 7: Oorzakenster, inclusief classificatie

Stap 4: De basisoorzaken zijn geclassificeerd met behulp van het ECM model. Daarbij zijn in eerste instantie de 21 subcategorieën gebruikt. Daarna is ook gekeken welk patroon indeling in de hoofdcategorieën oplevert.

Stap 5: De resultaten zijn verwerkt in een statistische weergave. Deze zijn terug te vinden in het volgende hoofdstuk.

Stap 6: De interpretatie van het gevonden oorzakenpatroon is gedaan met behulp van de classificatie/ actie matrix. De implementatie valt buiten het bereik van dit onderzoek.

Ter beantwoording van subvraag 4 is bovendien een contratest uitgevoerd over de derde en vierde stap. Deze is uitgevoerd door in totaal drie Security Managers, waaronder de initiële onderzoeker. Allen hadden geen of nauwelijks ervaring met de PRISMA-methode. De Contratest bestond uit de volgende elementen.

a) Aan de security manager die direct bij het incident betrokken is geweest en ook de melder van het incident was, is gevraagd of hij zich kon vinden in de gemaakte opgestelde oorzakenster. Dit is gebeurd bij alle 47 incidenten.

b) Bij tien incidenten is door twee security managers (niet noodzakelijkerwijs betrokken bij het incident) stap 3 en 4 van de PRISMA-methode uitgevoerd. Over stap 3 is alleen een controle uitgevoerd. Dit betekent dat op grond van eigen kennis of aangevuld door informatie van derden bekeken werd of de gevonden oorzaken klopten.

c) De resultaten van stap 3 en 4 zijn vergeleken en besproken. Indien er aanleiding was voor bijstelling van de resultaten, is dit gebeurd.

HOOFDSTUK 5: ONDERZOEKSRESULTATEN EN INTERPRETATIE

ONDERZOEKSRESULTATEN

UITKOMSTEN ONDERZOEKSVRAAG 1

De totale database van incidenten die in de periode van maart 2001 tot en met februari 2003 door de afdeling Security Management verzameld zijn bestaat uit 86 incidentbeschrijvingen. De beschrijvingen hebben allen dezelfde opbouw omdat voor de registratie een vast sjabloon wordt gebruikt. In totaal voldoen 47 incidenten van de 86 incidenten oftewel 55 % aan de opgestelde criteria. Daarnaast werden er 3 gevallen gevonden waarin sprake was van boze opzet.

UITKOMSTEN OORZAKENANALYSE

Op de selectie als het resultaat van vraag 1 is vervolgens de PRISMA-methode toegepast. De stappen 3 t/m 6 uit de PRISMA methode hebben de volgende resultaten[30] opgeleverd.

CONTRATEST

De eerste uitkomsten gaven het volgende beeld:

a) C. Neys in vergelijking tot M. Kimenai (C1/M1): 31/38 oorzaken zijn overeenkomstig. Dit is 79 %.

b) C. Neys in vergelijking tot T. Coppens (C1/ T1): 26/ 38 oorzaken zijn overeenkomstig. Dit is 68 %.

c) Bespreking van de gevonden resultaten gaf aan dat er een enkele keer sprake was van een vergissing, en dat er in andere gevallen sprake was van interpretatieverschillen bij de indeling in subcategorieën. Alle vergissingen zijn rechtgetrokken en enkele interpretatieverschillen zijn rechtgetrokken. De rechtgetrokken interpretatieverschillen waren allen te wijten aan een verschil in feitenkennis over het betreffende incident. Zodra alle feiten bekend waren werd overeenstemming bereikt over de oorzaken en de indeling in subcategorieën. Wat tenslotte overbleef waren die verschillen die te maken hadden met een verschil in inzicht over de achterliggende oorzaken.

d) Dit leidde tenslotte tot de volgende percentages van overeenstemming voor de 10 contra-testincidenten. : C. Neys in vergelijking tot M. Kimenai (C2/M2) : 33/38 overeenkomstige oorzaken. Dit is 87 %. C. Neys in vergelijking tot T. Coppens (C2/ T2) : 32/38 Overeenkomstige oorzaken. Dit is 84 %.

e) Een vergelijking van de drie onderzoekers geeft het volgende beeld: In 22 van de 38 oorzaken hadden alle drie de onderzoekers dezelfde classificatiecode toegekend. Dit is 58 %.

f) De grafiek 'Resultaten contratest' toont wat de resultaten zijn van deze contratest.

[30] De uitgebreide resultaten van ieder geanalyseerd incident is ter inzage bij de auteur. Gezien de gevoeligheid van de informatie kan deze niet openbaar gemaakt worden. In de bijlage staan de gegevenstabellen behorende bij deze grafieken.

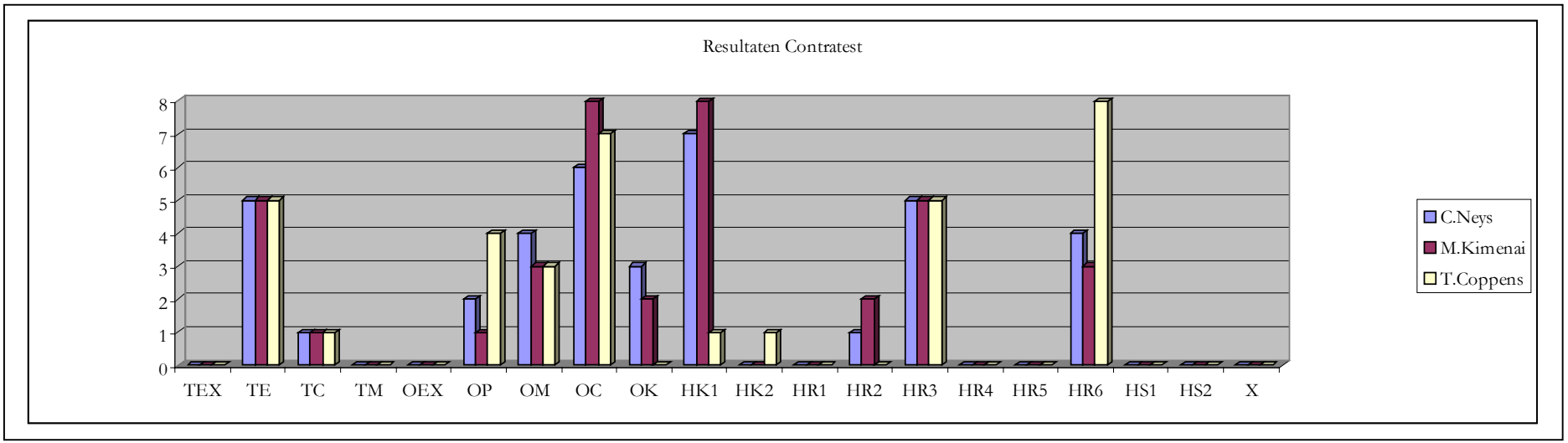
OORZAKENANALYSE 47 INCIDENTEN

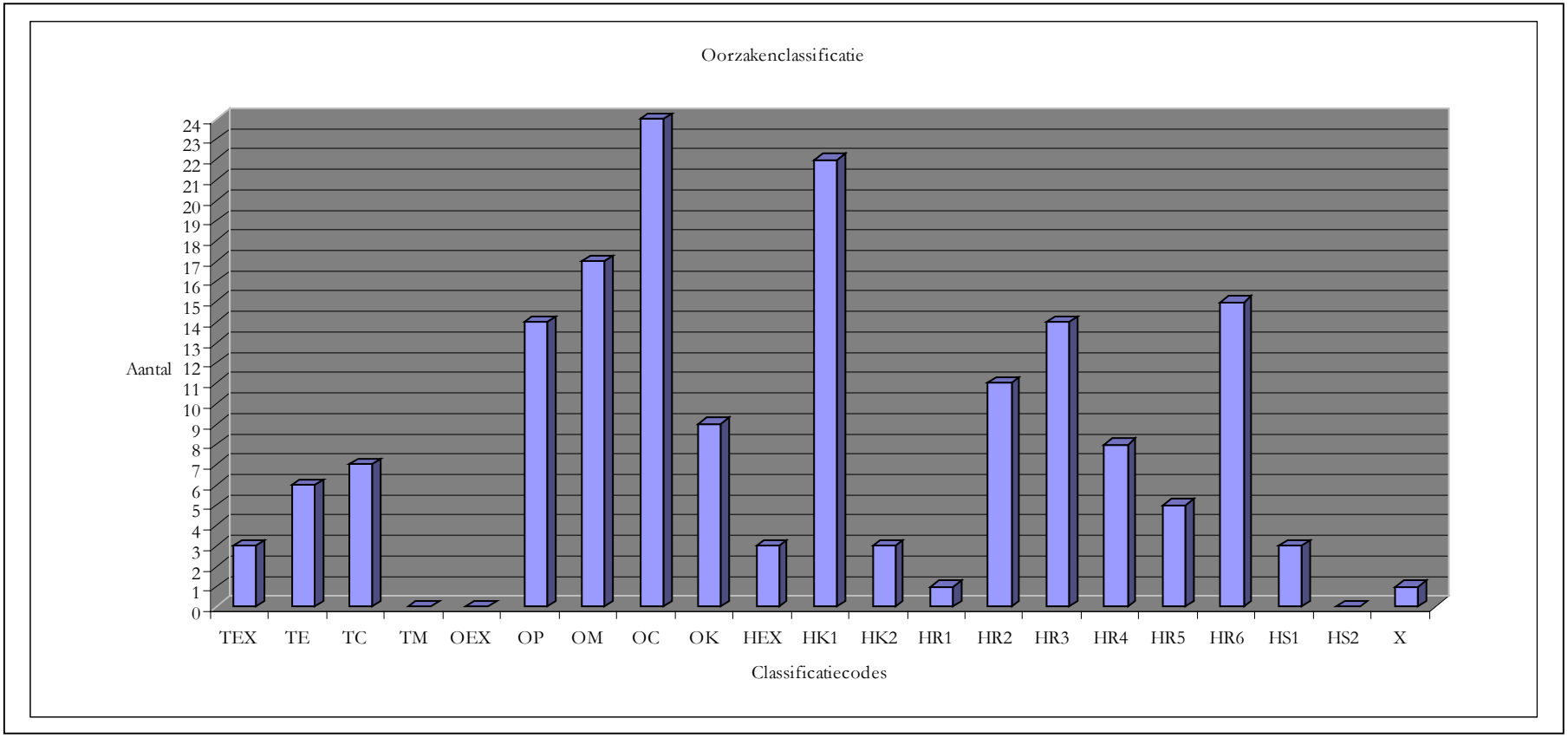
Van de 47 incidenten die op grond van de in onderzoeksvraag 1 geformuleerde criteria zijn geselecteerd, zijn even zoveel oorzakensterren gemaakt. Dit gaf een totaal van 166 achterliggende oorzaken. Deze konden, met behulp van het ECM classificatiemodel verdeeld worden over de 21 subcategorieën. Daarbij moet aangetekend worden dat het oorspronkelijke model 19 subcategorieën kent, maar dat in de gebruikte versie 2 categorieën zijn toegevoegd, te weten OC en OK. Voor een overzicht van de hier gebruikte categorieën, de uitleg van de codes en voorbeelden uit het onderzoeksgebied, zie bijlage 3.

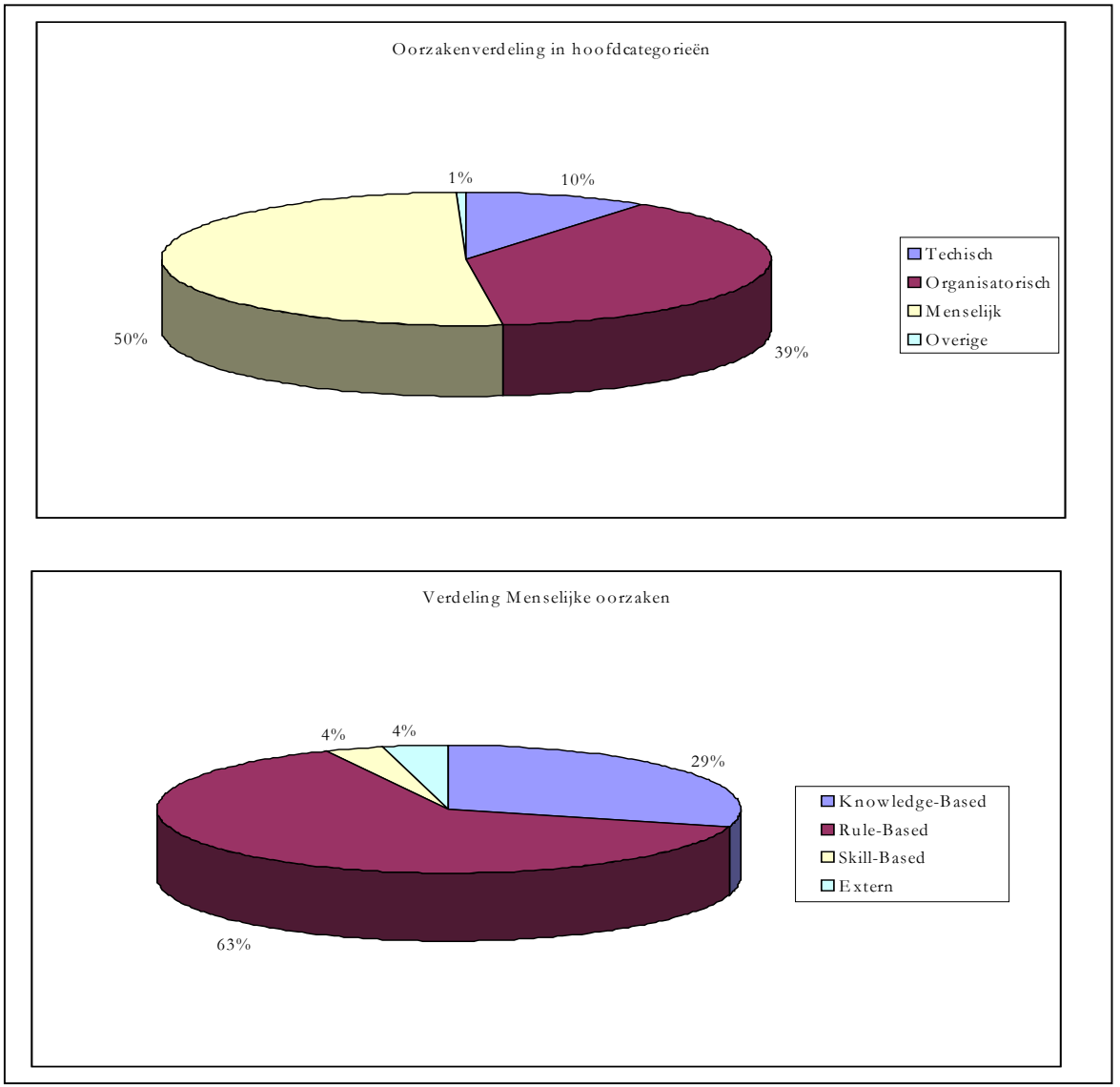
De uiteindelijke verdeling is als volgt:

TEX	TE	TC	TM	OEX	OP	OM	OC	OK	HEX	HK1	HK2	HR1	HR2	HR3	HR4	HR5	HR6	HS1	HS2	X
3	6	7	0	0	14	17	24	9	3	22	3	1	11	14	8	5	15	3	0	1

Dit resultaat is weergegeven in de grafiek 'Oorzakenclassificatie'. Tenslotte is een verdeling gemaakt naar hoofdcategorieën. Dit zijn de 'technische factoren', 'organisatorische factoren', 'menselijke factoren', en de restcategorie 'overige'. De menselijke factoren zijn apart genomen en verdeeld over de Knowledge-based, de Rule-based, de Skill-based en de Externe oorzaken(dus buiten het bereik van de organisatie liggend). Deze verdeling is te zien in de grafieken "Oorzakenverdeling in hoofdcategorieën", en "Verdeling Menselijke oorzaken". Beide grafieken geven inzicht in


Resultaten Contratest
8
7
6
5
4
3
2
1
0
TEX
TE
TC
TM
OEX
OP
OM
OC
OK
HK1
HK2
HR1
HR2
HR3
HR4
HR5
HR6
HS1
HS2
X
C.Neys
M.Kimenai
T.Coppens


Oorzakenclassificatie
Aantal
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
TEX
TE
TC
TM
OEX
OP
OM
OC
OK
HEX
HK1
HK2
HR1
HR2
HR3
HR4
HR5
HR6
HS1
HS2
X
Classificatiecodes


Oorzakenverdeling in hoofdcategorieën
1%
10%
50%
39%
Techisch
Organisatorisch
Menselijk
Overige
Verdeling Menselijke oorzaken
4%
4%
29%
63%
Knowledge-Based
Rule-Based
Skill-Based
Extern

BESPREKING VAN DE RESULTATEN

Als de uitkomsten van de analyse vergeleken worden met de verwachtte resultaten levert dat de volgende interpretatie op:

BESPREKING RESULTAAT ONDERZOEKSVRAAG 1:

Voor de uitkomst van de vraag hoe vaak er incidenten plaatsvinden waarbij (zonder boze opzet) beveiligingsregels overtreden worden geldt dat het verwachtte resultaat ruimschoots gehaald is. Het blijkt dat 56 % van alle incidenten voldoet aan de gestelde criteria. Deze uitkomst heeft twee betekenissen.

Ten eerste dat het inderdaad niet goed gesteld is met de menselijke bijdrage aan het niveau van informatiebeveiliging, en dit staaft de bewering dat Rabobank ICT een probleem heeft op het gebied van het gedrag van haar IT'ers. Dit gedrag draagt onvoldoende bij aan het vereiste niveau van informatiebeveiliging.

Ten tweede blijkt dat bij Rabobank ICT een groot aantal incidenten plaatsvinden die veroorzaakt worden door het overtreden van regels, terwijl bij slechts een klein aantal sprake is van boze opzet. De meeste overtredingen vallen dus in het door Clarke beschreven grijze gebied, wat het model van Clarke toepasbaar maakt op de situatie van Rabobank ICT. Uit Clarke's model blijkt dat medewerkers die door de eisen van de manager of een te hoge werkbelasting onder druk staan, gedwongen zijn de grens van de geldende regels te overschrijden, wat tot incidenten leidt. Dit is een belangrijke constatering omdat het de zoektocht naar achterliggende oorzaken, relevant maakt. Clarke toont middels haar model van de negatieve spiraal, waarbij strengere controle op regels leidt tot meer overtredingen en hoger risico, immers aan dat strengere regels geen optie zijn.

BESPREKING RESULTAAT CONTRATEST

Het resultaat[31] is dat respectievelijk 84 % en 87 % overeenkomstige oorzakenclassificaties werden gevonden. Deze resultaten werden behaald na bespreking van de eerste resultaten waarbij vergissingen en afwijkingen met als oorzaak een gebrek aan feitenkennis over de betreffende incidenten bij één van de onderzoekers eruit zijn gefilterd

Opvallend verschil is dat één van de onderzoekers (T. Coppens) opvallend veel vaker dan de anderen een HR 6 oorzaak vond Verklaring hiervoor moet gezocht worden in een verschil in inzicht in de consequentie waarmee regels toegepast moeten worden. In geval van gebruik van een niet-toegestaan hulpmiddel vond hij dat dit in álle gevallen voortkwam uit het maken van de verkeerde keuze in combinatie met laksheid. In zulke gevallen is door hem de code HR6 aan toegekend. Door de andere twee onderzoekers werd dit gedrag vaak beoordeeld als HK1 (medewerker beseft, door een gebrek aan kennis, niet wat voor schade hij kan inrichten met deze tool-keuze), soms in combinatie met OK (het is de medewerker nooit goed geleerd dat hij deze tool niet mag inzetten). Dit verklaart ook waarom T. Coppens geen enkele keer OK heeft gebruikt. Wat niet direct uit de testresultaten komt maar wel uit de bespreking is dat T. Coppens in die gevallen ook de OC code toekende voor 'laksheid' van de medewerker (die niet door de groep gecorrigeerd werd). Hiervoor kon hij geen andere, geschiktere code vinden. M. Kimenai en C. Neys kenden in die gevallen de OC code toe om aan te geven dat het gebruik van deze tool min of meer gewoon was binnen de afdeling. Blijkbaar wordt ook het oordeel van security managers beïnvloedt door de geldende organisatiecultuur.

[31] Dit resultaat is weergegeven in bijlage 1

BESPREKING VAN RESULTAAT OORZAKENCLASSIFICATIE VAN DE 47 INCIDENTEN

De statistische weergave (alle oorzaken van alle incidenten bij elkaar opgeteld) van de classificatie van de gevonden oorzaken laat inderdaad een oorzakenpatroon zien waarbij sprake is van een duidelijke verdeling van de oorzaken over de classificatiecodes. Indien de classificatie gebeurd op hoofdcategorieën laat dat een nog duidelijker beeld zien.

Zo wordt zichtbaar dat een relatief kleine rol is weggelegd voor de techniek. Slecht 10 % van de overtredingen kent een basisoorzaak die zijn oorsprong vindt in de techniek. Ontwerp of uitvoering van IT componenten vormen dus nauwelijks een bedreiging voor het niveau van beveiliging. Dit zegt overigens niets over de mate waarin technische maatregelen bijdragen aan het niveau.

Wat betreft de hoofdcategorieën waarbij de basisoorzaak zijn oorsprong vindt in organisatorische of menselijke factoren, met respectievelijke waarden van 39 % en 50 %, kan geconcludeerd worden dat beide een significante rol spelen bij de veroorzaking van overtredingen. Beiden vormen dus een bedreiging voor het niveau van beveiliging waarbij de menselijke factor het grootst is.

Opvallend in de verdeling in subcategorieën is dat er opvallend vaak een HK1 label aan een oorzaak toegekend is. HK 1 staat voor menselijk falen waarbij een individu een fout maakt bij het nemen van een bewuste beslissing doordat hij een gebrek aan kennis over het onderwerp heeft.

Op grond van deze resultaten blijkt het mogelijk om de aandachtsgebieden aan te wijzen waarop tegenmaatregelen zich zouden moeten richten. Het meeste resultaat zal worden geboekt indien de maatregelen gericht worden op de categorieën OC, HK1, OM en HR6. Gevolgd door HR3, HR2 en OK. Deze volgorde geeft meteen de meest efficiënte prioritering aan.

Indien de Classificatie/Actie matrix , die bij stap 6 van de PRISMA-methode hoort, ingezet wordt, kan een indicatie worden gegeven in welke richting de tegenmaatregelen gezocht moeten worden. De Classificatie/Actie matrix verbindt iedere hoofdcategorie aan een actie die als meest effectief beschouwd wordt. De categorie Menselijke factor is daarbij nog verder onderverdeeld naar Knowledge-based. Rule-base en Skill-based.

	Hulpmiddelen	Procedures	Informatie en Communicatie	Training	Motivatie
Technisch	X				
Organisatorisch		X			
Menselijk Knowledge-based			X		Nee !
Menselijk Rule-based				X	
Menselijk Skill-based	X				Nee !

Figuur 8: Classificatie/Actie Matrix X = meest effectieve tegenmaatregel Nee ! = ineffectieve tegenmaatregel

Toepassing van de matrix op de gevonden resultaten en prioritering geeft de volgende indicatie voor effectieve tegenmaatregelen voor de drie belangrijkste oorzaken:

OC: Dit is een nieuwe code waarbij de oorzaak gezocht wordt in de organisatiecultuur. Tegenmaatregelen moeten gezocht worden in de gezamenlijke en periodieke reflectie op het werk.

HK1: Informatie en communicatie. Omdat er in dit geval door de medewerker verkeerde beslissingen genomen worden omdat hij niet wist op grond van welke informatie hij moet handelen, waardoor hij een verkeerde inschatting maakt, zal veel winst worden behaald indien de juiste informatie op het juiste momentbeschikbaar is.

OM: Procedures in de zin van beleid en managementoverwegingen. Hieronder vallen ook de beslissingen van lager managementechelons die tegen (hogere) regels in gaan, of afwegingen maken waardoor er druk op de medewerker wordt gelegd om tegen de regels in te opereren.

HR6: training. In deze categorie is het type oorzaak terecht gekomen waarbij een medewerker een illegaal tool selecteert omdat dat a) makkelijk is of b) de gewoonte is binnen de afdeling of c) wel de beste optie is maar hij het dan wel had moeten voorleggen aan andere afdelingen die er last van kunnen hebben. Meestal is bij betreffende incidenten dus ook nog een andere basisoorzaak aangegeven conform deze drie opties bij b) is dat OC, bij c) is dat HR3. Bij a) ontstond echter een probleem: Het komt relatief vaak voor dat mensen regels overtreden uit een soort laksheid: de methode is voorhanden, dus waarom zou men moeilijk doen. Deze categorie werd niet teruggevonden in het classificatieschema.

Het blijkt dus mogelijk om, op grond van de gevonden resultaten en met behulp van het ECM classificatieschema en de bijbehorende Classificatie/actie matrix te komen tot, naar alle waarschijnlijkheid effectieve oplossingsrichtingen. Er is hier geen verdere invulling gegeven aan deze oplossingsrichtingen. Belangrijkste reden is dat het hier een 'vingeroefening' betreft om te kijken of de voorgestelde methode kan werken en geen compleet uitgevoerd proces.

HOOFDSTUK 6: CONCLUSIE EN AANBEVELINGEN

CONCLUSIE

Allereerst blijkt Rabobank ICT inderdaad een probleem te hebben. Het gedrag van haar IT'medewerkers draagt onvoldoende bij aan het niveau van beveiliging. Het onderzoek heeft inzicht gegeven in hoe vaak zich het probleem manifesteert in geëscaleerde incidenten. Het probleem blijkt te passen in het model van Clarke, omdat van het grote aantal incidenten dat als directe oorzaak een overtreding van een beveiligingsregel heeft slechts een zeer klein aantal (3 /50 = 6 %) met boze opzet gebeurd, is het aannemelijk dat ook Rabobank ICT een grijs gebied kent tussen de regels en de grens die bepaald wordt door de organisatiecultuur, waarbinnen overtredingen plaatsvinden die als 'normaal' worden beschouwd. Vaak wordt het risico dat de organisatie loopt door deze gedoogde overtredingen onderschat. Het is dus in het belang van de organisatie om deze overtredingen terug te dringen.

Clarke toont middels haar model van de negatieve spiraal, waarbij strengere controle op regels leidt tot meer overtredingen en hoger risico, immers aan dat strengere regels geen optie zijn. Dit betekent dat het niet zinvol is om een oplossing te zoeken in strengere controle of het aanscherpen van maatregelen, maar dat onderzocht moet worden wat binnen Rabobank ICT de werkelijke oorzaken zijn van deze overtredingen.

Een derde conclusie is dat de PRISMA-methode toepasbaar blijkt op het ICT domein. Het inzetten van de methode op 47 incidenten geeft zinvolle en bruikbare resultaten. Middels de contratestresultaten is bewezen dat de resultaten ook in voldoende mate betrouwbaar zijn. Dit blijkt uit de mate van overeenkomst in de gevonden oorzaken en de classificatie daarvan in de contratest.

Rabobank ICT blijkt de PRISMA-methode te kunnen gebruiken voor het achterhalen van de diepere oorzaken voor het incidentveroorzakend gedrag van haar IT'ers. Bij de gebruikte dataset aan incidenten bleek dat de belangrijkste oorzaken gezocht moeten worden in de organisatiecultuur, gebrek aan kennis over de systemen of andere kennis die essentieel is voor het maken van de juiste beslissingen, onduidelijke of tegenstrijdige managementbeslissingen en het niet gebruiken van de voorgeschreven hulpmiddelen.

Ook blijkt het mogelijk om op grond van het gevonden oorzakenpatroon aan te geven in welke richting de mogelijke oplossing gezocht moet worden. Voor Rabobank ICT bleek uit een snelle inventarisatie dat het meest effect wordt behaald indien er oplossingen worden gezocht in het inbouwen van periodieke reflectie-momenten, waarbij medewerkers inzicht krijgen in hun werk en hun werkomgeving door er vanaf enige afstand naar te kijken. Ook door het beschikbaar stellen van de juiste informatie aan de medewerkers, zodat deze in staat zijn de juiste beslissingen te nemen, zal effectief worden opgetreden tegen één van de belangrijkste oorzaken. Deze bevindingen zijn het resultaat van de toepassing van de classificatie/actie matrix op de twee belangrijkste oorzaken.

AANBEVELINGEN

Op grond van de conclusies en het voorafgaande onderzoek worden de volgende aanbevelingen gedaan aan Rabobank ICT:

De eerste aanbeveling is om de PRISMA-methode toe te passen binnen de IT afdelingen van de organisatie ter verbetering van de bijdrage van IT'ers aan het niveau van informatiebeveiliging. Voor dit doel is de gebruikte incidentrapportage van Security Management een goede gegevensverzameling. Eventueel kan deze rapportage aangepast worden zodat zonder veel moeite een selectie van te analyseren incidenten gemaakt kan worden.

Het is heel goed mogelijk alvast conclusies te trekken uit de resultaten van de oorzakenanalyse uit dit onderzoek. De belangrijkste aandachtsgebieden zijn al eerder genoemd en hebben betrekking op de OC en de HK1 classificatiecategorie. De matrix is vervolgens ingezet bij wijze van vingeroefening, maar zal bij toepassing op de volledige classificatie genoeg informatie opleveren voor mogelijke tegenmaatregelen. Een suggestie vormt de volgende aanbeveling.

Betrek IT'ers bij de uitvoering van de PRISMA-methode. Door de analyse van incidenten uit hun directe omgeving krijgen ze inzicht in hun dagelijkse praktijk, de mogelijke risico's die de organisatie loopt en, de invloed van hun gedrag daarop. Dit punt van reflectie op de eigen werkkring werd al eerder genoemd als mogelijke oplossing voor de OC categorie. Deze categorie kwam in het onderzoek als oorzaak nummer 1 naar voren.

In dit geval werd de PRISMA-methode gebruikt ter verbetering van de bijdrage van medewerkers aan het niveau van informatiebeveiliging. Deze methode van oorzakenanalyse biedt echter veel meer mogelijkheden voor een organisatie als Rabobank ICT. Maak daarbij gebruik van bestaande systemen zoals ITSM of gebruik de invoering van het nieuwe incident management systeem Peregrine als uitgelezen mogelijkheid om een begin te maken met het opzetten van een database. Dit kan door de incidentbeschrijvingen geschikt te maken voor analyse. Dat wil zeggen dat bij elk incident vaste gegevens genoteerd worden die al te veel navraag achteraf bij direct betrokkenen overbodig maken. De oorzakenanalyse van deze gegevens kan leiden tot een breed inzicht in de zwakke punten in de IT dienstverlening van Rabobank ICT. PRISMA wordt dan ingezet als methode om deze risico's te verminderen.

Het verdient aanbeveling om toepasbaarheid op het domein van de IT na verloop van tijd te evalueren. Eventueel kunnen kleine aanpassingen worden gemaakt in de classificatiecodes of in de classificatie/actie matrix, waardoor het model beter past bij de IT omgeving.

In het kader van dit onderzoek zijn ook 11 grotere incidenten geanalyseerd (MAAR's). MAAR staat voor Management Analyse en Aanbevelingen Rapportage. Een voorbeeld van zo'n uitgebreide analyse is te vinden in bijlage 2. Opvallend bij deze 11 incidenten was dat ook aan de herstelkant (beveiligings)regels werden overtreden. De herstelkant van een oorzakenboom beschrijft de feiten die geleid hebben tot het al dan niet tijdig herstellen van een verstoring. Indien de herstelkant faalt, kan de verstoring uitgroeien tot een incident met een grote impact, zoals bij de MAAR's het geval is. Het zou interessant zijn dit herstelgedrag aan een nader onderzoek te onderwerpen, omdat dit kan duiden op situaties waarin regels overtreden worden omwille van een hoger doel: het voorkomen van een incident. Dit soort gevallen van overtreding van regels zou je als organisatie juist willen aanmoedigen. Iets wat indruist tegen de gangbare theorieën voor beperking van (beveiligings)risico's.

LITERATUURLIJST

[ALB]	Alblas, G. en Wijsman, E.(2001),	Gedrag in organisaties	3e druk, Wolters-Noordhoff, ISBN 9001032117, 2001
[BA]	Basten, N.F.H.(2001)	Security Awareness - De zachte kant van informatiebeveiliging	Afstudeerreferaat EDP-auditing, Erasmus Universiteit Rotterdam, versie 2.0 april 2001
[BRO]	Brostoff, S. en Sasse, A. (2001)	Safe and Sound; a safety-critical approach to security	Paper presented at *New Security Paradigms Wokshop '01*, September 11-13, 2001, Cloudcroft, NM
[CL]	Clarke, S.(1997)	Violations as a Source of Project Risk	*The International Journal of Project & Business Risk Management*, Vol 1, Issue 2, 155-167. ISSN 1366-2163. Project Manager Today Publications, 1997
[CO]	Costelloe, M. (2002)	Security Awareness at AIB	Presentatie tijdens *ISF workshop Effective Security Awareness*, April 2002
[DY]	Dye, J. en v.d.Schaaf, T.W.(2002)	PRISMA as a quality tool for promoting customer satisfaction in the telecommunications industry	*Reliability Engineering and System Safety* 75 (2002), 303-311, Elsevier, 2002
[HE]	Hendrickson (2002)	Security Awareness Do's and Dont's	Presentatie tijdens *ISF workshopEffective Security Awareness*, April 2002
[IFS-1]	IFS publicatie (2002)	IFS Effective Security Awareness Workshop Report	IFS publicatie, April 2002

[IFS-2]	IFS publicatie (2000)	Information Security Culture: A preliminary investigation	IFS publicatie, November 2000
[IFS-3]	IFS publicatie (2000)	It Could Happen To You: A profile of major incidents	IFS publicatie, Februari 2000
[IFS-4]	IFS publicatie (1999)	Driving Information Risk out of the Business	IFS publicatie, April 1999
[IFS-5]	IFS publicatie (1999)	The Impact of Security Management	IFS publicatie, October 1999
[NOO]	Noord v., F. (2002)	Informatiebeveiliging: gepland veranderen van gedrag	*Jaarboek Informatiebeveiliging, 2002/2003*, ten Hagen & Stam Uitgevers, red. Huurman, Willem J. en Kanters, Frans M., ISBN 904400395X, 2002
[NOS]	Nosworthy, J. D. (2000)	Implementing Information Security In The 21ste Century - Do You Have the Balancing Factors ?	*Computers& Security*, v 19, no4 (2000), p. 337-347, Elsevier Advanced Technology, ISSN 01674048, 2000
[OU]	Oud, E. J.(2001)	Informatiebeveiliging: het menselijke aspect	*Jaarboek Informatiebeveiliging 2001/2002*, ten Hagen & Stam Uitgeverijen, red. Huurman W. en Jaarsma, J., ISBN 9044002058, 2001
[OV]	Overbeek, P. , Roos Lindgreen, E. en Spruit, M.(2000)	Informatiebeveiliging onder controle	Pearson Education Uitgeverij, ISBN 9043002895, 2000
[RO]	Roos Lindgreen, E.E.O. en Overbeek, P.(1999)	Over gedrag, communicatie en informatiebeveiliging	*Compact* 1999/6, 3-10, 1999

[SA]	Sasse, M.A. en Brostoff, S. en Weirich, D.(2001)	Transforming the 'weakest link'- an human/computer interaction approach to useable and effective security	*BT Technol J*, Vol 19, no 3, Juli 2001
[SCH-1]	v.d. Schaaf, T.W. (1992)	Near Miss Reporting in the Chemical Process Industry	Proefschrift, Technische Universiteit Eindhoven, ISBN 90-386-0181-6, 1992
[SCH-2]	v.d. Schaaf, T.W.(1996)	PRISMA: A Risk Management Tool Based on Incident Analysis	*Proceedings of the International Conference and Workshop on Process Safety Management and Inherently Safer Processes* (p.242-251) Orlando FL, October 8-11, 1996
[SI]	Sipman, W. red.(2002)	Bewust beveiligen. Een praktische handleiding voor betrouwbare informatievoorziening	Academic Services, ISBN 9039521336, 2002
[VE]	Verdelin, P. (2002)	Awareness Project - The elements	Presentatie tijdens *ISF workshop Effective Security Awareness*, 2002
[VU]	v.Vuuren, W.(2001)	Organisational failure, An exploratory study in the steel industry and the medical domain	Proefschrift, Technische Universiteit Eindhoven, ISBN 90-386-0589-7, 1998
[WO]	Wouters, E.M.E.(2001)	Alle zegen komt van boven: er zijn geen slechte werknemers, alleen slechte managers	Jaarboek Informatiebeveiliging 2001/2002, ten Hagen & Stam Uitgeverijen, red. Huurman W. en Jaarsma, J., ISBN 9044002058, 2001
[WU]	Wulteputte, S.(2002)	Information Security Awareness- How we failed & How we plan to do better in the future	Presentatie tijdens *ISF workshop Effective Security Awareness*, April 2002

BIJLAGE 1: ONDERZOEKSRESULTATEN UITGEBREID

Wegens de vertrouwelijke aard van de onderzoeksresultaten zijn deze niet bijgevoegd. Indien gewenst , zijn deze op te vragen bij de auteur:

Drs. C. Neys , Rabobank ICT, Laan van Eikenstein 9, 3705 AR Zeist, int. Locatie: ZL P 260 , 030-2158486, e-mail: c.neys@rf.rabobank.nl of c.neys@hccnet.nl

BIJLAGE 2: VOORBEELD UITGEBREIDE OORZAKENBOOM

Wegens de vertrouwelijke aard van de voorbeeld-oorzakenboom is deze niet bijgevoegd. Indien gewenst , is deze op te vragen bij de auteur:

Drs. C. Neys , Rabobank ICT, Laan van Eikenstein 9, 3705 AR Zeist, int. Locatie: ZL P 260, 030-2158486, e-mail: c.neys@rf.rabobank.nl of c.neys@hccnet.nl

BIJLAGE 3: CLASSIFCATIECODES ECM MODEL

Dit is niet het officiële schema, maar een versie die aangevuld is met voorbeelden uit de ICT-praktijk.

Code	**Beschrijving**	**Definitie**	**Voorbeeld**
TEX	External	Technische fouten buiten macht v. organisatie	KPN storing (1e x)
TE	Engineering	Slecht ontwerp/faciliteiten	Ook gebrekkige configuratie of ontbreken van hulpmiddelen (b.v scanningtools, indien daar nooit om gevraagd is, niet indien ze er niet zijn uit kostenoverwegingen, dan immers OM !)
TC	Construction	Goed ontwerp dat niet goed gevolgd is tijdens bouw	Configuratiefouten, programmeerfouten
TM	Materials	Materiaaldefecten of technische fouten	Bitjes die omklappen of onzichtbare breuken in nieuwe kabels, maar ook technische fouten waar (voorlopig) nog geen oorzaak voor is (nog in onderzoek)
OEX	External	Organisatorische falen dat buiten macht van organisatie ligt	NVB besluit dat de standaardchip op bankpassen model X moet zijn, terwijl die niet aan de eisen van de Rabobank zou voldoen
OP	Operating Procedures	Kwaliteit van procedures, ook compleetheid en accuraatheid (niet of ze gevolgd worden !)	Ook realistisch beleid. BV inzake Internet op de werkplek: mensen gaan allerlei illegale verbindingen leggen, die risico's met zich meebrengen: heroverweging van eerdere beslissing zou op zijn plaats zijn. Ook bijvoorbeeld het uitblijven van afspraken met KPN na 2e storing.
OM	Management Priorities	Beslissing van Management om bv productie of kostenbesparing boven beveiliging te laten prevaleren	Beslissing om geen Internet op de werkplek voor iedereen beschikbaar te stellen omdat dit ten kosten zou gaan van de productiviteit en dus geld kost. Bijvoorbeeld ook de bewuste beslissing om geen afspraken te maken met KPN of andere maatregelen te nemen na tweede storing
OC	Organisation Culture	Gedrag in groep (gewoontes)	Binnen de groep worden GIC-regels afgedaan als 'onbelangrijk'. Ook bijvoorbeeld de gewoonte om op de hoogte te zijn van elkaars paswoorden
OK	Organisation Knowledge	Kennisoverdracht aan nieuwe medewerker. Formele inwerkprocedure maar ook informele overdracht van gewoontes in inwerkperiode	Medewerker maakt kennis met GIC tijdens inwerkperiode (of niet). Ook feit dat externe geleerd krijgt dat zijn laptop niet aan het interne netwerk mag gekoppeld worden hoort hier bij.
HEX	External	Menselijke fout buiten de macht van de organisatie	Bij energiemaatschappij gooit iemand beker koffie over belangrijke server
	Knowledge-based	*Verkeerde beslissing. Bewuste afweging/niet begrijpen op grond van de beschikbare informatie*	
HK1	System status	Er is te weinig kennis over de correcte status of werking van het systeem bij het individu om een goede beslissing te nemen	Een medewerker van de brug weet niet hoe hij bepaalde waarden moet interpreteren, of iemand weet niet hoe hij een firewall moet configureren en daardoor wordt er een

			verkeerd besluit genomen.
HK2	Doel	Afweging van doelen op individueel niveau met de beste bedoelingen maar helaas is het niet de afweging die de organisatie voor staat	De medewerker maakt een afweging op grond van wat hij denkt dat in het belang van de organisatie is. Alleen zijn die organisatiebelangen net iets anders, of kennen ze een andere prioriteit. Een medewerker van een helpdesk vindt het in de lucht brengen van het interne e-mail verkeer zo belangrijk dat hij dat probleem eerder op gaat lossen dan een probleem met een netwerkverbinding tussen Zeist en Interpay. (Let op: zijn collega zou een andere afweging kunnen maken, anders is er eerder sprake van een organisatorische oorzaak !)
	Rule-based	*Verkeerde keuze*	
HR1	Licence (permanent)	Kwalificatie. Juiste niveau van kennis en ervaring voor het uitoefenen van bepaalde taken	Een medewerker van een non-skilled helpdesk kan een bepaald probleem niet oplossen door gebrek aan kennis en ervaring, maar ook omdat hij daar niet op geselecteerd is en dus niet het juiste niveau heeft.
HR2	Permit (Tijdelijk)	Juiste rechten voor bepaalde actie	Een bewaker zet de knop van een noodaggregaat om tijdens een stroomstoring, terwijl hij dit niet mag. Maar ook dat een beheerder beslissingen neemt over het (tijdelijk) uitzetten van een bepaald systeem, terwijl hij niet de systeemeigenaar is en deze ook niet geraadpleegd heeft (en dus geen toestemming heeft)
HR3	Coordination	Informatie-uitwisseling van status werkzaamheden met het oog op mogelijke impact voor werk anderen	Ploeg 1 van de brug draagt informatie over probleem niet goed over aan ploeg 2. Of er wordt geen informatie verstrekt aan anderen over een test die gehouden wordt.
HR4	Checks	Er moet gecheckt worden of het systeem voldoet aan te verwachtte condities, voor zover relevant voor werk	Check-dubbel-check (zoals in de luchtvaart) voordat het systeem weer in productie gaat na een belangrijke wijziging. Maar ook andere vormen van controle op werkzaamheden of instellingen
HR5	Planning	Correcte werkplanning: selectie juiste methode (procedure), en uitgevoerd in goede volgorde	Indien eerst een test wordt uitgevoerd en daarna pas betrokkenen op de hoogte worden gesteld, terwijl dit in omgekeerde volgorde in de procedures beschreven staat.
HR6	Equipment/information	De voorgeschreven tools en informatie voor het uitvoeren van het werk dient beschikbaar te zijn en gebruikt te worden	De handboeken Tandem zijn niet beschikbaar op het BPCC, zodat de medewerker niet de juiste keuze kan maken
	Skill-based	Dingen die per ongeluk fout gaan	
HS1	Controlled	Fijn-motorische fouten	Typefouten, vergissingen bij selecties uit lijsten. Koppelen van verkeerde bestanden/systemen
HS2	Whole-body	Bewegingen van het hele lichaam: vallen etc.	Struikelen over snoer in serverruimte waarbij snoer eruit gaat. Koffie over toetsenbord.
X	Unclassifiable	Fouten die niet in een van deze categorieën vallen	Alles wat je verder nog tegen komt