Risico's en firewalls

Bevindingen van een exploratief onderzoek naar risico-analyses van en aanvalsmethodieken op firewalls

Universiteit:	Radboud Universiteit Nijmegen
Faculteit:	Faculteit der Natuurwetenschappen, Wiskunde en Informatica
Afdeling:	Security of Systems
Opleiding:	Informatica
Variant:	Management en toepassing
Opdrachtgever:	Dr. Martijn Oostdijk
Referent:	Dr. Marko van Eekelen
Auteur:	Jasper Bart Berlijn
Datum:	18-04-2007
Versie:	Definitief
Begeleiders:	Dr. Martijn Oostdijk / Drs. ing. Pepijn Vos
Afstudeernummer:	559

Voorwoord

Dit onderzoek is uitgevoerd om mijn master aan de Radboud Universiteit Nijmegen, Faculteit der Natuurwetenschappen, Wiskunde en Informatica afdeling Security of Systems (SoS) te behalen. Het resultaat van dit onderzoek vormt mijn masterthesis binnen de opleiding Informatica, afstudeerrichting Security met specialisatie Management en Toepassing.

De volgende mensen wil ik bedanken voor hun hulp bij het schrijven van mijn masterthesis

- Dr. Martijn Oostdijk, afstudeerbegeleider Informatica, voor het zorgen dat de testomgeving binnen korte tijd gerealiseerd kon worden en het begeleiden van het informatica deel.
- Drs. ing. Pepijn Vos, afstudeerbegeleider Management, voor de snelle reacties, het voor mij klaar staan en het geven van bruikbare feedback op korte termijn.
- Dr. Cees-Bart Breunesse, voor het zorgen dat de testomgeving binnen korte tijd gerealiseerd kon worden.
- Dr. Marko van Eekelen, voor het optreden van referent binnen dit onderzoek.

Tevens wil ik Ingeborg Schouten BSc., Elwin Berlijn MSc. en Drs. Joost Retera bedanken voor het herhaaldelijk lezen van mijn conceptversies. Daarnaast wil ik mijn ouders bedanken voor hun financiële steun zodat ik mijn studie heb kunnen afronden.

Ik wens u veel plezier met het lezen van mijn masterthesis!

Jasper Bart Berlijn

Samenvatting

Deze sectie bevat de samenvatting van het master-onderzoek “Risico's en firewalls: Bevindingen van een exploratief onderzoek naar risico-analyses van en aanvalsmethodieken op firewalls”. Dit onderzoek bevat twee deelonderzoeken. Het eerste deelonderzoek is een management georiënteerd onderzoek, dat gaat over de criteria die de kwaliteit van een risico-analyse-rapport van een firewall bepalen. Het tweede deelonderzoek, informatica georiënteerd, gaat over het exploratief vinden van risico's waartegen firewalls zouden moeten beschermen.. Het management onderzoek gaat over het bepalen van risico's, terwijl het informatica onderzoek, indirect, bewijst dat er risico's in dit gebied zijn. Het eerste deelonderzoek richt zich met name op managers die moeten bepalen welke digitale informatie beveiligd moet worden. Het tweede onderzoek maakt voor managers duidelijk dat digitale informatie daadwerkelijk beveiligd moet worden. Tevens wordt hierin een methode beschreven voor aanvalsmethodieken die mogelijk gebruikt kunnen worden door onderzoekers die zich bezighouden met aanvallen op een firewall. Nu volgt eerst de samenvatting van het eerste deelonderzoek.

Deel A: “ Criteria die de kwaliteit van een risico-analyse-rapport van een firewall bepalen”

In het managementonderzoek is kennis gegenereerd over de criteria die de kwaliteit van een risico-analyse-rapport bepalen, ten behoeve van het verbeteren van de functionaliteit van een firewall. Deze kennis kan specifiek gebruikt worden om de kwaliteit van een risico-analyse-rapport te verbeteren. Hierdoor zal de beveiliging van de digitale informatie-uitwisseling tussen een organisatie en haar omgeving beter worden en het belang ervan meer in de organisatie worden gedragen. Dit is in volgende doelstelling geformuleerd;

De doelstelling van het eerste deelonderzoek luidt:

> “Het exploreren welke criteria de kwaliteit van een risico-analyse-rapport bepalen, ten behoeve van de functionaliteit van de firewall.”

De vraagstelling van het eerste deelonderzoek luidt:

> “Welke criteria bepalen de kwaliteit van een risico-analyse-rapport, ten behoeve van de functionaliteit van een firewall, welke van belang is voor een veilige digitale informatie-uitwisseling tussen organisaties en haar omgevingen?”

Op grond van bovenstaande vraagstelling zijn de volgende onderzoeksvragen geformuleerd:

> 1. Welke criteria worden gebruikt door de managers en / of technici voor het bepalen van de kwaliteit van een risico-analyse-rapport?
> 2. Welke factoren beïnvloeden de criteria die door managers en / of technici voor het beoordelen van de kwaliteit van een risico-analyse-rapport worden gebruikt ten behoeve van de functionaliteit van een firewall?

Binnen dit onderzoek is gebruik gemaakt van een analyse framework, literatuurstudie en empirisch onderzoek. Het analyse framework is gebruikt om de resultaten van de literatuurstudie en het empirisch onderzoek in te verwerken.

Het literatuuronderzoek, welke gebruikt is voor de beantwoording van onderzoeksvraag 1, heeft een

dertigtal criteria opgeleverd die de kwaliteit van een risico-analyse-rapport bepalen ten behoeve van de functionaliteit van de firewall. Deze criteria zijn onderverdeeld in drie categorieën, te weten:

- Scope: in deze categorie worden de criteria beschreven die gerelateerd zijn aan het domein en het bereik van de risico-analyse.
- Systeem karakteristieken: de criteria met betrekking tot de kenmerken van het systeem worden hier beschreven.
- Risico-analyse methode: criteria die beschrijven hoe het risico-analyse-rapport opgebouwd dient te worden.

Uit de interviews is gebleken dat er soms (basis) theoretische kennis over de criteria die de kwaliteit van een risico-analyse bepalen aanwezig is, maar dat deze kennis weinig tot niet expliciet wordt gebruikt. Daardoor zijn de resultaten van het literatuuronderzoek (theorie) niet bevestigd of ontkend door de respondenten (theorie en praktijk). Dit impliceert dat er geen antwoord is op onderzoeksvraag 2. Onderstaande punten kunnen hierbij nog wel voor een antwoord zorgen.

- De bereidheid van architecten voor deelname aan empirisch onderzoek.
- Vergroting van kennis (van respondenten) binnen organisaties met betrekking tot risico-analyse.
- Budget om de gesloten methoden (informatie risico analyse) te kunnen kopen.

Deel B: “Aanvalsmethodieken op een firewall”

In het informatica-onderzoek is onderzocht hoe een firewall aangevallen kan worden. Van deze aanvalsmethoden is een attacktree opgebouwd om te kijken of deze attacktree-methode toepasbaar is bij het beschrijven van aanvallen op een firewall. Door het aanvallen van een firewall en de beschrijving van deze aanval kan duidelijk worden welke informatie nu precies beveiligd moet worden. Tevens wordt onderzocht of de beschrijving van deze aanvallen door middel van een attacktree een bruikbare methode is voor onderzoekers die zich bezig houden met aanvallen op firewalls. Dit is in de volgende doelstellingen geformuleerd.

De doelstellingen van het tweede onderzoek zijn:

1. Het aanvallen van een blackbox firewall.
2. Het op een gestructureerde en documenterende methode beschrijven van de aanvallen op een blackbox firewall.
3. Het automatiseren van de bovenstaande methode.
4. Het ontwerpen van een attacktree van de bovenstaande methodiek en bepalen of de attacktree methode bruikbaar is in deze context.

De vraagstelling van het tweede onderzoek luidt:

> “Hoe kan een daadwerkelijk uitgevoerde aanval op een firewall beschreven worden op een gestructureerde en documenterende manier en is deze uitgevoerde aanval te automatiseren”

De volgende onderzoeksvragen zijn uit de doelstelling gedestilleerd:

1. Hoe kan een blackbox firewall worden aangevallen?
2. Zijn de bovenstaande aanvallen te beschrijven op een gestructureerde en documenterende manier?
3. Zijn de bij twee beschreven aanvallen op de blackbox firewall te automatiseren?
4. Is het mogelijk om een attacktree te ontwerpen op basis van een aanvallende methodiek?
5. Is de attacktree methode een bruikbare techniek om aanvallen op een blackbox firewall te modelleren?

Het informatica onderzoek betreft een explorerende studie. De nadruk lag hierbij op het uitvoeren van verschillende testen op een blackbox firewall.

Voor het aanvallen van een firewall wordt gebruik gemaakt van tooling. Deze tooling wordt gebruikt om te testen of de firewall volgens de specificaties werkt. Voor onderzoeksvraag 1 is een aanval op een blackbox firewall uitgevoerd waarbij de volgende tooling is gebruikt:

1. nmap (NetworkMAPer)
2. pingtunnel
3. ftester (Firewall tester)
4. ISIC (IP Stack Integrity Checker)

De tweede onderzoeksvraag is door middel van een beschreven aanvalsproces behandeld. Hierin staat precies beschreven welke stappen tijdens de aanval zijn gemaakt. De keuzes die gemaakt zijn tijdens het proces en de gedachtegangen die hierbij naar boven kwamen staan ook beschreven.

Na uitvoer van het exploratieve proces kan geconcludeerd worden dat het aanvalsproces niet volledig valt te automatiseren, vanwege de omvang, dan wel het aantal mogelijkheden. De omvang is ook het probleem bij het ontwerpen van een attacktree. De attacktree groeit zo snel uit dat een attacktree op schrift alsook geautomatiseerd niet te doen is. Er kan geconcludeerd worden dat het gebruik van een attacktree voor het beschrijven van aanvallen op een firewall geen bruikbare methode is.

De verbinding tussen de twee deelonderzoeken vanuit het management oogpunt is dat er gesproken wordt over het beveiligen van digitale informatie. Het informatica-onderzoek geeft indirect antwoord op de vragen die bij het management worden gesteld. Vanuit het informatica-onderzoek is gekeken of een fout in een firewall gevonden kan worden. Daarnaast is er gekeken in hoeverre de attacktree te gebruiken is als methode om aanvallen te beschrijven. Deze beschrijving kan een risico-analyse ondersteunen en zodoende managers meer informatie geven over de risico's die in het bedrijfsnetwerk aanwezig zijn.

Dit onderzoek heeft zich voornamelijk gericht op medeonderzoekers die werkzaam zijn of gerelateerd werk gedaan hebben op het gebied van digitale informatiebeveiliging; meer specifiek gericht op het onderdeel firewalls. Binnen organisaties is de beveiliging van digitale informatie vaak onduidelijk of wordt als niet bestaand ervaren. Dit kan veroorzaakt worden door:

- Beperkte verantwoordelijkheidsbesef bij experts en managers,
- Weinig impactbesef bij managers,
- Hoge financiële kosten voor beveiliging digitale informatie ((ROI = return on investment) lastig in te schatten)
- Beveiliging kent een lage prioriteit op de agenda van de spelers.

Dit vergt een cultuuromslag waarbij dit onderzoek handreikingen geeft om het onderzoeksgebied concreter te vertalen. Dit wil niet zeggen dat de onderzoeksresultaten voor organisaties niet gebruikt kunnen worden. Het onderzoeksgebied is in dit onderzoek concreter gemaakt waardoor het een aanzet kan geven tot meer bewustwording van een adequate risico-analyse, ten behoeve van een veilige digitale informatie-uitwisseling tussen organisaties en hun omgevingen, vanuit een theoretisch en praktijkgericht perspectief.

Inhoudsopgave

Inleiding

Deelonderzoek A

Deelonderzoek B

Algemene conclusie en aanbevelingen

Bijlagen

Inleiding

1 Inleiding

1.1 Aanleiding

De masterthesis is uitgevoerd als afsluiting van mijn studie Informatica, afstudeerrichting Security met specialisatie Management en Toepassing. De keuze voor het onderwerp komt voort uit mijn persoonlijke interesse op het gebied van digitale informatiebeveiliging. Daarnaast heeft dit onderwerp een relatief wetenschappelijke onbekendheid. Onderzoek is daarom gewenst.

Naast mijn studie ben ik werkzaam op het gebied van computerbeveiliging. Binnen deze branche is er onduidelijkheid hoe met de materie, die in dit onderzoek behandeld wordt, om moet worden gegaan. Ook vanuit het bedrijfsleven blijkt er interesse voor dit onderzoeksgebied, gezien de verkoop van firewalls en andere digitale informatiebeveilingsproducten.

Deze masterthesis bestaat uit een tweetal onderzoeken, te weten een management en een informatica onderzoek. Het eerste onderzoek gaat in op het bepalen van de kwaliteit van een risico-analyse. Hiermee wordt getracht een kwalitatief hoogwaardig rapport te kunnen opstellen over welke risico's organisaties lopen. Het tweede onderzoek gaat over aanvallen op een firewall. Aan de hand van een beschrijving van een aanval wordt gepoogd te achterhalen welke informatie beveiligd moet worden. Tevens wordt getoetst of de beschrijvingsmethode bruikbaar is voor onderzoekers.

Het onderzoek probeert het volgende te bereiken:

1. Het beantwoorden van de onderzoeksvragen.
2. Er wordt gepoogd om een kwalitatief van risico-analyse resultaat ten behoeve van het verbeteren van de veiligheid van digitale informatie inzichtelijk te maken.
3. Er wordt geprobeerd om bewustzijn te kweken over digitale informatie veiligheid met betrekking tot een firewall onder de personen waarmee ik in contact ben gekomen tijdens dit onderzoek.

Om inzicht te krijgen hoe de masterthesis is opgebouwd en hoe deze gelezen kan worden, wordt de structuur in de volgende paragraaf toegelicht.

1.2 Leeswijzer

Deze paragraaf beschrijft hoe dit document is opgebouwd. Eerst dient duidelijk te zijn dat er in totaal twee deelonderzoeken in deze masterthesis worden behandeld. Aangezien dit onderzoek verdeeld is in een management en een informatica gedeelte en deze beide hun eigen projectkader / afbakening, doel- en vraagstelling hebben, worden deze in desbetreffende hoofdstukken behandeld. Daarom bestaat dit onderzoek uit deelonderzoek A, het managementdeel, en deelonderzoek B. het informaticadeel. Deze onderzoeken zijn onderverdeeld in deelonderzoek A “Criteria die de kwaliteit van een risico-analyse-rapport van een firewall bepalen” en deelonderzoek B “Aanvalsmethodieken van een firewall”. Deze onderzoeken zijn aan elkaar gerelateerd.

De masterthesis heeft de volgende indeling:

1. Inleiding
2. Deelonderzoek A
3. Deelonderzoek B
4. Conclusies en aanbevelingen
5. Figuren, bronvermelding, afkortingen en appendix

Bovenstaande indeling wordt in de onderstaande secties uitgewerkt.

Inleiding

De masterthesis begint met de inleiding. In de inleiding staat de leeswijzer die U op dit moment aan het lezen bent.

Deelonderzoek A

Deelonderzoek A, het onderzoek voor het managementdeel van mijn masterthesis, staat beschreven in hoofdstuk 2 tot en met hoofdstuk 6. In hoofdstuk 2 wordt deelonderzoek A ingeleid. In dit hoofdstuk staat de doelstelling, vraagstelling en de relevantie van het management onderzoek beschreven. Daarna volgt hoofdstuk 3 waarin het projectkader wordt behandeld. Hierna volgen hoofdstuk 4, met daarin de toegepaste onderzoeksmethode en hoofdstuk 5 met de resultaten van dit deelonderzoek. Tot slot komt hoofdstuk 6 aanbod waarin de conclusies van dit deelonderzoek staan beschreven.

Deelonderzoek B

Deelonderzoek B, het onderzoek voor het informatica deel, staat beschreven in hoofdstuk 7 tot en met hoofdstuk 11. In hoofdstuk 7 wordt deelonderzoek B ingeleid. In dit hoofdstuk staat de doelstelling, vraagstelling en de relevantie van het informatica-onderzoek beschreven. Daarna volgt hoofdstuk 8 waarin het projectkader aan bod komt. Hoofdstuk 3 geeft een introductie van dit projectkader. Hierna volgen de hoofdstukken 9 en 10 waarin achtereenvolgens de onderzoeksmethode en de resultaten worden behandeld. Tot slot volgt hoofdstuk 11 met de conclusies van deelonderzoek B.

Algemene conclusies en aanbevelingen

In hoofdstuk 12 worden de conclusies en aanbevelingen van het totale onderzoek beschreven. Ook wordt hier de relatie tussen deelonderzoek A en deelonderzoek B nader behandeld.

Figuren, bronvermelding, afkortingen en appendix

In hoofdstuk 13 wordt de plaatsing van de figuren beschreven. In hoofdstuk 14 komt de Bronvermelding aan de orde, gevolgd door de Afkortinglijst in hoofdstuk 15. In deze afkortinglijst bevinden ter verduidelijking de afkortingen en hun betekenis aangezien in deze

masterthesis veel gebruikt maakt van afkortingen. Tot slot in hoofdstuk 16 de Appendix. In de Appendix worden de volgende onderwerpen besproken:

1. Analyse framework
2. Management literatuur samenvattingen
3. Interviewguide
4. Interviewguide presentatie
5. Verslaglegging interviews
6. Resultaten interviews

Deel A:

Criteria die de kwaliteit van een risico-analyse-rapport van een firewall bepalen

2 Inleiding

Om een helder beeld te krijgen van deelonderzoek A, “Criteria die de kwaliteit van een risico-analyse van een firewall bepalen”, wordt in dit hoofdstuk beschreven hoe dit deelonderzoek is opgebouwd.

Deelonderzoek A is als volgt opgebouwd:

- *Inleiding:* Hierin worden de doelstelling, vraagstelling en relevantie van dit onderzoek behandeld.
- *Projectkader:* In het projectkader worden begrippen die voor de context van dit onderzoek van belang zijn en de samenhang tussen deze begrippen behandeld.
- *Onderzoeksmethode:* Beschrijft de toepassing van de onderzoeksmethode van deelonderzoek A.
- *Resultaten:* Hierin worden de resultaten van het deelonderzoek gepresenteerd.
- *Conclusie:* De conclusies van deelonderzoek A staan hier beschreven.

Deze inleiding geeft tevens de opbouw van hoofdstuk 2 weer.

Hoofdstuk 2 heeft de volgende paragrafen:

- *Doelstelling:* Hierin wordt een introductie op de onderzoeksdoelstelling gegeven, gevolgd door de uiteindelijke doelstelling van dit deelonderzoek.
- *Vraagstelling:* Vanuit de doelstelling zijn een aantal onderzoeksvragen voortgekomen die hier worden weergegeven en beargumenteerd.
- *Relevantie:* De doelgroep en het nut van dit onderzoek worden in deze paragraaf uitgewerkt.

Nu volgt de introductie op de doelstelling.

2.1 Doelstelling

Organisaties zeggen veel in het beveiligen van hun informatie te investeren. Ze hebben afgesloten kantoren, laten vertrouwelijke documenten en archieven door gespecialiseerde bedrijven vernietigen, etc. etc. Het lijkt dat ze de beveiliging goed op orde hebben. Toch ontbreekt vaak een belangrijke schakel, namelijk het beveiligen van hun digitale informatie. Een schakel in het beveiligen van digitale informatie is het gebruik van een firewall.

Ondanks de belangrijke positie van een firewall in de ketting van (digitale) informatiebeveiliging, is de firewall onderbelicht wat betreft bedrijfs-(ondersteunde) processen over digitale informatiebeveiliging. Oftewel een firewall wordt gezien als een technisch apparaat wat er voor zorgt dat de digitale informatie veiliger gebruikt kan worden. Er zijn alleen niet voldoende ondersteunende bedrijfsprocessen om de firewall ook veilig operationeel te houden binnen een organisatie.

Een voorbeeld van een ondersteunend bedrijfsproces is het maken van een risico-analyse

van een firewall. Het resultaat van dit proces is een rapportage van de risico's die een organisatie loopt bij het koppelen van het bedrijfsnetwerk aan het Internet. Door middel van een firewall probeert de organisatie de risico's te beperken. Een firewall dient wel geconfigureerd te worden, zodat het bedrijfsnetwerk veilig blijft en tegelijkertijd de verbinding met het Internet operationeel wordt gehouden. Hoe een firewall geconfigureerd wordt is afhankelijk van de mate van risico die een organisatie wil lopen. Deze risico's worden beschreven in een risico-analyse-rapport. Maar hoe kan er bepaald worden of dit rapport van voldoende kwaliteit is om de organisatie te beschermen? Oftewel aan welke criteria dient een rapport te voldoen om een bepaald veiligheidsniveau te kunnen garanderen. Door het inzichtelijk maken van de criteria die de kwaliteit van de risico-analyse-rapportage bepalen, kan het risico-analyse proces beter aangestuurd worden. Dit kan vervolgens leiden tot een betere beveiliging van digitale informatie.

De doelstelling luidt:

> "Het exploreren welke criteria de kwaliteit van een risico-analyse-rapport bepalen, ten behoeve van de functionaliteit van een firewall."

Tevens probeert dit onderzoek bewustwording te creëren en ruimte te bieden aan verdere onderzoeken op het gebied van een risico-analyse van een firewall.

De functionaliteit van een firewall is van belang voor een veilige digitale informatie-uitwisseling tussen organisaties en haar omgevingen. Door middel van een exploratief onderzoek wordt er onderzocht wat de factoren zijn die de kwaliteit van een risico-analyse-rapport bepalen.

Nu de doelstelling duidelijk is, wordt in de volgende paragraaf de vraagstelling uitgewerkt.

2.2 Vraagstelling

De factoren, waarmee de kwaliteit van een risico-analyse wordt bepaald, ten behoeve van de functionaliteit van een firewall, zijn op dit moment, oktober 2006, niet bekend. Deze worden binnen dit onderzoek onderzocht. De volgende vraagstelling is uit de doelstelling af te leiden:

De vraagstelling luidt:

> "Welke criteria bepalen de kwaliteit van de risico-analyse-rapportage, ten behoeve van de functionaliteit van een firewall, welke van belang is voor een veilige digitale informatie-uitwisseling tussen organisaties en haar omgevingen?"

Op grond van bovenstaande vraagstelling zijn de volgende onderzoeksvragen geformuleerd:

1. Welke criteria worden gebruikt door managers en / of technici voor het bepalen van de kwaliteit van een risico-analyse-rapport?

2. Welke factoren beïnvloeden de criteria die door managers en / of technici voor het beoordelen van de kwaliteit van een risico-analyse-rapport worden gebruikt ten behoeve van de functionaliteit van een firewall?

De bovenstaande onderzoeksvragen zijn onderzocht. Hoe hierbij te werk is gegaan wordt in hoofdstuk 4 (Onderzoeksmethode) beschreven. In de volgende paragraaf wordt de relevantie van dit onderzoek beschreven.

2.3 Relevantie

De doelgroep van dit onderzoek zijn organisaties en instellingen, meer specifiek personen, die verbonden zijn met het gebruik van een risico-analyse-rapportage, zover mogelijk gericht op het toepassen van firewalls, ten behoeve van digitaal informatiebeleid. Met andere woorden; personen die invloed uitoefenen op het proces van het beveiligen van digitale informatie door middel van een firewall.

De hoeveelheid (wetenschappelijke) informatie omtrent dit onderwerp: de risico-analyse van firewalls en informatie over het gebruik ervan bij organisaties is schaars. Door middel van dit onderzoek wordt getracht meer kennis over het onderwerp te genereren.

Met dit onderzoek wordt geprobeerd meer kennis over het onderwerp te genereren. Aangezien de hoeveelheid (wetenschappelijke) informatie omtrent dit onderwerp schaars is is er gekozen om het onderzoek explorerend van aard te laten zijn zodat er nieuwe empirische kennis kan worden toegevoegd.

Aan de hand van de resultaten van dit onderzoek, het inzichtelijk maken van de factoren die de kwaliteit van een risico-analyse-rapportage bepalen, kan het risico-analyse proces beter aangestuurd worden. Dit resulteert in een verbeterd risico-analyse proces en daardoor een duidelijker inzicht in het beveiligen van digitale informatie met een firewall.

Onderzoeksvraag 1 is relevant voor organisaties aangezien er eerst duidelijk dient te zijn op welke punten een risico-analyse-rapportage ten behoeve van de functionaliteit van een firewall wordt beoordeeld. Op het moment dat dit niet inzichtelijk is, kan er niet eenduidig gediscussieerd worden over de kwaliteit van een rapportage.

Uit onderzoeksvraag 1 volgt onderzoeksvraag 2. De relevantie voor organisaties voor onderzoeksvraag 2 is dat op het moment dat het duidelijk is op welke criteria een risico-analyse-rapportage beoordeeld wordt (onderzoeksvraag 1) er bepaald kan worden welke kwaliteit het rapport heeft. Het is dan nog niet duidelijk welke factoren de criteria beïnvloeden om zodoende de risico-analyse-rapportage te verbeteren.

Na oriënterend onderzoek bleek dat er weinig 'open' informatie te vinden was over bovenstaande twee onderzoeksvragen. Dit betekent dat de huidige kennis ontbreekt, dan wel beperkt aanwezig of toegankelijk is. Het onderzoek is relevant voor organisaties en interessant voor de wetenschap, omdat er nieuwe kennis wordt ontwikkeld met betrekking tot het beoordelen van de kwaliteit van risico-analyse ten behoeve van de functionaliteit van een firewall. Vanaf dit moment wordt met “de risico-analyse” de “de risico-analyse ten

behoeve van de functionaliteit van een firewall” bedoeld.

Dit deelonderzoek levert een lijst van criteria op, die gebruikt worden om de kwaliteit van de risico-analyse te beoordelen. Daarnaast levert dit onderzoek een lijst van factoren die deze criteria, zowel positief als negatief, beïnvloeden.

Al met al wordt gepoogd om een kwalitatief risico-analyse resultaat (met onder andere financiële consequenties) ten behoeve van het verbeteren van de veiligheid van digitale informatie inzichtelijk te maken.

Tevens wordt er geprobeerd, mede door dit onderzoek een bewustzijn te kweken onder de personen waarmee ik in contact ben gekomen tijdens dit onderzoek. Hiermee wordt bedoeld dat de personen gaan nadenken over de besproken materie. Daarnaast kunnen de resultaten van dit onderzoek als basis gebruikt worden voor managers, technische en andere onderzoekers die zich in dit onderwerp willen verdiepen.

3 Projectkader

Om een helder beeld te krijgen van dit deelonderzoek, “Criteria die de kwaliteit van een risico-analyse van een firewall bepalen”, is het van belang duidelijkheid over het onderwerp te krijgen. De benaderingswijze is een andere dan die van het informatica-onderzoek. Vanuit het managementperspectief wordt vanuit een functionele en bedrijfsorganisatorische manier naar de materie gekeken. Daarom worden de belangrijkste begrippen en de samenhang daartussen, die voor de context van dit onderzoek van belang zijn, in de eerstvolgende paragrafen uiteengezet.

1. *Organisatie en informatie-uitwisseling:* Wat is een organisatie en waarom is de informatie-uitwisseling tussen een organisatie en haar omgeving van belang?

2. *Digitale informatie-uitwisseling tussen organisaties:* Wat is digitale informatie-uitwisseling (tussen een organisatie en haar omgeving) en waarom is digitale informatie-uitwisseling van belang voor de organisatie en haar omgeving?

3. *Informatiebeveiliging:* Wat houdt beveiliging van digitale informatie-uitwisseling tussen een organisatie en haar omgeving in en waarom is dit zo belangrijk?

4. *Incidenten bij digitale informatie-uitwisseling:* Welke beveiligingsincidenten kunnen zich voortdoen bij digitale informatie-uitwisseling?

5. *Wat is een firewall:* Wat is een firewall en waarom is deze van belang voor het beveiligen van digitale informatie-uitwisseling?

6. *Functionaliteit van een firewall:* Wat is de functionaliteit van een firewall met betrekking tot de veiligheid van digitale informatie-uitwisseling?

7. *Managen van een firewall:* Wat is het managen van firewalls?

8. *Firewall risico-analyse proces:* Wat is de rol van een risico-analyse proces in het verbeteren van de functionaliteit van firewalls, om zodoende de beveiliging van de digitale informatie-uitwisseling tussen een organisatie en haar omgeving te verbeteren?

9. *Resultaat van een firewall risico-analyse proces:* Wat is de output van een risico-analyse proces?

Bij de uitleg van de begrippen wordt er tevens een aanzet gegeven voor de impact van de begrippen op het onderzoek. Deze worden vervolgens in hoofdstuk 4 (Onderzoeksmethode) dan wel hoofdstuk 9 (Onderzoeksmethode) toegelicht.

3.1 Organisatie en informatie-uitwisseling

Binnen dit onderzoek wordt onder een organisatie verstaan, zoals Abels aangeeft (Abels, 1987): *“een groep of groepen van individuen die op min of meer afgesproken manier een gezamenlijk doel nastreven. De groep heeft hiertoe een bepaalde structuur en functioneert meestal in wisselwerking met de omgeving”*.

Een organisatie communiceert met haar omgeving om het gezamenlijke doel van de

organisatie na te streven. Organisaties worden steeds afhankelijker van hoog opgeleide medewerkers, omdat ieder met unieke kennis niet zonder meer vervangen kan worden. Informatie-uitwisseling kan gezien worden als de drager van deze unieke kennis binnen een organisatie (Mackenzie Owen, 2001).

Er zijn verschillende manieren om informatie uit te wisselen. De meest gebruikte communicatie methoden zijn:

- Mondelinge communicatie, ook wel face-to-face informatie-uitwisseling genoemd.
- Telefonische communicatie.
- Schriftelijke communicatie.
- Digitale informatie-uitwisseling.

Mondelinge informatie-uitwisseling gebeurt bijvoorbeeld tijdens het werk, dat kan door te praten met je collega's, het houden van toespraken en vergaderingen. Een speciale vorm van mondelinge communicatie is telefonische communicatie. Dit is communicatie waar door middel van een telefoon mondelinge informatie over langere afstanden uitgewisseld kan worden.

Daarnaast heb je schriftelijke communicatie. Hiermee wordt bedoeld alle communicatie die via schrift gecommuniceerd wordt, zoals een notitie of een verslag van een vergadering.

Met digitale informatie-uitwisseling wordt informatie-uitwisseling bedoeld welke via elektronische manieren plaatsvindt. Het meest bekende is het Internet, maar ook sms / mms en digitale TV zijn vormen van digitale informatie-uitwisseling. Binnen dit onderzoek wordt alleen gekeken naar digitale informatie-uitwisseling die via computernetwerken verloopt, zoals het Internet en een lokaal netwerk. Soorten digitale informatie-uitwisseling die via computernetwerken verlopen zijn:

- Email, bijvoorbeeld via webmail of Microsoft Outlook / Mozilla Thunderbird[1].
- Instant messaging, zoals Microsoft's MSN Messenger[2], jabber[3] en ICQ[4].
- World Wide Web, het welbekende surfen over het Internet met Microsoft's Internet Explorer of Mozilla Firefox[5]
- P2P, peer2peer zoals Bittorrent [6] en het eDonkey netwerk[7].

Vroeger was digitale informatie-uitwisseling een handig hulpmiddel, je kon namelijk altijd terugvallen op mondelinge, telefonische of schriftelijke informatie-uitwisseling. Tegenwoordig zijn er organisaties die enkel nog bereikbaar zijn via digitale informatie-uitwisseling, bijvoorbeeld het Internetbedrijf bol.com. Deze organisaties zijn volledig afhankelijk van digitale informatie-uitwisseling, aangezien zij deze vorm primair gebruiken (van Liere, 2005). Tegenwoordig maakt het bedrijfsleven steeds meer gebruik van digitale informatie-uitwisseling. Door de verandering in de manier van informatie-uitwisseling is

1 Zie http://www.mozilla.com/en-US/thunderbird/ voor meer informatie
2 Zie http://get.live.com/messenger/overview voor meer informatie
3 Zie http://www.jabber.org/ voor meer informatie
4 Zie http://www.icq.com/ voor meer informatie
5 Zie http://www.mozilla.com/en-US/ voor meer informatie
6 Zie http://www.bittorrent.org/ voor meer informatie
7 Zie http://en.wikipedia.org/wiki/EDonkey_network voor meer informatie

digitale informatie-uitwisseling steeds vaker van bedrijfskritisch belang en raken bedrijven steeds meer afhankelijk van deze manier van informatie-uitwisseling (van Liere, 2005). Hieruit valt op te maken dat dat digitale informatiebeveiliging steeds belangrijker wordt. Ook schriftelijke en telefonische communicatie kunnen via de digitale manier plaatsvinden. Met VoIP kun je telefoneren via digitale wegen (van Mastrigt, 2006). E-mail is een vorm van schriftelijke communicatie die via digitale communicatie verloopt.

Juist doordat digitale informatie-uitwisseling pas enkele decennia bestaat en ook nog eens explosief gegroeid is, zit de beveiliging van digitale informatie en het garanderen van deze digitale informatie-veiligheid nog in de ontwikkelingsfase.

Dit onderzoek richt zich op digitale informatie-uitwisseling binnen een organisatie en haar omgeving. Wat digitale informatie-uitwisseling precies is, wordt in de volgende paragraaf uitwerkt.

3.2 Digitale informatie-uitwisseling tussen organisaties

In de bovenstaande paragraaf is duidelijk geworden dat digitale informatie-uitwisseling van belang is bij organisaties. In deze paragraaf wordt uitgewerkt welke kenmerken digitale informatie-uitwisseling heeft.

Zoals elke vorm van informatie-uitwisseling heeft digitale informatie-uitwisseling een aantal basiskenmerken. Deze kenmerken zijn gebaseerd op de basiskenmerken van een computer (WWW-1)

1. *Invoer*: Het invoeren van digitale informatie. Voorbeelden zijn: een toetsenbord, een muis en een microfoon.

2. *Uitvoer*: Het uitvoeren van digitale informatie. Voorbeelden zijn: een monitor, een printer en een speaker.

3. *Uitwisseling:* Het uitwisselen van digitale informatie. Voorbeelden zijn: via het netwerk zoals een bedrijfsnetwerk, maar uitwisseling kan ook via het Internet plaatsvinden. Men kan hiervoor gebruik maken van bijvoorbeeld email, ftp of internet upload pagina's. Tevens kan er gebruik gemaakt worden van diskettes, usb-sticks of cd+r(w)/dvd+r(w)'s om digitale informatie uit te wisselen.

4. *Opslag:* Het fysiek vastleggen van digitale gegevens. Voorbeelden zijn: harddisk, cd-r(w), dvd-r(w) en usb-stick.

Elke interactie bij bovenstaande kenmerken geeft de mogelijkheid dat er informatie bewust, maar meestal onbewust aan derde gegeven kan worden. Zoals het bij 'invoer' van belang is dat men de invoer niet kan zien. Bij bijvoorbeeld geldautomaten is het niet de bedoeling dat iedereen je pincode af kan kijken. Een voorbeeld bij de 'uitvoer' is dat bij een gecentraliseerde printer er gelet dient te worden wie bij de printer kan. Zo dient beschermde informatie niet op een openbare printer geprint te worden. Tot slot de 'opslag, als iedereen bij de opgeslagen gegevens kan komen, bijvoorbeeld omdat de backups van die gegevens voor iedereen beschikbaar zijn, dan heeft het nut om digitale informatie-uitwisseling te beveiligen minder belang. Binnen dit onderzoek wordt er van uitgegaan dat de drie overige kenmerken, zit zijn invoer, uitvoer en opslag, afdoende beveiligd zijn.

Wat is nu precies een veilige manier van digitale informatie-uitwisseling is wordt in de volgende paragraaf uitgelegd.

3.3 Informatiebeveiliging

Informatiebeveiliging is tegenwoordig, en zal steeds meer, een belangrijk onderdeel zijn van de bedrijfsvoering van een organisatie. Zie paragraaf 3.4 (Incidenten bij digitale informatie-uitwisseling) voor de stijging van het aantal incidenten bij digitale informatie-uitwisseling. Informatiebeveiliging zorgt immers voor de bescherming van informatie tegen bedreigingen die de continuïteit van de bedrijfsvoering kunnen beschadigen. Daarom dient elke vorm van informatie, dus ook van digitale informatie, bij uitwisseling passend beveiligd te worden.

Informatiebeveiliging wordt, zoals gedefinieerd in Code voor Informatiebeveiliging, deel 1 gekarakteriseerd als het waarborgen van:

> 1. *Vertrouwelijkheid*: waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe geautoriseerd zijn;
> 2. *Integriteit:* het waarborgen van de correctheid en de volledigheid van informatie en de verwerking daarvan;
> 3. *Beschikbaarheid*: waarborgen dat geautoriseerde gebruikers op de juiste momenten toegang hebben tot informatie en aanverwante bedrijfsmiddelen. (NEN, 2000, ISO 27001: 8)

Deze drie kenmerken van informatiebeveiliging zijn ook van toepassing op digitale informatie-uitwisseling. Op het moment dat je digitale informatie uitwisselt, wil je dat deze digitale informatie alleen aankomt bij diegene voor wie de informatie bestemd is. Het is niet de bedoeling dat iemand anders dit kan lezen (Vertrouwelijkheid). Tevens wil je niet dat de digitale informatie die je verstuurt, anders ontvangen wordt door de ontvanger (Integriteit). Het laatste punt is dat wanneer er digitale informatie verstuurd dient te worden dit ook mogelijk is (Beschikbaarheid).

Waarom het beveiligen van digitale informatie-uitwisseling belangrijk is, is reeds uitgelegd. Maar is het beveiligen van digitale informatie nu ook nodig? Dit wordt in de volgende paragraaf uitgewerkt.

3.4 Incidenten bij digitale informatie-uitwisseling

In deze paragraaf wordt door middel van statistieken onderbouwd waarom het van belang is dat digitale informatie beveiligd wordt.

Het Computer Emergency Response Team, voortaan aangeduid met CERT[8], is een instituut dat zich bezig houdt met beveiligingsincidenten. De CERT beschrijft zichzelf als:

8 Zie http://www.cert.org/ voor meer informatie.

> "CERT is an organization devoted to ensuring that appropriate technology and systems management practices are used to resist attacks on networked systems and to limiting damage and ensure continuity of critical services in spite of successful attacks, accidents, or failures." (WWW-2).

Het CERT verstaat onder een incidenten het volgende:

> "An attack is a single unauthorized access attempt, or unauthorized use attempt, regardless of success. An incident, on the other hand, involves a group of attacks that can be distinguished from other incidents because of the distinctiveness of the attackers, and the degree of similarity of sites, techniques, and timing." (WWW-3).

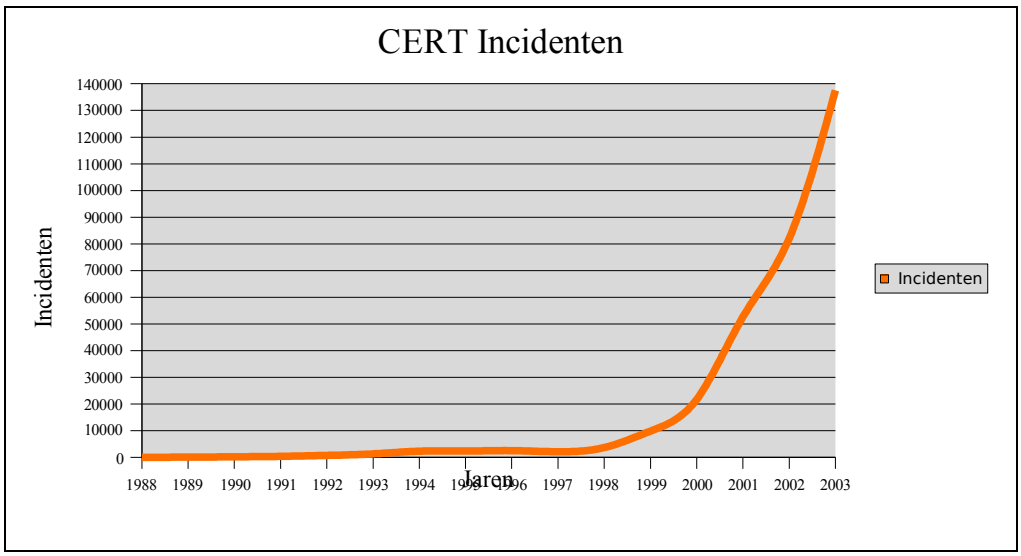
In de statistieken over het aantal beveiligingsincidenten van het CERT/Coordination Center, kun je zien dat het aantal incidenten exponentieel toeneemt. CERT/Coordination Center vanaf nu afgekort met CERT/CC. De statistieken beschrijven de incidenten welke in relatie liggen met systemen, aangesloten op een netwerk. De statistieken van de afgelopen jaren zijn in onderstaande tabel en figuur weergegeven.

Jaar	*Incidenten*	*Jaar*	*Incidenten*
1988	6	1996	2.573
1989	132	1997	2.134
1990	252	1998	3.734
1991	406	1999	9.859
1992	773	2000	21.756
1993	1.334	2001	52.658
1994	2.340	2002	82.094
1995	2.412	2003	137.529

Figuur 1: CERT/CC Incidenten 1988-2003 (WWW-4)

Er wordt geen verklaring gegeven voor de kleine terugloop in 1997, aangezien de statistieken gebruikt worden voor het globale overzicht. Daarnaast worden via deze methode, het tellen van het aantal gerapporteerde incidenten, geen statistieken na 2003

verzameld. De verklaring hiervoor is dat gebruikte methode door de groei van het Internet en geautomatiseerde systemen steeds minder betrouwbaar werd.



Figuur 2: CERT/CC Incidenten 1988-2003 (WWW-4)

Zoals je kunt zien aan de bovenstaande figuur, zie: Figuur 2, afgeleid uit de bovenstaande CERT incidenten tabel, is er een duidelijke stijging in het aantal gerapporteerde incidenten, op 1997 na.

De United States Computer Emergency Readiness Team (US-CERT) is een partnership tussen “Department of Homeland Security” en de publieke en private -sector. Sinds 2003 beschermt het de Internet infrastructuur door middel van het coördineren verdedigingen en antwoorden op cyber aanvallen.

De volgende taken heeft de US-CERT:

- Het analyseren van het verminderen van cyberdreigingen en kwetsbaarheden
- Het verspreiden van cyberdreigingen informatiebeveiliging
- Het coördineren van activiteiten ter beantwoording op cyberdreigingen

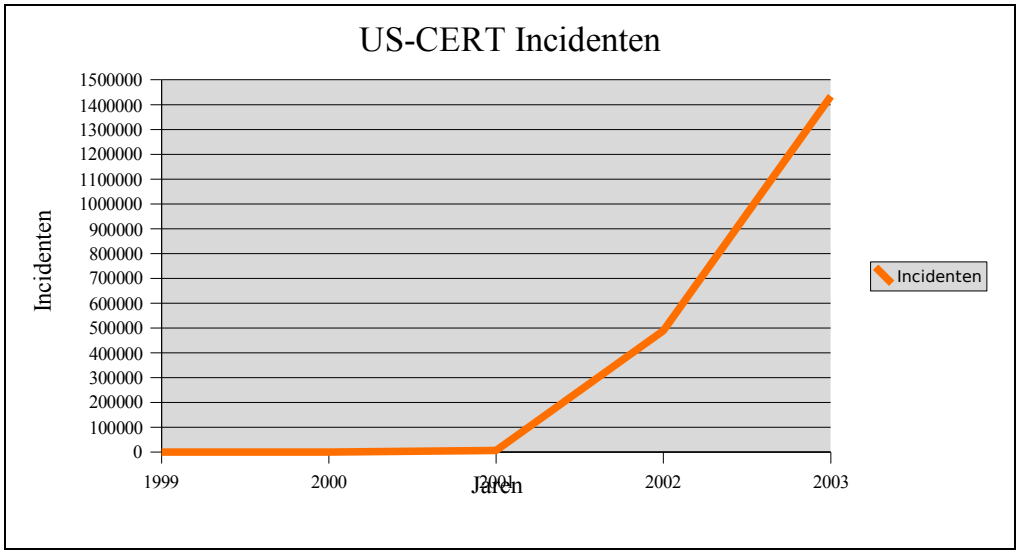
De US-CERT werkt samen met onder andere met overheidsinstellingen, industrie, publieke sector en onderzoeksinstellingen.

Ook het aantal US-CERT incidenten vertoont een stijgende lijn, zie Figuur 3.

Jaar	*Incidenten*
1999	454
2000	412
2001	6.555
2002	489.890
2003	1.433.916

Jaar	*Incidenten*
Jan-Jun 2004	56.034.751

Figuur 3: US-CERT Incidenten 1999-2004 (WWW-5)



Figuur 4: US-CERT Incidenten 1999-2003 (WWW-5)

In het jaar 2004 wordt weer een verhoging van het aantal incidenten verwacht. Er vanuit gaande dat er geen stijging, maar ook geen daling in de volgende kwartalen is, dan is het aantal verwachte incidenten van het jaar 2004, 2 X 56.034.751 = 112.071.502 incidenten. Doordat het aantal incidenten alleen maar toe neemt, dien je ook je netwerkbeveiliging naar een hoger niveau te krijgen om dezelfde beveiligingsgarantie te kunnen waarborgen.

Een methode van beveiliging van netwerkbeveiliging is het gebruik een firewall. Door middel van een firewall kan het risico dat er een incident plaatsvindt verkleind worden. Een firewall is een systeem dat digitale informatie-uitwisseling kan beschermen. Wat een firewall precies is komt in de volgende paragraaf aan bod.

3.5 Wat is een firewall

Computersystemen hebben gezorgd voor een grote stap vooruit in onze digitale revolutie. De

volgende stap in deze digitale revolutie is het verbinden van deze computersystemen, zodat deze met elkaar kunnen communiceren (Kurose e.a, 2001). Bij het onderling verbinden van computersystemen worden er netwerken van gekoppelde computersystemen gemaakt. Het Internet is op dit moment het grootste voorbeeld van een netwerk van gekoppelde computers. Op het Internet zijn grote hoeveelheden informatie en kennis beschikbaar die van groot belang zijn en in sommige gevallen essentieel zijn voor de continuïteit van een organisatie. Omdat het Internet zeer omvangrijk is, en er niet één instantie is die enige vorm van controle heeft over het Internet, is het Internet een vrijhaven voor mensen met verschillende ideeën en gedachten[9]. Helaas zijn er mensen die proberen in te breken in computersystemen om bewust dingen kapot te maken of zelfs specifiek op zoek gaan naar (bedrijfskritische) informatie. Bedrijven die zich verbinden met het Internet dienen op de hoogte te zijn van zowel de voordelen: het toegang hebben tot grote hoeveelheden informatie, als de nadelen: het gevaar dat er aanvallers kritische bedrijfssystemen en hun datagegevens kunnen aanvallen.

Digitale informatie-uitwisseling valt binnen het gebied van netwerkbeheer. In de Code voor Informatiebeveiliging, deel 2 staat het volgende geschreven over netwerkbeheer:

> Netwerkbeheer:
> "Het handhaven van de beveiliging van informatie in netwerken en de bescherming van de ondersteunde infrastructuur" (NEN, 2000, ISO 27003: 13).

De meest gebruikte bescherming tegen deze nadelen is het implementeren van een firewall in een netwerk (CSI/FBI, 2005). Een netwerk bestaat uit gekoppelde computers.

Een firewall wordt als volgt omschreven:

> Een firewall is een combinatie van apparatuur en programmatuur waarbij het mogelijk is om, via opgestelde regels, netwerkverkeer te beheersen. Hierdoor kan netwerkverkeer tussen verschillende domeinen gereguleerd worden (Pluis, 2005).

Een firewall beschermt het netwerk tegen aanvallers die de vertrouwelijkheid, integriteit en beschikbaarheid (zie paragraaf 3.3 (Informatiebeveiliging)) van de gekoppelde computers willen compromitteren (NEN, 2000, ISO 27001: 8).
Firewalls kun je opsplitsen in een tweetal groepen, software-firewalls en hardware-firewalls. De sofware-firewall wordt ook wel een hostbased of personal firewall genoemd en de hardware-firewall wordt ook wel networked-firewall genoemd. Als eerste wordt de software-firewall besproken.

Een software-firewall is een firewall die bedoeld is om één lokaal systeem, het systeem waar de software-firewall geïnstalleerd is, te beschermen. Voorbeelden hiervan zijn: Zone Alarm[10], Symantec Norton Personal Firewall[11].

Een hardware-firewall heeft deze benaming te danken aan het feit dat dit soort firewalls

9 Dat er geen instantie controle heeft over het Internet is tevens een groot voordeel aangezien je hierdoor ook geen censuur kan opleggen. Oftewel het Internet is een vrijhaven voor andersdenkenden.
10 Voor meer informatie bekijk: http://www.zonelabs.com/
11 Voor meer informatie bekijk: http://www.symantec.com/

meestal eigen hardware hebben. Een hardware-firewall probeert een netwerk van computers oftewel een Locale Area Network (LAN), zoals een bedrijfsnetwerk, te beveiligen tegen een groter netwerk ook wel Wide Area Network (WAN) genoemd, zoals bijvoorbeeld het Internet. Tevens kun je de WAN willen beschermen tegen de LAN. Een internet-café kan het internet willen beschermen tegen de klanten die de winkel heeft. Bijvoorbeeld een klant die spam wil versturen naar mensen op het internet.

Op het moment dat er gesproken wordt over het beveiligen van netwerken tegen elkaar worden eigenlijk de gebruikers van de netwerken bedoeld. De gebruikers van de netwerken communiceren immers met elkaar.

Binnen dit onderzoek wordt alleen gekeken naar hardware-firewalls. Daarom zal in de rest van het document bij de term firewall de hardware-firewall bedoeld worden. De reden van deze keuze is dat organisaties hardware-firewalls gebruiken om hun netwerk te beschermen.

In dit onderzoek wordt gekeken naar een firewall die data-stromen via het Internet Protocol tussen twee netwerken inspecteert, verdeelt en autoriseert. De datastromen bestaan uit kleine datagrammen (Stevens, 1994). Deze datagrammen dienen door de firewall geïnspecteerd, verdeeld en geautoriseerd te worden. Tevens dient de firewall de vertrouwelijkheid, integriteit en beschikbaarheid, zie paragraaf 3.3 (Informatiebeveiliging), van deze data-stromen te kunnen waarborgen.

In dit onderzoek wordt de volgende eigen definitie van een firewall gebruikt:

> Firewall:
> “Een apparaat dat datastromen die bestaan uit datagrammen via het Internet Protocol (IP) tussen twee netwerken inspecteert, verdeelt en autoriseert om de vertrouwelijkheid, integriteit en beschikbaarheid van de datastromen te waarborgen” (Berlijn, 2007).

Ondanks dat er een goed geïnstalleerde en geconfigureerde firewall in een bedrijfsnetwerk is opgenomen, is het nog steeds mogelijk dat beveiliging van digitale informatie niet optimaal is. Er zijn andere manieren voor een aanvaller om toegang te krijgen tot een bedrijfsnetwerk die buiten de werking van een firewall omgaan. Onder deze mogelijkheden valt het verkrijgen van autorisatierechten via onder andere sociaal-engineering en makkelijk te raden wachtwoorden. Zie paragraaf 8.1 (Aanvalsmethodieken) voor een uitgebreidere omschrijving. Ook bestaat er de mogelijkheid dat een aanvaller fysiek toegang heeft tot het systeem. Hiermee wordt bedoelt dat een aanvaller de hardware kan aanpassen en veranderen naar eigen inzicht. Bijvoorbeeld als er een firewall in een kantoorruimte staat waar iedereen toegang tot heeft. Daarmee is de veiligheid welke je van een firewall verwacht te niet gedaan. Het is duidelijk dat een firewall een onderdeel is van een totaal beveilingsplan.

In dit onderzoek wordt geen rekening gehouden met andere mogelijke aanvallen. Er wordt alleen gekeken naar aanvallen die via het netwerk op de firewall plaatsvinden. Dit zijn aanvallen die plaatsvinden door gebruik te maken van een netwerk. Door middel van dit netwerk probeert een aanvaller via zijn eigen netwerk toegang te verkrijgen tot het netwerk van het slachtoffer.

Nu we weten wat een firewall doet, gaan we wat dieper in op de materie. In de volgende paragraaf wordt beschreven wat de functionaliteit van een firewall is.

3.6 Functionaliteit van een firewall

Om de kwaliteit van risico-analyse-rapport van een firewall te kunnen verbeteren is het van belang om te weten welke functionaliteit een firewall heeft. Belangrijke functionaliteit die vaak de boventoon voeren zijn (WWW-6, WWW-7):

- Snelheid waarmee de firewall werkt.
- Betrouwbaarheid van de firewall.
- Het gebruikersgemak

Deze functionele beschrijvingen zijn voornamelijk vanuit een technisch oogpunt gemaakt, aangezien de technici vaak beslissen welke firewalls er aangeschaft dienen te worden. Op het moment dat er niet vanuit technisch perspectief wordt gekeken komen er nog andere factoren naar boven. Bijvoorbeeld:

- De snelheid waarmee een firewall te her-configureren valt. Hiermee wordt bedoeld de tijdsduur waarmee een firewall ingesteld kan worden naar de nieuwe gestelde veiligheidseisen.
- De kosten die gemaakt worden voor een firewall. Deze moeten evenredig zijn aan het profijt van de firewall. Met andere woorden het bestaansrecht van een firewall binnen een organisatie.
- De haalbaarheid van het gestelde beleid. Het is hierbij de vraag of de gestelde policies, bijvoorbeeld het toestaan van email verkeer, binnen de organisatie kunnen worden geïmplementeerd en door de firewall kunnen worden uitgevoerd (van Mastrigt, 2006).

Op het moment dat er besloten wordt om een firewall te gebruiken, dient een firewall en het bedrijfsproces eromheen ook onderhouden te worden. Dit is te vergelijken met het aanschaffen van een auto. Deze auto dient ook onderhoudsbeurten te krijgen om probleemloos te kunnen rijden. Als je dit niet doet, kan een auto mankementen gaan vertonen. Dit is vergelijkbaar met een firewall.

De functionele eisen die vanuit een organisatie gesteld worden zijn soms technisch niet haalbaar. Een manager wil veilige toegang hebben via het Internet tot het organisatie-netwerk om aan digitale informatie te komen en te versturen. Onder veilig wordt hier verstaan dat de vertrouwelijkheid, integriteit en beschikbaarheid (zie paragraaf 3.3 Informatiebeveiliging) van de digitale informatie intact blijven. Tevens wil een manager het organisatie-netwerk 100% veilig houden, voor zover mogelijk. De enige manier om een 100% veilig netwerk te hebben, is door het *niet* hebben van een bedrijfsnetwerk (Prins, 1997). De manager kan alleen proberen om een zo hoog mogelijk veiligheidspercentage te krijgen afhankelijk van zijn budget, zonder hierdoor andere bedrijfsprocessen te blokkeren. Bijvoorbeeld een manager van een webwinkel kan moeilijk besluiten om de webwinkel niet te koppelen aan het Internet.

Om een veilig netwerk te creëren, dien je alle aanvalsmogelijkheden op het netwerk vast te stellen en daar effectieve maatregelen tegen te treffen. Bij een huis wil je de deur op slot doen om te voorkomen dat een inbreker binnen komt. Maar omdat er continu nieuwe aanvalsmogelijkheden gevonden worden, is het vaststellen en het ontwikkelen van een standaardimplementatie, dit wil zeggen een standaard verdedigingsstrategie die de meeste

organisaties afdoende beschermt, erg moeilijk (WWW-8). Als een inbreker merkt dat een deur afsloten is kan de inbreker er voor kiezen om via een open raam naar binnen te komen. Mocht alles hermetisch afgesloten zijn kan de inbreker een andere huis proberen. Maar als de inbreker iets wil hebben wat alleen in de hermetisch afgesloten zit. Kan de inbreker proberen de deur kapot te zagen.

Aangezien er geen standaard verdedigingsstrategie voor netwerken bekend is, betekent dit impliciet dat de configuraties van firewalls ook niet standaard zijn. Daarnaast zijn configuraties zijn even uniek zijn als de organisaties zelf. Aangezien elke organisatie zijn eigen wensen heeft die vervolgens weer resulteren in eisen die ze stellen aan digitale informatie-uitwisseling. Deze eisen hebben vervolgens weer invloed hebben op de configuratie van de firewall.

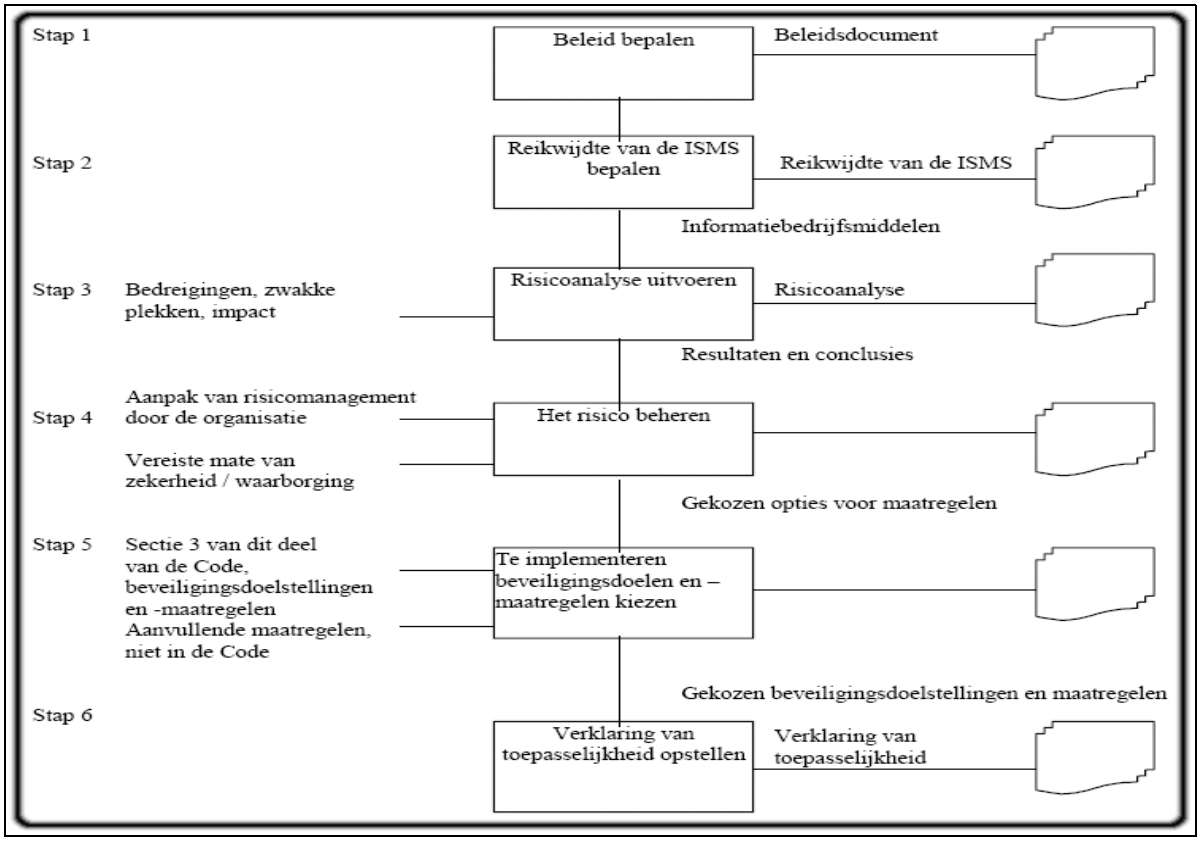
Organisaties met een firewall dienen de implementaties constant te controleren op nieuwe aanvalsmogelijkheden. Instanties zoals SANS (SysAdmin, Audit, Network, Security) Institute[12] en CERT leveren informatie over nieuwe aanvalsmogelijkheden. Beveiligen van digitale informatie richt zich dan ook op een 'Best Practice'-model. Dit is een model waarbij nieuwe ervaringen en informatie de implementatie en het bedrijfsproces continue aanvullen en verbeteren. Dit betekent dat ervaring wordt gebruikt om bestaande en nieuwe modellen te maken zodat deze modellen beter zijn de de vorige versies. De code voor Informatie Beveiliging is een voorbeeld van een 'Best Practice' model (Oud, 2002). Het bedrijfsproces om de firewall te managen wordt in de volgende paragraaf uitgewerkt.

3.7 Managen van een firewall

In deze paragraaf wordt uitgelegd welk bedrijfsproces / bedrijfsperspectief binnen dit onderzoek gebruikt wordt.

Het managen van een firewall proces valt binnen het Information Security Management System (ISMS) proces, wat een onderdeel is van de vele bedrijfsprocessen die gebruikt kunnen worden om een organisatie te sturen (WWW-9). Binnen dit onderzoek wordt er enkel gekeken naar het ISMS proces. Aangezien dit bedrijfsproces onderdeel is van de Code voor informatiebeveiliging (NEN, 2000, ISO 27003) en de Code voor infomatiebeveiliging een veel gebruikt bedrijfsproces binnen organisaties is.

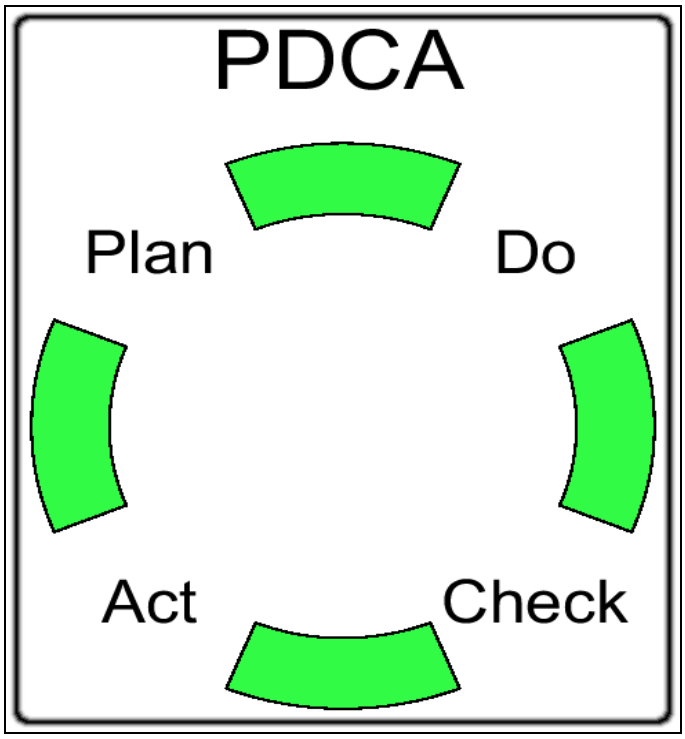
12 Zie http://sans.org voor meer informatie



Figuur 5: ISMS Code voor informatiebeveiliging, deel 2 (NEN, 2000, ISO 27003)

Het ISMS is een Internationale standaard voor informatiebeveiliging. Dit proces wordt als een stroomdiagram weergegeven, zie Figuur 5 (NEN, 2000, ISO 27003).

Het ISMS ontwerp van de Code voor informatiebeveiliging, deel 2 (Zie Figuur 5) bevat een zestal stappen, maar is nog niet helemaal compleet (NEN, 2000, ISO 27003). Het mist namelijk het “Check” punt van de Plan-Do-Check-Act (PDCA), een veel gebruikte management methode van Dr. W.E. Deming (Oud, 2002). Oftewel het ISMS onderwerp mist de evaluatie van het opgestelde beleid (Oud, 2002).



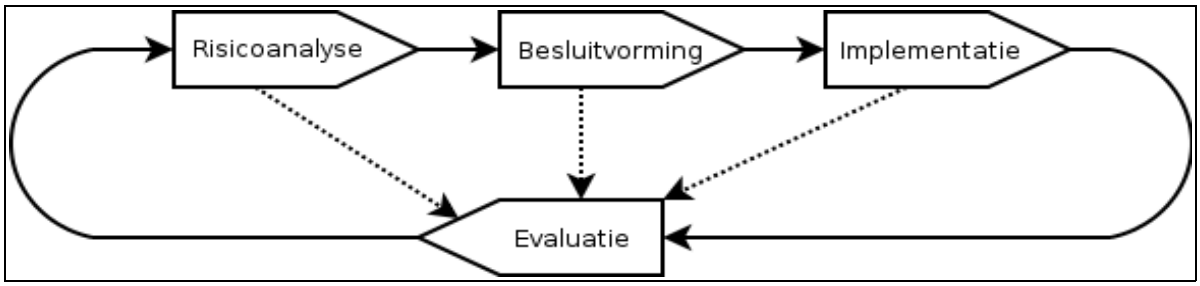
Figuur 6: Plan Do Check Act (PDCA)(Oud, 2002)

Voor dit onderzoek wordt gebruik gemaakt van een vereenvoudigd ISMS model. Dit model wordt in Figuur 7 weergegeven. Dit model combineert het ISMS ontwerp van de Code voor informatiebeveiliging, deel 2 (NEN, 2000, ISO 27003), zie Figuur 5, met het Plan-Do-Check-Act (PDCA) (Oud, 2002) zie Figuur 6.

Het aantal stappen van het ISMS is verminderd, maar er is wel een continu proces van gemaakt, aangezien het ISMS ontwerp dit niet in zich heeft. Op deze manier combineert het model goed met een firewall management proces, omdat dit een continu proces is dat constant zijn resultaten evalueert en, waar nodig, het proces kan aansturen en aanpassen.

Binnen het firewall management proces wordt er vanuit gegaan dat bekend is wat het beveiligingsbeleid en de scope van dit beleid is. Dit zijn stap 1 en stap 2 in Figuur 5. Dit vormt de basis voor de besluitvormingsstap in Figuur 7. Wel kan bij de evaluatie van dit proces input gegeven aan het management proces dat de beveiligingsbeleid bepaald. Hierdoor kan vanuit het firewall management proces aansturing gegeven worden aan het beveiligingsbeleid.

Dit proces, die interactie tussen de firewall management proces en het beveiligingsbeleid management proces, is niet meegenomen in Figuur 7. Stap 3 komt overeen met de Risico analyse en stap 4 en 5 komen overeen met implementatie fase. Stap 6 komt overeen met de evaluatie fase.



Figuur 7: Firewall risico-analyse proces (Berlijn, 2007)

Met andere woorden het proces beschreven in Figuur 7 is een proces dat bedoeld is om een firewall te managen. Dit proces heeft als input het beveiligingsbeleid van de organisatie nodig. De risico-analyse wordt gemaakt aan de hand van het beveiligingsbeleid.

Het risico-analyse proces genereert output welke als input dient voor de besluitvorming en ook onderwerp kan zijn van evaluatie. Hiermee wordt bedoelt dat de risico-analyse stap, als wel de besluitvorming en implementatie stap, als geheel ook geëvalueerd kan worden. In de besluitvorming wordt er een keuze gemaakt om een bepaald risico in te perken. Vervolgens worden de besluiten geïmplementeerd. Daarna wordt het totale proces geëvalueerd. Dit kan ook tijdens het firewall risico-analyse proces uitgevoerd worden, zodat er bijtijds gestuurd kan worden.

Nu er beschreven is wat voor soort proces er gebruikt wordt binnen dit onderzoek, wordt dit proces in de volgende paragraaf toegepast op de risico-analyse van een firewall.

3.8 Firewall risico-analyse proces

In deze paragraaf wordt beschreven wat de functie van een risico-analyse proces in het verbeteren van de functionaliteit van een firewall is. Als eerste de definitie van een risico-analyse die binnen dit onderzoek gebruikt wordt. De definitie van een risico-analyse volgens Code voor informatiebeveiliging, deel 1 is:

> Risico-analyse:
> "Beoordeling van de bedreiging voor, effecten op en kwetsbaarheden van informatie en IT-voorzieningen en de waarschijnlijkheid van het optreden van deze bedreigingen" (NEN, 2000, ISO 27001).

Aangezien deze definitie voor dit onderzoek niet volledig is en in andere literatuur geen eenduidige beschrijving gevonden is, wordt binnen dit onderzoek de volgende eigen definitie gebruikt. De bovenstaande definitie mist het aspect van preventie- en sturingsmaatregelen. Daarom wordt binnen dit onderzoek de volgende eigen definitie gebruikt:

> Risico-analyse:
> "Het geheel van activiteiten dat als doel heeft het systematisch en permanent identificeren van risicofactoren, en het vaststellen en evalueren van het risico, zowel kwantitatief als kwalitatief, met het oog op het bepalen van de preventie- en sturingsmaatregelen." (Berlijn, 2007).

Het risico-analyse proces (Zie Figuur 7) is een onderdeel van een continu proces, aangezien de risico's binnen de risico-analyse kunnen veranderen. In een eerste instantie laag ingeschat risico kan door een veranderde of nieuwe aanvalsmogelijkheid veranderen in een hoog risico. Er kan namelijk een fout ontdekt worden in een systeem die op dat moment operationeel is. Hierdoor kan de digitale informatie-uitwisseling in één keer onveilig worden in plaats van, wat eerst werd aangenomen, veilig. Aangezien er steeds meer kwetsbaarheden gevonden worden, dient men na een verandering zo snel mogelijk een nieuwe risico-analyse uit te voeren om te bepalen in hoeverre de gevonden kwetsbaarheden impact hebben op het huidige risicobeleid (WWW-4). Het versnellen van de risico-analyse geeft als resultaat dat er eerder een besluit genomen kan worden, dat hierdoor ook sneller geïmplementeerd kan worden. Oftewel de tijdsduur van de mogelijke aanwezigheid van een hoger risico wordt hiermee ingekort. Om ervoor te zorgen dat een risico-analyse sneller verloopt, dien je inzicht te hebben in de risico's die de organisatie loopt. Een andere vorm van implementatie, of een wijziging van de oude implementatie, kan hierbij nodig zijn. Je wilt gebruik kunnen maken van eerder verkregen onderzoeksgegevens, waarop reeds gemaakte risico-analyse gebaseerd zijn. Veranderingen die plotseling gebeuren kunnen vervolgens eenvoudig worden ingevoerd in de 'oude' risico-analyse om hieruit direct een 'nieuwe' risico-analyse te kunnen genereren. Tevens wil je gebruik maken van bekende, door empirisch onderzoek verkregen, gegevens die je kunt gebruiken in de risico-analyse zonder dat alles opnieuw hoeft te worden onderzocht.

Maar wat levert een risico-analyse proces nu op? Dat komt in de volgende paragraaf aan bod.

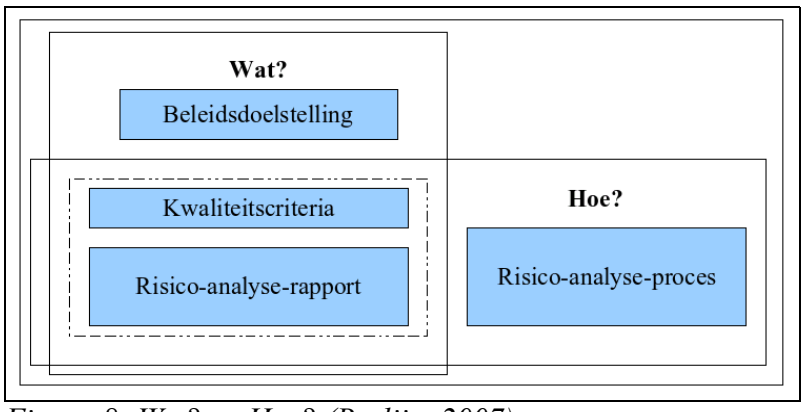
3.9 Resultaat van een firewall risico-analyse proces

Het resultaat van een firewall risico-analyse proces levert uiteindelijk een document op. In dit document, vanaf nu het risico-analyse-rapport geheten, staan de resultaten van de gegevens die tijdens het risico-analyse proces gevonden zijn. Maar hoe kan er bepaald worden of het resultaat van dit risico-analyse proces van voldoende kwaliteit is om beslissingen te nemen.

Op het moment dat er een risico-analyse-rapport geanalyseerd wordt om te bepalen hoe de risico-analyse verbeterd kan worden, dient eerst duidelijk te zijn aan welke criteria een risico-analyse moet voldoen. Met deze criteria, die in dit deelonderzoek onderzocht worden, kan iemand bepalen of de risico-analyse van voldoende kwaliteit is om te gebruiken om zodoende gestaafde beslissingen te kunnen nemen.

Er wordt in dit onderzoek niet naar de criteria gekeken "Hoe" een risico-analyse verbeterd kan worden. Oftewel er wordt niet gekeken naar criteria die gebruikt worden om het management risico-analyse-proces te verbeteren. Het risico-analyse-proces wordt gebruikt om een risico-analyse-rapport op te stellen. Er wordt tevens niet naar de "Wat" vraag

gekeken. Met andere worden welke criteria ten grondslag liggen aan de beleidsdoelstellingen. Maar er wordt gekeken naar het resultaat van de “Hoe” en “Wat” vraag, oftewel het risico-analyse-rapport en de criteria die de kwaliteit van dit rapport bepalen. Figuur 8 geeft een schematische weergave van de “Wat” en “Hoe” vraag en de resultaten hiervan.

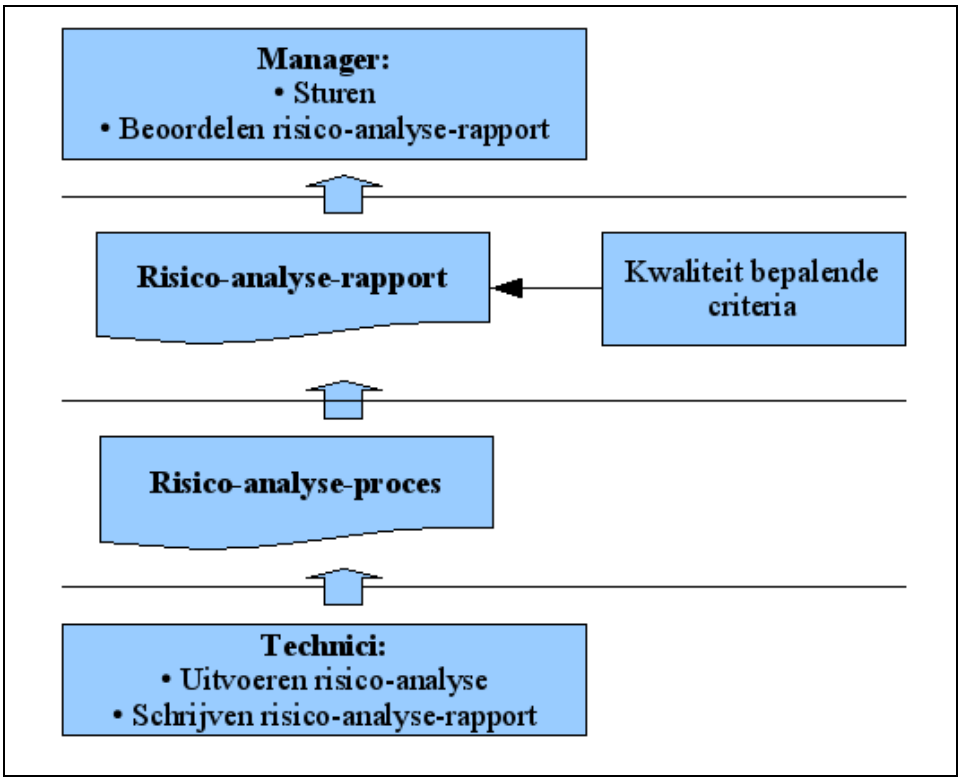


Figuur 8: Wat? en Hoe? (Berlijn, 2007)

Binnen het risico-analyse proces zijn verschillende functies betrokken, te weten die van de technicus en manager. In sommige bedrijven kunnen deze functies door één persoon bezet worden. Om de functiebeschrijvingen te verduidelijken is de relatie tussen technicus en manager weergeven in (Figuur 9). Een belangrijk onderscheid: managers zijn veelal economisch ingesteld terwijl de technici meer technologisch zijn ingesteld.

Managers die sturing geven over de firewall krijgen het resultaat van een risico-analyse en zullen aan de hand van de risico-analyse sturing geven. Om goed alle facetten van het veilig, functioneel een operationeel houden van een firewall te sturen dient de risico-analyse van goede kwaliteit te zijn. De manager dient te achterhalen wat de kwaliteit van de risico-analyse is. Bewust en misschien onbewust beoordeelt een manager een risico-analyse-rapport.

Technici van de risico-analyse, bijvoorbeeld auditors, hanteren kwaliteitscriteria bij de uitvoer van een risico-analyse. Bij het schrijven van een risico-analyse-rapport maken zij keuzes over wat wel en wat niet in het document gezet wordt en hoe bepaalde informatie wordt weergegeven.



Figuur 9: Manager / technici relatie (Berlijn, 2007)

Binnen dit onderzoek is gekeken naar welke criteria van invloed zijn op de kwaliteit van het risico-analyse-rapport. Dat wil zeggen er wordt gezocht naar een lijst van criteria die de kwaliteit van een risico-analyse-rapport bepalen. Door de kwaliteit van een risico-analyse-rapport beter in te kunnen schatten kan een betere besluitvorming plaatsvinden op basis van het resultaat, aangezien de informatievoorziening van de besluitvorming verbeterd is.

4 Onderzoeksmethode

Uit het vorige hoofdstuk komt naar voren dat het verbeteren van het risico-analyse-rapport van een firewall van toegevoegde waarde is voor een organisatie die gebruik maakt van een firewall. Door de kwaliteit van het risico-analyse-rapport te verbeteren kan een betere besluitvorming plaatsvinden op basis van het risico-analyse-rapport. Voor de leesbaarheid van dit onderzoeksdocument wordt met "risico-analyse" bedoeld: "risico-analyse ten behoeve van de functionaliteit van de firewall welke van belang is voor een veilige digitale informatie-uitwisseling tussen organisaties en haar omgevingen". Met de functionaliteit van de firewall wordt onder andere bedoeld; bewerkingen van datagrammen zoals het filteren van datagrammen door de firewall (Stevens, 1994).

Om de doelstelling van deelonderzoek A te bereiken, deze luidt:

> "Het exploreren welke criteria de kwaliteit van een risico-analyse-rapport bepalen, ten behoeve van de functionaliteit van de firewall."

wordt binnen dit onderzoek door middel van literatuurstudie en empirisch onderzoek bepaald welke kwaliteitseisen, zoals beschreven in bovenstaand hoofdstuk, gebruikt worden. Dit empirisch onderzoek betreft een explorerende studie en is door middel van literatuurstudie en open interviews uitgevoerd (Doorewaard, 2005).

De vraagstelling luidt:

> "Welke criteria bepalen de kwaliteit van de risico-analyse-rapportage, ten behoeve van de functionaliteit van een firewall, welke van belang is voor een veilige digitale informatie-uitwisseling tussen organisaties en haar omgevingen?"

Op grond van bovenstaande vraagstelling zijn de volgende onderzoeksvragen geformuleerd:

> 1. Welke criteria worden gebruikt door managers en / of technici voor het bepalen van de kwaliteit van een risico-analyse?
>
> 2. Welke factoren beïnvloeden de criteria die door managers en / of technici voor het beoordelen van de kwaliteit van een risico-analyse-rapport worden gebruikt ten behoeve van de functionaliteit van een firewall?

Het voorgaande hoofdstuk biedt het kader waarbinnen dit onderzoek plaatsvindt. Om antwoord te kunnen geven op de twee onderzoeksvragen is in deze paragraaf uiteengezet hoe dit deelonderzoek ingevuld is.

In dit hoofdstuk worden achtereenvolgens de volgende punten behandeld:

- *Onderzoeksaanpak:* Als eerste wordt een totaalbeeld geschetst van de opbouw van deelonderzoek A.

- *Analyse framework:* Het analyse framework heeft als doel het systematisch verzamelen van informatie om antwoord te kunnen geven op de onderzoeksvragen.
- *Literatuurstudie:* De literatuurstudie heeft als doel het verzamelen en analyseren van relevante literatuur.
- *Empirie: Interviews technici / managers:* Tijdens het empirisch onderzoek worden interviews gehouden om relevante informatie van managers en / of technici te verzamelen.
- *Vergelijking resultaten literatuurstudie en empirie:* Het vergelijken van de resultaten van de literatuurstudie en het empirisch onderzoek.

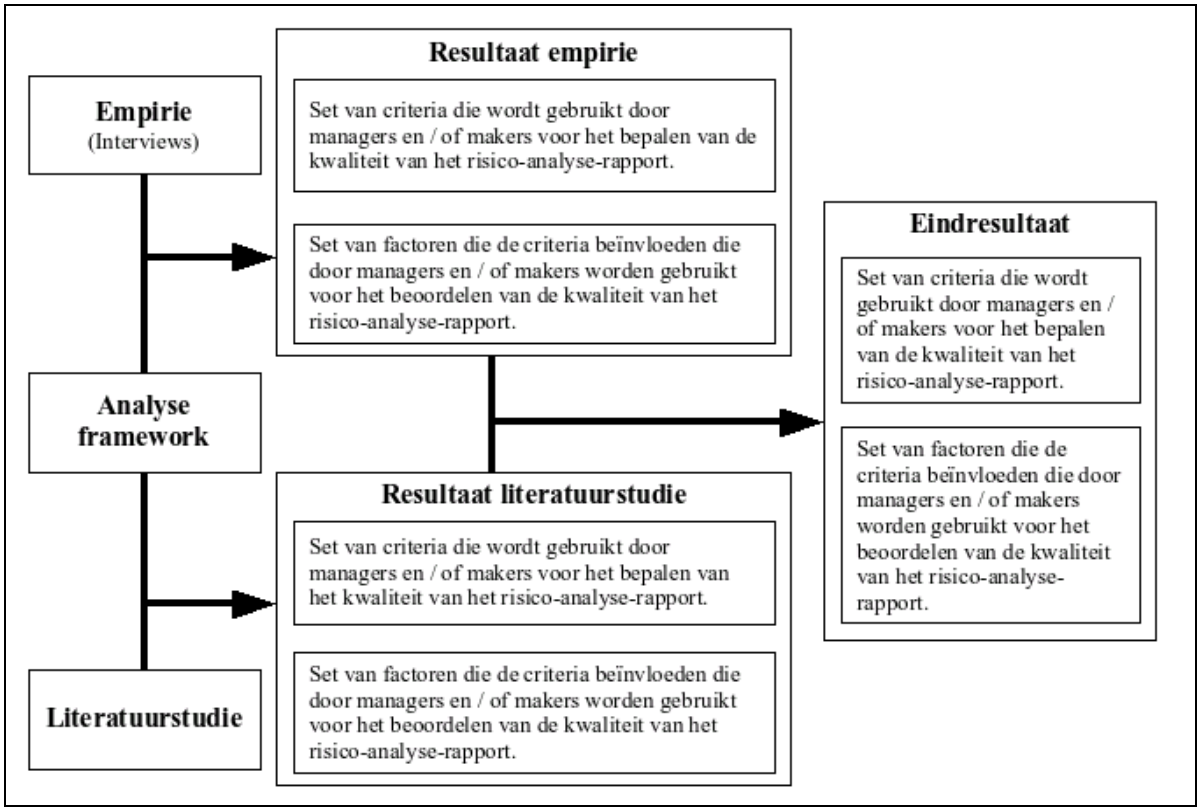
4.1 Onderzoeksaanpak

In deze paragraaf wordt in het kort uitgewerkt welke methodes er gebruikt worden binnen dit onderzoek en hoe deze zich tot elkaar verhouden. In paragraaf 4.2 komt het Analyse framework aan bod, paragraaf 4.3 gaat in op de Literatuurstudie en paragraaf 4.4 behandeld het Empirisch onderzoek (interviews).

Omdat dit deelonderzoek plaatsvindt op een relatief onbekend gebied is weinig kennis beschikbaar. Daarom is als strategie gekozen voor de combinatie van analyse framework, literatuurstudie en open interviews (empirisch onderzoek) als bronontginning (Doorewaard, 2005). Hier wordt in de volgende alinea's verder op ingegaan. Het deelonderzoek bestaat uit een viertal hoofdonderdelen:

1. Analyse framework
2. Literatuurstudie
3. Empirie: Interviews technici / managers
4. Vergelijking resultaten literatuurstudie en empirie

In Figuur 10 staat een schema waarin de relaties tussen bovenstaande onderdelen beschreven staan. In dit onderzoeksplan is sprake van een beperkte terugkoppeling. Er wordt weinig rekening gehouden met de evaluatie van de resultaten van dit onderzoek. Dit betekent onder andere dat interviews niet gebruikt zullen worden om andere interviews te sturen. Deze beperkte terugkoppeling wordt veroorzaakt door de beschikbare tijd in combinatie met de beperkte toepassing van een iteratief proces bij dit explorerend onderzoek. De gevonden resultaten zullen in het empirisch deel worden teruggekoppeld om zodoende de validiteit te kunnen waarborgen



Figuur 10: Onderzoeksplan (Berlijn, 2007)

Dit onderzoeksplan geeft een schematische weergave van de uitvoering van deelonderzoek A. Nu volgt de uitleg van de methoden, te beginnen met het analyse framework.

Analyse framework

Het analyse framework is gebruikt om een basis te creëren waarmee gediscussieerd kan worden. Dit analyse framework dient als basis om de resultaten van de literatuurstudie te organiseren. Het geeft een kader van waaruit naar verdere informatie kan worden gezocht. Zie paragraaf 4.2 (Analyse framework) voor meer informatie. Na het ontwikkelen van het analyse framework volgt de literatuurstudie.

Literatuurstudie

Om inzicht te krijgen in de materie over de criteria is een literatuurstudie uitgevoerd om reeds bekende criteria te verzamelen. Het resultaat van het literatuuronderzoek is beschreven in een conceptueel model, waarbij gebruik gemaakt wordt van het analyse framework. De informatie voor deze literatuurstudie is voornamelijk gezocht in de universiteitsbibliotheek en op wetenschappelijke internetsites. Zie paragraaf 4.3 (Literatuurstudie) voor meer informatie. Het resultaat van de literatuurstudie wordt gebruikt om antwoord te kunnen geven op de gestelde onderzoeksvragen vanuit de theorie.

De onderzoeksaanpak met betrekking tot de interviews wordt in de volgende alinea behandeld.

Empirie: Interviews technici / managers

Na de literatuurstudie hebben er interviews plaatsgevonden. Bij deze interviews is, tijdens het voorbereiden en het afnemen, geen gebruik gemaakt van de resultaten van de literatuurstudie, dit om een zo transparant mogelijk beeld te krijgen. De resultaten van de literatuurstudie worden wel gebruikt om de antwoorden van de respondenten te kunnen verwerken.

Gezien de complexiteit van het onderwerp en de specifieke technische afbakening kan in een open interview meer informatie over de criteria van een risico-analyse boven tafel gehaald worden dan bij een gesloten interview. De respondent kan vragen stellen wanneer deze de vraag niet begrijpt. Tevens kan doorgevraagd worden wanneer een vraag niet afdoende beantwoord is of kan men de respondent vragen om een toelichting wanneer het antwoord niet volledig begrepen wordt. Interviews kunnen telefonisch of face-to-face afgenomen worden. Er is gekozen voor een face-to-face benadering, omdat dit een meer vertrouwde omgeving creëert voor de respondenten. De keuze hiervoor is mede ingegeven door de bedrijfsgevoeligheid van de verstrekte informatie. Dit komt onder andere naar voren in de beperkte bereidwilligheid tot het geven van een interview omtrent dit onderwerp. Daarom is gekozen om de respondenten anoniem te houden binnen dit onderzoek. Tevens kan kennis uit eerdere interviews gebruikt worden in latere gesprekken. Er zijn een beperkt aantal interviews gehouden gezien het tijdsbestek en de beperkte bereidwilligheid van zowel technici als managers. Zie paragraaf 4.4 (Empirisch onderzoek (interviews)) voor meer informatie. Het resultaat van de empirie geeft antwoord op de gestelde onderzoeksvragen vanuit de praktijk.

De resultaten van de literatuurstudie en de interviews tezamen, geven antwoord op de gestelde onderzoeksvragen vanuit respectievelijk de theorie en de praktijk. De volgende stap is het vergelijken van de antwoorden die voorkomen uit de resultaten van de literatuurstudie en het empirisch onderzoek.

Vergelijking resultaten literatuurstudie en empirie

Als laatste zijn de resultaten van de literatuurstudie en het empirisch onderzoek onderzocht. Door middel van een systematische analyse wordt gekeken in hoeverre de resultaten van elkaar verschillen of overeenkomen.

De volgende punten worden bekeken:

1. Overeenkomsten tussen de resultaten van de literatuurstudie en het empirisch onderzoek

2. Verschillen van de resultaten van de literatuurstudie en het empirisch onderzoek

Het resultaat van de vergelijking van de literatuurstudie en het empirisch onderzoek geeft het finale antwoord op de onderzoeksvragen.

Nu de opbouw van het deelonderzoek duidelijk is, wordt in de volgende paragraaf de onderzoeksmethode van deelonderzoek A uitgewerkt.

4.2 Analyse framework

Om een kader te creëren waarbinnen gediscussieerd kan worden, is er gebruik gemaakt van

een analyse framework. Dit framework is de basis voor het conceptueel model waarin de resultaten van de literatuurstudie en de empirie worden weergegeven. Het analyse framework wordt opgebouwd na initiële analyse van de literatuur die gebruikt wordt in de literatuurstudie. Mocht er in de volgende stappen, de literatuurstudie en empirisch onderzoek, reden zijn om het analyse framework bij te werken, dan zal dit gebeuren.

Het analyse framework geeft een basis waarin de relatie tussen de gevonden criteria weergegeven kan worden. Het analyse framework is gebaseerd op een eerste analyse van de beschikbare literatuur en op literatuur waarin algemene modellen van relaties beschreven worden.

Nu bekend is waarom het analyse framework als kapstok gebruikt wordt, wordt in de volgende paragraaf de toepassing van de literatuurstudie uitgewerkt.

4.3 Literatuurstudie

Om inzicht te krijgen in de materie over de criteria die de kwaliteit bepalen van een risico-analyse-rapportage, is er begonnen met een literatuurstudie. Om versneld aan goede literatuur te komen is er aan Dr. Martijn Oostdijk en Dr. Cees-Bart Breunesse gevraagd welke literatuur het meest gebruikt wordt binnen het onderzoeksgebied. De enige referentie die ze wisten was de al bekende Code voor informatiebeveiliging (NEN, 2000, ISO 27001) (NEN, 2000, ISO 27003).

Om ervoor te zorgen dat de literatuurstudie van wetenschappelijk niveau is zullen in deze paragraaf twee vragen uitgewerkt worden. De vraag “Wat voor literatuur is er gezocht?” is beschreven in de sectie “Selectie literatuur” en de vraag “Waar is de literatuur gezocht?” is uitgewerkt in de sectie “ Literatuur onderzoek”. Als laatste wordt het resultaat van de literatuurstudie beschreven.

Selectie literatuur

Aangezien er weinig tot geen literatuur beschikbaar is over dit specifieke onderzoeksgebied, is eerst gezocht naar literatuur die te maken heeft met risico-analyse in het algemeen en risico-analyse in de informatietechnologie sector. Door middel van literatuurstudie is op een hoger abstractie niveau gezocht naar criteria die de kwaliteit van een risico-analyse kunnen bepalen. Met andere woorden er worden algemene criteria gezocht die gebruikt kunnen worden binnen dit specifieke onderzoeksgebied.

Literatuur onderzoek

In dit literatuur onderzoek wordt gekeken naar antwoorden op onderzoeksvraag 1: “Welke criteria worden gebruikt door de managers en / of technici voor het bepalen van de kwaliteit van de risico-analyse?”

Voor de literatuur is er op verschillende plaatsen gezocht. Het Internet, boeken en artikelen zijn de voornaamste bronnen. Voor boeken en artikelen is gebruik gemaakt van wetenschappelijke zoekmachines zoals Picarta[13] en Sciencedirect[14]. Google is voornamelijk

13 PiCarta is een dienst van OCLC PICA waarin kwalitatief hoogwaardige informatie gevonden en aangevraagd kan worden met behulp van een geavanceerde zoekmachine die in een aantal geïntegreerde bestanden zoekt. Voor meer informatie zie (http://www.picarta.nl)

14 Zie Science direct voor meer informatie. (http://www.sciencedirect.com /)

gebruikt om te zoeken op het Internet. De sites die gevonden zijn, staan bekend om het leveren van respectabele en kwalitatief hoogwaardige informatie.

De literatuur die gebruikt is dient aan een aantal criteria te voldoen om de literatuurstudie betrouwbaar te houden. De criteria zijn dat de literatuur betrouwbare, algemeen geaccepteerde theorieën bevat en van toepassing moet zijn op het onderzoeksgebied. Om aan het eerste criterium te voldoen -de literatuur moet betrouwbaar zijn- wordt er alleen gezocht op locaties waar wetenschappelijke publicaties geaccepteerd worden, zoals de universiteitsbibliotheek. Boeken en artikelen die in de universiteitsbibliotheek staan zullen voldoen aan dit criterium. Om te voldoen aan het criterium van algemeen geaccepteerde theorieën wordt gekeken of er gerefereerd wordt aan de gevonden literatuur of de auteur van de literatuur. Het laatste criterium “van toepassing op het onderzoeksgebied” wordt bewaakt door het zoeken via bestaande bronnen binnen het onderzoeksgebied.

De boeken worden voornamelijk gebruikt om een basis te creëren van bekende theorieën. Een nadeel is dat boeken relatief oude informatie bevatten. Artikelen (in tijdschriften) en het Internet bevatten informatie die recenter is, aangezien hier vaak over nieuwe onderzoeken gepubliceerd wordt. De wetenschappelijke validiteit hiervan is moeilijker aan te tonen. Om toch de kwaliteit te kunnen waarborgen, wordt er alleen gebruik gemaakt van gerenommeerde websites.

Onder een gerenommeerde website wordt binnen dit onderzoek verstaan een website die langer dan een twee jaar bestaat, goed geïndexeerd wordt door google en veel referenties heeft naar de website. De relatieve korte periode van twee jaar is gebruikt aangezien technologische ontwikkelingen zeer snel gaan en daardoor tevens snel verouderd zijn. Tevens dient de website een positieve indruk te geven wat betreft de inhoud en de lay-out. Dit is een eigen definitie.

Het resultaat van de literatuurstudie is een conceptueel model I dat is opgebouwd uit de resultaten van de literatuurstudie en het analyse framework.

4.4 Empirisch onderzoek (interviews)

Deze paragraaf beschrijft de onderzoeksmethode die gebruikt wordt in het empirisch onderzoek van deelonderzoek A. Er is gekozen om gebruik te maken van interviews voor het vergaren van informatie van managers en technici die expertise hebben in dit vakgebied.

Bij de interviews tijdens dit onderzoek is gekozen voor een geringe mate van voorstructurering in de interviewguide waarbij, door een open vraagstelling, ruimte voor de respondent gecreëerd wordt om te antwoorden (Doorewaard, 2005). De reden hiervoor is dat het onderwerp redelijk veel structuur (kaderschepping) vraagt, maar tevens ruimte moet bieden voor andere ideeën / opmerkingen vanwege het exploratieve karakter van het onderzoek en het expertisegebied.

Gebruik makend van het voorgaande literatuuronderzoek is een interviewguide opgesteld. Deze interviewguide is op een abstract niveau ontwikkeld, dit om te voorkomen dat de respondent antwoorden in de mond krijgt gelegd.

De keuzes die gemaakt zijn bij het selecteren van respondenten worden in de volgende subparagraaf beschreven. Er is niet beschreven welke organisaties of bedrijven er aangeschreven zijn, aangezien de respondenten anoniem wensen te blijven.

Selectie respondenten

In deze paragraaf worden de criteria beschreven die gebruikt zijn om respondenten te selecteren. Om een diverse groep van respondenten te krijgen is er een selectie uitgevoerd op de achtergrond en de organisatie grootte van de respondent. Daarnaast zijn er nog een aantal algemene criteria benoemd waaraan de respondent dient te voldoen. Nu als eerste de achtergrond van de respondenten.

Respondenten achtergrond

Voor de interviews worden respondenten aangeschreven die zich in twee groepen bevinden, deze groepen zijn:

- Respondenten uit de academische wereld
- Respondenten uit het bedrijfsleven

Respondenten uit de academische wereld

De literatuurstudie is theoretisch. Daarom is de keuze gemaakt om bij de eerste paar interviews alleen academische mensen te interviewen. Hierdoor is de kans groter dat het interview op een hoger abstractie (theoretischer) niveau plaats kan vinden. Tevens kunnen de respondenten nieuwe literatuur aanbrengen die bruikbaar kan zijn voor het (vervolg)onderzoek.

Om te kunnen garanderen dat de respondenten een wetenschappelijke achtergrond hebben, zijn er alleen personen aangeschreven die Professor of Promovendus zijn en bekend zijn met het onderzoeksgebied.

Respondenten uit het bedrijfsleven

De respondenten uit het bedrijfsleven dienen te zorgen voor een meer praktijkgerichte onderbouwing van het onderzoek. Tevens kan er vanuit de praktijk, theoretische aanvulling worden gegeven op het onderzoek en specifiek de risico-analyse.

Om te kunnen garanderen dat de respondent praktijkervaring heeft worden alleen personen gezocht die bij bedrijven werken en die zich actief bezig houden met digitale informatiebeveiliging en firewalls.

Respondent organisatie grootte

Voor de interviews worden de respondenten aangeschreven die zich in drie organisatiegroottes bevinden, deze groepen zijn volgens de Europese Unie en dus ook de Nederlandse overheid (WWW-10):

- Grote organisatie: > 250 personeel
- Midden en Kleinbedrijf: 50-250 man personeel
- Ondernemer: < 50 man personeel

De reden voor deze selectie is om mede te bepalen of de bedrijfsgrootte van invloed is op het

gebruik van de risico-analyse van de firewall. De grootte van bedrijven is namelijk een factor die invloed heeft op de bedrijfscultuur (Rood, 2001).

Daarnaast is er gezocht naar respondenten die in de detachering zitten. Medewerkers van detacheringsbedrijven werken vaker bij meerdere bedrijven, daardoor kunnen zij een bredere perceptie op dit expertisegebied hebben.

Criteria

De volgende criteria zijn gebruikt bij het aanschrijven van de respondenten.

De respondent dient:

- affiniteit met IT, risico-analyse en in mindere mate met de firewall te hebben. De firewall is vaak een onderdeel van de IT-afdeling.
- bij minimaal een van de onderstaande functies betrokken te zijn:
    - Manager: verantwoordelijk voor de firewall en / of beveiliging van het bedrijfsnetwerk.
    - Technici: verantwoordelijk voor de technische netwerkbeveiliging. Hiermee worden voornamelijk technici bedoeld die de firewall daadwerkelijk zelf onderhouden.
- eventueel betrokken te zijn bij het architectuur onderzoek. De reden voor deze keuze is dat zowel de risico-analyse als het technische onderzoek gebruik maken van de onderliggende architectuur. De vraag is in hoeverre de architectuur rekening houdt met beveiliging in het algemeen en specifiek het gebruik van een risico-analyse en technisch onderzoek.

Resultaat

Het resultaat van de interviews is een samenvatting van de gehouden interviews. Daarnaast wordt per vraag een opsomming gegeven van de antwoorden van de respondenten.

In de conclusie van deze paragraaf wordt beschreven in hoeverre de resultaten van het vooronderzoek, het conceptueel model I, overeen komen met antwoorden van de respondenten en wordt er gekeken naar causale verbanden tussen de resultaten. Daarnaast wordt aanvullende informatie beschreven die tijdens de interviews naar voren is gekomen.

Het resultaat van het empirisch onderzoek is een gewijzigde versie van conceptueel model I aan de hand van de resultaten van de interviews. De aanpassingen worden bepaald door de resultaten van de interviews.

4.5 Vergelijking resultaten literatuurstudie en empirie

In de laatste stap wordt door middel van een systematische analyse gekeken in hoeverre de resultaten van elkaar verschillen of overeenkomen. Doordat zowel de resultaten van de literatuurstudie als van het empirisch onderzoek in een analyse framework worden

weergegeven, wordt naar de volgende punten gekeken:

1. Overeenkomsten tussen de resultaten van de literatuurstudie en het empirisch onderzoek

2. Verschillen van de resultaten van de literatuurstudie en het empirisch onderzoek

Het resultaat van deze stap is de vergelijking van de resultaten van de literatuurstudie en het empirisch onderzoek.

5 Resultaten

In dit hoofdstuk zijn de resultaten van het deelonderzoek A gepresenteerd. De opbouw van het onderzoek komt overeen met de opbouw gepresenteerd in paragraaf 4.1 (Onderzoeksaanpak). De structuur / paragraafindeling is als volgt:

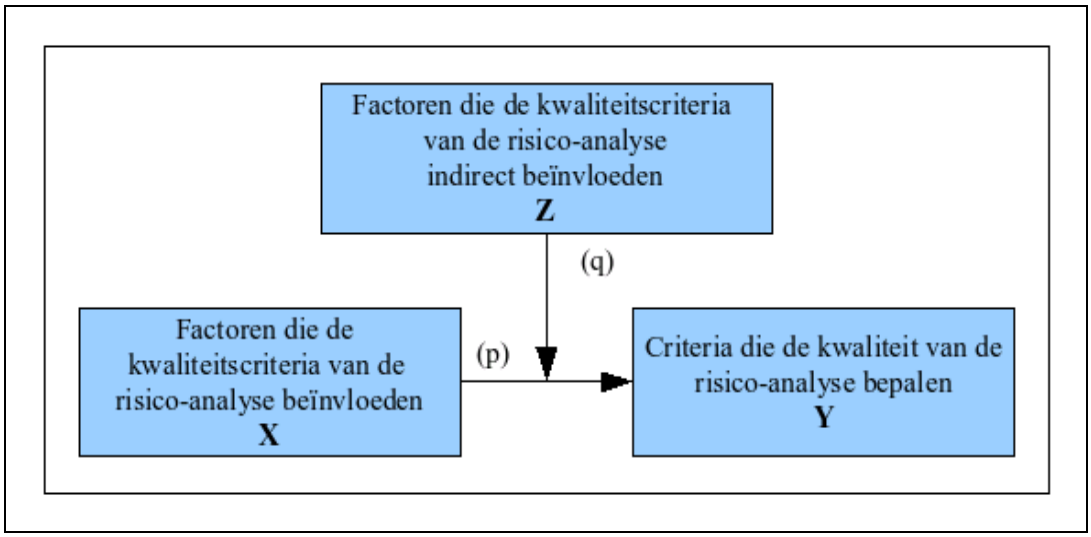
1. Analyse framework
2. Literatuurstudie
    - Conceptueel model I
3. Empirie: Interviews technici / managers
    - Conceptueel model II
4. Vergelijking resultaten literatuurstudie en empirie

De conclusie van deelonderzoek A staan in hoofdstuk 6 (Conclusies en reflectie) beschreven. De eerste stap is het analyse framework.

5.1 Analyse framework

Om een basis te creëren waarmee gediscussieerd kan worden is er gebruik gemaakt van een analyse framework (Zie Figuur 11). De argumentatie waarom er gekozen is voor dit conceptueel model is in de appendix uitgewerkt.

Figuur 11 is een initieel conceptueel model dat gebruikt is om de resultaten vanuit de literatuurstudie in te delen. Het is mogelijk dat het conceptueel model verandert in de loop van het onderzoek.



Figuur 11: Analyse framework (Berlijn, 2007)

De letters in Figuur 11 hebben de volgende betekenis:

- X, Y en Z zijn een verzameling

- (p) is de relatie tussen verzameling X en verzameling Y
- (q) is de relatie tussen Z en (p)

Aangezien dit de eerste insteek is geweest om de verkregen informatie te structureren kan de keuze van dit analyse framework verkeerd zijn geweest. Daarom wordt in dit onderzoek de ruimte geboden het conceptueel model bij te werken indien daar reden toe is. In dit onderzoek is er geen noodzaak geweest om het conceptueel model aan te passen.

X staat voor de factoren die de criteria beïnvloeden welke gezocht worden in onderzoeksvraag 2: “Welke factoren beïnvloeden de criteria die door managers en / of technici voor het beoordelen van de kwaliteit van de risico-analyse-rapport worden gebruikt ten behoeve van de functionaliteit van een firewall?”.

Y staat voor de criteria die worden gebruikt door managers en / of technici die gezocht wordt in onderzoeksvraag 1: “Welke criteria worden gebruikt door de managers en / of technici voor het bepalen van de kwaliteit van de risico-analyse?”.

Binnen dit onderzoek wordt voornamelijk gekeken naar de Y en X factoren. Oftewel de criteria die gebruikt worden door managers en / of technici voor het bepalen van de kwaliteit van de risico-analyse en de factoren die deze criteria beïnvloeden.

Buiten dit deelonderzoek vallen de Z factoren en de relaties (p) en (q). Oftewel de Z factoren en de relaties worden niet behandeld binnen dit deelonderzoek.

Resultaat analyse framework

Het analyse framework geeft geen antwoorden op de onderzoeksvragen 1 en 2. Het framework wordt gebruik om de resultaten van de literatuurstudie en het empirisch onderzoek te verwerken.

Nu duidelijk is wat de denkwijze is binnen dit onderzoek volgen de resultaten van de literatuurstudie.

5.2 Literatuurstudie

Om het risico-analyse resultaat te verbeteren, dient eerst inzichtelijk te worden welke criteria de kwaliteit van de risico-analyse bepalen en welke factoren deze criteria beïnvloeden.

Zoals beschreven in paragraaf 4.3 (Literatuurstudie) is gebruik gemaakt van Picarta en Sciencedirect. Daarnaast is er nog gebruik gemaakt van Association for Computing Machinery (ACM)[15] en google[16].

De volgende zoektermen zijn gebruikt binnen bovenstaande zoekmachines met verschillende combinaties:

15 Zie Association for Computing Machinery voor meer informatie (http://www.acm.org/)
16 Zie google voor meer informatie (http://www.google.com)

Engels	*Nederlands*
risk management	risico management
risk analysis	organisaties
scenario-based risk identification	
risk assessment	
firewall	
information technology	
protecting digital information	

Het resultaat van de zoektocht is heel divers. Het gebiedt te zeggen dat geen enkel resultaat een directe relevantie had met het gezochte onderwerp. Om toch aan de benodigde kennis te komen is een procedure ontwikkeld. Deze procedure wordt later in deze paragraaf uitgelegd, om zodoende tot een basis te komen vanuit de literatuur.

Uiteindelijk is er een selectie uit de gevonden en beschikbare literatuur gemaakt. Veel gevonden literatuur was niet van toepassing op het onderzoeksgebied of was niet van voldoende niveau. Met het laatste wordt bedoeld dat ze niet voldeden aan de wetenschappelijke criteria die gesteld zijn. Om een zo breed mogelijke basis te creëren is er gekozen om literatuur uit drie verschillende bronnen te gebruiken. Wel te verstaan:

- Nederlands Adviesbureau voor Risicomanagement
- National Institute of Standards and Technology
- The Journal of System and Software

Uiteindelijk is de keuze op de onderstaande literatuur gevallen:

1. Haisma, G., 1999; Riscomanagement: een bijdrage aan continuïteit in organisaties (Haisma, 1999)

Dit artikel is gekozen omdat dit document komt van het “Nederlands Adviesbureau voor Risicomanagement[17]”. Dit bureau geeft advies met betrekking tot risicomanagement en heeft onderzoek in dit gebied gedaan.

2. Stoneburner, G., 2002; Risk Management Guide for Information Technology Systems (Stoneburner, 2002)

Voor dit artikel is gekozen omdat dit document aanbevelingen bevat van de “National Institute of Standards and Technology”[18] Dit document geeft standaarden voor risicomanagement, welke bruikbaar kunnen zijn voor de ontwikkeling van een risico-analyse.

17 Zie http://www.risicomanagement.nl/ voor meer informatie.
18 Voor meer informatie zie: http://www.nist.gov/

3. Pfleeger, S.L., 2000; Risky business: What we have yet to learn about risk management (Pfleeger, 2000)

De reden voor dit artikel is dat dit artikel gepubliceerd is in “The Journal of System and Software”[19]. Dit artikel is volgens scopus[20] 4 keer geciteerd. Dit geeft aan dat het een veel gebruikt artikel is en waarschijnlijk bruikbare informatie kan opleveren. Scopus is een website waarop gegevens met betrekking tot abstracts en citaten wordt bijgehouden.

In de gevonden literatuur staan voornamelijk management processen beschreven waarbij aangegeven wordt hoe je een risico-analyse-rapport kunt maken. Er worden verder geen kwaliteitseisen gesteld waaraan het risico-analyse-rapport dient te voldoen. Daarom zijn de criteria gedestilleerd vanuit de managementprocessen die in de literatuur beschreven staan.

Het destillatieproces is als volgt geïmplementeerd:

1. Er wordt gekeken welke processen in de artikelen beschreven worden om een risico-analyse te maken. Er wordt aangenomen dat de auteur alleen processen beschrijft die hij belangrijk vindt. Met andere woorden, de auteur vindt het belangrijk dat processen doorlopen en ook beschreven worden. Deze beschrijvingen komen tot uiting in een risico-analyse-rapport.

2. Van de gebruikte artikelen is een samenvatting gemaakt. De samenvattingen van de literatuur zijn te vinden in paragraaf 16.2 (Management literatuur samenvattingen).

3. Vervolgens worden criteria in de meest elementaire vorm uit de samenvattingen gehaald en beschreven in een conceptueel model.

De gevonden criteria zijn door middel van het analyse framework, zie paragraaf 5.1 (Analyse framework), uitgewerkt in conceptueel model I.

Resultaat literatuurstudie

De resultaten van de literatuurstudie zijn uitgewerkt volgens de twee onderzoeksvragen. Onderzoeksvraag 1 wordt uitgewerkt in de sectie “Kwaliteit bepalende criteria” en de uitkomst van onderzoeksvraag 2 wordt beschreven in sectie “Factoren die de kwaliteit bepalende criteria beïnvloeden”.

Kwaliteit bepalende criteria

Aan de hand van de literatuur en bovenstaand proces zijn bijna dertig criteria gevonden, die antwoord geven op onderzoeksvraag 1: ”Welke criteria worden gebruikt door de managers en / of technici voor het bepalen van de kwaliteit van de risico-analyse?”. Om de criteria inzichtelijk te houden, is er een onderverdeling in de volgende categorieën gemaakt:

- *Scope;* in de sectie scope worden de criteria beschreven die gerelateerd zijn aan het domein en het bereik van de risico-analyse.

- *Systeem karakteristieken;* in de sectie systeem karakteristieken worden de kenmerken van het systeem, in dit onderzoek meestal het netwerk en de firewall, beschreven.

19 Voor meer informatie zie: http://www.elsevier.com/locate/jss
20 Zie http://www.scopus.com/ voor meer informatie.

- *Risico-analyse methode;* tot slot wordt in de risico-analyse methode beschreven hoe het risico-analyse-rapport tot stand is gekomen.

Nu duidelijk is hoe de onderverdeling tot stand is gekomen wordt in de volgende sectie de uitwerking van de literatuur tot een conceptueel model beschreven.

Conceptueel model

Aangezien de uitwerking van het conceptueel model I een aantal pagina's in beslag neemt, wordt eerst de uitwerking van het resultaat beschreven, hierna volgt de reflectie van het resultaat. Aan het einde van deze sectie staat de volledige uitwerking van het conceptueel model beschreven.

Gebruik makend van het eerder beschreven analyse framework model, zie Figuur 11, en het destillatie proces van de literatuur, zie 5.2 (Literatuurstudie), is het conceptueel model I ontwikkeld. Ter verduidelijking hoe de resultaten zijn weergegeven de volgende voorbeeld hoe een criterium beschreven is:

Voorbeelden van het criterium	criterium

Criterium P: criterium beschrijving
Uitleg van het criterium

Figuur 12: Format beschrijving criterium (Berlijn, 2007)

Het criterium komt overeen met Y van het Figuur 11. De “Voorbeelden van het criterium” zijn de voorbeelden van de beschreven “criterium”. Tevens staat er per criterium een referentie waar het criterium in de literatuur gevonden is. Onder de tabel staat uitgeschreven wat precies met de criteria bedoeld wordt.

Om een overzicht te houden over de criteria zijn deze onderverdeeld in een aantal categorieën. Het resultaat van het conceptueel model I is onderverdeeld in de volgende categorieën:

- Scope
- Systeem karakteristieken
- Risico-analyse methode

Conceptueel model I

Scope

Bank Webwinkel Transporteur	Organisatie / Business Unit soort

Criterium 1: Organisatie soort (Haisma, 1999: 14)

Afhankelijk van het soort organisatie kan de kwaliteitsperceptie van een risico-analyse verschillen. Een bank of een webwinkel zal veel hogere eisen stellen aan de beveiliging van

haar netwerk, dan een schoonmaakbedrijf die geen bedrijfskritische processen op zijn netwerk heeft draaien.

Aantal werknemers Aantal gebruikers van de infrastructuur	Organisatie / Business Unit grootte

Criterium 2: Organisatie grootte (Haisma, 1999: 14)

De grootte van een organisatie / business unit kan bepalend zijn voor de kwaliteit van een risico-analyse. Een klein bedrijf waar iedereen elkaar kent is een totaal andere omgeving dan een grote universiteit waar vrijwel niemand elkaar kent. Men gaat er vanuit dat bij een groot bedrijf de kans groter is dat er niet geautoriseerde personen rondlopen die kwaad willen doen dan bij een klein bedrijf.

Afnemers Klanten Medewerkers (intern/extern) Leveranciers	Doelgroep (soort)

Criterium 3: Doelgroep (Stoneburner, 2002)

De doelgroep (soort) is een belangrijk criterium binnen de risico-analyse. De grootte van een doelgroep is van invloed op de impact die een eventuele storing van communicatie kan hebben. Een doelgroep afnemers die alles via het netwerk regelt is vaak belangrijker dan een medewerker die informatie via het netwerk opzoekt.

Script Kiddy Veiligheidsdienst / Overheid	Aanvallers soort

Criterium 4: Aanvallers soort (Stoneburner, 2002: 12-14)

Wat voor aanvallers worden er verwacht? Zijn het een soort vandalen, script kiddies (dit zijn een soort vandalen op het Internet die zonder enige vorm van kennis aanvallen plegen. Vaak gebeurt dit door geautomatiseerde systemen) of gaat het echt om bedrijfsspionage waarbij men uit is op bedrijfskritische informatie.

20 100 5235	Hoeveelheid aanvallers

Criterium 5: Hoeveelheid aanvallers (Stoneburner, 2002: 12-14)

Afhankelijk van het soort aanvaller is ook het aantal van belang. Duizenden script kiddies kunnen gevaarlijker zijn dan één echte aanvaller.

Manager Beleidsmaker	Voor wie is het risico-analyse-rapport bedoeld

Criterium 6: Doelgroep risico-analyse (Stoneburner, 2002: 18-19)

Een raad van bestuur / manager wil een ander soort risico-analyse-rapport hebben dan een manager van de security-afdeling. Waar voor een raad van bestuur / manager een percentage of een verhouding voldoende is, wil een manager van een security-afdeling een uitgewerkt verslag hebben zodat hij daarop kan sturen.

Systeem karakteristieken

Versies / Tijd	Systeem afkadering

Criterium 7: Afkadering systeem (Stoneburner, 2002: 10)

Binnen welke grenzen valt het onderzochte systeem. Oftewel afkadering van de systemen die binnen de risico-analyse vallen.

E-mailserver WWW-Server	Systeem functies

Criterium 8: Systeemfuncties (Stoneburner, 2002: 10-11)

Welke functionaliteit heeft het totale systeem dat binnen de afkadering valt van de risico-analyse. Voor welke doeleinden wordt het systeem gebruikt.

Systeem data sensitiviteit	Systeem data criteria

Criterium 9: Data criteria (Stoneburner, 2002: 10, 21)

Wat voor data, belangrijke of onbelangrijke informatie, wordt er door het totale systeem binnen de afkadering verwerkt.

	Overzicht communicatiestromen

Criterium 10: Communicatiestromen (Stoneburner, 2002: 11)

Overzicht hoe de communicatiestromen binnen het systeem plaatsvinden.

Risico-analyse methode

Up-to-date	Representatief

Criterium 11: Representatief (Pfleeger, 2000), (Stoneburner, 2002: 22)

Zijn de resultaten die in het risico-analyse resultaat staan nog representatief. Als een risico-analyse een te lange doorlooptijd heeft, kan het zijn dat de risico's die er zijn veranderen. Deze veranderingen zijn dan nog niet in het risico-analyse resultaat verwerkt.

Up-to-date	Samenvatting

Criterium 12: Samenvatting (Stoneburner, 2002: 26)

In de samenvatting dienen de volgende onderwerpen terug te komen:

- Totaal aantal van observaties.
- Samenvatting van de observaties, het geassocieerde risiconiveau en commentaren in tabel formaat om de implementatie van aanbevolen beheersing te faciliteren.

Technici Managers	Participanten

Criterium 13: Participanten (Stoneburner, 2002: 6)

Welke medewerkers hebben deel uitgemaakt van de ontwikkeling van de risico-analyse. Risico-analyses kunnen op verschillende abstractie niveaus gemaakt worden. Afhankelijk van het abstractie niveau zijn andere participanten nodig.

	Technieken die gebruikt worden voor dataverzameling

Criterium 14: Data verzamelings technieken (Stoneburner, 2002: 11-12)

Welke technieken zijn er gebruikt bij het maken van een dataverzameling om zodoende tot een risico-analyse te komen. Hoe zijn de risico's bepaald?

	Ontwikkeling en beschrijving van risico schalen

Criterium 15: Risico schalen (Stoneburner, 2002)

Hoe zitten de risicocriteria in elkaar. Is het uiteindelijke resultaat wel representatief?

	Alle risico's dienen herkenbaar te zijn

Criterium 16: Herkenbaarheid risico's (Pfleeger, 2000)

Alle risico's in het document dienen eenduidig, bijvoorbeeld door nummering, door het gehele document aangegeven te worden.

	Risico's verdelen in aantal hoofdgroepen

Criterium 17: Risicoverdeling (Pfleeger, 2000: 266)

Risico's kun je in een aantal klassen classificeren. Deze klassen zijn: Algemene risico's en project specifieke risico's.

- Algemene risico's zijn risico's die op de algehele organisatie betrekking hebben en zodoende een grotere impact hebben dan op het project waarvoor de risico-analyse wordt gemaakt. Bijvoorbeeld het risico dat de totale stroom van de organisatie wegvalt.

- Projectrisico's zijn risico's die een specifiek impact hebben op een project. Andere afdelingen binnen de organisatie hebben geen last van het risico op het moment dat een functionaliteit van een afdeling wordt aangevallen. Deze afdelingen kunnen wel last krijgen als door die risico's de functionaliteiten die binnen hun eigen project vallen niet meer werken.

Er zijn twee verschillende soorten risico's:

- *Vrijwillige risico's:* je maakt moedwillig een keuze om een bepaald risico aan te gaan, bijvoorbeeld gebruik maken van mensen met weinig expertise op een gebied van het project.

- *Onvrijwillig risico's:* zijn risico's waar je geen keuze hebt. Bijvoorbeeld het gebruik

maken van een nieuw ontwikkel platform op het moment dat het oude platform niet meer functioneert.

	Risicogebied / Gevaren identificatie

Criterium 18: Risicogebied (Haisma, 1999: 3-4)

De risico-analyse dient alle risicogebieden te bestrijken. De risicocategorieën die worden gebruikt als een checklist om vanuit een 'volledig' aantal invalshoeken naar risico's in een risicogebied te kunnen speuren zijn:

1. Materiële risico's
2. Procesrisico's
3. Aansprakelijkheidsrisico's
4. Productrisico's
5. Imagorisico's
6. Financiële risico's
7. Milieurisico's
8. Arbeidsrisico's
9. Informatierisico's

Opsomming 1: Invalshoeken risico gebieden(Haisma, 1999: 3-4)

	Potentiële kwetsbaarheden identificatie

Criterium 19: Kwetsbaarheden (Stoneburner, 2002: 20)

Lijst van potentiële kwetsbaarheden welke op dit moment bekend zijn en welke in de toekomst verwacht kunnen worden. Oftewel het samenstellen en categoriseren van potentiële dreiging-sources en de daaraan gerelateerde dreiging-acties die van toepassing zijn op het systeem.

	Verlies identificatie

Criterium 20: Identificatie (Pfleeger, 2000: 266)

Een verlies geassocieerd met een gebeurtenis. De gebeurtenis creëert een situatie waarin iets negatiefs gebeurt met betrekking tot het project. Verlies van tijd, kwaliteit, geld, sturing etc. Bijvoorbeeld als een bank gehacked wordt dan zal een bank dit snel melden aan de politie, aangezien de schade die negatieve publiciteit over een gelukte hack poging vaak meer is dan de gelede schade. Organisatie en personen die lid zijn van deze bank zullen deze bank gaan identificeren als een bank die hun geld verliest en zullen daardoor naar een andere bank gaan.

	Huidige risico beperking implementatie

Criterium 21: Risico beperking (Stoneburner, 2002: 27)

Hoe worden op dit moment de huidige risico's beperkt.

	Waarschijnlijkheids (kans) bepaling

Criterium 22: Kansbepaling (Stoneburner, 2002: 24), (Pfleeger, 2000: 266)

Wat is de kans dat een bepaalde gebeurtenis plaatsvindt. Met andere woorden de waarschijnlijkheid waarmee een gebeurtenis kan plaatsvinden. Op het moment dat je een risico wilt bepalen moet er enig idee van een kans zijn waarmee een gebeurtenis kan plaatsvinden.

	Risico beoordeling / bepaling

Criterium 23: Risicobeoordeling (Haisma, 1999: 7-8), (Pfleeger, 2000: 266)

Hoe wordt de risico beoordeling gemaakt. Via een methode als: Risicobeoordeling=Kans*Gevolgen Financieel*Bedrijfsimpact. Wat voor invloed heeft een bepaalde gebeurtenis op de rest van de organisatie. In welke mate kan de invloed van een gebeurtenis veranderd worden? Voor elk risico moet worden bepaald hoe de impact van een gebeurtenis geminimaliseerd kan worden.

	Proces aansturing / aanbevelingen

Criterium 24: Aanbevelingen (Stoneburner, 2002), (Haisma, 1999: 8)

Eventuele aanbevelingen met betrekking tot proces aansturing om bepaalde risico's in te perken.

Percentage	Verwacht veiligheidsniveau

Criterium 25: Veiligheidsniveau (Stoneburner, 2002: 4)

Hoe veilig verwacht men te zijn? Dit is een keuze die gemaakt dient te worden. Dit is te vergelijken met de keuze of je iets in een brandkast / kluis zet of gewoon in een kast legt. De kans dat er succesvol wordt ingebroken en vervolgens ook de kluis gekraakt, is kleiner dan dat er succesvol ingebroken wordt ingebroken en men vervolgens de kast opent.

	Systematisch en analytische geschreven

Criterium 26: Systematisch en analytische uitvoering (Stoneburner, 2002: 26)

Een risico management rapport dient niet veroordelend geschreven te worden, dit wil zeggen dat er geen verwijten in het rapport staan. Het rapport dient op een systematische en analytische manier geschreven te worden.

Valse precisie Slechte wetenschap Verwarring tussen feiten en waarden	Valse precisie

Criterium 27: Valse precisie (Pfleeger, 2000: 269-271)

Er zijn drie grote problemen met risicomanagement:

1. Valse precisie, fouten en onbetrouwbaarheid worden onderschat wanneer de populatiegrootte te klein is. “Both scientists and lay people may underestimate the error and unreliability in small samples of data, particularly when the results are consistent with preconceived, emotion-based beliefs" (Whittemore, 1983)

1. Slechte wetenschap (Laat je niet voor de gek houden door “bediscussieerde

wetenschap")

2. Verwarring tussen feiten en waarden, een numerieke beschrijving van een risico geeft meer geloofwaardigheid dan een kwalitatieve beschrijving van een risico. De kwantitatieve beschrijving lijkt betrouwbaarder dan het feitelijk is. De wetenschap van psychologie van risicoperceptie vertelt dat: "Numerical assessments possess a kind of symbolic neutrality that is rarely attained by qualitative formulations about the 'weight' or 'suffiency' of the evidence" (Jasano, 1991)

1 uur 8 uur 24 uur	Tijdsduur maken risico-analyse

Criterium 28: Tijdsduur (Pfleeger, 2000: 266)

Terwijl het risico-analyse resultaat voldoende representatief is, kan de doorlooptijd van het maken van de risico-analyse te lang duren. Hierdoor kunnen risico's langer onopgemerkt blijven. De mate van risico's en de gebeurtenissen veranderen over tijd, zoals ook de impact. Deze dienen dus van tijd tot tijd in de gaten gehouden te worden. In andere woorden als normaal gesproken een doorlooptijd van een jaar representatief is kan de omgeving veranderen waardoor die jaar tijdelijk niet meer representatief is. Men dient dus altijd alert te blijven op plotselinge veranderingen.

Ervaring Opleiding	Personeel

Criterium 29: Personeel (Algemeen)

De kwaliteit van de risico-analyse is afhankelijk van de ervaringen, zowel ervaring van het bedrijf, als ervaring van het schrijven van een risico-analyse, die schrijvers van de risico-analyse hebben. Hoe meer / betere ervaring de schrijvers van een risico-analyse hebben, des te beter de beoordeling van de risico's zal zijn.

Afhankelijk van de opleiding wordt er ook verschillend naar een risico-analyse gekeken. Meer technisch georiënteerde medewerkers zullen vaak een andere perceptie van een risico hebben, dan medewerkers die bedrijfskundig georiënteerd zijn.

Bovenstaand conceptueel model I geeft de criteria aan die het resultaat vormen voor onderzoeksvraag 1.

Factoren die de kwaliteit bepalende criteria beïnvloeden

Tijdens de literatuurstudie is geen antwoord gevonden op onderzoeksvraag 2. In de gebruikte literatuur zijn geen factoren gevonden die de criteria beïnvloeden welke de kwaliteit van een risico-analyse bepalen. Dit komt doordat de kennis met betrekking tot dit onderzoeksgebied niet is terug te vinden in de literatuur of de literatuur niet voldeed aan de wetenschappelijke criteria die zijn opgesteld. Dit insinueert dat er nog geen (wetenschappelijk) onderzoek is gedaan naar factoren die mogelijk de kwaliteit bepalende criteria beïnvloeden. Wellicht zijn er factoren te destilleren uit literatuur die niet aan de wetenschappelijke criteria voldoet. Voor dit onderzoek is dergelijke literatuur niet bruikbaar bevonden. De literatuur die wel aan de opgestelde criteria voldoet geeft een beschrijving van managementprocessen, waarbij is aangegeven hoe een risico-analyse-rapport gemaakt kan worden. Vanuit deze literatuur zijn de criteria, die de kwaliteit van een dergelijk rapport

bepalen, gedestilleerd. Hieruit waren echter geen factoren te destilleren die deze criteria mogelijk konden beïnvloeden.

5.3 Empirie: Interviews technici / managers

In deze paragraaf worden de resultaten van de interviews beschreven.

De benaderde personen met een academische achtergrond, of bedrijfsachtergrond, en 'managers' van een firewall alswel van technische netwerkbeveiliging waren bereid om een interview te geven. Benaderde personen die in de architectonische hoek zaten, waren minder bereidwillig. Na een aantal personen te hebben aangeschreven bleek dat niet één persoon bereid was tot het geven van een interview. Er is geen enkele respondent gevonden die vanuit de architectuurhoek een interview wilde geven. Zij antwoordden op de vraag of ze bereid waren tot het geven van een interview veelal: “Architectuur houdt zich niet bezig met dit soort onderwerpen”. Het lijkt er op dat informatiebeveiliging bij architecten geen issue is. Dit geeft het signaal af dat het belang van informatiebeveiliging niet overal in de organisatie als belangrijk wordt gezien door belanghebbenden, dan wel goed geplaatst is in de organisatie.

Nu bekend is wie de respondenten zijn volgt de gebruikte interviewguide. Zie voor de volledige interviewguide appendix 16.3 (Interviewguide).

Het interview is in drie delen opgesplitst:

1. Algemene introductie door middel van een kleine presentatie. Hierbij wordt een toelichting gegeven over het risico-analyse resultaat en het gebruik van een firewall voor de contextbepaling van de respondent.

2. Aantal open vragen die de volgende doelstelling beogen:

    1. Inzicht krijgen in de organisatie en positie, opleiding van de respondenten

    2. Inzicht krijgen in het eventueel aanwezige risico-analyse proces.

3. Het open interview.

De algemene introductie heeft als doel om de respondent precies op de hoogte te stellen waarom dit onderzoek gedaan wordt en waarnaar gezocht wordt. Tevens dient deze introductie om het interview in te leiden. De inleidende presentatie staat beschreven in appendix 16.4 (Interviewguide presentatie).

De open vragen hebben als doel inzicht te krijgen in de organisatie waar de respondent werkzaam is en de positie die de respondent bekleedt. Ook wordt nagegaan welke opleiding de respondent heeft gevolgd en of er eventueel al risico-analyse processen binnen de organisatie gebruikt worden. De uitwerking van de interviews per respondent staat beschreven in appendix 16.5 (Verslaglegging interviews).

Het open interview heeft als doel om verbanden te leggen tussen de resultaten van de literatuurstudie, zie 5.2 (Conceptueel model) en het bedrijfsleven. Deze resultaten zijn uitgewerkt in 16.6 (Resultaten interviews).

In de volgende paragraaf zijn de resultaten van het empirisch onderzoek uitgewerkt.

Resultaat empirie: Interviews technici / managers

Conceptueel model II wordt gebruikt om de antwoorden op onderzoeksvraag 1 en 2 vanuit het empirisch onderzoek weer te geven.

Conceptueel Model II

De resultaten van de literatuurstudie zijn uitgewerkt volgens de twee onderzoeksvragen. Onderzoeksvraag 1 wordt uitgewerkt in de sectie “Kwaliteit bepalende criteria” en de uitkomst van onderzoeksvraag 2 wordt beschreven in sectie “Factoren die de kwaliteit bepalende criteria beïnvloeden”.

Kwaliteit bepalende criteria

Zoals gebleken is uit de resultaten van de interviews zijn de bedrijven nog niet zo ver dat ze zich actief en bewust met risico-analyses van een firewall bezighouden. Het blijkt dat er soms (basis) theoretische kennis over de criteria die de kwaliteit van een risico-analyse bepalen aanwezig is, maar dat deze kennis weinig tot niet wordt gebruikt. Verschillende respondenten hebben de nieuwe versie van Code van informatie beveiliging aangehaald als gebruikte instrument. Mogelijk zijn hier nieuwe criteria uit te halen maar deze nieuwe versie was niet beschikbaar voor dit onderzoek. Daardoor is het antwoord op onderzoeksvraag 1 vanuit de literatuurstudie (theorie) niet bevestigd of ontkend door de respondenten (theorie en praktijk). Dit houdt in dat er vanuit het conceptueel model I geen aanpassingen volgen. Het conceptueel model I dat ontwikkeld is door middel van literatuurstudie blijkt op dit moment het maximaal haalbare binnen dit onderzoek. Met betrekking tot onderzoeksvraag 1: “Welke criteria worden gebruikt door de managers en / of technici voor het bepalen van de kwaliteit van de risico-analyse?”, heeft het empirisch onderzoek niets toegevoegd aan de resultaten die de literatuurstudie reeds opleverde.

Factoren die de kwaliteit bepalende criteria beïnvloeden

Het niet kunnen bevestigen / verder uitwerken van onderzoeksvraag 1 impliceert dat er geen antwoorden zijn op onderzoeksvraag 2: “Welke factoren beïnvloeden de criteria die door de managers en / of technici voor het bepalen de kwaliteit van de risico-analyse gebruikt worden?”. Tevens ontbreekt een groep respondenten die de systemen ontwikkelen. De architecten waren immers niet bereid aan het onderzoek mee te doen. Hun kennis met betrekking tot risico-analyse kon dus niet worden meegenomen. Als laatste was er een probleem met betrekking tot de toegankelijkheid van sommige risico-analyse methoden, hieronder valt ook de onder Kwaliteit bepalende criteria aangehaalde nieuwe versie van de Code voor informatiebeveiliging. Door een aantal grote organisaties zijn risico-analyse-methoden opgesteld. Deze zijn enkel toegankelijk wanneer men hiervoor betaald. Binnen dit onderzoek was hiervoor geen budget, waardoor de kennis uit deze methoden niet kon worden gebruikt. Factoren die mogelijk in deze documenten staan vermeld konden niet worden benaderd. Vanwege bovenstaande tekortkomingen is geen antwoord gevonden op onderzoeksvraag 2.

Daarom worden in 12.2 (Aanbevelingen) aanbevelingen gegeven om in een nieuw onderzoek gerichter te kunnen zoeken.

Overige bevindingen

Alle respondenten, op de architecten na, stonden positief tegenover de vraag om geïnterviewd te worden. Alle interviews zijn zonder problemen verlopen. Ondanks dat de beveiliging van een organisatie een kritiek punt is, waren de respondenten open in hun antwoorden. Het inwilligen van de wens om anoniem te blijven heeft hier mede aan bijgedragen. Er wordt vanuit gegaan dat de verkregen antwoorden ook eerlijke antwoorden zijn. Een belangrijk punt voor deze openheid kan gelegen zijn in het feit dat er niet naar specifieke technische implementaties gevraagd werd, maar meer naar de procesmatige uitvoering.

Wat opvalt is dat er weinig tot geen aandacht wordt besteed aan het maken van een risico-analyse. Toch zijn er vanuit de interviews processen te herkennen die delen van een risico-analyse behandelen. Omdat er geen duidelijk risico-analyse proces is, wordt er geen risico-analyse-rapport gemaakt. Oftewel een interview over de criteria van een document was niet mogelijk, daarom zijn in delen van de interviews hypothetische vragen gesteld.

Bij de respondenten zitten geen architecten die systemen ontwikkelen. Er zijn alleen respondenten die gebruik maken van de systemen. In hoeverre er nagedacht kan worden over de risico-analyse bij het ontwikkelen van een systeem, kan in dit onderzoek weinig over gezegd worden.

Tijdens de interviews kwam naar voren dat een aantal grote organisaties een eigen (risico-analyse) methode ontwikkeld heeft, waar je alleen gebruik van kunt maken wanneer je hiervoor betaald. In hoeverre de gesloten literatuur ook daadwerkelijk vernieuwend is, kan in dit onderzoek niet bepaald worden, aangezien er geen toegang is gegeven tot deze gesloten gegevens.

Alle respondenten waren van mening dat het maken van een risico-analyse een belangrijk onderdeel is van een veiligheidsprocedure voor een firewall, maar dit heeft in de huidige omgevingen weinig tot geen prioriteit.

Het door respondenten aangehaalde CvIB (code voor informatiebeveiliging) verschijnt dit jaar in een nieuwe versie. Deze was tijdens de uitvoering van dit onderzoek nog niet beschikbaar. Gezien de relatieve bekendheid van dit document, alsmede de benoeming van de risico-analyse van de firewall, kan dit zorgdragen voor een betere bewustwording bij organisaties. De benoeming zorgt ervoor dat er duidelijkheid bestaat of deze risico-analyse gericht op de firewall daadwerkelijk wordt gemaakt.

Uit de resultaten van de interviews blijkt verder dat er weinig aan beveiliging wordt gedaan, op een enkele uitzondering na. Men is al blij is als er überhaupt iets aan beveiliging gedaan wordt. De noodzaak van een goede firewallbeveiliging wordt niet direct ervaren door een deel van de organisatie. De kosten die verbonden zijn aan een goede beveiliging van de firewall kunnen hoog oplopen. Managers zijn zich nog onvoldoende bewust van het belang en hebben geen armslag / voldoende bevoegdheden, dan wel expertise om het belang van een goede beveiliging te ondersteunen (Jentjens e.a., 2004)

De resultaten uit de interviews geven aanleiding tot onderzoek naar een betere bewustwording van de risico-analyse van een firewall en hoe dit binnen een organisatie te realiseren is. Hierbij dient rekening gehouden te worden met;

- De bereidheid van architecten voor deelname aan empirisch onderzoek.
- Vergroting van kennis (van respondenten) binnen organisaties met betrekking tot

risico-analyse.

- Budget om de gesloten methoden (informatie risico analyse) te kunnen kopen.

5.4 Vergelijking resultaten literatuurstudie en empirie

Resultaat literatuurstudie

Zoals in paragraaf 5.2 (Literatuurstudie) reeds is aangegeven heeft de literatuurstudie een dertigtal criteria opgeleverd. Deze zijn onder te verdelen in de volgende categorieën:

- *Scope;* in de sectie scope worden de criteria beschreven die gerelateerd zijn aan het domein en het bereik van de risico-analyse.
- *Systeem karakteristieken;* in de sectie systeem karakteristieken worden de kenmerken van het systeem, in dit onderzoek meestal het netwerk en de firewall, beschreven.
- *Risico-analyse methode;* tot slot wordt in de risico-analyse methode beschreven hoe het risico-analyse-rapport tot stand is gekomen.

Resultaat empirie

Vanuit de empirie zijn geen antwoorden gevonden op de twee onderzoeksvragen. Er blijkt bij de respondenten soms (basis) theoretische kennis over de criteria die de kwaliteit van een risico-analyse bepalen aanwezig te zijn. Deze kennis wordt weinig tot niet gebruikt. Tevens bleek dat bedrijven zich veelal niet actief en bewust bezighouden met de risico-analyse van een firewall.

- De bereidheid van architecten voor deelname aan empirisch onderzoek.
- Budget om de gesloten methoden (informatie risico analyse) te kunnen kopen.

Reflectie

Het resultaat van de interviews was dat bedrijven nog niet zo ver zijn dat ze zich actief en bewust met risico-analyses van een firewall bezighouden. De opgestelde categorieën binnen het conceptueel model I (scope, systeemkarakteristieken en risico-analyse methode) zijn wel naar voren gekomen in de interviews. Deze werden echter niet expliciet benoemd, maar wel onderkend door de respondenten. Aangezien zij geen verdere verdieping hebben naar criteria is het niet mogelijk om factoren te destilleren die deze criteria te beïnvloeden. Daardoor is er ook geen conceptueel model II gemaakt. Hierdoor kan geen vergelijking plaatsvinden tussen de resultaten van de literatuurstudie en de empirie. Uit beide stappen blijkt dat er mogelijk antwoorden op de onderzoeksvragen zijn te verkrijgen uit literatuur die voor dit onderzoek niet beschikbaar was.

Uit de vergelijking tussen de resulaten vanuit de literatuurstudie en empirie kunnen een drietal conclusies getrokken worden:

1. Er is onvoldoende (wetenschappelijke) kennis over dit onderzoeksgebied

beschikbaar.

2. Er is mogelijk een verkeerde selectie van respondenten gemaakt.
3. Organisaties zijn niet actief bezig met risico-analyses van een firewall.

Het conceptueel model I dat ontwikkeld is door middel van de literatuurstudie blijkt op dit moment het maximaal haalbare binnen dit onderzoek.

6 Conclusies en reflectie

Voordat dit deelonderzoek van start ging was al duidelijk dat het onderzoeksgebied een moeilijk gebied is om te onderzoeken. Het is een onontgonnen gebied waarover relatief weinig wetenschappelijke literatuur beschikbaar is en toepassing in de praktijk vaak diffuus wordt uitgevoerd. Mede daarom is dit onderzoek interessant. Het risico van dit deelonderzoek daarentegen is dat de resultaten kunnen tegenvallen. Deze factoren hebben wel enige druk op de uitkomsten van het onderzoek gelegd.

Het hoofdstuk kent de volgende opbouw:

1. Kwaliteit bepalende criteria
2. Factoren die de kwaliteit bepalende criteria beïnvloeden
3. Bewustwording
4. Reflectie
5. Aanbevelingen

6.1 Kwaliteit bepalende criteria

De literatuurstudie heeft zo'n dertig criteria, onderverdeeld in een drietal categorieën, opgeleverd die gezien de onderzoeksmethode valide zijn. De lijst van criteria geeft antwoord op onderzoeksvraag 1: ”Welke criteria worden gebruikt door de managers en / of technici voor het bepalen van de kwaliteit van de risico-analyse?”.

Om de criteria inzichtelijk te houden, is er een onderverdeling in de volgende categorieën gemaakt:

- *Scope;* in de sectie scope worden de criteria beschreven die gerelateerd zijn aan het domein en het bereik van de risico-analyse.
- *Systeem karakteristieken;* in de sectie systeem karakteristieken worden de kenmerken van het systeem, in dit onderzoek meestal het netwerk en de firewall, beschreven.
- *Risico-analyse methode;* tot slot wordt in de risico-analyse methode beschreven hoe het risico-analyse-rapport tot stand is gekomen.

Hieronder volgende de criteria, die volgens de literatuurstudie, gebruikt kunnen worden om de kwaliteit van een risico-analyse te bepalen. Dit wil echter nog niet zeggen dat deze ook daadwerkelijk door de managers en technici worden gebruikt. De categorieën worden wel gebruikt in de praktijk, maar niet als zodanig benoemd (Zie 5.2 (Literatuurstudie)).

Scope

- Organisatie soort
- Organisatie grootte
- Doelgroep
- Aanvallers soort
- Hoeveelheid aanvallers

- Doelgroep risico-analyse

Systeem karakteristieken
- Afkadering systeem
- Systeemfuncties
- Data criteria
- Communicatiestromen

Risico-analyse methode
- Representatief
- Samenvatting
- Participanten
- Data verzamelings technieken
- Risico schalen
- Herkenbaarheid risico's
- Risicoverdeling
- Risicogebied
- Kwetsbaarheden
- Identificatie
- Risico beperking
- Kansbepaling
- Risicobeoordeling
- Aanbevelingen
- Veiligheidsniveau
- Systematisch en analytische uitvoering
- Valse precisie
- Tijdsduur
- Personeel

Zoals gebleken is uit de resultaten van de interviews, zijn de bedrijven nog niet zo ver dat ze zich actief en bewust met risico-analyses van een firewall bezighouden. Het blijkt dat er soms (basis) theoretische kennis over de criteria die de kwaliteit van een risico-analyse bepalen aanwezig is, maar dat deze kennis weinig tot niet wordt gebruikt. De opgestelde categorieën binnen het conceptueel model I (scope, systeem karakteristieken en risico-analyse methode) zijn wel naar voren gekomen in de interviews. Deze werden echter niet expliciet benoemd, maar wel onderkend door de respondenten.

Het conceptueel model I dat ontwikkeld is door middel van literatuurstudie blijkt op dit moment het maximaal haalbare binnen dit onderzoek.

6.2 Factoren die de kwaliteit bepalende criteria beïnvloeden

Vanuit de literatuurstudie zijn geen factoren gevonden die de criteria beïnvloeden die de kwaliteit van een risico-analyse bepalen. Dit komt doordat informatie met betrekking tot dit onderwerp niet is terug te vinden in de literatuur; en een deel van de literatuur die het onderwerp wel raakt, niet voldoet aan de wetenschappelijk criteria die zijn opgesteld. Dit is mede het gevolg van de geringe kennis die er op dit onderzoeksgebied 'expliciet' aanwezig is. De literatuur die wel aan bovenstaande voldoet beschrijft met name managementprocessen waarbij is aangegeven hoe een risico-analyse-rapport gemaakt kan

worden. Vanuit deze literatuur zijn de criteria, die de kwaliteit van een dergelijk rapport bepalen, gedestilleerd, maar niet de factoren die deze criteria kunnen beïnvloeden.

Ook het empirisch onderzoek geeft geen antwoord op onderzoeksvraag 2: “Welke factoren beïnvloeden de criteria die door de managers en / of technici voor het bepalen de kwaliteit van de risico-analyse gebruikt worden?” Mogelijke verklaringen hiervoor zijn: (Zie 5.3 (Empirie: Interviews technici / managers) en 5.4 (Vergelijking resultaten literatuurstudie en empirie))

- Het ontbreken van een groep respondenten die de systemen ontwikkelen. De architecten waren immers niet bereid aan het onderzoek mee te doen. Hun kennis met betrekking tot risico-analyse kon dus niet worden meegenomen.
- Vanuit de resultaten van de interviews is gebleken dat binnen bedrijven weinig aan beveiliging wordt gedaan. Hierdoor wordt weinig tot geen aandacht (bewustwording) besteed aan het maken van een risico-analyse. De kennis binnen organisaties met betrekking tot risico-analyse is hierdoor beperkt.
- Er is geen toegankelijkheid tot sommige risico-analyse methoden. Door een aantal grote organisaties zijn risico-analyse-methoden opgesteld. Deze zijn enkel toegankelijk wanneer men hiervoor betaald. Binnen dit onderzoek was hiervoor geen budget, waardoor de kennis uit deze methoden niet is gebruikt.
- Er is mogelijk een verkeerde selectie van respondenten gemaakt.

Dit deelonderzoek levert een lijst van criteria op die gebruikt worden om de kwaliteit van de risico-analyse ten behoeve van de functionaliteit van een firewall te beoordelen. In deelonderzoek B wordt gekeken of een fout in een firewall gevonden kan worden. Ook wordt onderzocht of een attacktree te gebruiken is als methode om een aanval op een firewall te beschrijven. Deze beschrijving zou mogelijk een risico-analyse kunnen ondersteunen en informatie kunnen geven over de risico's die in het bedrijfsnetwerk aanwezig zijn.

In de volgende paragrafen van hoofdstuk 6 wordt teruggekomen op de mogelijke verklaringen voor het ontbreken van een antwoord op onderzoeksvraag 2. In 12.2 (Aanbevelingen) worden aanbevelingen gedaan om in een nieuw onderzoek gerichter te kunnen zoeken.

6.3 Bewustwording

Zoals de antwoorden op onderzoeksvraag 1 en 2 reeds aangegeven wordt in het bedrijfsleven 'relatief' weinig aandacht besteed aan beveiliging van digitale informatie. Men houdt zich zelden actief en bewust bezig met risico-analyse van een firewall. Binnen organisaties is soms (basis) theoretische kennis over criteria die de kwaliteit van een risico-analyse bepalen aanwezig, maar deze kennis wordt weinig tot niet toegepast.

Beschikbare literatuur

Literatuur met betrekking tot risico-analyse blijkt beperkt aanwezig en toegankelijk te zijn. De literatuur die aanwezig is en tevens voldoet aan de wetenschappelijke criteria beschrijft met name managementprocessen waarbij is aangegeven hoe een risico-analyse-rapport

gemaakt dient te worden. Meer wetenschappelijke artikelen over dit onderwerp kunnen een bijdrage leveren aan een verdere bewustwording.

Beveiliging digitale informatie

Dit onderzoek levert mogelijk een bijdrage aan de beperking zoals hierboven beschreven. Door het interviewen van respondenten is gepoogd meer bewustwording over het onderwerp binnen een organisatie te creëren. Indien mensen binnen een organisatie met bepaalde verantwoordelijkheden zich bewust worden van de risico's die een slechte beveiliging van digitale informatie met zich mee brengt, kan dit gevolgen hebben voor de rest van de organisatie. Door middel van de interviews is getracht één schaap over de dam te krijgen. En zoals het spreekwoord zegt: “Als er één schaap over de dam is, volgen er meer”. Om te toetsen of er door de interviews daadwerkelijk meer bewustwording is ontstaan de respondenten zou er opnieuw een vraaggesprek moeten plaatsvinden. Hierbij zou nagegaan moeten worden welke invloed het gehouden interview heeft gehad of de beveiliging van digitale informatie binnen het bedrijf en of er meer kennis is opgedaan over risico-analyse.

Dit onderzoek levert tevens een bijdrage aan de literatuur die beschikbaar over risico-analyse en hoe de kwaliteit daarvan te bepalen. Er is immers onderzocht welke criteria de kwaliteit van een risico-analyse bepalen. Dit kan een aanleiding zijn voor andere onderzoekers om zich verder in de materie te verdiepen om zodoende het relatief onbekende terrein van risico-analyse van een firewall verder in kaart te brengen.

6.4 Reflectie

Tijdens de uitvoering van het onderzoek zijn een aantal punten opgevallen die hieronder zullen worden benoemd.

Bereidheid van de architecten tot deelname aan interviews

Een opvallende waarneming bij de uitvoering van het onderzoek is de reactie van de architecten. Zij waren niet bereid tot het geven van een interview aangezien dit dit niet in hun vakgebied zou liggen. Architecten leggen een basis voor het gebruik van computersystemen en in het verlengde daarvan ook voor de toepassing van een firewall. Het is daarom vreemd te noemen dat ze niet bereid waren tot een interview.

Beschikbare literatuur

Er is vrijwel geen literatuur te vinden die dit onderwerp specifiek behandeld. De literatuur die gebruikt is behandeld veelal managementprocessen waarin is aangegeven hoe een risico-analyse-rapport opgesteld dient te worden. Een aantal grote organisaties hebben een eigen (risico-analyse) methode ontwikkeld, maar hiervoor dient betaald te worden. Dit is veelal het gevolg van bedrijfsgevoelige informatie. Sommige bedrijven maken hier winst op en er ontstaat mogelijke imagoschade van bedrijven op het moment dat deze methodes worden onderzocht. In hoeverre de gesloten literatuur ook daadwerkelijk vernieuwend is, kon in dit onderzoek niet bepaald worden, aangezien er geen toegang is gekregen tot deze gesloten gegevens. Mede door de beperkt beschikbare literatuur is geen antwoord kunnen geven op onderzoeksvraag 2.

De meest recente versie van Code voor informatiebeveiliging deel een en deel twee was tijdens de uitvoering en de uitkomsten van het onderzoek nog niet beschikbaar. Hierdoor kan informatie die vanuit deze bron is onttrokken niet geheel up-to-date zijn. Het vrijkomen van deze literatuur kan mogelijk een verdere aanvulling en onderbouwing geven voor dit onderzoek.

Beschikbare tijd

De voor dit onderzoek beschikbare tijd staat niet in verhouding tot het gevraagde eindresultaat. Het dient duidelijk te zijn dat er een beperkte hoeveelheid tijd beschikbaar was voor het totale onderzoek. Deze tijdsbeperking geeft een limitatie in de mogelijkheden tot uitvoering en uitwerking. Desondanks is een methode uitgewerkt die waardevolle en bruikbare kennis over het onderwerp heeft opgeleverd, voor beide onderzoeken. Dit heeft echter wel extra tijd in beslag genomen.

Aanwezige kennis

Tijdens het onderzoek is naar voren gekomen dat er binnen organisaties, zowel bij technici als managers, weinig kennis is over risico-analyse. Dit is mede te wijten aan de veelal beperkte aandacht voor het beveiligen van digitale informatie. Pas als er daadwerkelijk iets is voorgevallen worden maatregelen genomen. Een tweetal oorzaken hiervan zijn: een hoge werkdruk waardoor dergelijke beveiligingsmaatregelen een lage prioriteit krijgen en de hoge kosten die hier veelal aan verbonden zijn.

Verantwoordelijkheid

Technici zien het risico-analyse-rapport veelal als administratieve overhead en geven het minder prioriteit dan andere uit te voeren zaken. Het rapport wordt dus als niet noodzakelijk gezien. Managers besteden weinig tijd en zijn zich weinig bewust van het feit dat zij ook invloed hebben, zowel met het geven van voldoende mankracht, als het bewust maken van het management van andere afdelingen, die moeten bepalen hoe waardevol de gegevens zijn van een risico-analyse van een firewall. Daarnaast hebben ze veelal weinig expertise om het belang van een goede beveiliging te ondersteunen.

Verwachting is dat deze situatie voor de meeste organisaties voorlopig zal blijven gelden, ondanks het feit dat de eerste signalen vanuit de organisaties bij de uitvoering van dit onderzoek positief waren. De betrokkenen, de managers (financieel verantwoordelijken) en de technici, nemen in deze materie geen verantwoordelijkheid.

6.5 Aanbevelingen

De resultaten vanuit het onderzoek geven aan dat bij een verder onderzoek naar risico-analyse van een firewall rekening gehouden dient te worden met de volgende punten. Verdere uitwerking is te vinden in 12.2 (Aanbevelingen):

Aanbeveling 1: Bewustwording risico-analyse van firewall bij organisaties, met name bij beslissers, architecten en uitvoerders.

Aanbeveling 2: Het houden van een risico-analyse

Aanbeveling 3: Budget vrijmaken

Aanbeveling 4: Bewustwording dat digitale informatie van 'levensbelang' is voor organisaties

Deelonderzoek B:

Aanvalsmethodieken van een firewall

7 Inleiding

In navolging van deelonderzoek A “Criteria die de kwaliteit van een risico-analyse van een firewall bepalen” wordt in de komende hoofdstukken deelonderzoek B “Aanvalsmethodieken van een firewall” beschreven.

Deelonderzoek B is als volgt opgebouwd:

- *Inleiding:* Hierin worden de doelstelling, vraagstelling en relevantie van dit onderzoek behandeld.
- *Projectkader:* In het projectkader worden begrippen die voor de context van dit onderzoek van belang zijn en de samenhang tussen deze begrippen behandeld.
- *Onderzoeksmethode:* Beschrijft de opbouw van het deelonderzoek.
- *Resultaten:* Hierin worden de resultaten van het deelonderzoek gepresenteerd.
- *Conclusie:* De conclusies van het deelonderzoek komen hier aan bod.

In dit hoofdstuk worden de doel- en vraagstelling beschreven, alsmede de relevantie van dit onderzoek.

Hoofdstuk 7 heeft de volgende paragrafen:

- *Doelstelling*: Hierin wordt een introductie op de doelstelling gegeven, gevolgd door de uiteindelijke doelstelling.
- *Vraagstelling*: Vanuit de doelstelling zijn een aantal onderzoeksvragen voorgekomen die binnen dit onderzoek onderzocht worden.
- *Relevantie*: De doelgroep en het nut van dit onderzoek worden in deze paragraaf uitgewerkt.

Nu volgt de introductie op de doelstelling.

7.1 Doelstelling

In “Attacktrees: door de bomen de bedreigingen zien” bestuderen Dr. Sjouke Mauw en Dr. Martijn Oostdijk de attacktree methode (Mauw, 2006). Zie paragraaf 8.7 (Attacktree) voor meer informatie over de attacktree (methode). Binnen het onderzoeksteam heerst de vraag of de attacktree methode te gebruiken is om aanvallen op een beveiligde-computer-netwerk-omgeving te modelleren (Mauw, 2006). Deze vraag is ontstaan nadat er aan het onderzoeksteam en aan Dr. Cees-Bart Breunesse gevraagd is om een firewall van Compumatica[21], onderdeel van een beveiligde-computer-netwerk-omgeving, te testen en te beoordelen. Dit onderzoek heeft hierbij een ondersteunende functie voor het onderzoeksteam. Vragen die na de opdracht om een Compumatica firewall te testen bij het team op kwamen zijn:

- Is het aanvallen van een firewall 'finger-spitzen-gevoel'?

21 Voor meer informatie bekijk: http://www.compumatica.de/

- Welke methodieken worden gebruikt om een firewall aan te vallen?
- Welke opensource tools zijn er beschikbaar?
- Zijn de aanvalsmethodieken te gebruiken in een blackbox test omgeving? Zie paragraaf 8.5 (Firewall) voor uitleg blackbox firewall.
- Kunnen deze methodieken gedocumenteerd worden?
- Is het mogelijk om de gebruikte methodieken te automatiseren?
- Is het mogelijk om van de documenterende methodieken een attacktree te maken?
- Is de gebruikte attacktree methode een handige manier om dit soort aanvallen te beschrijven?

Aangezien er meer vragen waren dan er antwoorden gegeven konden worden binnen de beschikbare tijd is er gekozen om het deelonderzoek in te perken. Met de opdrachtgever Dr. Martijn Oostdijk is besloten om de volgende doelstellingen te onderzoeken.

1. Het aanvallen van een blackbox firewall.
2. Het op een gestructureerde en documenterende methode beschrijven van de aanvallen op een blackbox firewall.
3. Het automatiseren van bovenstaande methode.
4. Het ontwerpen van een attacktree van de bovenstaande methodiek en bepalen of de attacktree methode bruikbaar is in deze context.

Uit de bovenstaande doelstellingen wordt in de volgende paragraaf de vraagstelling onttrokken.

7.2 Vraagstelling

Om de bovenstaande doelstellingen te realiseren is de onderstaande vraagstelling geformuleerd:

De vraagstelling luidt:

> “Hoe kan een daadwerkelijk uitgevoerde aanval op een firewall beschreven worden op een gestructureerde en documenterende manier en is deze uitgevoerde aanval te automatiseren?”

Op grond van bovenstaande vraagstelling en de bij 7.1 (Doelstelling) beschreven doelstellingen zijn de volgende onderzoeksvragen geformuleerd:

1. Hoe kan een blackbox firewall worden aangevallen?
2. Zijn de bovenstaande aanvallen te beschrijven op een gestructureerde en documenterende manier?
3. Zijn de bij twee beschreven aanvallen op de blackbox firewall te automatiseren?
4. Is het mogelijk om een attacktree te ontwerpen op basis van een aanvallende methodiek?
5. Is de attacktree methode een bruikbare techniek om aanvallen op een blackbox firewall te modelleren?

De bovenstaande vragen worden door middel van een case-study onderzocht. Duidelijk dient te zijn dat het hierbij niet gaat om een theoretisch onderbouwde aanval, maar dat bestaande technieken worden gebruikt om daadwerkelijk een aanval uit te voeren.

In de volgende paragraaf wordt ingegaan op de relevantie van het onderzoek.

7.3 Relevantie

De doelgroep(en) van dit onderzoek zijn personen, voornamelijk onderzoekers gespecialiseerd in digitale beveiliging, die bekend zijn met het gebruiken van firewalls om digitale informatie te beschermen.

Beveiliging van informatie wordt binnen de samenleving steeds belangrijker gevonden (Grashion, 2006). Waar vroeger op het moment dat er informatie uitlekte meestal een beperkte hoeveelheid mensen toegang tot deze informatie had, is tegenwoordig door middel van het Internet de mogelijkheid ontstaan om zeer snel en relatief anoniem informatie te verspreiden, zodat veel mensen toegang kunnen krijgen tot de informatie (Prins, 1997). Dit onderzoek richt zich op de blackbox firewall welke een onderdeel van een beveiligde-computer-netwerk-omgeving is dat ervoor moet zorgen dat digitale informatie beschermd blijft. Met andere woorden de informatie moet alleen beschikbaar zijn voor de daartoe bevoegde personen.

Binnen deelonderzoek B, het informatica-onderzoek, wordt gekeken naar een firewall als middel om risico's in te perken. Door middel van dit onderzoek wordt aangetoond dat een blackbox firewall niet altijd veilig hoeft te zijn. Een firewall kan falen in zijn functioneren. Daarnaast wordt er gekeken naar een manier om dit soort aanvallen te beschrijven. Het management onderzoek, deelonderzoek A, richt zich op risico-analyse om deze risico's te beheersen.

8 Projectkader

Om een helder beeld te krijgen van deelonderzoek B, “Aanvalsmethodieken van een firewall”, is het van belang duidelijkheid over het onderwerp te krijgen. De benaderingswijze is een andere dan die van het managementonderzoek. Bij het managementdeel wordt vanuit een functionele en bedrijfsorganisatorische manier naar de materie gekeken. Het informatica-onderzoek kijkt vanuit een technisch perspectief. Vanwege de eenduidigheid worden ook in het informatica-onderzoek de belangrijkste begrippen en de samenhang daartussen, die voor de context van dit onderzoek van belang zijn, in de eerstvolgende paragrafen uiteengezet. Dit hoofdstuk bevat de volgende paragrafen.

1. *Aanvalsmethodieken:* Aangezien dit onderzoek over aanvalsmethodieken gaat, worden in deze paragraaf verschillende aanvalsmethodieken uitgewerkt.
2. *Fouten in software en configuratie:* In deze paragraaf wordt beschreven wat fouten in software of configuratie zijn.
3. *Veiligheid digitale informatie:* Wat houdt beveiliging van digitale informatie in.
4. *Digitale informatie en bedrijfsnetwerken:* Hoe relateren digitale informatie en bedrijfsnetwerken zich tot elkaar. Deze paragraaf legt tevens het verband met deelonderzoek A.
5. *Firewall:* Beschrijving van de functionaliteit van een firewall.
6. *Het Internet Protocol:* Beschrijving van het internet protocol dat gebruikt wordt door de firewall.
7. *Attacktree:* Overzicht van een methode om aanvallen op een firewall te beschrijven

De woorden “aanval” en “aanvallen” kunnen binnen deze masterthesis op verschillende manieren geïnterpreteerd worden. Dit komt doordat bij één aanval meerdere deelaanvallen kunnen plaatsvinden. Bijvoorbeeld een inbreker steelt sieraden uit een slaapkamer van een huis. Eerst zal de inbreker zich toegang moeten verlenen tot het huis. Dit kan door middel van het openen van een slot. Daarna zal de inbreker moeten bepalen waar de slaapkamer zich bevindt. Vervolgens dient hij in de slaapkamer de sieraden te zoeken en eventueel een kluis openen. Oftewel bij een inbraak dient de inbreker 'kleinere' inbraken te doen om tot zijn doel te komen. Hetzelfde geldt ook voor een aanval.

Nu als eerst de aanvalsmethodieken.

8.1 Aanvalsmethodieken

Aanvallers, ook wel crackers genoemd, proberen vaak toegang te krijgen tot digitale informatie. Hackers is in de media ook een veel gebruikte benaming om crackers te beschrijven. Dit is helaas een foutief gebruikte benaming vanuit een puristisch perspectief [22]. Crackers, ook wel 'black hat' aanvallers genoemd, handelen uit crimineel of vernielzuchtig oogpunt. 'Black hat' aanvallers zijn aanvallers die doelbewust systemen aanvallen om daar zelf beter van te worden. Dit kan zowel betrekking hebben op het financieel beter worden,

22 Zie “Hacker_definition_controversy” (http://en.wikipedia.org/wiki/Hacker_definition_controversy) voor meer informatie.

als het uiten van bepaalde meningen. Zij misbruiken de gevonden lekken voor hun eigen doeleinden (WWW-11). Een hacker, ook wel een 'white hat' aanvaller genoemd, is een persoon die een intellectuele uitdaging heeft om op een creatieve, onorthodoxe manier aan technische beperkingen te ontsnappen. Oftewel een hacker heeft goede intenties in zijn handelingen. Met goede intenties wordt bedoeld dat ze geen schade willen aanrichten bij de aangevallen systemen. De 'white hats' zullen, als ze een lek hebben gevonden, de eigenaren van het systeem op de hoogte brengen. Tevens maken ze deze informatie openbaar zodat andere onveilige systemen veilig gemaakt kunnen worden. Ook wel full-disclosure genoemd (Schneier 2001). Op deze manier zorgen ze ervoor dat het systeem zo veilig mogelijk blijft voor de 'black hat' aanvallers.

In dit onderzoek wordt de term aanvaller gebruikt om zowel de 'white hat', de goede aanvallers, als de 'black hat', de slechte aanvallers, te beschrijven. Dit aangezien beide aanvallers op één en dezelfde manier een systeem aanvallen.

Aanvallers proberen aan digitale informatie te komen door gebruik te maken van een aantal methoden:

- *"Social enginering"*: hiermee probeert een aanvaller gegevens te verkrijgen door middel van het manipuleren van gebruikers. Dit kan gedaan worden door het bellen naar een gebruiker waarbij de aanvaller zich "voordoet" als bijvoorbeeld een helpdesk medewerker. Een andere manier zijn "scam" mailtjes, ook wel "phishing" mailtjes genoemd. Dit zijn e-mails waarbij de afzender de gebruiker laat denken dat de mail van bijvoorbeeld een bank afkomstig is (WWW-12).

- "*Dumpster diving*": oftewel "het afvalbak duiken", hierbij gaat een aanvaller in (digitale) afval snuffelen. Soms wordt dit wel erg gemakkelijk gemaakt, zoals door de Amsterdamse officier van justitie J. Tonino, die een computer vol vertrouwelijke informatie bij het grofvuil op straat zette (WWW-13). Ook is men vaak geïnteresseerd in informatie over de naam van de hond, geboortedatum en andere persoonlijke informatie van personen die toegang hebben tot belangrijke informatie. De kans is namelijk aanwezig dat dit soort informatie wordt gebruikt om wachtwoorden te bedenken, aangezien dit gemakkelijk te onthouden is (WWW-14).

- *Brute force cracking*: de aanvaller probeert toegang te verkrijgen door miljoenen (zij het niet miljarden) keren wachtwoorden proberen te raden. Dit gebeurt veelal op een geautomatiseerde manier (Bernstein, 2005).

- *Via fouten in software en configuratie*: Door middel van deze fouten kan een aanvaller de software andere taken laten doen dan waarvoor het oorspronkelijk bedoeld is. Zie paragraaf 8.2 (Fouten in software en configuratie) voor de onderbouwing.

Binnen dit onderzoek wordt alleen gekeken naar het verkrijgen van digitale informatie door middel van fouten in software. Dit aspect wordt in de volgende paragraaf uitgediept.

8.2 Fouten in software en configuratie

De internetpopulatie is steeds meer een afspiegeling van de maatschappij. Er zitten mensen met goede bedoelingen op het Internet, maar helaas ook mensen met minder goede bedoelingen. Daarom wordt steeds meer software geschreven om goedwillende internetgebruikers te beschermen tegen kwaadwillende internetgebruikers. Windows Internet

Explorer staat bekend om zijn hoeveelheid gevaarlijke fouten (WWW-15, WWW-16). Fouten waardoor de computer, waar Windows Internet Explorer op draait, volledig overgenomen kan worden door een cracker. De cracker kan op dat moment alles doen met de computer wat de cracker wil. Dit ondanks de miljoenen dollars die Microsoft heeft geïnvesteerd in de ontwikkeling en de beveiliging van Windows Internet Explorer. Firefox, een webbrowser die open-source[23] is, staat bekend als een veilige browser, maar desondanks worden ook hier fouten gevonden. Open Source Software (OSS) is software waarvan de broncode vrijelijk voor het publiek beschikbaar wordt gesteld door de technici. Iedereen kan hierdoor de broncode inzien en verbetering aanbrengen of fouten ontdekken. Helaas kunnen crackers dit ook. Dit in tegenstelling tot gesloten software waarbij een beperkt aantal ontwikkelaars zich bezig houden met de broncode. Software schrijven is nu eenmaal een complexe aangelegenheid. Software wordt door mensen geschreven en mensen maken nu eenmaal fouten. Je kunt dus stellen dat er ook fouten in elk stuk software zitten. Hieruit is het volgende te concluderen, zoals Dan Farmer en Wietse Venema zeggen:

> "As every good programmer knows, software will eventually fail—no matter how well it is written. The same applies to systems, networks and security mechanisms; and a system that is prepared for failure has safety nets in various places." (WWW-17).

Dit betekent dat in complexe omgevingen, hiermee wordt een opeenstapeling van verschillende systemen bedoeld, een opeenstapeling van fouten kan voorkomen. Wanneer een fout optreedt in een eenvoudig, niet complex, systeem hoeft dit niet erg te zijn. Een aanvaller kan een fout in de software gebruiken om meer rechten te verkrijgen binnen het systeem. Dit wil echter nog niet zeggen dat hij voldoende rechten heeft verkregen om ook daadwerkelijk bij de digitale / bedrijfskritische informatie te komen. Een opeenvolging van fouten kan wel funest zijn. Stel, als er een kluis in een huis staat, dan moet een aanvaller, in dit geval dus een inbreker, eerst in dit huis zien te komen. Stel dat door een makkelijk open te breken sluitwerk de inbreker gemakkelijk in het huis komt, dan heeft de inbreker nog steeds zijn doel niet bereikt. De kluis moet immers nog gevonden worden en vervolgens worden geopend. Maar stel dat de bewoner vergeten is om de kluis dicht te doen, omdat er gedacht wordt dat het slot van de deur voldoende bescherming biedt, dan is de inbreker, wanneer hij de kluis gevonden heeft, bij de inhoud van de kluis en is het doel van de inbreker bereikt.

Aanvallers maken gebruik van fouten in software. Er wordt dus aangenomen dat software fouten bevat (WWW-17). Fouten in software zijn:

- Fouten die ervoor zorgen dat de software dingen doet die niet gespecificeerd zijn.
- Fouten die ervoor zorgen dat de software andere dingen doet dan gespecificeerd zijn.

Met andere woorden de software wordt door de aanvaller gebruikt op een manier die niet bedoeld is om iets voor elkaar te krijgen. Er zitten dus ook fouten in computersystemen, aangezien die gebruik maken van software, om digitale informatie te beveiligen. In de volgende paragraaf wordt verder ingegaan op de veiligheid van digitale informatie.

23 Zie Vereniging Open-source Nederland (http://www.vosn.nl) voor meer informatie.

8.3 Veiligheid digitale informatie

Hoe veilig moet digitale informatie zijn? Dat is een vraag die niet eenduidig te beantwoorden is. Digitale informatie kan voor de ene organisatie weinig betekenen, maar voor een andere organisatie juist heel waardevol zijn. Er zal een afweging gemaakt dienen te worden tussen de hoeveelheid energie, capaciteit en / of geld die in het beveiligen van digitale informatie gestoken wordt en / of het investeren in digitale informatiebeveiliging het geld waard is (van Mastrigt, 2006). Op het moment dat er besloten is om geld te investeren in het beveiligen van digitale informatie moeten er keuzes worden gemaakt welke informatie er beveiligd dient te worden en hoe deze digitale informatie te beveiligen.

Welke criteria worden gebruikt om te bepalen of digitale informatie echt veilig is? Hiervoor worden de volgende criteria gebruikt die opgesteld zijn in de Code voor Informatiebeveiliging, deel 1 (NEN, 2000, ISO 27001):

1. *Vertrouwelijkheid*: waarborgen dat informatie alleen toegankelijk is voor diegenen, die hiertoe geautoriseerd zijn;

2. *Integriteit*: het waarborgen van de correctheid en de volledigheid van informatie en verwerking daarvan;

3. *Beschikbaarheid*: waarborgen dat geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot informatie en aanverwante bedrijfsmiddelen.

Zie paragraaf 3.3 (Informatiebeveiliging) voor verdere uitwerking.

Binnen dit deelonderzoek wordt niet gekeken naar de bedrijfsorganisatorische aspecten van digitale informatie beveiliging. Hiermee worden de volgende aspecten bedoeld: (van Mastrigt, 2006)

- Beveiliging van de fysieke toegang tot belangrijke apparatuur.

- Hoe de authenticiteit / identiteit bepaald wordt. Hiermee wordt bedoeld; het bewijzen dat een bepaald persoon ook daadwerkelijk de persoon is, die hij zegt dat hij is.

- Hoe de autorisatie bepaald wordt. Dat wil zeggen welke bevoegdheden een bepaald persoon heeft op het moment dat die persoon zichzelf geïdentificeerd heeft.

Binnen dit onderzoek wordt er vanuit gegaan dat dit soort bedrijfsorganisatorische aspecten voldoende veilig zijn.

Naast bedrijfsorganisatorische aspecten zijn er ook technische aspecten van veilige digitale informatie.

Bij technische aspecten wordt dit in drie gebieden verdeeld: (Berlijn, 2007)

1. *De 'cliënts'*: Dit zijn computersystemen waar de werknemers op werken.

2. *De 'servers'*: Dit zijn meestal grote zwaardere computersystemen die services aanbieden aan de cliënts. Hieronder wordt onder andere verstaan het verzorgen van email, intranet, webpagina's en fileservers.

3. *Het 'netwerk':* Dit zijn alle cliënts en servers die onderling verbonden zijn en eventueel ook de verbinding met het Internet verzorgt.

In dit onderzoek wordt enkel gekeken naar punt drie. Van punt een en twee wordt aangenomen dat de systemen op een voldoende niveau zijn beveiligd.

Via bedrijfsnetwerken wordt digitale informatie uitgewisseld. In de volgende paragraaf 8.4 (Digitale informatie en bedrijfsnetwerken) wordt de relatie tussen digitale informatie en bedrijfsnetwerken kort beschreven. Zie paragraaf 3.2 (Digitale informatie-uitwisseling tussen organisaties) voor meer achtergrond informatie

8.4 Digitale informatie en bedrijfsnetwerken

Binnen een bedrijf zijn vaak verschillende afdelingen. Deze afdelingen beschikken soms over informatie die andere afdelingen niet mogen inzien, bijvoorbeeld bij de afdeling personeelszaken (van Liere, 2005). Elk van deze afdelingen hebben vaak hun eigen infrastructuur. Het is mogelijk om een afdeling af te schermen door geen fysieke verbinding te leggen. Hiermee wordt voorkomen dat er überhaupt personen op het afgeschermde netwerk kunnen komen. Door deze oplossing kunnen de medewerkers van desbetreffende afdeling ook niet op andere systemen komen, zoals een fileserver, die ze misschien voor hun werkzaamheden nodig hebben.

Een andere manier om een bedrijfsnetwerk infrastructuur te beveiligen is door middel van een firewall, zie paragraaf 3.6 (Functionaliteit van een firewall). Tevens kan een firewall gebruikt worden om gebruikers op het Internet van het locale bedrijfsnetwerk af te schermen. Een bekend voorbeeld is “SPAM”. Om de risico's te beperken dat een medewerker (on)bewust spam gaat versturen, kan een firewall zorgen dat het systeem van de medewerker niet direct een email kan versturen. Een email versturen is dan alleen mogelijk als er gebruik gemaakt wordt van een email server, dit is dus ook een relayserver, van de organisatie zelf. Het systeem kan ingrijpen als in één keer duizenden mails worden verstuurd door een bepaald persoon of computersysteem. Dit zal normaal gesproken geen standaard email activiteit zijn van een medewerker. Met andere woorden: een firewall kan email, dat van het interne netwerk komt, verplichten om via een mail relay server te gaan. De relay server controleert vervolgens of de verzonden email daadwerkelijk normaal email verkeer is dat binnen de bedrijfspolicies valt.

Binnen dit onderzoek wordt alleen gekeken naar een firewall en niet naar de omgeving. Wanneer een firewall is geïnstalleerd kun je er niet standaard van uit gaan dat alles naar wens functioneert aangezien een firewall een complex apparaat is. Het is daarom van belang om een goede werking van een firewall te kunnen garanderen.

In paragraaf 3.6 (Functionaliteit van een firewall) is de functionaliteit van de firewall algemeen beschreven. In de komende paragraaf wordt de functionaliteit van de firewall technisch nader uitgewerkt.

8.5 Firewall

Op het moment dat er besloten is om geld te investeren in het beveiligen van de infrastructuur van het bedrijfsnetwerk en er gekozen is om een firewall aan te schaffen, welke manieren zijn er dan om te kunnen garanderen dat de firewall ook echt naar behoren functioneert? Of wordt er standaard vanuit gegaan dat het veilig is, omdat er een firewall geïnstalleerd is om het netwerk te beschermen?

Een firewall wordt gebruikt om een veiliger bedrijfsnetwerk te creëren. Een firewall

beschermt het bedrijfsnetwerk niet tegen alle kwade bedoelingen. Zie paragraaf 3.6 (Functionaliteit van een firewall) voor meer informatie over een firewall. Een firewall verbetert de bedrijfsnetwerkbeveiliging, maar maakt het netwerk niet absoluut veilig. Een andere mogelijkheid om digitale informatie veilig te stellen is om een computersysteem helemaal niet op te nemen in een netwerk. Het is dan mogelijk dat de functionaliteit van het computersysteem in het gedrang komt, aangezien mensen die bevoegd zijn om digitale gegevens in te zien ook niet tot die gegevens kunnen komen: zie paragraaf 8.4 (Digitale informatie en bedrijfsnetwerken).

Een firewall is geschreven software, dit betekent dat een firewall fouten kan bevatten. Hoe ernstig de fouten zijn en wat voor impact deze fouten hebben is veelal onbekend. Buiten dat er software fouten in een firewall zitten, is een firewall een complex apparaat dat gemakkelijk foutief of anders ingesteld kan worden dan bedoeld. Deze complexiteit heeft weer gevolgen voor het kunnen garanderen van de goede werking van een firewall.

De firewall wordt in dit onderzoek als een 'blackbox' firewall gezien, dit vanwege de wens van de opdrachtgever. Dat wil zeggen dat bij de aanvallen er niet naar de firewall zelf gekeken wordt. Met andere woorden er wordt alleen gekeken wat er in de firewall gestopt wordt (input) en wat uit de firewall komt (output). Er wordt niet gekeken naar de processen die zich in de firewall afspelen.

Computersystemen kunnen binnen een netwerk op verschillende manieren met elkaar communiceren, maar ze moeten wel op dezelfde manier communiceren om elkaar te kunnen verstaan. Op de wereld worden meerdere talen gesproken om met elkaar te kunnen praten, je moet alleen wel de juiste taal kennen om elkaar te kunnen verstaan. Om computers met elkaar te laten communiceren bestaan er verschillende protocollen, dit zijn talen, zoals het IPX / SPX (Internet Packet eXchange / Sequensed Packet) protocol, een standaard gebruikt door Novell, of het IP (Internet Protocol), de huidige standaard van het Internet. Om netwerken van elkaar af te schermen dient een firewall het protocol te ”verstaan” die gebruikt wordt door het het netwerk. Bijvoorbeeld: op het moment dat je een netwerk hebt waarin zowel IP als IPX / SPX gebruikt worden en er wordt een firewall geïnstalleerd die alleen IP ondersteund, dan zal het IPX / SPX verkeer niet gefilterd worden. Om zo'n netwerk veiliger te krijgen dien je zowel een firewall voor het IP verkeer als een firewall voor het IPX / SPX verkeer te installeren. Binnen dit onderzoek wordt er alleen naar IP gekeken aangezien dit de standaard van het Internet is en er op het Internet firewalls nodig zijn (Kurose e.a., 2001). Oftewel firewalls zijn nodig om 'digitaal-verkeer', waarin informatie is opgeslagen, dat gebruikt wordt door een bepaald netwerk, te controleren en de authenticiteit te kunnen garanderen. Dit om de vertrouwelijkheid, integriteit en beschikbaarheid van digitale informatie (zie paragraaf 3.3 (Informatiebeveiliging)) te kunnen garanderen.

Als twee computers via IP met elkaar communiceren ontstaat er een data-stroom, ook wel gegevens-stroom, tussen deze computers. Deze data-stromen bestaan uit een groot aantal IP-datagrammen. IP-datagrammen zijn de basisunits, met andere woorden de bouwstenen van informatie, die door een IP netwerk verwerkt worden. In de header, dat is het begin stuk van het datagram, staat onder andere de bron (source) en de bestemming (destination) van de verbinding beschreven. Op het moment dat computers met elkaar verbonden zijn door middel van een switch, hub of een cross-kabel kunnen deze computers met elkaar communiceren. Op het moment dat de bestemming verder ligt, is er een router nodig. Een router is een apparaat die de IP datagram analyseert en vervolgens naar het juiste netwerk stuurt. Een firewall is in de basis een router met een extra functionaliteit. Deze extra functionaliteit houdt in dat een firewall IP-datagrammen kan inspecteren, verdelen en autoriseren, dat wil zeggen dat een firewall een filter heeft die op bepaalde criteria de IP-datagrammen wel of niet doorlaat (Kurose e.a., 2001). Een router heeft deze functionaliteit

niet.

De blackbox firewall die voor dit onderzoek gebruik wordt, maakt gebruik van het Internet Protocol (IP). Het IP wordt in de volgende paragraaf uitgewerkt.

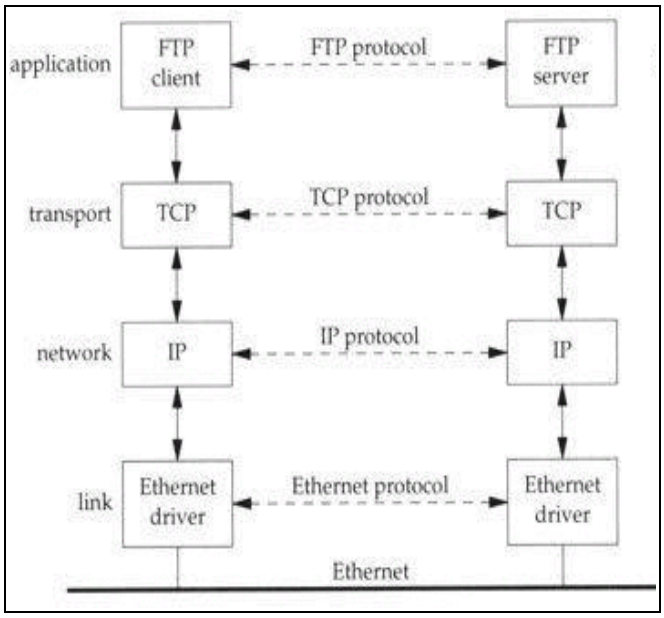
8.6 Het Internet Protocol

Binnen dit onderzoek wordt alleen gekeken naar een firewall die het IP (Internet Protocol) verwerkt. Omdat een firewall filtert op criteria van het IP, wordt in deze paragraaf het IP uitgelegd.

Het IP is een onderdeel van het TCP / IP referentie model, dat is gedefinieerd in RFC (Request For Comments) 791 (Kaufman, 2002). “Request For Comments” documenten zijn documenten die de technische en organisatorische aspecten van het Internet beschrijven. De meest gebruikte protocollen zijn gestandaardiseerd door de IETF (Internet Engineering Task Force) (Kaufman, 2002). Het TCP / IP referentie model heeft een gelaagde architectuur welke uit vier lagen bestaat (Zie: Figuur 13) (Stevens, 1994). Deze lagen zijn: de toepassingslaag, de transportlaag, de netwerklaag en de datalinklaag (Kurose e.a., 2001).

Op het moment dat twee verschillende apparaten communiceren, communiceren de lagen van de twee apparaten met elkaar, oftewel de toepassingslaag communiceert met de toepassingslaag, de transportlaag communiceert met de transportlaag, de netwerklaag communiceert met de netwerklaag en de datalinklagen communiceren met elkaar. In Figuur 13 zijn deze logische communicatielijnen horizontaal verbonden met een onderbroken pijl.

De daadwerkelijk / fysieke communicatie verloopt via de verschillende lagen onderling. Oftewel de toepassingslaag communiceert met de transportlaag, de transportlaag communiceert met de netwerklaag, de netwerklaag communiceert met de datalinklaag en de datalinklaag communiceren met de daadwerkelijk fysieke verbindingen.



Figuur 13: Vier laags IP model (Stevens, 1994)

De toepassings-, transport-, netwerk- en datalinklaag van het vier laags model hebben de volgende betekenis (Zie: Figuur 13), (Kurose e.a., 2001):

1. *Toepassingslaag:* In deze laag bevinden zich de eindgebruiker applicaties. In Figuur 13 staat FTP beschreven maar in deze laag vallen ook andere protocollen bijvoorbeeld HTTP (HyperText Transport Protocol) voor het gebruik van je webbrowser en SMTP (Simple Mail Transfer Protocol) voor e-mail.

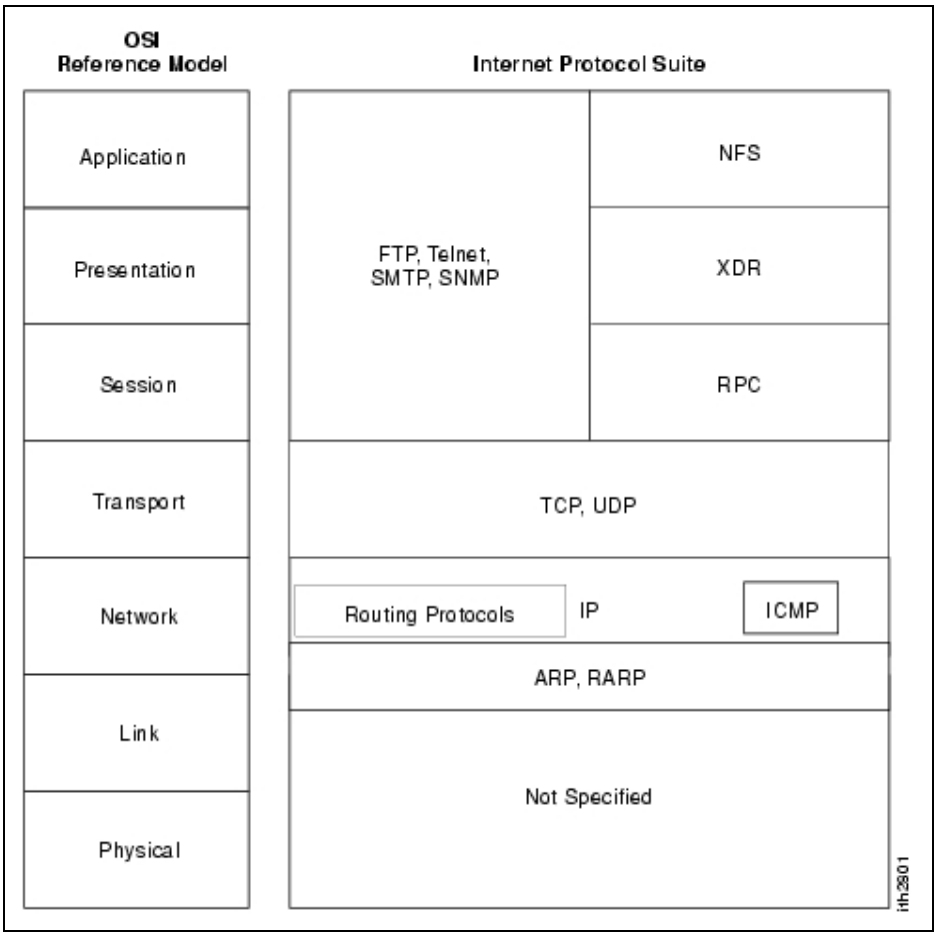
2. *Transportlaag:* De transportlaag zorgt voor de informatie-uitwisseling tussen programma's. Bijvoorbeeld door TCP (Transmission Control Protocol) en UDP (User Datagram Protocol).

3. *Netwerklaag:* De netwerklaag zorgt voor de elementaire informatie-uitwisseling, adressering en routering. Voorbeelden hiervan zijn IP (Internet Protocol) en ICMP (Internet Control Message Protocol).

4. *Datalinklaag:* De datalinklaag zorgt voor de fysieke verbinding en aansturing. Bijvoorbeeld de netwerkdriver in een operating-systeem met de wired of wireless verbinding. Dit kunnen ethernet, tokenring of WiFi netwerkdrivers en infrastructuur zijn.

Op het moment dat je via een webbrowser (a.k.a. HTTP-server), bijvoorbeeld firefox (WWW-18), een webpagina opvraagt, communiceert firefox met een webserver, bijvoorbeeld apache (WWW-19). De firefox browser, die werkt in de toepassingslaag, communiceert direct met de webserver en heeft geen idee hoe de onderliggende lagen, transport- netwerk- en datalinklaag, werken. Firefox praat met de webserver via het HTTP-protocol (WWW-20). Firefox vraagt volgens een vast gedefinieerde methode aan de transportlaag om een betrouwbare verbinding te leggen naar de webserver. Firefox weet verder niet hoe en of wat de transportlaag verder doet. De transportlaag zorgt door middel van bijvoorbeeld het TCP protocol dat er een betrouwbare verbinding gelegd wordt tussen de transportlaag van het systeem waar de webserver op draait, met de transportlaag van het systeem waar firefox op draait. De transportlaag gebruikt de netwerklaag, die zorg draagt voor de elementaire informatie-uitwisseling, voor de adressering en routering. Daarna geeft de netwerklaag de webaanvraag plus overhead van de eerder doorlopen lagen door aan de datalinklaag. De datalinklaag zorgt ervoor dat het uiteindelijk fysiek op de netwerk, bijvoorbeeld ethernet, terecht komt.

Het OSI (Open System Interconnection) model wordt gebruikt om informatie-uitwisseling over netwerk architectuur te verduidelijken (Zie Figuur 14). Zelden kunnen huidige gelaagde netwerkarchitectuurmodellen volledig en gepast gemodelleerd worden in het OSI model (Kaufman, 1995). Ondanks dat het TCP / IP model niet volledig past in het OSI model, wordt voor de duidelijkheid een overzicht gegeven van hoe de verschillende lagen met elkaar overeen komen (Zie Figuur 14).



Figuur 14: OSI Reference Model - Internet Protocol Suite (WWW-21)

Figuur 14 is verder alleen ter verduidelijking aangegeven en wordt niet verder uitgewerkt.

Het IP, dat in de netwerklaag zit, is een connectieloos, onbetrouwbaar op datagrammen gebaseerd protocol. Dit protocol biedt geen enkele garantie over de aankomst van een datagram. Dit betekent dat datagrammen niet hoeven aan te komen, gecorrumpeerd kunnen zijn, gedupliceerd worden of in de verkeerde volgorde kunnen worden afgeleverd. Het IP is alleen verantwoordelijk voor het adresseren en routeren van pakketten tussen verschillende systemen. Op dit moment zijn er twee verschillende versies van dit protocol beschikbaar, het IPv4 en het IPv6. IPv6 is een nieuw protocol dat ontwikkeld is om IPv4 te vervangen. De belangrijkste reden voor de ontwikkeling van dit protocol is dat er een tekort is ontstaan in de hoeveelheid beschikbare IP nummers (WWW-22), (WWW-23).

De transportlaag, die boven de netwerklaag ligt, bevat twee veel gebruikte protocollen. Het Transmission Control Protocol (TCP), die is gedefinieerd in RFC 793, en het User Datagram Protocol (UDP), welke is gedefinieerd in RFC 768. TCP zorgt voor een connectie georiënteerde, betrouwbare verbinding en UDP zorgt voor een connectieloze, onbetrouwbaar verbinding.

Op elke laag van het vier laags model kunnen datastromen toegestaan en geblokkeerd worden (Zie Figuur 13) (Kurose e.a., 2001). De toepassingslaag wordt meestal afgehandeld door computerprogramma's die specifiek een bepaald protocol, een soort verkeer zoals HyperText Transfer Protocol (HTTP), afhandelen. Dit soort programma's worden vaak proxies genoemd. Proxies kunnen aan de hand van inhoudelijke informatie toegang geven of weigeren. Bijvoorbeeld: bij HTTP kan men niet toestaan dat in de organisatie naar sexsites

wordt gesurft. De datalinklaag wordt meestal afgehandeld door switches, op dit niveau kan er gekeken worden of bepaalde computers wel of geen toegang hebben tot het netwerk.

Voor de afkadering binnen dit onderzoek wordt niet naar de toepassingslaag en de datalinklaag gekeken, maar enkel naar de transportlaag en de netwerklaag. Aangezien de firewall die binnen dit onderzoek alleen op deze twee lagen functioneert.

Nu uitgelegd is wat een firewall doet,wat er met een firewall binnen dit onderzoek bedoeld wordt en hoe apparaten met elkaar communiceren, wordt in de volgende paragraaf beschreven wat een attacktree is. De attacktree wordt in dit onderzoek gebruikt om een aanval op een firewall te beschrijven. Daarna wordt gekeken of de beschrijving van de aanval op de firewall van toegevoegde waarde is.

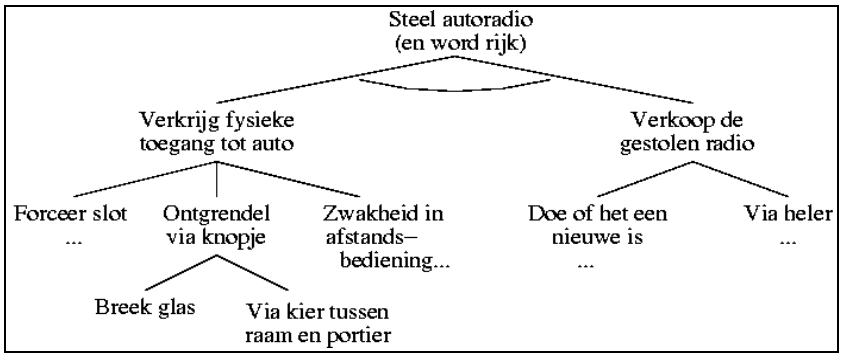
8.7 Attacktree

De attacktree methode is een nieuwe methode, die op dit moment in de beginfase van onderzoek zit. Verwacht wordt dat hiermee een tweetal problemen: het hergebruik van de risico-analyse gegevens van het risico van de mogelijke aanvallen en het versnellen van de risico-analyse, opgelost, dan wel beter onderbouwd kunnen worden.

De attacktree methode is een documenterende en gestructureerde methode om aanvallen op een beveiligde-computer-netwerk-omgeving te beschrijven. Een belangrijk punt waarop de attacktree methode verschilt met andere methoden, is dat bij de attacktree methode gekeken wordt vanuit het perspectief van de aanvaller (Mauw, 2006). Andere methoden kijken voornamelijk vanuit de defender, oftewel vanuit het perspectief van de verdediger.

Het onderzoek naar attacktrees wordt gedaan door Dr. Sjouke Mauw en Dr. Martijn Oostdijk (Mauw, 2006). Zij beschrijven de attacktree methode als volgt:

> “Een manier om de bedreigingen toch systematisch in kaart te brengen, attacktrees, werd voorgesteld door Bruce Schneier in zijn artikel uit 1999 in Dr. Dobb’s journal (Schneier, 1999). Dit formalisme werkt goed om een beeld te krijgen van de mogelijkheden van een aanvaller. Schneier kiest duidelijk voor het perspectief van de aanvaller: de aanvaller wil een bepaald doel bereiken (weergegeven in de wortel van de boom) en het doel kan op meerdere manieren bereikt worden (een nieuwe vertakking in de boom). Soms is zelfs al ongeveer duidelijk welke deeldoelen tezamen bereikt moeten worden om een doel te bereiken (een aantal “gebundelde” takken). Een voorbeeld van een eenvoudige attacktree is gegeven in Figuur 15.”(Mauw, 2006)



Figuur 15: Eenvoudige attacktree (Mauw, 2006)

De attacktree methode kan ook gebruikt worden met het perspectief van de verdediger in plaats van het perspectief van de aanvaller, zoals hierboven beschreven. Op het moment dat je het perspectief van de verdediger kiest, creëer je een defensetree, verdedigings boom, in tegenstelling tot een attacktree, aanvals boom. Binnen dit onderzoek wordt alleen gekeken naar de attacktree methode oftewel vanuit het perspectief van de aanvaller.

9 Onderzoeksmethode

Uit het vorige hoofdstuk komt naar voren dat het onderzoeken van de veiligheid van de firewall van toegevoegde waarde is voor organisaties die gebruik maken van een firewall. Dit omdat een firewall gebruikt wordt om het netwerk van bedrijven te beveiligen zonder dat het duidelijk is hoe veilig een firewall is. Zie paragraaf 3.3 (Informatiebeveiliging) voor meer informatie over het management aspect van de beveiliging. In dit deelonderzoek B wordt gekeken naar het technische veiligheidsaspect van een firewall.

Om de doelstellingen van deelonderzoek B te bereiken, deze luiden:

1. Het aanvallen van een blackbox firewall.
2. Het op een gestructureerde en documenterende methode beschrijven van de aanvallen op een blackbox firewall.
3. Het automatiseren van bovenstaande methode.
4. Het ontwerpen van een attacktree van de bovenstaande methodiek en bepalen of de attacktree methode bruikbaar is in deze context.

worden door middel van een exploratieve casestudie de onderzoeksvragen onderzocht, zoals beschreven in 7.2 (Vraagstelling). Het onderzoek is explorerend van aard. De keuze hiervoor is bewust gemaakt door de opdrachtgever Dr. Martijn Oostdijk aangezien deze een realistische / praktijk gedreven onderzoek wenste. Dit onderzoek is samen met Dr. Martijn Oostdijk en Dr. Cees-Bart Breunesse uitgevoerd.

De vraagstelling luidt:

> “Hoe kan een daadwerkelijk uitgevoerde aanval op een firewall beschreven worden op een gestructureerde en documenterende manier en is deze uitgevoerde aanval te automatiseren”

Op grond van bovenstaande vraagstelling zijn de volgende onderzoeksvragen geformuleerd:

1. Hoe kan een blackbox firewall worden aangevallen?
2. Zijn de bovenstaande aanvallen te beschrijven op een gestructureerde en documenterende manier?
3. Zijn de bij twee beschreven aanvallen op de blackbox firewall te automatiseren?
4. Is het mogelijk om een attacktree te ontwerpen op basis van de bij een uitgevoerde aanvallen.
5. Is de attacktree methode een bruikbare techniek om aanvallen op een blackbox firewall te modelleren?

Het voorgaande hoofdstuk biedt het kader waarbinnen dit deelonderzoek plaatsvindt. Om antwoord te kunnen geven op de onderzoeksvragen is in deze paragraaf uiteengezet hoe dit deelonderzoek ingevuld is. In dit hoofdstuk worden achtereenvolgens de volgende punten behandeld:

Onderzoeksaanpak: In deze paragraaf wordt de opbouw van het exploratieve deelonderzoek B onderbouwd, tevens beschrijft deze paragraaf de relatie met de onderzoeksvragen.

Representatieve firewall testomgeving: Een representatieve testomgeving is nodig om kwalitatief gefundeerde testresultaten op te kunnen leveren, daardoor is voor dit deelonderzoek een testomgeving onderzocht en gebouwd.

Tooling voor aanvallen op een firewalls: Tools zijn programma's waarmee je bepaalde, meestal zeer specialistische, handelingen kunt verrichten. Er wordt specifiek gezocht naar opensource tools die firewalls kunnen testen door middel van aanvallen op de firewall.

Beschrijving van aanvallen op een firewall: In deze paragraaf wordt een methode uitgewerkt die wordt gebruikt om de aanval te beschrijven. Tevens worden, gebruik makend van de tools die gevonden zijn bij “Tooling voor aanvallen op een firewalls”, aanvallen beschreven.

Automatisering van casestudie aanval op firewall: Hier wordt beschreven of het zinvol is om een firewall te testen door middel van het automatiseren van de bovenstaande aanvallen.

Attacktree beschrijving aanval op firewall: In deze paragraaf wordt beschreven of het maken van een attacktree van bovenstaande aanvallen van toegevoegde waarde is voor het verbeteren van de veiligheid.

Nu als eerst de opbouw van deelonderzoek B.

9.1 Onderzoeksaanpak

Het onderzoek is in te delen in de voorstudie en de empirie. In de voorstudie zitten de volgende punten:

- Representatieve firewall testomgeving
- Tooling voor aanvallen op firewalls

Deze onderzoekspunten zijn nodig, omdat voor het empirische deel een representatieve testomgeving nodig is om kwalitatief gefundeerde testresultaten op te kunnen leveren. In de empirie komen de volgende punten aan bod:

- Beschrijven van aanvallen op een firewall
- Automatiseren van casestudie aanval op firewall
- Attacktree beschrijving aanval op firewall

Aangezien de onderzoeksmethode een exploratieve casestudie betreft zullen er daadwerkelijk aanvallen op een firewall uitgevoerd dienen te worden. Om antwoord te kunnen geven op onderzoeksvraag 1 “Hoe kan een blackbox firewall worden aangevallen?”, onderzoeksvraag 2 “Zijn de bovenstaande aanvallen te beschrijven op een gestructureerde en documenterende manier?” en onderzoeksvraag 3 “Zijn de bij twee beschreven aanvallen op de blackbox firewall te automatiseren?” worden de volgende stappen uitgevoerd:

1. Het creëren van een representatieve testomgeving voor een blackbox firewall.
2. Het vinden van tooling om een blackbox firewall aan te vallen.
3. Het beschrijven van mogelijke aanvallen op de firewall van Compumatica door middel van een casestudie. Het resultaat is een verslag van de methodieken die gebruikt zijn om de firewall aan te vallen.

Het resultaat van deze stappen is:

1. Een ontworpen en gebouwde representatieve testomgeving.
2. Een beschrijving van aanvallen op een firewall in de testomgeving.

Om antwoord te kunnen geven op onderzoeksvraag 4 “Is het mogelijk om een attacktree te ontwerpen op basis van een aanvallende methodiek?” en onderzoeksvraag 5 “Is de attacktree methode een bruikbare techniek om aanvallen op een blackbox firewall te modelleren?” worden de volgende stappen ondernomen:

1. Het formaliseren van de gebruikte methodieken van de aanval op de Compumatica firewall in een attacktree samen met Dr. Martijn Oostdijk.
2. Het analyseren van de gebruikte attacktree methode op bruikbaarheid om de aanval op de firewall te beschrijven.

Het resultaat van deze stappen is:

1. Een attacktree van een aanval op de firewall van Compumatica
2. De onderbouwing dat de attacktree methode wel of niet geschikt is voor dit soort beschrijvingen.

Als eerste is onderzocht hoe een representatieve testomgeving gecreëerd wordt. Dit wordt in de volgende paragraaf uitgewerkt.

9.2 Representatieve firewall testomgeving

Een representatieve testomgeving is nodig om kwalitatief gefundeerde testresultaten op te kunnen leveren. Het ontwikkelen van een testomgeving heeft zijn beperkingen in de hoeveelheid beschikbare middelen zoals tijd, financiën, apparatuur en ruimte.

Door middel van een exploratief onderzoek, gebruik makend van kennis welke beschikbaar is op het Internet en eigen ervaringen, wordt een representatieve testomgeving opgebouwd. Deze testomgeving wordt geëvalueerd door Dr. Martijn Oostdijk en Dr. Cees-Bart Breunesse om de representatie ervan te waarborgen.

9.3 Tooling voor aanvallen op firewalls

Voor dit onderzoek wordt er gezocht naar tools, waarmee je een firewall kunt testen. Tools zijn programma's waarmee je bepaalde, meestal zeer specialistische, handelingen kunt verrichten. De letterlijke vertaling van tools is gereedschap, oftewel er wordt gezocht naar programma's die als gereedschap gebruikt kunnen worden om dit onderzoek mee te ondersteunen. Al het zoekwerk is gebeurd via het Internet. Door middel van Google en specialistische websites is naar informatie gezocht waaruit de tooling gehaald kan worden. Onder specialistische website wordt verstaan website die bekend zijn binnen het vakgebied.

9.4 Beschrijven van aanvallen op een firewall

Het aanvallen van een firewall is een exploratief proces aangezien een firewall niet op een vaste manier wordt aangevallen. Daarom is het beschrijven van de aanvallen geen eenvoudige taak. Desondanks wordt in dit verslag een methode gebruikt om de aanvallen te beschrijven.

Er zijn twee processen van belang:

- Kennisvergaring
- Aanvalproces

Als eerste kennisvergaring:

> Voordat je überhaupt een firewall aan kunt vallen, dient er informatie beschikbaar te zijn over de firewall. Vaak kan via Internet, een handleiding, speciale websites of via white-hat vrienden kennis worden opgedaan over een bepaalde firewall. Op het moment dat er geen informatie beschikbaar is, dient er op een andere manier naar informatie gezocht te worden. Aangezien dit onderzoek via een blackbox methode werkt, is het geen mogelijkheid / optie om informatie op te doen via de handleiding van het systeem, aangezien je niet weet wat voor firewall het is (zie paragraaf 8.5 (Firewall). Er mag wel gebruik gemaakt worden van andere informatiebronnen. Door middel van tooling is het mogelijk om een firewall te scannen om zodoende meer informatie te verkrijgen. Tevens dient duidelijk te zijn dat alle vormen van informatie (of juist het verkrijgen van geen informatie) de kennis over een bepaald systeem doet toenemen. Oftewel bij elke poging om informatie te krijgen wordt kennis opgedaan over het systeem. De kennis dient ook bijgehouden te worden, aangezien sommige kennis in eerste instantie helemaal niet belangrijk lijkt te zijn, terwijl het later in het aanvalproces juist wel belangrijk kan zijn.

Als tweede het aanvalproces:

> Een aanvalproces is het proces waarbij er daadwerkelijk doelgericht actie wordt ondernomen. Dit hoeft echter niet direct tot het einddoel te leiden. Een aanval kan ook een informatie scanning aanval zijn. Het verschil met het vorige proces is dat deze aanval specifiek informatie probeert te verkrijgen. Dat wil zeggen dat er naar de firewall wordt gekeken om te ontdekken wat voor systeem het is en hoe deze is geconfigureerd. Met deze kennis kan een aanvaller een volgende stap maken. Daarnaast zijn er aanvallen die daadwerkelijk bepaalde acties uitvoeren, zoals digitale informatie versturen via een firewall zonder dat dit is toegestaan. Tevens kan een cracker gebruik maken van legale communicatie methoden om beveiligde digitale informatie te versturen.

Eigenlijk is er een derde proces, te weten ”reproduceren”. Op het moment dat je kennis opdoet en een firewall aanvalt, zou het kunnen zijn dat de aanval de eerste keer direct lukt, maar alle daaropvolgende keren niet. In eerste instantie is een bepaald aanvalproces doorlopen waardoor er toegang is verkregen tot bepaalde informatie, maar zolang dat niet reproduceerbaar is, kan dit ook niet goed worden getest om zodoende te kunnen achterhalen waar de fout zit. Het is te vergelijken met een doolhof. Op het moment dat er op de juiste manier naar links en naar rechts wordt gegaan, kom je uiteindelijk bij het einde. Maar stel dat de volgorde onbekend is, dan is de kans klein dat de uitgang ook een tweede keer wordt gevonden. Het is ook mogelijk om een andere route te bewandelen dan de keer daarvoor, maar daardoor alsnog bij de uitgang te komen. Dit kan als er meerdere wegen naar de uitgang lopen.

Op welke manier zijn bovenstaande processen goed te beschrijven? Binnen het onderzoek gebeurt dit op de volgende manier. De in het vooronderzoek gevonden tools, zie sectie 10.2 (Tooling voor aanvallen op firewalls) worden gebruikt voor het handmatig testen van de firewall. Tijdens het onderzoek zijn een aantal stappen doorlopen. Stappen die tot niks leiden zijn niet verwerkt (terwijl dit terdege kennis is waarmee een andere aanvaller gestuurd kan worden). Stappen die tot nieuwe informatie of inzichten leiden zijn chronologisch verwerkt in het resultaat wat volgt in paragraaf 10.3 (Beschrijving aanval op een firewall).

Aangezien er bij een aanvalsproces veel alternatieve processen beschikbaar zijn, worden er in de 'grijze' blokken gedachtegangen / opmerkingen en constateringen beschreven, die nader onderzoek behoeven, maar in dit onderzoek niet nader worden uitgewerkt. Oftewel niet compleet uitgewerkte aanvallen, maar ideeën van mogelijke andere aanvalspaden.

Wat wordt er precies onderzocht? Ondanks het feit dat het makkelijk is om verder te kijken dan alleen de firewall, worden hier nog eens een aantal punten uitgesloten van onderzoek.

- Er wordt niet gekeken naar hoe er toegang gekregen kan worden tot de configuratie interface.
- Er wordt niet gekeken naar wat achter de firewall staat. Zoals overige systeemelementen.
- Fouten in de configuratie van een firewall worden niet besproken. Op het moment dat er door een fout in de configuratie een firewall openstaat, dan functioneert een firewall naar behoren, maar een aanvaller kan alsnog naar binnen komen.

Nu het duidelijk is hoe het onderzoek ontworpen en ingekaderd is, wordt in de volgende paragraaf bekeken hoe de aanval beschrijving in een attacktree gezet kan worden.

9.5 Automatiseren van casestudie aanval op firewall

In deze paragraaf wordt beschreven welke methodes er gebruikt worden om te kijken of de aanvallen beschreven in paragraaf 10.3 (Beschrijving aanval op een firewall) te automatiseren zijn.

Aan de hand van de gevonden aanvallen wordt geanalyseerd of de gevonden en gebruikte tools te automatiseren zijn. Tevens wordt naar het tijdaspect gekeken. Met andere woorden er wordt gekeken of aan de hand van de configuratie, de resultaten van de gebruikte tooling en de aanvallen zelf het mogelijk is om bepaalde aspecten van de aanval te automatiseren.

9.6 Attacktree beschrijving aanval op firewall

In deze paragraaf wordt beschreven of de attacktree methode een methode is die te gebruiken is om een aanval op een firewall te modelleren. Gebruik makend van de resultaten van het onderzoek, zie paragraaf 10.3 (Beschrijving aanval op een firewall), wordt een attacktree gemodelleerd.

Samen met Dr. Martijn Oostdijk wordt een attacktree ontwikkeld. Dr. Martijn Oostdijk geeft voornamelijk input op het gebied van de attacktree. Daarnaast worden de resultaten uit de beschrijving van de aanval op de firewall gebruikt als input voor de attacktree. Deze samenwerking heeft als voordeel dat de attacktree door twee personen bekeken wordt en er feedback gegeven kan worden. Tevens kunnen eventuele problemen met betrekking tot de opbouw snel worden opgelost.

Het resultaat is een attacktree van een aanval op de firewall van Compumatica en de onderbouwing dat de attacktree methode wel of niet geschikt is voor dit soort beschrijvingen.

10 Resultaten

In het vorige hoofdstuk is de onderzoeksmethode van dit onderzoek beschreven. In dit hoofdstuk bevinden zich de resultaten die uit deelonderzoek B naar voren gekomen zijn. De volgende resultaten worden achtereenvolgens behandeld:

Voorstudie:

- Representatieve firewall testomgeving
- Tooling voor aanvallen op firewalls

Empirie:

- Beschrijving aanval op een firewall
- Automatiseren van casestudie aanval op firewall
- Attacktree van bovenstaande aanvallen op firewall

10.1 Representatieve firewall testomgeving

Voor het onderzoek naar het vinden van fouten in een firewall is een omgeving nodig om de aanvallen te kunnen uitvoeren. De keuze is gemaakt om een testomgeving te bouwen en niet een firewall in een operationele omgeving te plaatsen. Dit heeft als voordeel dat, bij het uitvoeren van de aanvallen op de firewall, de rest van de organisatie er geen last van heeft. Daarnaast is er geen last van “ruis” vanuit de organisatie die de testresultaten kan beïnvloeden. Tevens kunnen in de testomgeving op verschillende plekken sensoren worden aangebracht om het verloop van de test te kunnen monitoren. Dit dient gedaan te worden om:

1. Als er fouten gevonden worden, de test en dus ook de fouten te kunnen reproduceren.
2. Te controleren of de test doet wat deze behoort te doen.
3. De teststappen later te kunnen traceren.

Binnen dit onderzoek wordt gebruik gemaakt van een representatieve testomgeving. Direct volgt de vraag wat een representatieve testomgeving is. Zoals geen enkele organisatie hetzelfde is, zijn een firewall en netwerkconfiguratie van een organisatie ook niet gelijk. Daarom wordt een selectie gemaakt van de meest gebruikte protocollen, zoals email, webservers en VPN (Virtual Private Network) oplossingen, die organisaties gebruiken.

Tevens is er een beperking van het budget en de beschikbare tijd om een testomgeving op te zetten en te testen. Ook dient de testomgeving dusdanig opgesteld te zijn, dat er een willekeurige firewall getest kan worden. In dit onderzoek wordt alleen naar de Compumatica firewall gekeken.

In de volgende alinea's wordt beschreven wat binnen de testomgeving wordt aangenomen en waar binnen dit onderzoek niet naar gekeken wordt.

Afkadering firewall testomgeving

De volgende aannames worden binnen dit onderzoek gebruikt:

1. Naïeve gebruikers maken gebruik van een standaard set software welke aangeleverd wordt door een systeembeheerder. Met naïeve gebruikers worden personen bedoeld die normaal gebruik maken van een computersysteem, zonder interesses en capaciteiten om zich in de materie te verdiepen. Hiermee worden dus gebruikers bedoeld die standaard op "ok" klikken op het moment dat er een waarschuwing komt. Meestal omdat ze niet begrijpen waar de waarschuwing op slaat. Deze naïeve gebruikers hebben niet de intentie om het netwerk aan te vallen.

2. De firewall wordt als een blackbox benaderd. Met de blackbox benadering wordt in dit onderzoek bedoeld dat er niet specifiek naar de firewall zelf gekeken wordt. Er worden alleen op afstand testen op de firewall gedaan. De reden hiertoe is dat de aanvallers één en dezelfde perceptie hebben. Indien er toch informatie vanuit de firewall gegenereerd wordt, zoals output op het console scherm van de firewall, zal deze niet gebruikt worden binnen dit onderzoek. Zie paragraaf 8.5 (Firewall) voor meer informatie.

3. Er worden geen specifieke eisen gesteld aan de hardware en de software van de cliënts. De cliënts zijn de gebruikers van het netwerk en dus ook de firewall. Er wordt vanuit gegaan dat er aan de netwerk-standaarden wordt voldaan. In dit onderzoek worden het TCP / IP referentiemodel, dat is gedefinieerd in RFC 791 en het User Datagram Protocol (UDP), welke is gedefinieerd in RFC 768 als netwerk-standaard gebruikt.

4. Een aanvaller mag alles doen wat binnen zijn mogelijkheden ligt. Een aanvaller mag bijvoorbeeld "gecrippelde" pakketten versturen naar de firewall. Met gecrippelde pakketten worden IP pakketten bedoeld die niet hoeven te voldoen aan de IP specificaties die gespecificeerd zijn in RFC 791. Met andere woorden stel dat volgens de RFC de pakketten een waarde van 0 tot 10 mag bevatten. Aan een pakketje wordt vervolgens de waarde 11 toegekend. Dit pakketje voldoet niet aan de RFC, maar hoe reageert de software op deze niet gedefinieerde waarde.

De volgende onderwerpen worden uitgesloten van onderzoek:

1. De applicatie-protocol niveaus.

2. Het testen van de stabiliteit van de firewall. Mocht de firewall ophouden met functioneren, dan wordt dit als fout aangezien.

3. Er wordt niet naar de performance van de firewall gekeken . Echter wanneer de performance dusdanig laag wordt dat dit problemen veroorzaakt met de verbinding, dan wordt dit als fout gekenmerkt.

Nu er gekeken is naar de aannames en de uitsluitingen, wordt in de volgende alinea de testomgeving beschreven.

De testomgeving

De volgende onderwerpen worden behandeld om ervoor te zorgen dat de testomgeving voldoet aan de opgestelde criteria voor een representatieve testomgeving:

1. Hardware testomgeving.
2. Operatingsysteem testomgeving.
3. Configuratie van de firewall voor de testomgeving.

Gezien de financiële- en de tijdbeperking is er gekozen voor hardware en software welke binnen de organisatie (Radboud Universiteit) aanwezig zijn. Enkele kleine hardware onderdelen zijn bijbesteld om de testomgeving compleet te maken.

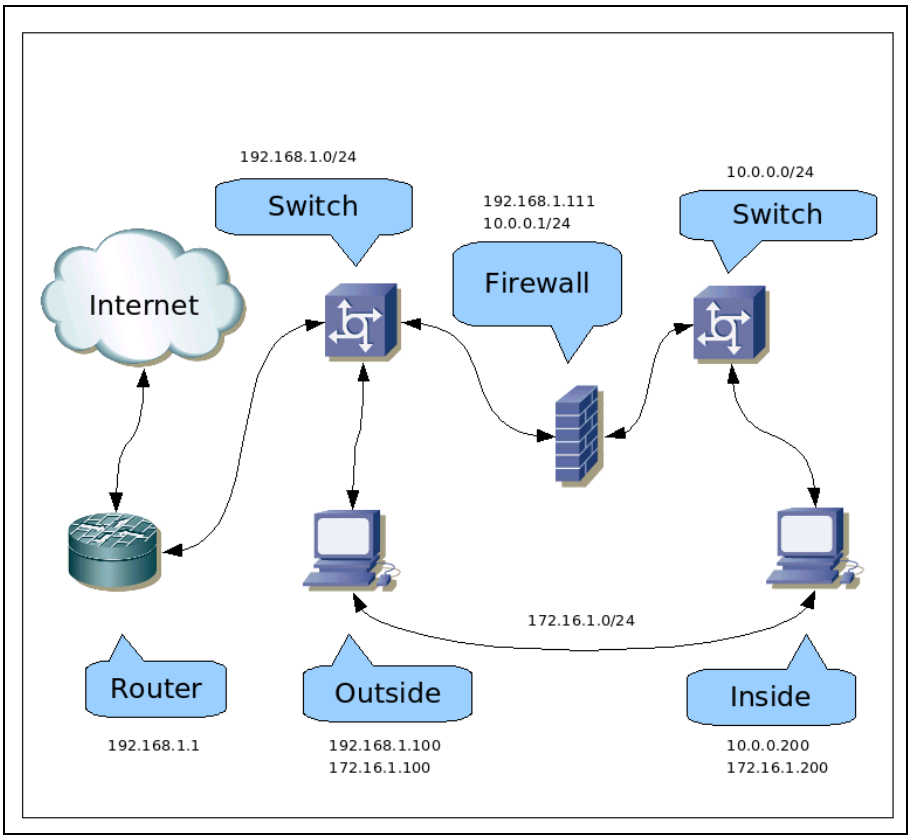
In het volgende deel wordt uitgewerkt hoe de testomgeving is opgebouwd. Als eerst wordt beschreven hoe de testomgeving in hardware eruit ziet en welke keuzes er gemaakt zijn.

Hardware

Wegens de beschikbare middelen is ervoor gekozen om de testomgeving uit de volgende onderdelen op te bouwen:

- *Tweetal standaard computers:* Dit zijn standaard Intel computers met ieder twee netwerk kaarten.
- *Een Firewall:* In deze testopstelling wordt de Compumatica Firewall gebruikt.
- *Tweetal switches:* Een switch is een apparaat waarmee een netwerk gecreëerd kan worden. Hiermee wordt gezorgd dat de computers en de firewall met elkaar kunnen communiceren (Kurose, e.a. 2001).
- *Een router:* Een router is een apparaat dat er voor zorgt dat het afgeschermde netwerk van de buitenkant te benaderen is (Kurose, e.a. 2001)(Baas e.a., 1997).
- *Cross cable:* Deze kabel is gebruikt zodat er geen switch nodig is voor het netwerk tussen de twee computersystemen. Aangezien deze verbinding alleen gebruikt wordt voor het monitoren van de testomgeving en deze verbinding geen onderdeel is van het 'normale' testnetwerk is om budgettaire redenen hier geen switch geplaatst.

In Figuur 16 is getekend hoe de testomgeving is opgebouwd.



Figuur 16: Testconfiguratie (Berlijn, 2007)

De router wordt voor een tweetal doeleinden gebruikt:

1. Om toegang te krijgen tot de testsystemen vanuit andere locaties. Hierdoor is het mogelijk om vanaf andere werkplekken de progressie van bepaalde aanvallen te kunnen volgen.

2. Het afschermen van het lokale netwerk van de testomgeving en vice versa.

De extra verbinding waar het 172.16.1.0/24 netwerk over loopt, wordt gebruikt om vanuit het outside systeem het inside systeem te kunnen controleren. Er dient wel rekening mee gehouden te worden dat bij bepaalde aanvallen deze verbinding een valse fout vindt.

Tevens is er gekozen om alleen gebruik te maken van non-routable IP-nummers om netwerkproblemen naar buiten te voorkomen. Non-routable IP-nummers zijn IP-nummers die niet op het internet worden gebruikt.

De onderstaande configuratie is gebruikt:

Alle IP's hebben hun eigen interface en zijn als volgt verdeeld:

Systeem	***IP***	***Netwerk***	***Beschrijving***
Outside	192.168.1.100 172.168.1.100	Switch 1 Cross	Representeert 'het Internet' / het onveilige netwerk

Systeem	*IP*	*Netwerk*	*Beschrijving*
Inside	10.0.0.200 172.168.1.200	Switch II Cross	Representeert het organisatienetwerk
Firewall	192.168.1.111 10.0.0.1	Switch I Switch II	Representeert de firewall
Router	192.168.1.1 Externe IP	Switch I Externe switch	De router heeft IP op het interne onveilige netwerkdeel. Het echte internetadres wordt automatisch verkregen. De router verzorgt ook de internetconnectiviteit.

De routering is als volgt verdeeld:

Systeem	*default gateway*	*netwerk*	*gateway*
Outside	192.168.1.1	10.0.0.0/24	192.168.1.100
Inside	10.0.0.1		
Firewall	192.168.1.1		
Router	Externe IP		

De netwerken zijn als volgt verdeeld:

Netwerk	*IP Range*
insidenet	10.0.0.0/24
testnet	172.16.1.0/24
outsidenet	192.168.1.0/24

Nu duidelijk is hoe de testomgeving is opgebouwd, wordt in de volgende alinea's beschreven welk operatingsysteem gebruikt is in deze testomgeving.

Operatingsysteem testomgeving

Het operatingsysteem dient aan de volgende eisen te voldoen om goed aan te sluiten bij de testomgeving:

1. Er dienen tools beschikbaar te zijn waarmee low level netwerk data geanalyseerd kan worden.
2. Er dient een ontwikkelomgeving op te staan om eventueel eigen tools te ontwikkelen of bestaande tools uit te breiden.
3. De kosten dienen geminimaliseerd te worden voor de aanschaf van het operatingsysteem.
4. De mensen die gaan testen dienen bekend te zijn met het operatingsysteem.
5. Het operatingsysteem dient makkelijk en met zo min mogelijk inspanning geïnstalleerd en onderhouden te kunnen worden.

Vanuit de eerste drie punten is af te leiden dat de keuze zou vallen op een opensource operating systeem zoals FreeBSD, OpenBSD en Linux. Aangezien deze operatingsystemen aan deze punten voldoen:

1. De volgende tools zijn beschikbaar om low level netwerk data te analyseren:
    1. tcpdump[24], tcpdump wordt gebruikt op unix om het netwerkverkeer te monitoren.
    2. wireshark[25] wireshark is een network protocol analyzer. Een network protocol analyzer is een programma dat op bit niveau netwerk pakketjes kan analyseren.
2. Op alle platformen draait GCC als ontwikkel-omgeving.
3. Kosteloos te gebruiken en te downloaden.
4. Via internet te updaten.

De personen die gebruik maakte van de testopstelling hadden geen voorkeur voor: FreeBSD, OpenBSD en Linux. Aangezien ze met alle besturingssystemen konden werken.. Hiermee is ook aan punt vier voldaan.

Uiteindelijk is de keuze gevallen op Ubuntu versie 6.06 LTS. De reden hiervoor is dat deze Linux distributie vrij beschikbaar en net gereleased is. Tevens is deze versie, de LTS versie wat staat voor Long Term Support, een versie waarbij voor minimaal drie jaar support is. Dat wil zeggen dat er updates en security updates voor de release gemaakt worden. Tevens is Ubuntu 6.06 LTS gebaseerd op een andere bekende distributie, Debian genaamd. Debian staat bekend als stabiele release, maar daardoor zijn ze traag met releasen, oftewel de laatste recente stabiele versie van Debian is al een paar jaar oud. De ontwikkeling van Ubuntu, specifiek de packages die meegeleverd worden, gaat daarentegen sneller. Oftewel er is een

24 Zie http://www.tcpdump.org/ voor meer informatie.
25 Zie http://www.wireshark.org/ voor meer informatie.

stabiele basis waarop nieuwe software geïnstalleerd is. Daarnaast is Ubuntu 6.06 LTS eenvoudig te installeren en de testers zijn bekend met dit systeem.

Nu bekend is waarom er voor Ubuntu 6.06 LTS is gekozen, volgt hoe een firewall geconfigureerd dient te worden.

Configuratie van de firewall voor de testomgeving

Er is geen standaard manier om een firewall te configureren. Er zijn wel standaard modellen hoe een firewall geconfigureerd kan worden. Deze modellen zijn afhankelijk van hoe het netwerk in elkaar zit. Bijvoorbeeld of er wel of niet een demilitarized zone (DMZ) in het netwerk gerealiseerd moet worden. Een DMZ is een gedeelte van het netwerk dat zowel voor het externe netwerk, het Internet, als het interne netwerk, het organisatie netwerk, toegankelijk is (WWW-24). In de DMZ staan systemen die diensten verlenen voor zowel het interne- als het externe netwerk. Deze diensten kunnen e-mail, (secure) webserver of VPN diensten zijn. Deze standaard modellen worden altijd aangepast aan de verwachtte functionaliteit en de opbouw van het netwerk. Juist omdat er geen standaard manier is om een firewall te configureren, rijst de vraag “Hoe wordt een representatieve testopstelling gemaakt?”.

In dit onderzoek wordt de firewall met een 'standaard' model geconfigureerd. Ondanks dat er geen standaard bestaat, wordt er een minimalistische configuratie gemaakt die hoogstwaarschijnlijk bij alle configuratie gebruikt wordt. Dit wil zeggen dat de meest eenvoudige testomgeving gemaakt wordt, waarbij de basis functionaliteit van de firewall getest kan worden.

Als eerste de verbindingen in de testomgeving. Deze bestaan uit een tweetal netwerken: het interne- en het externe netwerk. Er wordt vanuit gegaan dat het interne netwerk met het externe netwerk mag communiceren, zonder enige beperkingen. Het externe netwerk mag daarentegen alleen maar via een bepaald aantal protocollen communiceren. Deze protocollen zijn:

- E-mail, SMTP (Simple Mail Transfer Protocol) poort 25
- Webserver, HTTP (HyperText Transfer Protocol) poort 80
- Secure Webserver, SSL (Secure Sockets Layer) + HTTP poort 443
- OpenVPN, OpenVPN (Virtual Private Network) poort 1194

Respectievelijk werken deze protocollen op de volgende standaard TCP poorten: 25, 80, 443 en 1194. Deze beperkingen worden door de firewall afgedwongen. Voor sommige testen wordt er gekozen om de firewall geheel dicht te zetten. Hiermee wordt bedoeld dat er geen verkeer tussen outside en inside meer mogelijk is. Dit vergemakkelijkt het verkrijgen van de testresultaten aangezien elk pakketje wat bij het testsysteem inside aankomt, door de firewall wordt doorgelaten. Oftewel dat betekent dat de firewall dan niet goed functioneert.

Er zijn ook nadelen van de gebruikte testomgeving. Deze nadelen zijn in de volgende sectie beschreven.

Nadelen testomgeving

Bij het testen van de firewall wordt gebruik gemaakt van voor geconfigureerde IP-nummers. Dit wil zeggen dat in de testen alleen gebruik gemaakt wordt van het 10.0.0.0/24 netwerk en het 192.168.1.0/24 netwerk. Bij een normale operatie van een firewall, mits deze is aangesloten op het Internet, kunnen de mogelijke source IP-adressen uit een willekeurig IP-adres bestaan. Het blijkt dat in deze test, fouten die ontstaan door het foutief behandelden van het source adres, niet worden opgevangen. Bijvoorbeeld de testen werken perfect met de IP-range 10.0.0.0/24, maar werken totaal niet met IP-range 195.234.100.0/24.

Er is echter een uitzondering. Sommige testen gebruiken een 'faked' IP-adres. Deze testen zullen wel gebruik maken van echte IP's. Echter deze testen zullen nooit compleet zijn, aangezien het testen van alle IP-nummers een tijdrovende aangelegenheid is. Stel je wilt alle source IP-testen, dan dien je 2^{32}=4.294.967.296 keer de test te draaien. Stel dat een test gemiddeld genomen 1 seconde duurt dan heb je maximaal 4.294.967.296 seconden nodig om een fout te vinden. Oftewel:

- 4.294.967.296/60=71582788,27 Minuten
- 71582788,27/60=1193046,47 Uur
- 1193046,47/24=49710,27 Dagen
- 49710,27/365=136,19 Jaar

Ondanks dat er geprobeerd wordt de test te versnellen of meerdere installaties te gebruiken, vergt het testen veel tijd. Er wordt voor dit onderdeel veelal een deelset getest. De volledigheid / compleetheid van een test is hiermee moeilijker te garanderen. Het eindresultaat is hierdoor niet compleet.

Tevens wordt in de testopstelling geen gebruik gemaakt van een applicatie die UDP nodig heeft om te communiceren. Hiertoe is besloten om het onderzoek sterker in te kaderen, zodat het binnen de beschikbare tijd haalbaar was. De keuze om TCP te gebruiken is gemaakt, aangezien de meeste gebruikte protocollen over TCP draaien.

Wat is fout en wat is goed?

Zoals in de bovenstaande alinea's is beschreven, is een firewall configuratie niet standaard. Op het moment dat je een firewall gaat testen dien je eigenlijk elke mogelijke combinatie van configuratie opties te testen om een complete test te verkrijgen. Dit is door de bijna oneindige mogelijkheden aan combinaties onmogelijk. Daarom kan alleen een gedeelte van de functionaliteit getest worden. Dit betekent dat als er iets gevonden wordt, dat er iets fout zit. Maar dat sluit niet uit dat als er niets gevonden wordt, er geen fouten in zitten.

In dit onderzoek definiëren we 'goed' als volgt:

- Alle communicatie die toegestaan is, moet zonder problemen werken.
- Alle communicatie die expliciet **niet** is toegestaan, mag niet werken. Hiermee wordt bedoeld dat na de firewall, in de beschermde zone, geen enkel effect zichtbaar mag zijn van de niet toegestane verbinding. In de onbeschermde zone dient de niet toegestane verbinding volgens de regels verbroken (deny) of genegeerd (drop) te worden.

En 'fout' definiëren we als:

- Als communicatie die niet gespecificeerd is, wel werkt of andere niet gedefinieerde effecten teweeg brengt.
- Als de toegestane gespecificeerde communicatie met problemen werkt. Hiermee wordt bedoeld als de communicatie anders functioneert dan wanneer er geen firewall tussen de twee systemen staat.

10.2 Tooling voor aanvallen op firewalls

Voor dit onderzoek wordt er gezocht naar tooling, waarmee je een firewall kunt testen. Om de zoektocht eenvoudiger te maken wordt het zoekgebied in drie deelgebieden opgesplitst (Berlijn, 2007). Deze opsplitsing is gemaakt om duidelijk weer te geven welke functionaliteit een bepaalde tool heeft.

1. *Informatie vergaring (Information gathering) tools*: Dit zijn tools die expliciet bedoeld zijn om informatie te verzamelen. Binnen dit onderzoek is gekeken naar tools die informatie kunnen verzamelen over de functionaliteit van een firewall.
2. *Testing tools:* Testing tools vallen gedeeltelijk onder de informatie vergaring tools aangezien door gebruik te maken van deze tools er informatie vergaard wordt. Deze groep heeft echter het specifieke doel om bepaalde onderdelen, van bijvoorbeeld een firewall, te testen.
3. *Hacking tools:* Met deze selectie van tools worden tools bedoeld waarmee er daadwerkelijk digitale informatie verzonden kan worden. Deze tools kunnen ingezet worden nadat er kennis is opgedaan na het gebruik van informatie vergaring en testing tools.

Sommige tools zijn een combinatie van deze deelgebieden. De reden waarom er gezocht wordt naar tooling, is dat er te weinig tijd beschikbaar is om zelf tools te schrijven. Er wordt, net als bij de operating systemen, gezocht in het opensource domein, aangezien er geen budget is om eventuele commerciële tools aan te schaffen. Gezien de aard van dit onderzoek heeft dit geen negatieve gevolgen op het eindresultaat. De meeste commerciële tools zijn rapportage systemen, die vaak gebouwd zijn op al bestaande opensource tools, zoals bijvoorbeeld snort[26].

Het onderzoek naar geschikte tooling heeft de onderstaande tools opgeleverd:

1. nmap (NetworkMAPer)
2. pingtunnel
3. ftester (Firewall tester)
4. ISIC (IP Stack Integrity Checker)

Nmap is een tool die puur bedoeld is om informatie te vergaren. Pingtunnel daarentegen is een tool die bedoeld is om te hacken. Zowel ftester en ISIC zijn tools die bedoeld zijn om te testen.

26 Voor meer informatie zie: http://www.snort.org/

Tevens heeft Dr. Cees-Bart Breunesse nog enkele dagen gezocht naar alternatieve tools, maar deze niet gevonden.

De geschikt bevonden tools worden achtereenvolgens beschreven, te beginnen bij de nmap tool.

Nmap (NetworkMAPer)

Nmap[27] is een zeer populaire en vaak gebruikte netwerk security en auditing tool. De nmap tool is voornamelijk bedoeld om informatie te winnen over een netwerk of bepaald systeem. De software kan computersystemen en netwerken scannen om te zien welke poorten op welke systemen open staan. Dit scannen gebeurt door middel van ruwe IP-pakketten. Dit wil zeggen IP-pakketten die op bit niveau worden aangepast en niet door de IP-stack van het systeem waar het nmap programma op draait. Tevens kan afhankelijk van de open poort bepaald worden welke applicaties er worden gebruikt (WWW-25). Door middel van deze technologie bepaald nmap welke systemen er beschikbaar zijn op het netwerk, welke services deze beschikbaar hebben (applicatie en versie) en wat voor operatingsysteem er wordt gebruikt. Ook kan nmap bepalen wat voor type firewall / packetfilters er gebruikt worden.

Gezien de hoeveelheid technieken die nmap gebruikt, zoals beschreven in “The Art of Port Scanning” by Fyodor de maker van nmap, is de output ingewikkeld te interpreteren (WWW-25). Dat wil zeggen dat de output van het programma niet gemakkelijk te begrijpen is.

Ftester (Firewall tester)

Ftester is een programma dat ontwikkeld is om firewall policies en Intrusion Detection Systemen (IDS) te testen[28]. Ftester bestaat uit een cliënt en een server. De cliënt probeert constant verbinding te zoeken met de server. Op het moment dat een verbinding succesvol is, wordt deze verbinding door de server gelogd. Dat wil zeggen dat elke gemaakte verbinding door de server in een log file wordt opgeslagen. Door middel van een bijgeleverde tool kunnen de logfiles van de cliënt evenals van de server met elkaar vergeleken worden, zodat een rapport opgesteld kan worden.

Pingtunnel

Een pingtunnel is een applicatie welke in staat is een betrouwbare TCP verbinding op te bouwen van een cliënt naar een server, gebruik makend van ICMP echo request en ICMP replay datagrammen[29]. De ICMP datagrammen worden gebruikt door het ping programma om ping requests en replies te ontvangen.

ISIC (IP Stack Integrity Checker)

De IP Stack Integrity Checker[30] (ISIC) is een pakket van programma's die de stabiliteit van een IP-stack kunnen testen. Dit gebeurt door middel van het genereren van pseudo random datagrammen die het target protocol op mogelijke fouten testen. Deze datagrammen worden

27 Voor meer informatie zie: http://www.insecure.org/nmap/
28 Voor meer informatie zie: http://dev.inversepath.com/trac/ftester/
29 Voor meer informatie zie: http://www.cs.uit.no/~daniels/PingTunnel/
30 Voor meer informatie zie: http://www.packetfactory.net/projects/ISIC/

vervolgens verstuurd naar een doel-systeem, daar worden deze pseudo random datagrammen, de IP-stacks van de firewall, en indirect ook het doelsysteem, getest.

Een voorbeeld van een andere tool, die niet gebruikt is in deze test is Fragroute.

Fragroute

Deze tool is laat tijdens het onderzoek gevonden, te laat om nog effectief een test mee te doen, maar deze tool is interessant genoeg om hier te vermelden.

Flagroute[31] onderschept, verandert en herschrijft egress verkeer. Dit zijn datagrammen die van buiten het netwerk naar het interne netwerk gaan, voor een gespecificeerd doelsysteem.

Flagroute gebruikt de meeste aanvallen zoals beschreven in Secure Networks "Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection" (WWW-26).

10.3 Beschrijving aanval op een firewall

In deze paragraaf wordt beschreven hoe het onderzoek naar mogelijke aanvallen op een blackbox firewall verlopen is. Een van de doelstellingen is: “Het op een gestructureerde en documenterende manier testen van een blackbox firewall met een aanvallende methodiek”. Door middel van een verslag van de onderzoekspogingen en de genomen beslissingen wordt geprobeerd om een gestructureerde methodiek te ontwikkelen. Door gebruik te maken van de bovenstaande testopstelling, zie paragraaf 10.1 (Representatieve firewall testomgeving), wordt verwacht dat er een voordeel is ten opzichte van een echte cracker, dit aangezien je alles onder controle hebt en weet dat er een aanval aankomt. Oftewel je bent er op voorbereid. Voor eigen 'home made' applicaties is dit het geval, maar de meeste firewalls worden commercieel verkocht. Een cracker kan dus ook beschikken over een eigen testomgeving. De cracker is mogelijk in het voordeel aangezien hij een groter budget en meer mogelijkheden tot zijn beschikking heeft, want hij verkrijgt misschien op een minder legale manier zijn middelen. Tevens heeft een cracker veelal meer tijd ter beschikking. Dit is een voordeel aangezien onderzoekers beperkt zijn met hun beschikbare tijd gezien de beperking in het budget.

Kennisvergaring

De eerste vraag is: “Wat te doen om een aanval uit te voeren op een firewall?” Het eerste wat gedaan kan worden is het verzamelen van informatie. Want de welbekende uitspraak “Kennis is macht!” geldt ook hier (WWW-27). Er wordt geprobeerd zoveel mogelijk informatie te verzamelen. Met name informatie die antwoord kan geven op vragen zoals:

1. Wat voor systeem probeer je aan te vallen?
2. Welk(e) software / besturingsysteem wordt gebruikt?
3. Wat voor hardware wordt gebruikt?

Vervolgens is de vraag, “Wat kunnen we met dit soort kennis?” Op het Internet zijn verschillende sites te vinden, die zich bezighouden met het onderzoeken en het publiceren

31 Voor meer informatie zie: http://monkey.org/~dugsong/fragroute/

van kennis over hoe systemen gehacked kunnen worden. Met andere woorden de white-hats wisselen hun kennis met elkaar uit, aangezien de complexiteit van de aanvallen steeds groter wordt. Tevens bestaat het vermoeden dat er een underground (The Black hat community) is waar dit soort kennis ook gedeeld wordt.

Bekende informatieve sites zijn:

- http://www.microsoft.com/technet/security/advisory/default.mspx
- http://www.linuxsecurity.com/
- http://msgs.securepoint.com/bugtraq/
- http://www.securityfocus.com/
- http://www.metasploit.com/
- http://sectools.org/
- http://www.cert.org/

Er is ook een Nederlandstalig site beschikbaar:

- http://www.security.nl/

Kennis wordt vergaard door middel van tooling, die gebruikt kan worden om informatie over een onbekend systeem te verkrijgen. Nmap is een tool die hier veel voor wordt gebruikt. Ook binnen dit onderzoek wordt nmap gebruikt om gegevens over een systeem te verzamelen. Hieronder wordt uitgelegd hoe dit gebeurd.

Nmap

Nmap is zoals eerder beschreven in paragraaf 10.2 (Tooling voor aanvallen op firewalls) een netwerk security en auditing tool. Nmap kan computersystemen en netwerken scannen om te zien welke poorten op welke systemen open staan.

Testomgeving nmap

Op de outside wordt nmap geïnstalleerd. Verder wordt er gebruik gemaakt van de beschreven testconfiguratie, zie paragraaf 10.1 (Representatieve firewall testomgeving).

Configuratie nmap

Voor nmap dient verder geen configuratie gegeven te worden. Alles wordt aangestuurd via commandline opties. Bij elk uitgevoerde nmap commando wordt de gebruikte commandline optie beschreven.

Resultaat nmap

In het onderstaande kader staat de output van het nmap programma welke op de firewall

gedraaid is.

```
jasper@outside:~$ sudo nmap -A 192.168.1.111
Password:

Starting Nmap 4.03 (http://www.insecure.org/nmap/) at 2006-08-04 18:53 CEST
Interesting ports on 192.168.1.111:
(The 1670 ports scanned but not shown below are in state: closed)
PORT STATE SERVICE VERSION
11/tcp open systat?
22/tcp open ssh OpenSSH 4.1 (protocol 2.0)
59/tcp open ssl/unknown
87/tcp open priv-term-l?
1 service unrecognized despite returning data. If you know the
service/version, please submit the following fingerprint at
http://www.insecure.org/cgi-bin/servicefp-submit.
cgi :
SF-Port11-TCP:V=4.03%I=7%D=8/4%Time=44D37B7F%P=i686-pc-linux-gnu%r(NULL,27
SF:97,"Date\x20\+\x20Time\t\tText\n\r\n04\.08\.2006\x2018:13:29\.10\tctrld
SF::\x20\x200\x200\r\n04\.08\.2006\x2018:14:00\.14\tctrld:\x203\x202\x200\
SF:.03\x2014\.53\x200\.00\x200\x200\x200\.00\x200\.00\x200\.00\x2035\x200\
SF:x200\x200\x200\x200\x200\x200\x202455290\x2097380\x201828\x201837\x200\
SF:x20108\x203032\x203040\x200\x200\x200\x200\x200\x202421834\x20392449594
SF:4\x2075199\x206159149\x200\x201\x200\x200\x200\x200\x200\x202\x2080886\
SF:x206898490\x2069595\x205512990\x200\x203\x200\x200\x200\x200\x200\r\n04
SF:\.08\.2006\x2018:14:31\.16\tctrld:\x203\x202\x200\.03\x2014\.53\x200\.0
SF:0\x200\x200\x200\.00\x200\.00\x200\.00\x2035\x200\x200\x200\x200\x200\x
SF:200\x200\x202455296\x2097386\x201828\x201837\x200\x20108\x203032\x20304
SF:0\x200\x200\x200\x200\x200\x202421839\x203924496358\x2075204\x206159527
SF:\x200\x201\x200\x200\x200\x200\x200\x202\x2080891\x206898904\x2069600\x
SF:205513368\x200\x203\x200\x200\x200\x200\x200\r\n04\.08\.2006\x2018:15:0
SF:2\.18\tctrld:\x203\x202\x200\.03\x2014\.55\x200\.00\x200\x200\x200\.00\
SF:x200\.00\x200\.00\x2035\x200\x200\x200\x200\x200\x200\x200\x202455302\x
SF:2097392\x201828\x201837\x200\x20108\x203032\x203040\x200\x200\x200\x200
SF:\x200\x202421844\x203924496772\x2075209\x206159905\x200\x201\x200\x200\
SF:x200\x200\x200\x202\x2080895\x206899258\x2069604\x205513704\x200\x203\x
SF:200\x200\x200\x200\x200\r\n04\.08\.2006\x2018:15:21\.18\tctrld:\x20The\
SF:x20Licence\x20is\x20expired!\r\n04\.08\.2006\x2018:15:21\.18\tctrld:\x2
SF:0Wrong\x20Licence\x20for\x20this\x20computer!\r\n04\.08\.2006\x2018:15:
SF:21\.18\tctrld:\x20Software\x20li")%r(GenericLines,C841,"Date\x20\+\x20T
SF:ime\t\tText\n\r\n04\.08\.2006\x2018:13:29\.10\tctrld:\x20\x200\x200\r\n
SF:04\.08\.2006\x2018:14:00\.14\tctrld:\x203\x202\x200\.03\x2014\.53\x200\
SF:.00\x200\x200\x200\.00\x200\.00\x200\.00\x2035\x200\x200\x200\x200\x200
SF:\x200\x200\x202455290\x2097380\x201828\x201837\x200\x20108\x203032\x203
SF:040\x200\x200\x200\x200\x200\x202421834\x203924495944\x2075199\x2061591
SF:49\x200\x201\x200\x200\x200\x200\x200\x202\x2080886\x206898490\x2069595
SF:\x205512990\x200\x203\x200\x200\x200\x200\x200\r\n04\.08\.2006\x2018:14
SF::31\.16\tctrld:\x203\x202\x200\.03\x2014\.53\x200\.00\x200\x200\x200\.0
SF:0\x200\.00\x200\.00\x2035\x200\x200\x200\x200\x200\x200\x200\x202455296
SF:\x2097386\x201828\x201837\x200\x20108\x203032\x203040\x200\x200\x200\x2
SF:00\x200\x202421839\x203924496358\x2075204\x206159527\x200\x201\x200\x20
SF:0\x200\x200\x200\x202\x2080891\x206898904\x2069600\x205513368\x200\x203
SF:\x200\x200\x200\x200\x200\r\n04\.08\.2006\x2018:15:02\.18\tctrld:\x203\
SF:x202\x200\.03\x2014\.55\x200\.00\x200\x200\x200\.00\x200\.00\x200\.00\x
SF:2035\x200\x200\x200\x200\x200\x200\x200\x202455302\x2097392\x201828\x20
SF:1837\x200\x20108\x203032\x203040\x200\x200\x200\x200\x200\x202421844\x2
SF:03924496772\x2075209\x206159905\x200\x201\x200\x200\x200\x200\x200\x202
SF:\x2080895\x206899258\x2069604\x205513704\x200\x203\x200\x200\x200\x200\
SF:x200\r\n04\.08\.2006\x2018:15:21\.18\tctrld:\x20The\x20Licence\x20is\x2
SF:0expired!\r\n04\.08\.2006\x2018:15:21\.18\tctrld:\x20Wrong\x20Licence\x
SF:20for\x20this\x20computer!\r\n04\.08\.2006\x2018:15:21\.18\tctrld:\x20S
SF:oftware\x20li");
MAC Address: 00:08:9B:14:8F:00 (ICP Electronics)
Device type: general purpose
Running: Linux 2.4.X|2.5.X
OS details: Linux 2.4.0 - 2.5.20
```

```
Uptime 10.195 days (since Tue Jul 25 14:12:21 2006)

Nmap finished: 1 IP address (1 host up) scanned in 21.502 seconds
jasper@outside:~$
```

De eerste vragen die naar aanleiding van de output opkwamen zijn:

Waarom staan de onderstaande poorten open en waarom draaien deze applicaties achter deze poorten?

1. Poort: 11/tcp open systat?
2. Poort: 22/tcp open ssh OpenSSH 4.1 (protocol 2.0)
3. Poort: 59/tcp open ssl/unknown
4. Poort: 87/tcp open priv-term-l?

Er is veel belangrijke informatie verkregen uit deze run. Maar in hoeverre kun je deze informatie vertrouwen? Alle informatie die verkregen is kan nagemaakt zijn door de firewall. De firewall kan informatie 'gespoofed' hebben. Dit wil zeggen dat de firewall andere informatie geeft dan dat de firewall daadwerkelijk heeft. Bijvoorbeeld op de firewall kan ssh 2.1 draaien terwijl de firewall zegt dat die versie 4.1 draai. Met deze kennis in gedachte kunnen we uit de output van het nmap programma het volgende concluderen:

- Het systeem draait een Linux versie tussen 2.4.0 – 2.5.20, dit impliceert dat er bepaalde software specifiek voor het netwerkdeel gebruikt wordt.
- Het draait op een Intel platform, dit wil zeggen dat de software geschreven is voor een i386 architectuur.
- Er draait OpenSSH 4.1 (protocol 2.0) op. OpenSSH[32] is een applicatie waarmee veilig ingelogd kan worden op een computersysteem op het netwerk.
- De licentie is verlopen

De aanvaller weet nu dat het een Intel platvorm betreft. Hierbij heeft hij een voordeel aangezien de meeste hardware en daardoor ook de meeste aanvallen voor dit platform beschikbaar zijn. Ook weet de aanvaller welke versie van OpenSSH draait en welke versie van Linux. Door gebruik te maken van informatie op het Internet, zoals Bugtraq[33], kan een aanvaller al snel bepalen of er al bestaande beveiligingslekken zijn. Een deel van de informatie is 'bekend'. Wat er met deze informatie gedaan kan worden is nog niet bekend, maar de mogelijkheid voor een aanval wordt steeds groter.

32 Zie http://www.openssh.org/ voor meer informatie
33 Zie http://msgs.securepoint.com/bugtraq/ voor meer informatie

Gebaseerd op bovenstaande informatie kan onderstaande informatie gevonden worden.

> A vulnerability was discovered in the Linux kernel versions 2.4.22 and previous. A flaw in bounds checking in the do_brk() function can allow a local attacker to gain root privileges. This vulnerability is known to be exploitable; an exploit is in the wild at this time.

en

CAN-2003-0364:

> The TCP/IP fragment reassembly handling in the Linux kernel 2.4 allows remote attackers to cause a denial of service (CPU consumption) via certain packets that cause a large number of hash table collisions (WWW-7)

Doordat er wordt vermoed dat de firewall Linux draait, is het mogelijk dat de firewall ook de native firewall implementatie gebruikt, oftewel de standaard implementatie van Linux. Dit hoeft niet het geval te zijn. Een firewall producent kan er ook voor kiezen om een eigen firewall te implementeren op de Linux kernel.

Vervolgens wordt geprobeerd informatie te achterhalen over het netwerk dat de firewall afschermt.

```
jasper@outside:~$ sudo nmap -sP 10.0.0.0/24
Starting Nmap 4.03 (http://www.insecure.org/nmap/) at 2006-08-04 18:33 CEST
Host 10.0.0.200 appears to be up.
Nmap finished: 256 IP addresses (1 host up) scanned in 24.007 seconds
jasper@outside:~$
```

Via deze netwerk scan kun je zien dat in ieder geval een systeem op IP 10.0.0.200 actief is.

> Normaal gesproken zou je verwachten dat geen enkel systeem binnen het afgeschermde netwerk te bereiken is. Dus ook niet via een nmap commando! Toch is er een systeem te bereiken.

Ondanks het bovenstaande resultaat, is geprobeerd om direct 10.0.0.200 te pingen.

```
jasper@outside:~$ sudo nmap -sP 10.0.0.200
Starting Nmap 4.03 (http://www.insecure.org/nmap/) at 2006-08-04 19:30 CEST
Host 10.0.0.200 appears to be up.
Nmap finished: 1 IP address (1 host up) scanned in 0.117 seconds
jasper@outside:~$
```

Het blijkt dat, ondanks dat er niks het netwerk in mag, er toch een host 'gepinged' kan worden.

Waarom is bij de eerste scan de host 10.0.0.200 niet te zien? Dit komt waarschijnlijk doordat er in de firewall een soort van 'rate'-limiting is geïnstalleerd. Dat wil zeggen dat bij veel verbindingen in korte tijd de firewall de verbinding gaat blokkeren. Dit soort beveiligsmechanismen is meestal bedoeld om te beschermen tegen Denial of Service Attacks (DOS attacks).

Denial Of Service Attacks zijn te karakteriseren als (WWW-28):

- Het overspoelen van een netwerk met netwerkverkeer, waardoor legitiem netwerkverkeer niet meer mogelijk is.
- Het interrumperen van een een netwerkverbinding tussen een tweetal systemen waardoor mogelijke diensten niet meer toegankelijk zijn voor legitieme systemen.
- Het weigeren van toegang van een individu tot een bepaalde dienst waartot de individu legitiem toegang heeft.
- Het proberen om bepaalde diensten van bepaalde systemen of personen niet mogelijk te maken.

Dit wil zeggen dat op het moment dat je een langzame scan doet, je alle systemen die op het netwerksegment aanwezig zijn te zien krijgt.

Aangezien het mogelijk was om van buitenaf de binnenkant te bereiken door middel van een ping, is de volgende stap na te gaan of het mogelijk is om ook daadwerkelijk digitale gegevens uit te wisselen. Dit kan op verschillende manieren getest worden. Gezien de hoeveelheid beschikbare tijd is gekozen voor de pingtunnel tool

Het resultaat van de pingtunnel tool is in de volgende alinea's beschreven.

Pingtunnel

Een pingtunnel is een applicatie welke in staat is een betrouwbare TCP verbinding op te bouwen van een cliënt naar een server, gebruik makend van ICMP echo request en ICMP replay datagrammen, zie ook paragraaf 10.2 (Tooling voor aanvallen op firewalls).

Testomgeving pingtunnel

Voor de testomgeving dient zowel op de inside als de outside een programma geïnstalleerd te worden. De discussie of dat nu wel of niet een reëel scenario is laten we in het midden, aangezien we de firewall aan het testen zijn en niet de 'compremised' host.

Configuratie pingtunnel

Voor een pingtunnel zijn geen configuratie files, maar wordt het programma via de command line geconfigureerd. Als eerst op de server, aangezien deze geen opties heeft.

Op het interne netwerk wordt het volgende programma gestart:

```
jasper@inside:~$ sudo./ptunnel
```

Alle verdere opties worden door de cliënt geconfigureerd. Op extern, dus het afgeschermde netwerk wordt het volgende commando gedraaid.

```
jasper@outside:~$ sudo./ptunnel -p 10.0.0.200 -lp 8000 -da 10.0.0.200 -dp 22
```

De '-p' optie dient om het systeem aan te geven waar de ptunnel server op draait. In de testomgeving is hier voor de host 10.0.0.200 gekozen.

De '-lp' geeft de lokale poort aan waar ptunnel op gaat luisteren. Op het moment dat een programma hiermee een verbinding wil leggen, wordt deze verbinding getunneld naar het opgegeven adres en port gedefinieerd door '-da' en '-dp'.

De '-da' en de '-dp' optie geven respectievelijk het doel, het doelsysteem en de poort weer. In deze testomgeving is gebruik gemaakt van 10.0.0.200 en poort 22. Met andere woorden, op het moment dat er een verbinding gemaakt wordt, maakt het remote systeem een connectie met host 10.0.0.200 op poort 22.

Met de bovenstaande configuratie kan, als de ICMP echo request en ICMP replay datagrammen doorgelaten worden, vanuit het externe systeem een tcp verbinding worden opgebouwd. “Echo request” en “replay” zijn speciale ICMP datagrammen die gebruikt worden door het ping programma. Dit betekent dat de aanvaller een mogelijkheid heeft om een verbinding naar het veilige netwerk te maken. Vervolgens kan de aanvaller digitale-informatie verkrijgen van het “veilige” netwerk.

Resultaat pingtunnel

Het blijkt dat er, hoewel het op het eerste gezicht niet echt stabiel lijkt, door middel van de pingtunnel een TCP sessie opgezet kan worden. Dit wil zeggen dat de 'extra' payload die door de ICMP request gestuurd wordt, geheel gedupliceerd wordt in de firewall. Op dit niveau kan informatie naar binnen en naar buiten gebracht worden.

De niet stabiele verbinding van de pingtunnel en het niet vinden van alle hosts bij een snelle netwerk scan, lijkt op de aanwezigheid van een rate limiting, zoals hierboven beschreven. Rate limiting wil in dit geval zeggen dat er een beperking van het aantal ICMP verbindingen plaatsvindt.

Dit heeft tot gevolg dat er ICMP datagrammen kwijtraken. Zodoende kan er geen stabiele verbinding opgebouwd worden. Bij een scan wordt een gedeelte van de scan niet doorgelaten.

Op het moment dat er een langzame scan wordt uitgevoerd en een langzame verbinding wordt opgezet, lekt er digitale informatie door de firewall.

De vraag is dan: Hoe onveilig is dit? Het volgende bericht geeft dit aan “Malicious Code / Phishing Alert: Data Stolen via ICMP” (WWW-29). Dit kan dus erg onveilig zijn.

Tot nu toe zijn we voornamelijk bezig geweest met het informatie winnen vanuit het systeem. Eerst nog een enkele gedachten.

> Een andere vraag die op komt is:
>
> Is de firewall een statefull of een stateless inspection firewall?
>
> Met deze informatie kan een aanvaller gerichter zoeken naar mogelijke fouten in de firewall. Een statefull firewall is een firewall die alle gegevens van alle connecties bijhoudt en controleert. Een stateless firewall controleert alleen datagrammen en niet de volledige connecties. Op het moment dat een aanvaller dit weet kan hij zijn manier van aanvallen hierop aanpassen.

Vervolgens is verder onderzocht hoe de firewall rule sets in elkaar zitten. Rule sets zijn de meest elementaire configuratie regels voor een firewall.

Firewall rule set testing

Hoe valt een firewall te testen, zodat er op vertrouwd kan worden dat een firewall ook daadwerkelijk naar behoren werkt. Er zijn verschillende leveranciers van firewalls. Elke leverancier zegt dat hun firewall de beste en veiligste is. Maar hoe kan bepaald worden of dat daadwerkelijk zo is? Sommige firewalls worden gebouwd op al bestaande technologieën zoals Linux en Cisco firewalls, die door hun jaren lange ervaringen als operationele systemen een soort van betrouwbaarheidsstempel hebben gekregen. Maar hoe zit het met nieuwe systemen waarvoor de firewall totaal opnieuw geschreven is?

Zoals beschreven in paragraaf 8.2 (Fouten in software en configuratie) zitten in software fouten. Dit zou je ook door kunnen trekken naar de configuratie van een firewall. Aangezien het opzetten van een firewall door mensen gedaan wordt en een configuratie een soort van programmeren van de firewall is.

Aannames bij aanvalmethodes

1. Vaak worden in software fouten gemaakt op plekken waarbij informatie van de ene functie overgaat naar andere functies. Dit kan zijn tussen functies in een programma zelf en tussen functies in een programma en functies in een library. Een library is software die functies levert aan verschillende programma's. Libraries bevatten functies die door meerdere programma's gebruikt kunnen worden. Samengevat kan er gesteld worden dat de meeste fouten worden gemaakt tussen overgangen naar verschillende lagen van software (van der Vliet e.a, 2006).

2. Mensen, zowel gebruikers al ontwikkelaars, maken fouten. Dus er kunnen fouten in zowel de configuratie als in de software zitten. Maar in hoeverre zijn ondoorzichtige configuraties een fout van de software? Er worden steeds meer eenvoudigere interfaces gemaakt om een firewall te configureren, maar een firewall blijft een complex apparaat. Hoeveel “foutieve” aannames maakt een klant bij het configureren van een firewall, waarbij het niet duidelijk is hoe bepaalde punten geconfigureerd worden.

Ftester

Met de ftester tool kan een firewall getest worden op zijn functionaliteit. Er wordt een cliënt en een server geïnstalleerd. Eenvoudig gezegd probeert de cliënt de server te bereiken en de server luistert of die wat kan ontvangen. Er moet wel een 'kanaal' gedefinieerd zijn waarmee de twee tools met elkaar kunnen communiceren om zodoende te bepalen wanneer de test afgelopen is.

Testomgeving ftester

Op de outside wordt de cliënt (ftest) geïnstalleerd, deze probeert door middel van onderstaande configuratie de inside te scannen. Tevens wordt op de outside de server (ftestd) geïnstalleerd.

Configuratie ftester

Vanwege de beperkt beschikbare tijd is de keuze gemaakt om alleen TCP te testen. Aangezien de meeste protocollen die door een firewall heen moeten TCP verbindingen zijn (Kurose, e.a. 2001). Gezien de hoeveelheid connecties die er getest worden, zal het testen van UDP verkeer de testduur verdubbelen.

```
192.168.1.100:1-65535:10.0.0.200:1-65535:S:TCP:0
connect=192.168.1.100:1-65535:10.0.0.200:1-65535:AP:TCP:0
stop_signal=192.168.1.100:80:10.0.0.200:80:S:TCP:0
```

Configuratie 1: ftest.conf

```
192.168.1.100:1-65535:10.0.0.200:1-65535:S:TCP:0
connect=192.168.1.100:1-65535:10.0.0.200:1-65535:AP:TCP:0
stop_signal=192.168.1.100:80:10.0.0.200:80:S:TCP:0
```

Configuratie 2: ftestd.conf

Conclusie / aanbevelingen ftester

Ftester is een test tool die meer geschikt is voor een lang draaiende testomgeving. In de huidige configuratie heeft ftester twee weken operationeel gedraaid. Voor dit soort testen dien je lange termijn testen in te plannen. Oftewel de resultaten zijn niet compleet. Het scannen gebruikt een andere mogelijkheid om de IP-range in klassen te configureren om vervolgens semi-random door deze klassen te scannen en niet, zoals nu geconfigureerd, via een lineaire segment. Voordeel van deze methode is dat er een breder gebied van mogelijke fouten wordt gevonden.

ISIC -- IP Stack Integrity Checker

De IP Stack Integrity Checker[34] (ISIC) is een pakket van programma's dat de stabiliteit van een IP-stack kan testen. Door middel van dit programma wordt geprobeerd om de firewall te testen door misvormde IP-pakketten op en / door de firewall te sturen. Dit heeft als doel te kijken of de firewall IP-pakketten doorlaat of dat de firewall niet meer naar behoren functioneert.

Voor deze test wordt de firewall totaal dicht gezet. Dit wil zeggen dat je vanaf de buitenkant niet naar binnen mag komen. Vanuit de binnenkant mag je wel naar buiten.

Testomgeving ISIC

Het doel van de testomgeving is het bepalen of door middel van de tcpsic, dit is een onderdeel van ISIC die specifiek TCP en tcpdump test, zie 10.1 (Representatieve firewall testomgeving), datagrammen door de firewall gestuurd kunnen worden die niet gespecificeerd zijn. Hiervoor wordt op de outside een week lang een sessie gedraaid die de inside probeert te bereiken. Tevens wordt op de inside een tcpdump gedraaid om te kijken of er pakketten doorkomen. Om te controleren of de firewall werkt, wordt vanuit inside naar buiten gepinged om te kijken of de server nog aan het routeren is. Wanneer deze blijft routeren wordende ping replies ontvangen.

```
jasper@outside:~$ ./isic -s rand -d 10.0.0.200
jasper@outside:~$ ./udpsic -s rand -d 10.0.0.200
jasper@outside:~$ ./tcpsic -s rand -d 10.0.0.200
```

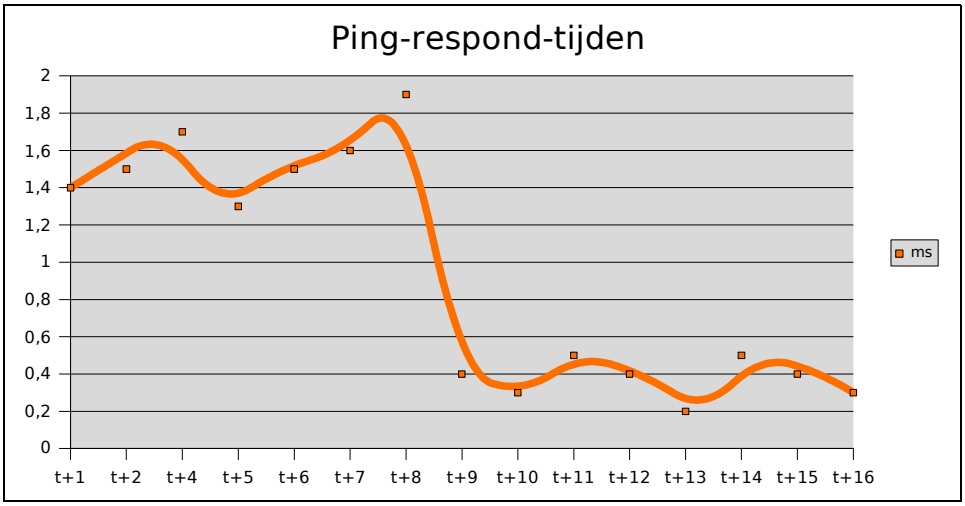
Resultaat ISIC

Na de run van een week is er geen lek in de firewall ontdekt. De isic tool heeft er minimaal één keer voor gezorgd dat de firewall op een bepaald moment niet meer functioneerde. Dit werd ontdekt nadat er vanuit inside geprobeerd werd een connectie op te bouwen. Dit werkte niet meer. Oftewel de firewall kon geen verkeer van inside naar outside versturen /

34 Voor meer informatie zie: http://www.packetfactory.net/projects/ISIC/

ontvangen. Dit betekent dat de firewall mogelijk voor langere tijd niet goed gefunctioneerd heeft. Het is onbekend hoe lang dit het geval is geweest. Nadat de firewall gereboot is, functioneerde de firewall weer naar behoren.

Een ander punt dat opviel is dat bij de testrun de latency van de ping duidelijk toenam en weer afnam. De latency is de tijd die het duurt dat een ICMP request verstuurd en een ICMP reply ontvangen wordt. De latency is afhankelijk van de hoeveelheid systemen waardoor de datagrammen gaan en afhankelijk van het soort netwerk. Aangezien in de testomgeving niks veranderd is, zit de oorzaak van het verschil in de firewall. De firewall is druk bezig met het verwerken van de verstuurde pakketten. De pingtijden van het moment dat de testrun werd gestopt zijn te zien in Figuur 17.



Figuur 17: Pingtijden (onderzoeksresultaat)(Berlijn, 2007)

Figuur 17 laat de laatste zestien seconden van de test zien. Zoals waar te nemen is vanuit het figuur zijn de pingtijden in het begin gemiddeld 1,6 ms. Nadat de test stopte dook de gemiddelde pingtijd naar 0,4 ms. Dat kan een aantal oorzaken hebben:

- Aangezien er constant data naar de firewall gestuurd wordt heeft de netwerkkaart het zeer druk. De netwerkkaart genereert vervolgens gigantisch veel IRQ's. IRQ is een mechanisme waarmee een netwerkkaart een signaal aan het operatingsysteem kan geven dat de netwerkkaart gegevens heeft die het operatingsysteem dient te verwerken. Dit mechanisme kost veel tijd, waardoor de firewall minder tijd beschikbaar heeft om andere taken uit te voeren.

- Ook bestaat een mogelijkheid dat er vertraging optreed in de software die de firewall gebruikt. Dit kan duiden op problemen in de software, deze problemen zouden ook misbruikt kunnen worden. Met een speciaal aangepaste testopstelling zou bepaald kunnen worden welk type pakketten de meeste vertraging opleveren.

Conclusies / aanbevelingen ISIC

Helaas is het door de huidige test-setup niet gelukt om het datagram of de stroom van datagrammen te loggen, hiermee wordt bedoeld de activiteiten te registreren waardoor de gebeurtenissen herhaald kunnen worden, om zodoende te bepalen wanneer de firewall niet meer functioneerde. Tevens is niet te bepalen wanneer de gebeurtenis plaatsvond, aangezien de ping bleef functioneren.

In een volgende test zou de volgende test-setup kunnen worden gebruikt om dit soort effecten wel te kunnen loggen: Het configureren van een webserver op de outside die bij een request de huidige tijd doorgeeft aan de cliënt, inside, die deze vervolgens logt. Mocht door omstandigheden de firewall niet meer functioneren, dan kan door deze logging achterhaalt worden wanneer de firewall gestopt is met functioneren.

Uit het resultaat valt te concluderen dat er met het ICMP ping verkeer anders wordt omgegaan dan met het TCP verkeer, aangezien de ICMP ping bleef functioneren, terwijl een TCP sessie niet meer werkte.

> Dit was de laatste test die binnen de beschikbare tijd effectief te doen was. Behalve de pingtunnel zijn er geen echte problemen gevonden in deze test. Let op, dit wil niet zeggen dat er **geen** fouten in de firewall zitten, maar dat er geen fouten gevonden zijn.

Automatiseren van casestudie aanval op firewall

In deze sectie wordt bediscussieerd of de aanvallen beschreven in paragraaf 10.3 (Beschrijving aanval op een firewall) te automatiseren zijn. Eerst wordt omschreven wat het doel van automatiseren is.

Het doel van automatiseren is:

- Het vergemakkelijken van het werk van beveiligingsadviseurs om te kunnen bepalen of een firewall veilig is.
- Het bepalen van een veiligheidsniveau dat valt binnen een gedefinieerd veiligheidsniveau door middel van een geautomatiseerd systeem.

Op het moment dat er gekeken wordt naar het verloop van de casestudie “Aanval op de Compumatica firewall” is er naar verhouding veel tijd gestoken in het vinden van geschikte software en een geschikte test omgeving. Zie respectievelijk paragraaf 10.1 (Representatieve firewall testomgeving) en paragraaf 10.2 (Tooling voor aanvallen op firewalls). Eerst wordt dieper ingegaan op het automatiseren van de testen, daarna wordt specifiek het testsoftware deel en het automatiseren van de testomgeving beschreven.

Testen

Een aanvaller gebruikt zijn menselijke manier van denken om bepaalde keuzes te maken. Dit betekent dat een aanvaller keuzes kan maken die van te voren niet te bepalen zijn. Een geautomatiseerd systeem kan deze keuzes niet van te voren bepalen en dient dus alle mogelijke combinaties te testen. Zoals verder beschreven in de sectie software is het onmogelijk om alles te testen. Er dienen keuzes gemaakt te worden wat er wel en wat er niet getest wordt. Een testsysteem dat zo compleet mogelijk is, probeert het aantal mogelijke aanvalspaden van een aanvaller drastisch te verminderen en het liefst te reduceren tot nul.

Een nadeel van een open testsysteem is dat aanvallers de kennis kunnen gebruiken van het feit dat een firewall bestand is tegen een bepaald type aanval. De aanvaller kan er dan voor kiezen om de firewall niet aan te vallen of andere methoden te gebruiken waardoor eventuele detectie vermeden kan worden. De detectie kan vermeden worden aangezien de aanvaller weet welke aanvalsmethoden er getest worden. Op deze manier kan een aanvaller,

door het vermijden van die testen, detectie voorkomen of juist door gebruik te maken van de detectie andere aanvallen maskeren.

Software

In de casestudie zijn een viertal software problemen aan de orde gekomen. Deze worden in deze sectie uitgelegd.

Probleem 1: Verspreiding beschikbare software om te testen

De gevonden sofware is verspreid over het Internet en er is geen gecentraliseerde plek beschikbaar waar alle software beschreven staat. Tevens is er weinig coöperatie tussen de gevonden software. Elke software heeft zijn eigen specifieke doel welke een deel van de functionaliteit van de firewall betreft.

Probleem 2: Configuratie van de testen

Elk software pakket dient geconfigureerd te worden. Binnen de casestudie is de configuratie op de volgende plekken aangepast:

- De firewall
- De computersystemen die in de testomgeving zitten
  - Systeem inside
  - Systeem outside
- Software / Tooling:
  - nmap (NetworkMAPer)
  - pingtunnel
  - ftester (Firewall tester)
  - ISIC (IP Stack Integrity Checker)

Er dient op meer dan zeven verschillende verschillende plekken geconfigureerd te worden, aangezien software zoals ftester zowel een cliënt kant heeft als een server kant die apart geconfigureerd dienen te moet worden.

Probleem 3: De tijdsduur van de testen

Vervolgens dient men rekening te houden met de tijd die de software dient de draaien. Zoals beschreven in paragraaf 10.3 (Beschrijving aanval op een firewall) draaien sommige testen dusdanig lang dat het product allang end-of-live is voordat de tests klaar zijn.

Probleem 4: Analyseren resultaat van testen

Het draaien van tests brengt uitkomsten met zich mee. De resultaten van deze tests dienen eerst geanalyseerd te worden om hieruit daadwerkelijk nuttige informatie te kunnen halen.

Zoals beschreven in bovenstaande paragraaf zijn er een viertal problemen gevonden in de casestudie.

De vier problemen zijn:

1. Verspreiding beschikbare software om te testen
2. Configuratie van de testen
3. De tijdsduur van de testen
4. Analyseren resultaat van testen

Voor deze problemen kunnen mogelijke geautomatiseerde oplossingen zijn:

Oplossing 1: Verspreiding beschikbare software om te testen

Het centraliseren van alle beschikbare software en kennis omtrent dit onderwerp. Hiermee wordt bedoeld dat het via één website mogelijk moet zijn om alle software te downloaden en te installeren.

Oplossing 2: Configuratie van de testen

Configuratie blijft een moeilijk aspect, aangezien het niet mogelijk is om alle mogelijke combinaties te kunnen testen. Zie ook probleem 3: De tijdsduur van de testen. Er dienen keuzes gemaakt te worden welke tests er wel gedraaid moeten worden en welke niet.

Een mogelijke automatisering is dat alle configuratie gebaseerd is op de configuratie van de firewall en dat afhankelijk van de configuratie van de firewall ook de resultaten van de testsoftware geïnterpreteerd worden. Het is mogelijk dat van de configuratie van de firewall automatisch test configuratiefiles worden gecreëerd.

Als hulpmiddel kunnen er 'templates' worden gebruikt,om een firewall te testen. Met een template wordt bedoeld dat er een test beschreven is met daarbij behorend testresultaat. Afhankelijk van dit resultaat kan er automatisch bepaald worden of de firewall deze test goed doorlopen heeft of niet. Zo kan er snel en automatisch bepaald worden of een bepaalde firewall gevoelig is voor een bekende zwakheden. Deze 'templates' kunnen gebouwd worden op al bestaande 'exploits'. Met andere woorden, er worden automatisch configuraties aangemaakt die expliciet bepaalde problemen in de firewall proberen te vinden.

Oplossing 3: De tijdsduur van de testen

De enige echte oplossing van dit probleem is de testen te categoriseren en te accepteren dat de testen niet volledig zijn. Dit wil zeggen dat als de tests een probleem vinden, dat er een probleem is, maar als de tests geen probleem vinden, het niet betekent dat er **geen** problemen in de firewall zitten.

Oplossing 4: Analyseren resultaat van testen

De analyse van de resultaten is een complexe aangelegenheid, aangezien de resultaten afhankelijk zijn van:

1. Netwerk opstelling

2. Configuratie firewall
3. Configuratie testsoftware
4. Categoriseren van de testen

Op het moment dat punt één tot en met punt vier vast liggen is het mogelijk om de resultaten van de testen automatisch te analyseren. Aangezien aan de hand van deze punten het verwachte resultaat te bepalen is. Mocht het resultaat van een test niet overeenkomen met het bepaalde resultaat dan is er ergens een fout. Mocht één van de vier punten veranderen, dan is de automatische analyse van het resultaat stukken moeilijker, zo niet onmogelijk.

Gezien de bovenstaande problematiek met het automatiseren van een firewall test is het nuttig om hier tijd en energie in te steken. Op het moment dat er testen geautomatiseerd worden via vaste templates, kan men een firewall testen via deze templates. Deze templates dienen bijgehouden te worden, dat wil zeggen, op het moment dat er een nieuw probleem is gevonden en geanalyseerd dat het probleem ook in een template wordt gezet. Dit kan vergeleken worden met de huidige virusscanners. Op het moment dat er een bepaalde versie van een virusscanner geïnstalleerd is, weet je dat alle virussen die deze versie van de virusscanner moet herkennen, ook daadwerkelijk worden herkend. Hetzelfde geldt voor de firewall tests. Op het moment dat een firewall alle tests tot een bepaalde versie X doorstaat, dan weet je dat alle aanvallen die getest worden door versie X niet werken op die firewall. Dit wil niet zeggen dat de firewall foutloos is, aangezien er nog problemen kunnen zijn die nog niet gevonden / bekend zijn. Er moet dus wel opgepast worden dat dit soort testen niet een vals gevoel van veiligheid opwekken, aangezien er constant nieuwe fouten gevonden worden.

Testomgeving

Het resultaat van een test valt of staat bij een testomgeving die te vertrouwen is. Een testomgeving die tests kan verstoren dient vermeden te worden. Daarom valt snel de keuze om een aparte testomgeving te maken waarop de tests gedraaid kunnen worden. Dit aangezien in een aparte testomgeving alle factoren bepaald en gecontroleerd kunnen worden. Bijkomend voordeel is dat bij de tests eventuele operationele netwerken niet verstoord worden. Op het moment dat er gebruik gemaakt wordt van 'templates', zoals beschreven in de sectie software, dient ook de testomgeving aan de voorwaarden te voldoen die de templates voorschrijven. Dit omdat de analyse van de resultaten van de software tools gebaseerd zijn op de netwerk topologie van de testomgeving. Een bijkomend voordeel kan zijn dat bij een gecontroleerde en vastgelegde testomgeving, de testomgeving gemakkelijk en snel opgezet kan worden. Tevens kan bij een testopstelling gedacht worden aan een eenvoudigere interface om de testen uit te voeren, zodat alle tools automatisch gebruikt worden. Hiermee kan gedacht worden aan een 'cliënt' en een 'server' systeem, die een firewall rule set als input hebben en vervolgens alles proberen wat mogelijk is binnen de beschikbare tijd.

Conclusie

De testen die zijn uitgevoerd in dit onderzoek zijn al gedeeltelijk geautomatiseerd, maar de tools zijn nog niet volledig uitontwikkeld. Vooral op het gebied van het automatisch testen zou de doorontwikkeling verder kunnen gaan. Een mogelijke ontwikkeling is het gebruiken van de bovenstaande beschreven templates methode.

Een aanvaller gebruikt zijn menselijke manier van denken om bepaalde keuzes te maken. Een geautomatiseerd systeem kan deze keuzes niet van te voren bepalen. Een alternatief is om op alle mogelijke manieren te testen, maar een volledig testsysteem blijkt onmogelijk.

Daarentegen kan een aanvaller dit geautomatiseerde systeem ook gebruiken om informatie te krijgen over een bepaald systeem. Mocht het geautomatiseerde systeem geen fouten vinden, dan weet de aanvaller dat de aanvallen die in het geautomatiseerde systeem aanwezig zijn niet gebruikt kunnen worden.

10.4 Attacktree van bovenstaande aanvallen op firewall

In paragraaf 10.3 (Beschrijving aanval op een firewall) is een beschrijving gegeven van een aanval op een firewall. Dit is zeer waarschijnlijk een niet volledige aanval, aangezien niet alle mogelijke aanvalspaden bewandeld zijn. Dit betekent dat bij het maken van een attacktree van de beschreven aanvallen de attacktree ook niet volledig / compleet is.

Het eerste probleem wat opdook bij het maken van de attacktree is het beschrijven van de wortel van de boom. Dit is een speciale knoop binnen de boom die het begint van de boom vormt. In deze knoop staat het antwoord op de vraag: “Wat wil een aanvaller aanvallen?”. Om deze vraag te kunnen beantwoorden is deze vraag veranderd in “Wat willen wij beschermen”. Om dit te kunnen bepalen kan een risico analyse gemaakt worden. Het antwoord op de vraag “Wat willen wij beschermen” hoeft niet hetzelfde te zijn als “Wat wil een aanvaller aanvallen?”, maar er wordt vanuit gegaan dat als een aanvaller iets bereikt wat niet valt onder de vraag “Wat willen wij beschermen”, het niet belangrijk is om deze informatie te beschermen.

Een voorbeeld kan zijn dat een bedrijf zijn interne email communicatie niet afschermt. Aangezien alle belangrijke digitale informatie op een afgeschermde computer staat die niet op het netwerk is aangesloten. De aanvaller kan niet direct de digitale informatie op de afgeschermde computer aanvallen. De aanvaller probeert zich te infiltreren in het interne email communicatie systeem, om vervolgens speciaal aangepaste “emails” te versturen naar medewerkers van het bedrijf. Aangezien het lijkt dat de email van een andere collega afkomt, en niet van de aanvaller, kan de collega reageren op de email door belangrijke digitale informatie te mailen. Deze mail gaat vervolgens naar de aanvaller, in plaats van naar de collega. Dit voorbeeld is een combinatie van “sociaal” engineering en een “technische” aanval op computersystemen.

Op de vraag “Wat willen wij beschermen” is als antwoordt in deze case geformuleerd “Een firewall dient digitale informatie selectief door te laten”. En firewall dient dus allen digitale informatie door te laten die toegestaan is. Binnen deze aanvalt wordt gekeken of het mogelijk is om digitale informatie te versturen die niet expliciet is toegestaan door de firewall. Met dit antwoord reist meteen een aantal andere vragen: “Welke digitale informatie?”, “Willen we uitgaande digitale informatie of ingaande digitale informatie beschermen? of “Hoe snel gaat de digitale informatie langs de firewall?”.

Het feit dat er nog vragen zijn met betrekking tot de wortel van de attacktree betekend dat de top van de attacktree die binnen dit onderzoek gemaakt gaat worden niet daadwerkelijk de top van de gehele / totale attacktree is. Met andere woorden de attacktree gemaakt binnen deze case zal een deel zijn van een totale attacktree.

De reden waarom dit antwoord is gekozen, “Digitale informatie die door / langs een firewall loopt” is dat bij het onderzoek, zie paragraaf 10.3 (Beschrijving aanval op een firewall), daadwerkelijk een fout gevonden is die er voor kon zorgen dat digitale informatie uitgewisseld kon worden.

Er wordt begonnen met de knoop “Digitale informatie die door / langs een firewall loopt”. De volgende stap is de mogelijke aanvalspaden te bedenken die als resultaat hebben dat er digitale informatie langs / door de firewall gaat. Mogelijke manieren zijn:

1. *Sluiproute langs / door de firewall,* hiermee wordt bedoeld dat de informatie buiten de firewall om verstuurd wordt. Bijvoorbeeld door gebruik te maken van een inbel modem die de gegevens verstuurd via het modem in plaats via de firewall.

2. *Firewall configuratie fout,* aangezien het configureren van een firewall mensenwerk is en een complexe aangelegenheid, bestaat de kans dat een firewall functioneel goed werkt, maar door een fout toch digitale informatie kan versturen.

3. *'Bug' in firewall,* met andere woorden er zit een fout in de software van de firewall waar de aanvaller gebruik van maakt.

Buiten de bovenstaande manieren zijn er nog tal van scenario's te bedenken waarmee digitale informatie langs de firewall te krijgen is. Een bekend ander voorbeeld is het gebruik van usbsticks / laptops die vervolgens ook weer kwijt kunnen raken (WWW-13).

In Figuur 18 is een mogelijke attacktree weergegeven. Hierin staan de bovenstaande aanvallen uitgewerkt. Aangezien de attacktree nogal explosief aan het groeien is, wordt alleen de 'Bug' in de firewall tekstueel uitgewerkt. De rest van de boom wordt ter informatie beschreven.

Vanuit het perspectief *'Bug' in firewall* zijn er een aantal mogelijkheden. Gezien de afkadering van dit onderzoek wordt alleen gekeken naar een firewall die gebruik maakt van het IP. Dit betekent dat er alleen gekeken wordt naar fouten die binnen dit protocol zitten. Fouten is misschien een verkeerde benaming, aangezien de functionaliteit van het IP soms expres geblokkeerd wordt door de firewall. Een veel voorkomende fout die door technici gemaakt wordt, is het totaal blokkeren van ICMP. Dit is een vitaal onderdeel van IP. Een onderdeel van ICMP is het Path MTU Discovery protocol. Dit protocol zorgt ervoor dat de datagrammen van voldoende grootte zijn voordat ze verstuurd worden. Mocht dit protocol niet actief zijn, dan kunnen er te grote datagrammen verstuurd worden die vervolgens maar gedeeltelijk over komen. Op het moment dat de ICMP berichtgeving wordt geblokkeerd, en dus ook de Path MTU Discovery, kunnen er netwerkproblemen ontstaan (WWW-30).

Veelgebruikte protocollen op IP zijn:

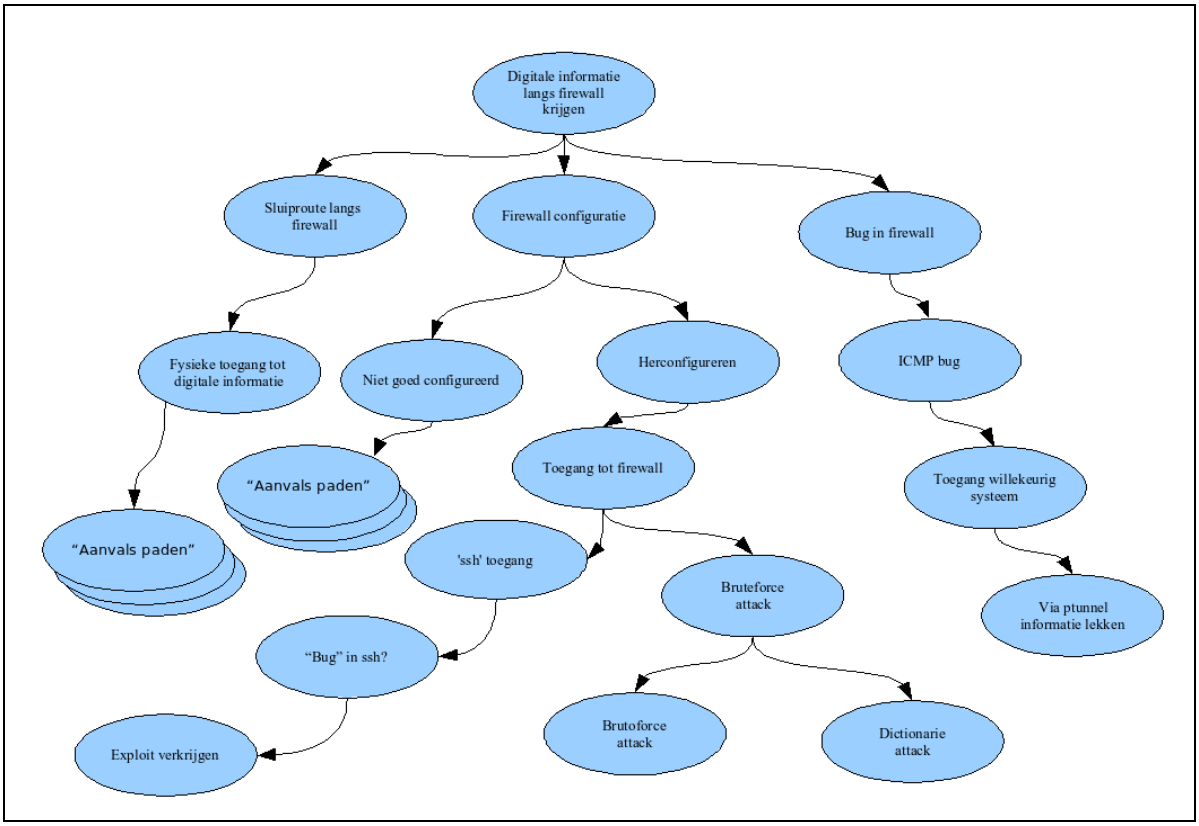
- UDP
- TCP
- ICMP

In het onderzoek, 10.3 (Beschrijving aanval op een firewall), is er getest op zowel UDP / TCP en ICMP. Binnen deze test zijn alleen problemen gevonden in het ICMP verkeer.

Aangezien nu 'bekend' is dat dit type firewall dit probleem heeft, dient de aanvaller er voor te zorgen dat hij deze fout kan 'misbruiken'. Op het moment dat de aanvaller er voor kan

zorgen dat hij toegang kan krijgen tot een systeem op het netwerk, dan kan de aanvaller ongemerkt van buitenaf gegevens op het interne netwerk bekijken. Als eerste het probleem van het toegang krijgen tot het systeem. Een aanvaller kan 'virussen' versturen naar de medewerkers in het bedrijf. Het virus kan geactiveerd worden omdat een gebruiker er op klikt of omdat er gebruik gemaakt wordt van het systeem waar de medewerker op werkt, zodat het virus automatisch opgestart wordt. De medewerker zal ontkennen dat hij een virus heeft, omdat hij in het bezit is van een virusscanner. Het is alleen zo dat een virusscanner alleen virussen blokkeert die hij herkent. Als de aanvaller besluit om een nieuw virus te schrijven is de kans groot dat een virusscanner deze niet herkent.

Op het moment dat het de aanvaller gelukt is om een virus te activeren, dan kan de aanvaller via een 'ICMP' tunnel de computer op afstand controleren en via die computer andere systemen aanvallen.



Figuur 18: Attacktree (Berlijn, 2007)

Bij het maken van aantal schetsen van de attacktree bleek dat een handmatige attacktree niet werkbaar was, aangezien in korte tijd de attacktree exponentieel groeide. Om deze problematiek te beschrijven is in deze masterthesis één schets behandeld.

De bovenstaande attacktree is samen met Dr. Martijn Oostdijk ontwikkeld. Deze incomplete, zeer eenvoudige attacktree zal zeer snel, zeer groot worden op het moment dat deze uitgebreid wordt. In deze attacktree zijn niet alle mogelijkheden getekend. Ondanks dat de attacktree relatief klein is, zal deze attacktree al voor veel discussie zorgen.

Een eerste reactie zal zijn om een elektronische vorm te creëren. In een elektronische vorm kun je veel meer informatie kwijt. Maar hoe specifiek moet alles dan verwerkt worden? Wat is het meest atomaire element wat door dit systeem verwerkt dient te worden?

Daarnaast zal de hoeveelheid discussie alleen maar toenemen naarmate de boom groter

wordt. Er zullen aanvallen zijn die zich niet aan het model willen conformeren. Tevens denkt een aanvaller vaak anders, een aanvaller 'ruikt' onderaan de knopen van een attacktree en probeert daarmee een stapje verder te komen. Hiermee wordt bedoeld dat een aanvaller niet vanuit zijn doel denkt, maar vanuit de mogelijkheden die hij heeft om een doel te bereiken. Dat wil ook zeggen dan een aanvaller niet altijd de meest logische, snelste of kortste weg gebruikt, maar veelal een omweg neemt om tot zijn uiteindelijke resultaat te komen. Vandaar dat attributen, oftewel extra informatie, toevoegen aan de attacktree (in de elektronische versie) voor het tegenhouden van aanvallers niet nuttig is. Deze informatie kan wel gebruikt worden om inzichtelijk te krijgen wat voor schade een aanvaller kan maken.

11 Conclusies

In dit hoofdstuk wordt de conclusie beschreven van deelonderzoek B “Aanvalsmethodieken van een firewall”. Hoofdstuk 12 (Algemene conclusies en aanbevelingen) beschrijft de algemene resultaten van dit deelonderzoek.

Het onderzoek bestaat uit twee delen, de voorstudie en het empirisch onderzoek. Het resultaat van de vooronderstudie wordt gebruikt om het empirische deel te kunnen uitvoeren.

Het resultaat van de voorstudie is een opgebouwde representatieve firewall testomgeving en een verzameling van tools die gebruikt worden om een firewall aan te vallen / testen. Door middel van een exploratief onderzoek, gebruik makend van kennis welke beschikbaar is op het Internet, literatuurstudie en eigen ervaringen, is een representatieve testomgeving opgebouwd.

Het resultaat van het empirisch onderzoek is een verslaglegging van de methode en gebruikte tools om een firewall aan te vallen en de uitwerking van de aanvallen in een attacktree.

Het hoofdstuk is als volgt opgebouwd:

De resultaten van de voorstudie worden beschreven in:

- Representatieve firewall testomgeving
- Tooling voor aanvallen op firewalls

De resultaten vanuit het empirisch onderzoek worden beschreven in:

- Problemen testomgeving
- Attacktree van bovenstaande aanvallen op een firewall

Vervolgens worden de resultaten van het onderzoek per onderzoeksvraag gegeven.

11.1 Representatieve firewall testomgeving

In paragraaf 10.1 (Representatieve firewall testomgeving) is door middel van literatuur onderzoek en zoeken op Internet een testomgeving ontwikkeld, geïnstalleerd en geconfigureerd. Het ontwikkelen van een testomgeving heeft zijn beperkingen in de hoeveelheid beschikbare middelen zoals tijd, financiën, apparatuur, tooling en ruimte.

Een gesloten testomgeving is een goede basis om de aanvalstesten op te draaien. Toch is een gesloten testomgeving iets anders dan een 'operationele' firewall. Een operationele firewall krijgt meer te voortduren dan een firewall die in een gesloten testomgeving zit, aangezien een operationele firewall door honderden misschien wel duizenden mensen gebruikt wordt. Een firewall in een gesloten testomgeving heeft alleen te maken met de testers die gebruik maken van deze omgeving. Elke gebruiker heeft zijn eigen soort en manier om een firewall te gebruiken. Dit valt in een gesloten testomgeving niet na te bootsen. Wel heeft een gesloten testomgeving als voordeel dat, zonder last te hebben van operationeel verkeer, bepaalde problemen onderzocht kunnen worden.

11.2 Tooling voor aanvallen op firewalls

Het vinden van goede tooling bleek een moeilijke taak te zijn. Uiteindelijk zijn er een aantal tools gevonden aan de hand van opgestelde eisen, zie paragraaf 10.2 (Tooling voor aanvallen op firewalls). De beschikbare tooling heeft de functionaliteit om een test te draaien, maar het vergt veel tijd om de testomgeving gereed te maken en om de testen te draaien. Daarnaast kan niets met de testomgeving gedaan worden op het moment dat een test draait, aangezien er bij een probleem achterhaald dient te kunnen worden hoe het probleem ontstaan is. Als er op dat moment meerdere testen in dezelfde testomgeving draaien is dat bijna een onmogelijke taak, aangezien niet bekend is welke test het probleem veroorzaakt heeft. Het is ook mogelijk dat juist een combinatie van testen de fout veroorzaakt heeft.

11.3 Problemen testomgeving

Ondanks dat er problemen aan het licht zijn gekomen, zoals het ping tunnel probleem, zie paragraaf 10.3 (Beschrijving aanval op een firewall), is het oordeel dat er relatief weinig problemen te vinden zijn door het gebruik van een blackbox testomgeving. Regelmatig worden kleine afwijkingen of onregelmatigheden ontdekt die interessant zijn om verder te onderzoeken, maar door de beperking dat er alleen vanaf de buitenkant een benadering kan plaatsvinden, kan er geen verder onderzoek gedaan worden. De gebruikte testomgeving, waarin een blackbox firewall was aangesloten werkte prima. Bij vervolgonderzoek zou een benaderingsmogelijkheid via de binnenkant gewenst zijn. Dit om de kleine afwijkingen en onregelmatigheden die tijdens dit onderzoek naar voren zijn gekomen te kunnen onderzoeken. Het gebruik van een blackbox firewall is hierdoor uitgesloten.

11.4 Attacktree van bovenstaande aanval op een firewall

Van de aanvallen zijn een aantal schetsen gemaakt voor de attacktree. Deze schetsen zijn samen met Dr. Martijn Oostdijk besproken. Tijdens deze interactie bleek dat het ontwikkelen van een handmatige attacktree niet werkbaar was, aangezien in korte tijd de attacktree dusdanig groot werd dat het uitwerken ervan op papier geen doen meer was. Uiteindelijk is er één attacktree van de uitgevoerde aanvallen opgenomen in deze masterthesis, zie 10.4 (Attacktree van bovenstaande aanvallen op firewall). In onderstaande paragraaf wordt aan de hand van de onderzoeksvragen dieper op deze problematiek ingegaan.

11.5 Vraagstellingen

In de komende paragrafen wordt de conclusie per vraagstelling beschreven. De volgende vraagstellingen worden beschreven:

1. Hoe kan een blackbox firewall worden aangevallen?
2. Zijn de bovenstaande aanvallen te beschrijven op een gestructureerde en documenterende manier?
3. Zijn de bij twee beschreven aanvallen op de blackbox firewall te automatiseren?

4. Is het mogelijk om een attacktree te ontwerpen op basis van een aanvallende methodiek?

5. Is de attacktree methode een bruikbare techniek om aanvallen op een blackbox firewall te modelleren?

Hoe kan een blackbox firewall worden aangevallen?

Door middel van de resultaten van de voorstudie, specifiek paragraaf 10.2 (Tooling voor aanvallen op firewalls), zijn een aantal mogelijke aanvallen gedaan op de firewall. De resultaten van deze aanvallen zijn te vinden in paragraaf 10.3 (Beschrijving aanval op een firewall). De volgende tooling is gebruikt:

1. nmap (NetworkMAPer)

2. pingtunnel

3. ftester (Firewall tester)

4. ISIC (IP Stack Integrity Checker)

Ondanks dat er een beperkt aantal aanvallen op de firewall gedaan zijn, zijn er problemen gevonden in de firewall. In hoeverre deze problemen daadwerkelijk gevaar kunnen opleveren dient verder onderzocht te worden. Het feit blijft dat met de gevonden problemen een aanval daadwerkelijk succesvol is geweest.

Zijn de bovenstaande aanvallen te beschrijven op een gestructureerde en documenterende manier?

Een aanval op een blackbox firewall kan op een gestructureerde en documenterende manier beschreven worden door de gedane stappen op schrift te zetten. Bij dit stappenplan dient ook duidelijk aangegeven te worden welke keuze er is gemaakt en waarom juist deze keuze. Op deze manier kan de gehele aanval nagekeken worden wanneer bijvoorbeeld het einddoel niet is bereikt. Een deel van de aanval kan hierdoor herhaald worden, maar het is ook mogelijk halverwege een andere keuze te maken. Op deze manier hoeft men niet te gaan gissen welke paden men is ingeslagen, maar kan men deze nalezen in een document. Bij elke stap dienen ook alternatieve gedachten genoteerd te worden.

In het verslag van de aanval, zie paragraaf 10.3 (Beschrijving aanval op een firewall) wordt aan de hand van bovenstaande manier gedocumenteerd. Er wordt gebruik gemaakt van 'gedachten' kaders die de gedachten beschrijven op het moment dat een aanval plaatsvond. Sommige gedachten zijn gevolgd om zo tot een succesvolle aanval te komen. Andere gedachten zijn niet gevolgd aangezien ze op dat moment niet de goede keuze bleken. Men kan dit vergelijken met het finger-spitzen-gevoel' zoals beschreven in de doelstelling.

Zijn de bij twee beschreven aanvallen op de blackbox firewall te automatiseren?

Zijn de aanvallende methodieken op de firewall te automatiseren? Het antwoord is ja, maar niet volledig. De testen die zijn uitgevoerd in dit onderzoek zijn al gedeeltelijk geautomatiseerd, maar de tools zijn nog niet volledig uitontwikkeld. Vooral op het gebied

van het automatisch testen zou de ontwikkeling verder kunnen gaan. Zoals een eenvoudigere interface om de testen uit te voeren, zodat alle tools automatisch gebruikt worden. Hiermee kan gedacht worden aan een 'cliënt' en een 'server' systeem, die een firewall rule set als input hebben en vervolgens alles proberen wat mogelijk is binnen de beschikbare tijd.

Een aanvaller gebruikt zijn menselijke manier van denken om bepaalde keuzes te maken in een aanvalsmethodiek. Dit betekent dat een aanvaller keuzes kan maken die van te voren niet te bepalen zijn. Een geautomatiseerd systeem kan dit niet. Een geautomatiseerd systeem, dat zo compleet mogelijk is, zal het aantal uit te proberen aanvalspaden van een aanvaller drastisch verminderen. Aan de andere kant kan een aanvaller dit geautomatiseerde systeem ook gebruiken om fouten te vinden in een bepaald systeem. Mocht het geautomatiseerde systeem geen fouten vinden, dan weet de aanvaller dat de aanvallen die in het geautomatiseerde systeem aanwezig zijn niet gebruikt kunnen worden.

Is het mogelijk om een attacktree te ontwerpen op basis van een aanvallende methodiek?

Binnen dit onderzoek is een attacktree opgesteld waarin een aantal van de gevonden aanvallen verzameld is. De boom werd in korte tijd echter dusdanig groot, dat het handmatig uitwerken niet werkbaar bleek. Een elektronische vorm is daarentegen misschien wel een mogelijkheid. Een systeem dat een attacktree beheert zal veel onderhoud vergen. In hoeverre dit dan nog een handige methodiek is, is de vraag. Daarnaast blijft de vraag in hoeverre het systeem om kan gaan met aanvallen die niet te modelleren zijn in een attacktree.

Is de attacktree methode een bruikbare techniek om aanvallen op een blackbox firewall te modelleren?

Een 'typische' aanvaller laat zich niet conformeren aan de ontwikkelde aanvalsbomen. Een aanvaller 'ruikt' onderaan de knopen van een attacktree of hier mogelijkheden zitten. Oftewel een aanvaller denkt niet vanuit zijn doel, maar vanuit de mogelijkheden die hij heeft om zijn doel te bereiken. Hij probeert via diverse paden tot het uiteindelijke resultaat te komen.. Dit betekent dat een aanvaller niet altijd het meest eenvoudige pad hoeft te nemen, maar het pad neemt dat hij in zijn aanvalstocht tegenkomt.

Uit bovenstaande kan geconcludeerd worden dat een attacktree geen handig instrument is voor de analyse van een aanval op een firewall.

Algemene conclusies en aanbevelingen

12 Algemene conclusies en aanbevelingen

In dit hoofdstuk worden de conclusies met betrekking tot het management- en informatica-onderzoek gegeven. Het hoofdstuk is als volgt opgebouwd:

1. Conclusies
2. Aanbevelingen
3. Aanzet vervolgonderzoek

12.1 Conclusies

In deze paraaf wordt eerst de conclusie van het managementonderzoek, “Criteria die de kwaliteit van een risico-analyse van een firewall bepalen”, beschreven. Daarna volgt de conclusie van het informatica-onderzoek, “Aanvalsmethodieken van een firewall”. In “Verhoudingen onderzoek” wordt de link tussen beide deelonderzoeken gelegd. Tot slot worden in “Beperkingen onderzoek” de problemen besproken waar tijdens dit onderzoek tegenaan gelopen is.

Mijn verwachtingen van dit onderzoek zijn tweeledig. Aan de ene kant verwacht ik dat er weinig animo voor is, aangezien beveiliging van digitale informatie wel belangrijk is, maar nog steeds financieel ondergewaardeerd. Tevens zijn managers onbekend met de gevaren van een slechte beveiliging van firewalls. Met andere woorden de managers die de financiële toezeggingen doen, meestal geen technisch onderlegde managers, willen liever geld investeren in een nieuwe computer of laptop, dan in een firewall of andere beveilingsmaatregelen, aangezien ze daar niets tastbaars voor terugkrijgen. Aan de andere kant zijn managers zich steeds meer bewust, onder andere door de media, dat computersystemen / -netwerken beveiligd dienen te worden. Hierdoor kan het zijn dat managers zich er meer in willen verdiepen. Dit onderzoek kan hieraan een bijdrage leveren.

Criteria die de kwaliteit van een risico-analyse van een firewall bepalen

Het managementonderzoek heeft een dertigtal criteria opgeleverd die de kwaliteit van een risico-analyse bepalen.

Om de criteria inzichtelijk te houden, is er een onderverdeling in de volgende categorieën gemaakt:

- *Scope;* in de sectie scope worden de criteria beschreven die gerelateerd zijn aan het domein en het bereik van de risico-analyse.
- *Systeem karakteristieken;* in de sectie systeem karakteristieken worden de kenmerken van het systeem, in dit onderzoek meestal het netwerk en de firewall, beschreven.
- *Risico-analyse methode;* tot slot wordt in de risico-analyse methode beschreven hoe

het risico-analyse-rapport tot stand is gekomen.

Hieronder volgen de criteria, die gebruikt kunnen worden om de kwaliteit van een risico-analyse te bepalen. Dit wil echter nog niet zeggen dat deze ook daadwerkelijk door de managers en technici worden gebruikt. De categorieën worden wel gebruikt in de praktijk, maar niet als zodanig benoemd (Zie 5.2 (Literatuurstudie)).

Scope
- Organisatie soort
- Organisatie grootte
- Doelgroep
- Aanvallers soort
- Hoeveelheid aanvallers
- Doelgroep risico-analyse

Systeem karakteristieken
- Afkadering systeem
- Systeemfuncties
- Data criteria
- Communicatiestromen

Risico-analyse methode
- Representatief
- Samenvatting
- Participanten
- Data verzamelings technieken
- Risico schalen
- Herkenbaarheid risico's
- Risicoverdeling
- Risicogebied
- Kwetsbaarheden
- Identificatie
- Risico beperking
- Kansbepaling
- Risicobeoordeling
- Aanbevelingen
- Veiligheidsniveau
- Systematisch en analytische uitvoering
- Valse precisie
- Tijdsduur
- Personeel

Zoals beschreven in hoofdstuk 6 (Conclusies en reflectie) blijkt er te weinig aandacht te worden besteed aan het verbeteren van de criteria die de kwaliteit van een risico-analyse voor een firewall bepalen. Er is een beperkte hoeveelheid wetenschappelijke literatuur beschikbaar. De (wetenschappelijke) kennis over dit onderzoeksgebied blijkt te beperkt. Daarnaast zijn sommige (wetenschappelijke) artikelen omtrent deze materie gesloten, ofwel niet openbaar toegankelijk.

Ondanks het feit dat er bij organisaties geringe kennis aanwezig is over het gebruik van risico-analyses,zie paragraaf 5.3 (Empirie: Interviews technici / managers), is duidelijk geworden dat men wel steeds meer inziet dat risico-analyse nodig is, maar aan de andere kant wordt er weinig tot niet naar geacteerd. Capaciteiten en prioriteiten van managers en

technici belemmeren het uitvoeren van volledige risico-analyses binnen organisaties. Dit terwijl het belang en de validiteit wel erkend wordt, maar vooralsnog te weinig prioriteit krijgt. Ook het kijken naar de kostenaspecten op de korte termijn heeft een belemmerende werking.

Persoonlijk vind ik de resultaten van de uitkomst van dit onderzoek tegenvallen. Mijn verwachting was dat door de berichtgeving en het vele gebruik van Internet en de daarbij behorende kennis, er meer tijd en energie gestoken zou worden in het bepalen en inschatten van risico's. Dit bleek tegen te vallen / beperkt. Zeker gezien het feit dat men steeds vaker werknemers een bepaalde functionaliteit verbied, zoals het gebruik van “MSN / Jabber” onder de noemer van “beveiliging”. Dit terwijl daar eigenlijk geen echte basis / reden voor is.

Aanvalsmethodieken van een firewall

Gezien de diversiteit van dit onderzoek verwijs ik naar hoofdstuk 11 (Conclusies) voor de complete discussie. De resultaten van het informatica-onderzoek zijn in het kort:

- Blackbox testing is geen goede manier om een firewall volledig te testen omdat er een beperking is. Er kan immers alleen vanaf de buitenkant een benadering plaatsvinden waardoor verder onderzoek bemoeilijkt wordt.
- De aanvallen op een blackbox firewall kunnen op een gestructureerde en documenterende manier beschreven worden door de aanvalsmogelijkheden op schrift te zetten.
- De aanvallen zijn gedeeltelijk te automatiseren, gezien de complexiteit van de omgeving waar een firewall in staat en het aantal mogelijke toestanden waar een firewall zich in kan bevinden. Daarnaast is de output van de meeste tools dusdanig complex dat automatisch analyseren van de output vaak niet compleet zal zijn.
- De attacktree is geen goede methodiek om een aanval te beschrijven, aangezien deze methode niet dynamisch genoeg is. Hiermee wordt bedoeld dat de stappen van een aanvaller niet goed te modelleren zijn.

Verhoudingen onderzoek

Hoe beide onderzoeken zich tot elkaar verhouden wordt in de volgende alinea verduidelijkt.

In het onderzoek “Aanvalsmethodieken van een firewall” zijn problemen gevonden die de vertrouwelijkheid, integriteit en beschikbaarheid kunnen beïnvloeden. Dit is een direct risico dat bepaald en ingeschat dient te worden door een risico-analyse. De kwaliteit hiervan wordt bepaald door het onderzoek van “Criteria die de kwaliteit van een risico-analyse van een firewall bepalen”.

Beperkingen onderzoek

De grootse beperking binnen dit onderzoek was de beschikbare tijd. Voor het totale onderzoek, dus met de deelonderzoeken “Criteria die de kwaliteit van een risico-analyse van een firewall bepalen” en “Aanvalsmethodieken van een firewall” is een periode van zes maanden gemoeid. Oftewel gemiddeld drie maanden per onderzoek. Dit betekent dat er

tweemaal een onderzoeksmethode en onderzoeksdoel- / vraagstelling bepaald, gemaakt en uitgevoerd moest worden. Dit is gezien de verwachte resultaten binnen zo'n tijdsbestek niet reëel.

Uit het onderzoek is duidelijk naar voren gekomen dat het een exploratief onderzoek betrof. Er was relatief weinig wetenschappelijke literatuur beschikbaar. Ook de bekendheid binnen organisaties over de materie dan wel het belang ervan liet te wensen over. Duidelijk is geworden dat de beschreven materie steeds meer gewaardeerd wordt en in de toekomst een belangrijke rol gaat spelen.

De verwachting is echter dat het eerst goed mis dient te gaan alvorens er voldoende besef en draagvlak binnen de organisaties aanwezig is om het centrale onderwerp binnen dit onderzoek constructief aan te pakken. Dit is algemeen bekend, maar nog steeds niet onderkend.

De resultaten van dit onderzoek geven een goede aanzet voor vervolgonderzoek naar deze materie, wat voor de komende jaren voor veel bedrijven van belang zal zijn.

12.2 Aanbevelingen

In deze paraaf worden eerst de aanbevelingen van het managementonderzoek beschreven. Deze aanbevelingen richten zich op organisaties (technici en managers) en onderzoekers. Daarna komen de aanbevelingen met betrekking tot het informatica-onderzoek aan bod. Deze aanbevelingen kennen dezelfde doelgroep als het managementonderzoek. Er dient rekening mee gehouden te worden dat er weinig tijd beschikbaar was voor het geheel uit diepen van het onderzoek.

Criteria die de kwaliteit van een risico-analyse van een firewall bepalen

Aanbeveling 1: Bewustwording risico-analyse van een firewall bij organisaties, met name bij beslissers, architecten en uitvoerders.

Dit is een moeizame taak aangezien niemand zich 'echt' verantwoordelijk voelt voor het onderzochte gebied. Er is een tweedeling tussen de managers en hun bedrijfsprocesmatig denken en de technische mensen die vanuit technisch oogpunt denken. Oftewel er dient relatief veel aandacht aan deze doelgroepen te worden besteed. Vanuit de respondenten is er positief op het onderzoek gereageerd, maar tevens de kanttekening geplaatst dat het een relatief onbekend gebied betreft. Dit gebied heeft veelal geen duidelijke plek in de organisatie. Met andere woorden niemand voelt er zich verantwoordelijk voor.

Aanbeveling 2: Het houden van een risico-analyse

Het hoeft geen formeel document te zijn, maar er dient wel duidelijkheid te bestaan over waar de risico's zich bevinden. Meestal is deze kennis aanwezig binnen de groep, maar voor sturing is het belangrijk om deze kennis op papier te hebben. Waar op gelet dient te worden is dat het niet een te formeel document wordt, waardoor niemand meer met het document werkt. Het verwerken van de kennis in een operationele omgeving is een goede manier om deze kennis te bewaren en up-to-date te houden.

Aanbeveling 3: Budget vrijmaken

Ondanks dat er vaak gepraat wordt over informatiebeveiliging zijn er weinig bedrijven die zich daar ook effectief mee bezighouden. Het advies naar deze bedrijven toe is om budget vrij te maken om een specifieke risico-analyse te maken en deze ook te onderhouden. Dit budget komt vaak pas bij echte problemen vrij, ofwel reactief handelen in plaats van proactief.

Aanbeveling 4: Bewustwording dat digitale informatie van levensbelang is voor organisaties

Gezien de snelheid waarmee tegenwoordig via het Internet digitale informatie kan worden verspreid, dient men zich bewust te zijn dat digitale informatie en daarmee dus ook kennis veel vluchtiger is geworden. Oude bestaande informatiebeveiliging procedures zijn vaak niet ontworpen om met de huidige beveiliging issues om te gaan.

Aanvalsmethodieken van een firewall

Aanbeveling 1: Gebruiksgemak tooling

Binnen het gebied van gebruiksgemak van de gebruikte tooling zou het automatisch testen beter kunnen. Zoals een eenvoudigere interface die alle tools automatisch gebruikt om de testen uit te voeren. Hiermee kan gedacht worden dat je een 'cliënt' en een 'server' systeem hebt die een firewall rule set als input hebben en vervolgens alles proberen wat mogelijk is binnen een bepaald tijdsbestek.

Aanbeveling 2: Afbakening van de definitie van de firewall vergroten.

Binnen dit onderzoek is alleen gekeken naar de packetfilter van een firewall. Dit is een sterk afgebakend gebied. Wat echter opvalt is dat in het onderzoek deze afbakening regelmatig een beperkende factor was. De aanbevelingen voor een vervolgonderzoek is om de afbakening minder klein te maken. Hoogstwaarschijnlijk resulteert dit in een langduriger onderzoek, aangezien je met meerdere facetten, zoals al de aangekoppelde systemen, rekening dient te houden.

Aanbevelingen 3: Perceptie op het geheel en niet alleen op de firewall

Een vervolg onderzoek dient meer rekening te houden met de omgeving. Aangezien een firewall een relatief statisch apparaat is. Dat wil zeggen dat als de firewall zijn werk niet helemaal correct doet, daar zelf geen last van ondervind. Het grootste gevaar ligt bij de systemen die de firewall probeert te beschermen, hierop staat immers de digitale informatie die men wil beveiligen. Met andere woorden de combinatie firewall met de systemen dient inzichtelijk te zijn.

12.3 Aanzet vervolgonderzoek

Vanwege de afkadering van dit onderzoek zijn verschillende elementen onderbelicht. De resultaten van de deelonderzoeken geven aanleiding tot het doen van vervolgonderzoek.

Aandacht voor de volgende punten kan nuttig en bruikbaar zijn voor de verdere verdieping in dit onderwerp. De punten voor zowel vervolg- als aanvullend onderzoek uit zowel deelonderzoek A als B worden hieronder weergegeven. Na de opsomming volgt de uitleg per aangegeven aanzet.

Deelonderzoek A: Vervolgonderzoek

Vervolgonderzoek 1: Toetsen van het conceptueel model I.

Het resultaat van het literatuuronderzoek is een conceptueel model I waarin een dertigtal criteria beschreven staan. Deze criteria zouden worden getoetst aan de criteria die als resultaat uit de interviews kwamen (Conceptueel model II). Aangezien de interviews geen resultaten hebben opgeleverd dienen de criteria alsnog te worden getoetst. Deze toetsing kan pas plaatsvinden wanneer de risico-analyse vaker in de praktijk wordt toegepast.

Vervolgonderzoek 2: Verder onderzoek naar de factoren die de criteria kunnen beïnvloeden die de kwaliteit van een risico-analyse bepalen.

Het ontwikkeld conceptueel model I is een basis van waaruit verder exploratief onderzoek gedaan kan worden. Onderzocht kan worden welke factoren de criteria beïnvloeden die de kwaliteit van een risico-analyse bepalen.

Vervolgonderzoek 3: Bewust maken van architecten.

Architecten dienen bewust gemaakt te worden dat zij mogelijk bruikbare informatie kunnen leveren voor een vervolgonderzoek waarin conceptueel model I getoetst wordt. Zij leggen immers de basis voor het bouwen en ontwikkelen van nieuwe systemen die beveiligd moeten worden. Tevens kunnen zij mogelijk een bijdrage leveren aan een verder onderzoek naar de factoren die de criteria beïnvloeden die de kwaliteit van een risico-analyse bepalen.

Vervolgonderzoek 4: Het vrijmaken van voldoende budget.

Dit budget is nodig om risico-analyse methoden aan te kunnen schaffen waarvoor betaald moet worden. Een aantal grote organisaties hebben immers een eigen (risico-analyse) methode ontwikkeld, maar om deze in te kunnen zien dient betaald te worden. Indien budget beschikbaar is kunnen deze methoden worden aangeschaft, zodat deze gebruikt kunnen worden in vervolgonderzoek.

Vervolgonderzoek 5: Het bestuderen van de nieuwste versie van Code voor informatiebeveiliging deel een en twee.

De meest recente versie van Code voor informatiebeveiliging deel een en deel twee was tijdens de uitvoering en de uitkomsten van het onderzoek nog niet beschikbaar. Hierdoor kan informatie die vanuit deze bron is onttrokken niet geheel up-to-date zijn. Het gebruik van de nieuwste versie kan mogelijk een verdere aanvulling en onderbouwing geven voor de reeds gevonden antwoorden.

Vervolgonderzoek 6: Het vrijmaken van voldoende tijd.

Voor vervolgonderzoek moet voldoende tijd worden ingepland zodat het gevraagde eindresultaat in verhouding staat met de beschikbare tijd. Tevens ontstaat er door voldoende beschikbare tijd geen limitatie in de mogelijkheden tot uitvoering en uitwerking van het vervolgonderzoek.

Vervolgonderzoek 7: Het houden van een enquête.

Het blijkt dat de respondenten te weinig kennis over het onderzoeksgebied hadden. Dit kan in vervolgonderzoek worden ondervangen door het houden van een enquête zodat er meer mensen vanuit de praktijk ondervraagd kunnen worden. Tevens zouden de vragen op een

hoger abstractie niveau moeten worden gesteld om van daaruit verder de diepte in te kunnen gaan.

Deelonderzoek A: Aanvullend onderzoek

Aanvullend onderzoek 1: Nagaan of door middel van de interviews de respondenten zich bewuster zijn geworden van de beveiliging van digitale informatie en daaraan gekoppeld het opstellen van een risico-analyse.

In een aanvullend onderzoek zou kunnen worden nagegaan of de interviews invloed hebben gehad op het bewustzijn van de respondenten met betrekking tot digitale informatie. Kanttekening hierbij is dat dit onderzoek moet worden uitgevoerd met behulp van de interviewer van de 'eerste ronde' om zodoende de anonimiteit van de respondenten te kunnen waarborgen.

Aanvullend onderzoek 2: Ontwerpen van een procedure voor het ontwikkelen van een eenvoudigere risico-analyse.

Het boekwerk Code voor informatiebeveiliging kan erg overweldigend zijn. De vraag achter dit onderzoek is of het mogelijk is om een procedure te schrijven die minder overweldigend overkomt. Hiermee wordt bedoeld dat er een overvloed aan informatie naar de lezer toekomt. Tevens dient het resultaat meteen inzetbaar te zijn in een bestaande omgeving zonder dat er teveel overhead wordt veroorzaakt.

Aanvullend onderzoek 3: Onderzoek naar hoe technici en managers bewust kunnen worden gemaakt voor de gevolgen van een niet aanwezige / beperkte digitale informatie beveiliging.

Proberen inzicht te krijgen waarom er zo weinig draagvlak is voor digitale informatiebeveiliging en daaraan gekoppeld het maken van een risico-analyse van een firewall. Vervolgens kan worden gekeken hoe dit te verbeteren.

Aanvullend onderzoek 4: Nagaan hoe het re-actieve gedrag bij organisaties met betrekking tot het beveiligen van digitale informatie kan worden omgezet naar pro-actief gedrag.

Voortvloeiend uit aanvullend onderzoek 3, kan worden nagegaan waarom organisaties re-actief gedrag vertonen met betrekking tot het beveiligen van digitale informatie. Vervolgens kan worden onderzocht hoe dit te wijzigen in pro-actief gedrag.

Deelonderzoek B: Vervolgonderzoek

Vervolgonderzoek 1: Het automatiseren van firewall test producten

Er kan gebruik worden gemaakt van de tooling gevonden in paragraaf 9.3 (Tooling voor aanvallen op firewalls) om een programma te schrijven dat automatisch output verzameld en daar conclusies uit kan destilleren. Vervolgens kunnen uit deze conclusies nieuwe acties aangestuurd worden. Tevens kan er gezocht worden naar nieuwe tooling. Aantekening hierbij is dat een gebruiker wel ten alle tijden de automatische testen dient te kunnen beïnvloeden.

Vervolgonderzoek 2: Firewall benaderen via de binnenkant

Door gebruik te maken van een benaderingsmogelijkheid via de binnenkant kunnen kleine afwijkingen en onregelmatigheden die zich in de firewall voordoen worden onderzocht. Het gebruik van een blackbox firewall is hierdoor uitgesloten.

Deelonderzoek B: Aanvullend onderzoek

Aanvullend onderzoek 1: Hoeveel onderhoud vergt een elektronische vorm van een systeem dat een attacktree beheert en is zo'n systeem een handige methodiek om risico's te managen.

Het handmatig onderhouden van een attacktree is een onmogelijke taak. Maar in hoeverre is een elektronisch systeem een oplossing voor deze problematiek en in hoeverre is een elektronisch systeem bruikbaar om een attacktree te beheren.

Aanvullend onderzoek 2: Is een attacktree te gebruiken als een documentatie instrument voor de risico-analyse.

In het onderzoek is gebleken dat het gebruik van een attacktree niet handig is om te gebruiken als een instrument om aanvallen te voorkomen. Maar is de attacktree een methode die gebruikt kan worden als documentatie instrument, zodat het achteraf gebruikt kan worden om de aanval na te gaan.

Dat een firewall steeds vaker gebruikt wordt om digitale informatie af te schermen is bekend. Maar wie zegt dat de firewall inderdaad ook veilig is? Is er een algemeen keurmerk dat een bepaald kwaliteitsniveau voor firewalls garandeert? Of vertrouwen we de verkopers van de firewalls? Eigenlijk zijn we op zoek naar een testmethode waarbij een firewall een bepaald veiligheidscertificaat kan krijgen. Dit onderzoek geeft aanzet tot het ontwikkelen van zo'n soort certificaat. Eerst dient duidelijk te zijn hoe een firewall op een gestructureerde en documenterende manier aangevallen kan worden.

Bijlagen

13 Figuren

14 Bronvermelding

14.1 Literatuur

Abels, A.A., 1987, De relatie tussen organisatie en omgeving, een beschouwing over enkele elementen uit de afhankelijkheidstheorie, uit Kijk op organisaties, 1987, Stenfert Kroese, Leiden

Baas, K., K. Anzenhofer, C. Hendriks, 1997, Beginselen van bedrijfsnetwerken, Kluwer bedrijfsinformatie, Deventer

Baron, R.M., D.A. Kenny, 1986, The moderator-mediator variable distinction in social psychological research, conceptual, strategic and statistical considerations, Journal of personality and social psychology, vol. 51, afl. 6, ISSN 0022-3514

Berlijn, J.B., 2007, Risico's en firewalls, Bevindingen van een exploratief onderzoek naar risico-analyses van en aanvalsmethodieken op firewalls

Bernstein, D.J., 2005, Understanding brute force, Department of Mathematics, Statistics, and Computer Science (M/C 249), The University of Illinois, Chicago

Doorewaard, H., P. Verschuren, 2005, Het ontwerpen van een onderzoek, derde druk, Uitgeverij LEMMA BV Utrecht

Gorden, L.A., Loeb, M.P. Loeb, Luchyshen W, Richardson R, 2005, CSI/FBI Computer Crime and Security Survey, Computer Security Institute

Grashion, A., 2006, Veilig (net)werken met Enterprise Infranet, in Telematica, Nieuwsbrief over ontwikkkelingen en toepassingen, jaargang 17, nummer 1/2, januari 2006

Haisma, G., 1999, Risicomanagement: een bijdrage aan continuïteit in organisaties, Organisatie instrumenten: Sturingsinstrumenten voor de manager, December 1999

Jasano, S., M. Deborah, H. Rachelle, 1991, Accepteble evidence in a pluralistic society, Accepteble Evidence: Science and values in risk management, Oxford University Press

Jentjens, V., M. de Graaf, 2004, Geïntegreerde informatiebeveiliging, De sleutel tot succesvolle implementatie, Lemma BV, Utrecht

Kaufman, C., R. Perlman en M. Speciner, 2002, Network security, Private communication in a public world Second Edition, Prentice Hall

Kurose, J.F., K.W. Ross, 2001, Computernetwerken, Een 'top-down'-benadering, Addison Wesley Longman

Liere, A. van, 2005, Strategische inzet van internet, uit Management tools en communicatie, nummer 2, april 2005, Kluwer

Mackenzie Owen, J.S., 2001, Kennismanagement, Handboek Informatiewetenschap

Mastrigt, R.H. van, 2006, Informatiebeveiliging VoIP noodzaakt integrale benadering, uit Telematica, Nieuwsbrief over ontwikkelingen en toepassingen, jaargang 17, nummer 5, mei 2006

Mauw, S., M. Oostdijk, 2006, Foundations of attacktrees, In the proceedings of the International Conference on Information Security and Cryptology (ICISC 2005, Seoul), LNCS 3935, pp. 186-198, attacktrees: door de bomen de bedreigingen zien, ICISC`05, via http://www.win.tue.nl/~sjouke/publications/papers/gvib.pdf

NEN, 2000, ISO 27001, Deel 1: Code voor informatiebeveiliging, Nederlands Normalisatie-instituut, Normcommissie 38127

NEN, 2000, ISO 27003, Deel 2: Specificatie voor managementsystemen voor informatiebeveiliging, Nederlands Normalisatie-instituut

Oud, E.J., 2002, Praktijkgids Code voor informatiebeveiliging, De standaard voor informatiebeveiliging met succes invoeren bij uw organisatie, Academic Services

Pfleeger, S.H., 2000, Risky Business: What we have yet to learn about risk management, The Journal of Systems and Software 53, p. 265-273

Pluis, R., 2005, Firewalls, Lemma

Prins, J, 1997, De informatie-markt, De zakelijke mogelijkheden van Internet, Samsons bedrijfsinformatie

Rood, G, A, M, 2001, Bedrijfscommunicatie & bedrijfscultuur, Kluwer

Schneier, B., 1999, attacktrees: modeling security threats, Dr. Dobb`s journal, december 1999

Schneier, B., 2001, Full Disclosure, Crypto-Gram Newsletter, 15 November 2001

Stevens, W.R., 1994, TCP/IP Illustrated, Volume 1: The Protocols, Addison-Wesley

Stoneburner, G., A. Goguen en A. Feringa, 2002, Risk management guide for information technology systemems, National Institute of Standards and Technology

Vliet, E. van der, R. Solingen, H. Westerink, 2006, Van je fouten moet je leren, uit Informatie, Maandblad voor informatievoorziening, jaargang 48/2, maart 2006

Whittemore, S., 1983, Facts and values in risk analysis for environmental toxicants

14.2 Websites

WWW-1
Peripheral
http://en.wikipedia.org/wiki/Peripherals
Laatst bekeken: 20 Augustus 2006

WWW-2
Frequently Asked Questions (FAQs) about CERT
http://www.cert.org/faq/cert_faq.html
Laatst bekeken: 13 Augustus 2006

WWW-3
An Analysis of Security Incidents on the Internet 1989-1995
http://www.cert.org/research/JHThesis/Chapter1.html
Laatst bekeken: 20 Augustus 2006

WWW-4
CERT/CC Statistics 1988-2006
http://www.cert.org/stats/cert_stats.html
Laatst bekeken: 13 augustus 2006

WWW-5
Statistics on Federal Incident Reports
http://www.us-cert.gov/federal/statistics/
Laatst bekeken: 20 Augustus 2006

WWW-6
Cisco Catalyst 6500 Series Firewall Services Module
http://www.cisco.com/en/US/products/hw/modules/ps2706/ps4452/index.html
Laatst bekeken: 20 Augustus 2006

WWW-7
Switched firewalls
http://products.nortel.com/
go/product_content.jsp?segId=0&catId=null&parId=0
&prod_id=36220&locale=en-US
Laatst bekeken: 20 Augustus 2006

WWW-8:
Diensten van de productgroep security
http://snow.nl/sn/Security/
Laatst bekeken: 13 Augustus 2006

WWW-9:
Information security
http://www.bsi-emea.com/InformationSecurity/index.xalter
Laatst bekeken: 13 Augustus 2006

WWW-10
Het midden- en kleinbedrijf in een oogopslag
http://www.mkb.nl/Het_midden-_en_kleinbedrijf
Laatst bekeken: 20 Augustus 2006

WWW-11
White hat, gray hat, black hat
Hackers can teach government and industry valuable IT security lessons
http://www.fcw.com/article90994-10-03-05-Print
Laatst bekeken: 20 Augustus 2006

WWW-12:
Sterke groei phishing-mails in maart,
http://www.nu.nl/news/505834/50/'Sterke_groei_phishingmails_in_maart'.html
Laatst bekeken: 13 Augustus 2006

WWW-13:
Officier zet pc vol gevoelige informatie op straat (video)
http://www.nu.nl/news.jsp?n=422656&c=14
Laatst bekeken: 13 Augustus 2006

WWW-14:
Sesam open U
http://www.netkwesties.nl/editie35/artikel4.html
Laatst bekeken: 13 Augustus 2006

WWW-15:
Myspace infecteert miljoen gebruikers
http://www.webwereld.nl/articles/42085/explorer
Laatst bekeken: 13 Augustus 2006

WWW-16:
Helft fouten Microsoft gevolg van paar bugs
http://www.webwereld.nl/articles/7003
Laatst bekeken: 13 Augustus 2006

WWW-17:
Being prepared for intrusion,
http://www.ddj.com/184404565
Laatst bekeken: 13 Augustus 2006

WWW-18:
The award-winning, free webbrowser
http://www.mozilla.com/firefox/central
Laatst bekeken: 13 Augustus 2006

WWW-19:
The apache http server is an open-source http server for modern operating systems
http://httpd.apache.org/
Laatst bekeken: 13 Augustus 2006

WWW-20:

List of all http rfcs
http://www.w3.org/Protocols/Specs.html
Laatst bekeken: 13 Augustus 2006

WWW-21:
Internet protocols background,
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ip/htm
Laatst bekeken: 13 Augustus 2006

WWW-22:
IPv6
http://www.ipv6.org/
Laatst bekeken: 13 Augustus 2006

WWW-23:
Internet Protocol Version 6
http://nl.wikipedia.org/wiki/IPv6
Laatst bekeken: 13 Augustus 2006

WWW-24:
"DMZ - Demilitarized Zone"
http://compnetworking.about.com/cs/networksecurity/g/bldef_dmz.htm
Laatst bekeken: 13 Augustus 2006

WWW-25:
The art of port scanning,
http://insecure.org/nmap/nmap_doc.html
Laatst bekeken: 13 Augustus 2006

WWW-26
Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection
http://insecure.org/stf/secnet_ids/secnet_ids.html
Laatst bekeken: 13 Augustus 2006

WWW-27:
Gepeilde kennis is macht
http://www.leidenuniv.nl/mare/2004/07/libri07.html
Laatst bekeken: 13 Augustus 2006

WWW-28
Denial of Service Attacks
http://www.cert.org/tech_tips/denial_of_service.html
Laatst bekeken: 17 Augustus 2006

WWW-29
Malicious Code / Phishing Alert: Data Stolen via ICMP
http://www.websense.com/securitylabs/alerts/alert.php?AlertID=570
Laatst bekeken: 13 Augustus 2006

WWW-30
CVE-2003-0364
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0364

Laatst bekeken: 20 Augustus 2006

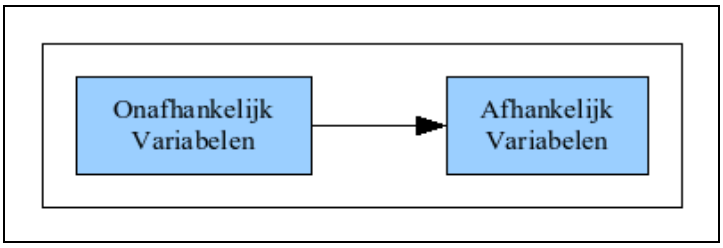
15 Afkortinglijst

Afkorting	*Betekenis*
IP	Internet Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
ICMP	Internet Control Message Protocol
ssh	Secure Shell
RFC	Request For Comments
IETF	Internet Engineering Task Force)
HTTP	HyperText Transfer Protocol
WWW	World Wide Web
OSI	Open System Interconnection
SSL	Secure Sockets Layer
VPN	Virtual Private Network
SMTP	Simple Mail Transfer Protocol

16 Appendix

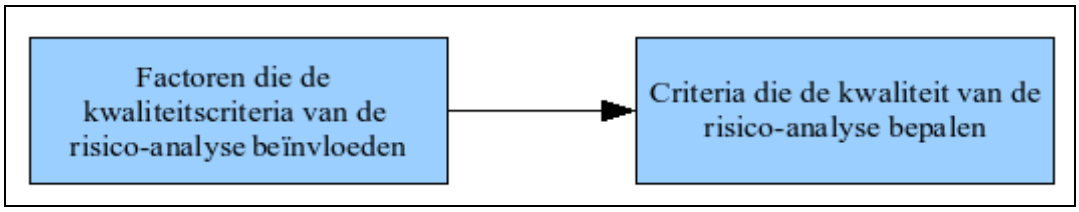
16.1 Analyse framework

Om het resultaat van dit onderzoek te verduidelijken wordt in deze paragraaf het analyse framework uitgewerkt. Het analyse framework geeft de relatie weer tussen de gevonden criteria in dit onderzoek. Als basis is gebruikt gemaakt van het volgende (Zie Figuur 19) causale model.



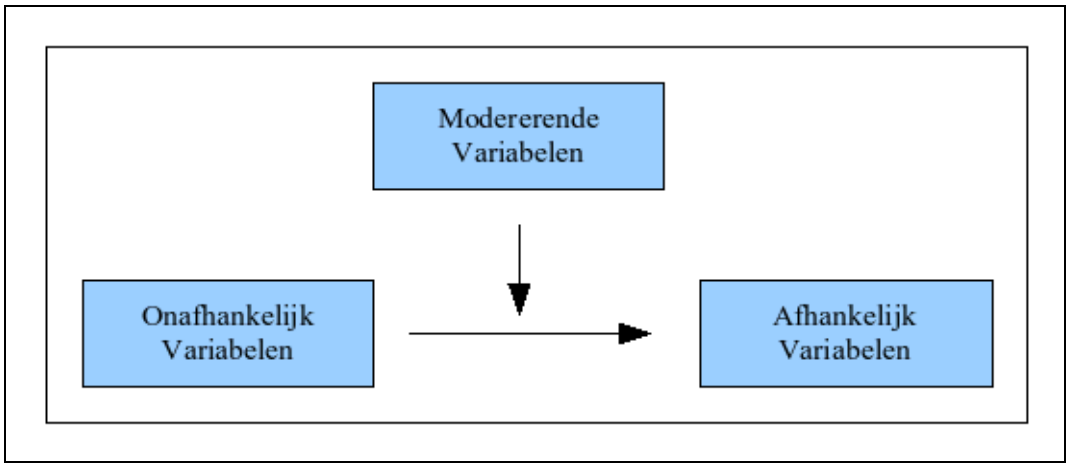
Figuur 19: Standaard causale relatie (Berlijn, 2007)

De onafhankelijke variabelen zijn de factoren die de kwaliteit van de risico-analyse beïnvloeden. De afhankelijke variabelen zijn de factoren die de kwaliteit van de risico-analyse bepalen. Oftewel er wordt een relatie gelegd tvan de factoren die de kwaliteit van de risico-analyse beïnvloeden naar de factoren die de kwaliteit van van de risico-analyse bepalen (Zie Figuur 20).



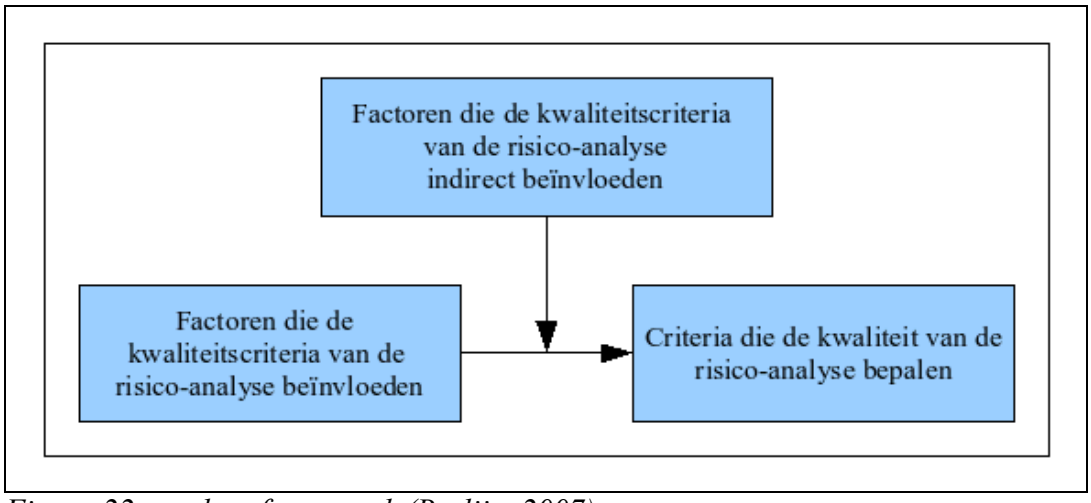
Figuur 20: analyse framework (Berlijn, 2007)

Toch kunnen er factoren zijn die de kwaliteit van de risico-analyse beïnvloeden, maar niet direct in relatie staan met de factoren die de kwaliteit van de risico-analyse bepalen. Daarom wordt er een modererende variabele, zoals gedefinieerd door Baron & Kenny, geïntroduceerd (Baron, 1986: 1173).



Figuur 21: Basic modererende causale relatie (Berlijn, 2007)

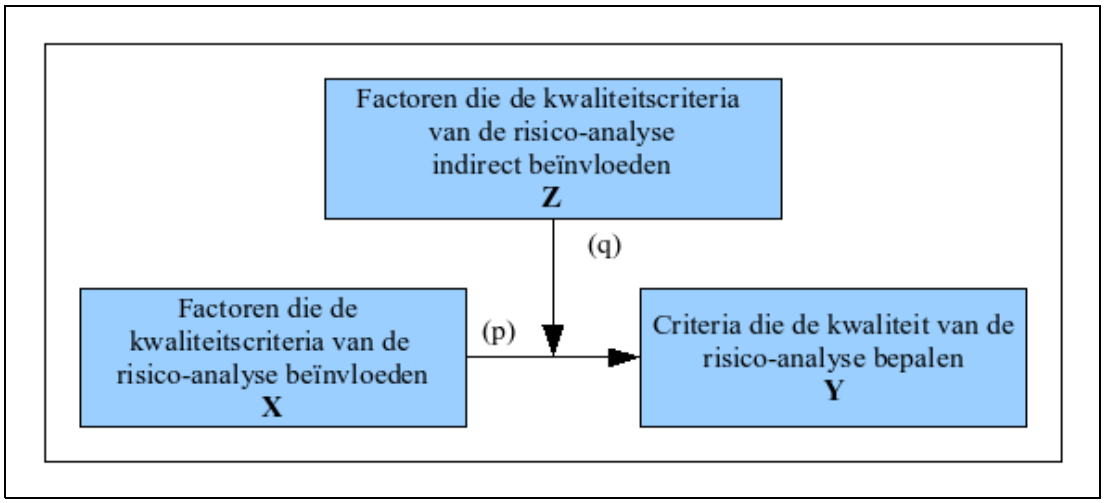
Zie Figuur 21 en Figuur 22 voor de vernieuwde modellen. In deze modellen is de modererende variabele verwerkt.



Figuur 22: analyse framework (Berlijn, 2007)

De onafhankelijke variabelen zijn de factoren die de kwaliteit van de risico-analyse beïnvloeden. De afhankelijke variabelen zijn de factoren die de kwaliteit van de risico-analyse bepalen. De modererende variabelen zijn de factoren die de kwaliteit van de risico-analyse indirect beïnvloeden (Zie Figuur 22).

Aangezien er regelmatig geschreven wordt over verschillende soorten factoren en de relatie tussen deze factoren, gebruiken we Figuur 23 als het uiteindelijk analyse framework binnen dit onderzoek. In dit model wordt elke factor benoemd zodat door middel van deze benoeming er duidelijker gerefereerd wordt naar de juiste factor of de relatie tussen een tweetal factoren.



Figuur 23: Labeled analyse framework (Berlijn, 2007)

Voorbeeld:

Er is een kwaliteitsfactor **Y** "stabiliteit", dat wil zeggen in hoeverre een firewall operationeel moet zijn of i hoe vaak de firewall niet hoeft te werken. Bijvoorbeeld om een up-grade, het vernieuwen van software / hardware, uit te voeren. Als we daarbij voor factor **X** een standaard "negen tot vijf" organisatie nemen, dan hoeft in dit geval de firewall maar van "negen tot vijf" operationeel te zijn. Tevens gaan we er vanuit dat er een relatie **(p)** bestaat die factor **X**, de organisatie, verbind met factor **Y**, de kwaliteits factor "stabiliteit".

Als daarentegen leveranciers of klanten, factor **Z**,van organisatie **X** van zeven tot acht uur werken, dan dient de firewall van zeven tot acht uur operationeel te zijn. Dit is de relatie **(q)** die effect heeft op relatie **(p).**

Maar stel dat organisatie **X** een webwinkel is. Dit soort organisaties willen dat hun beschikbaarheid zeer hoog ligt, dat wil zeggen vierentwintig uur per dag, zeven dagen in de week. Dan dient de firewall dus ook 24 / 7 operationeel te zijn. (Hier wordt automatisch vanuit gegaan dat we dus inderdaad praten over een firewall die gebruikt wordt om te communiceren tussen factor **X** en factor Y.

16.2 Management literatuur samenvattingen

Binnen dit onderzoek is volgende literatuur is gebruikt:

1. Haisma, G; 1999; Riscomanagement: een bijdrage aan continuïteit in organisaties (Haisma, 1999).
2. Stoneburner, G; 2003;Risk Management Guide for Information Technology Systems (Stoneburner, 2002).
3. Pfleeger, S; 2000; Risky Business: what we have yet to learn about risk management (Pfleeger, 2000).

In de volgende secties worden de samenvattingen beschreven:

Risicomanagement: een bijdrage aan continuïteit in organisaties

Als eerst de resultaten van “Risicomanagement: een bijdrage aan continuïteit in organisaties”, geschreven door drs.G. Haisma in december 1999. De onderstaande kenmerken komen in dit artikel naar voren.

- Structuur factoren (Hoe zit het document in elkaar)
    - Moet alle gebieden bestrijken; de risicocategorieën worden gebruikt als een checklist om vanuit een `volledig' aantal invalshoeken naar risico's te speuren binnen een risicogebied.
        - Materiële risico's
        - Procesrisico's
        - Aansprakelijkheidsrisico's
        - Productrisico's
        - Imagorisico's
        - Financiële risico's
        - Milieurisico's
        - Arbeidsrisico's
        - Informatierisico's
- Risicobeoordeling=Kans*Gevolg Financieel*Bedrijfsimpact

Risk Management Guide for Information Technology Systems

Als tweede de resultaten van “Risk Management Guide for Information Technology Systems”, geschreven door Gary Stoneburner, Alice Goguen en Alexis Feringa van de NIST National Institute of Standards and Technology. De onderstaande kenmerken komen uit dit artikel. (Stoneburger, 2006)

Output:

- Systeem karakteristieken
  - Systeem grenzen
  - Systeem functies
  - Systeem data criteria
  - Systeem data sensitiviteit
- Gevaar identificatie
  - Gevaar “statement”
- Kwetsbaarheden identificatie
  - Lijst van potentiële kwetsbaarheden
- Proces aansturing analyse
  - Lijst van huidige en geplande Proces aansturing
- Waarschijnlijkheid bepalen
  - Waarschijnlijkheid classificatie
- Risico bepaling
  - Risico en aanverwante risico niveaus
- Proces aansturing aanbevelingen
  - Proces aansturing aanbevelingen

Een risico management rapport is een rapport dat senior management helpt om beslissingen te kunnen nemen over strategie, procedure en management veranderingen. Een risico management rapport dient niet veroordelend geschreven, dit wil zeggen dat er geen verwijten in het rapport staan, te worden maar op een systematisch en analytische manier geschreven te zijn.

Opbouw van een management rapport

1. Introductie
2. Scope van het document

3. Beschrijf de systeem componenten, gebruikers, locatie en andere systeem details vande omgeving die in de risico-analyse zitten.
4. risico-analyse benadering
    1. De participanten (het risico-analyse team)
    2. Technieken die gebruikt worden om de informatie te verzamelen (gebruik van tooling en questionairs)
    3. De ontwikkeling en beschrijving van de risico schalen
5. Systeem kenmerken:
    1. Het karakteriseren van het systeem dat bestaat uit:
        1. Hardware: Server, routers, Switch
        2. Software: Application, Operating System Protocol
        3. Systeem interfaces: Communicatie Link (remote, local)
        4. Data:
        5. Gebruikers:
    2. Een overzicht van een connectiviteit diagram of een input en output flowchart die de scope en de afkadering van de risico-analyse beschrijven
6. Gevaar statement
    1. Samenstellen en categoriseren van potentiële dreiging-sources en de daaraan gerelateerde dreiging acties die van toepassing zijn op het systeem.
7. risico-analyse resultaat
    1. Een lijst van observaties van kwetsbaarheden / dreigingen. Elke observatie dient minimaal de volgende kenmerken te bevatten:
        1. Observatie nummer een een korte beschrijven van de observatie, bijvoorbeeld Gebruiker wachtwoorden kunnen makkelijk geraden of gekraakt worden.
        2. Een discussie van de dreiging-source en het kwetsbaarheden paar.
        3. Identificatie van de bestaande soepele security aansturing
        4. Waarschijnlijkheid discussie en evaluatie (hoog, medium, laag waarschijnlijkheid)
        5. Impact analyse en evaluatie (hoog, medium, laag impact)
        6. Risico rating gebaseerde risico niveau matrix (hoog, medium, laag niveau)
        7. Aanbevolen beheersing of alternatieve opties om risico te reduceren
8. Samenvatting
    1. Totaal aantal van observaties. Samenvatting van de observaties, de geassocieerde risico niveau en commentaren in tabel formaat om de implementatie van aanbevolen beheersing te faciliteren.

Risky Business: what we have yet to learn about risk management

Als derde “Risky Business: what we have yet to learn about risk management” is geschreven door Shari Lawrence Pfleeger De onderstaande kenmerken komen uit dit artikel.

- Er zijn drie grote problemen met risico management
  - Valse precisie
  - Slecht wetenschap
  - Verwarring tussen feiten en waarden
- Laat je niet voor de gek houden door “bediscussieerde wetenschap”
- Splits feiten en waarden als het mogelijk is
- In verschillende boeken, artikels, tutorials en boeken worden een drietal punten gekeken om te beslissten hoe wat risico's zijn:
  - Een verlies geassocieerd met een gebeurtenis. De gebeurtenis creëert een situatie waar iets negaties gebeurt tot het project. Verlies van tijd, kwaliteit, geld, sturing etc.
  - De waarschijnlijkheid waarmee een gebeurtenis gebeurt. Er moet enige idee van waarschijnlijkheid zijn waarmee een gebeurtenis zal kunnen gebeuren.
  - In welke mate kan de resultaat van een gebeurtenis veranderd worden. Voor elke risico zal er bepaald meoten worden hoe de impact van een gebeurtenis geminimaliseerd kan worden.
- Risico waarschijnlijkheid veranderd over tijd zoals ook de impact. Deze dienen dus van tijd tot tijd in de gaten gehouden te worden.
- Er zijn een tweetal verschillende grote risico groepen: Algemene risico en project specifieke risico's.
  - Algemene risico's algemeen bij software projecten zijn:
    - Mis-interpretatie van requirements
    - Verlies van belangrijke personeel (voor het project)
    - Onvoldoende tijd om te testen
- Project risico's zijn:
    - Onveiligheden van specifiek aan het projecten
- Er zijn een tweetal verschillende type risico's:
  - Vrijwillig
    - Gebruik maken van mensen met weinig expertise op een gebied van het project
  - Onvrijwillig risico
    - Het gebruik maken van een nieuw ontwikkel platform
- Een numerieke beschrijving van risico geeft meer geloofwaardigheid dan kwalitatief beschrijving van risico ook al is de kwantitatief beschrijving onbetrouwbaar lijkt.
- “Numerical assessments possess a kind of symbolic neutrality that is rarely attained by qualitative formulations about the 'weight' or 'suffiency' of the evidence”[9]
- Fouten en onbetrouwbaarheid zijn onderschat wanneer de populatie grote te klein is.
- De wetenschap van psychologie van risico perceptie verteld dat:

  > “Both scientists and lay people may underestimate the error and unreliability in small samples of data, particularly when the results are consistent with preconceived, emotion-based beliefs"[8]

16.3 Interviewguide

Deze appendix beschrijft de interviewguide. Hier worden de vragen, die gesteld zijn in de interviews en de reden waarom die gesteld zijn, beschreven. Sommige vragen zijn geclusterd om de reden dat deze vragen één en dezelfde doel hebben.

Algemene hoofdvraag

Vraag 1: Technicus / Manager

Deze vraag wordt gesteld om duidelijk te maken vanuit welke visie de respondent werkt. Het is mogelijk dat een respondent beide activiteiten ontplooit.

Organisatie

Vraag 2: Technicus / Manager
Vraag 3: Wat doet uw organisatie?
Vraag 4: Uit hoeveel personeel leden bestaat uw organisatie?
Vraag 5: Wat doet uw business unit / afdeling?
Vraag 6: Uit hoeveel personeel leden bestaat uw business unit / afdeling?

De bovenstaande vragen worden gesteld om inzicht te krijgen of er nog grote verschillen zijn tussen verschillende organisaties met betrekking tot dit onderzoek. Elke vraag is bedoeld om een betere afkadering te krijgen.

Functie

Vraag 7: Wat is uw functie beschrijving en hoe verbind u zich met informatie beveiliging?

De vraag is bedoeld om een indicatie te krijgen of er een aparte functie voor dit onderwerp is of dat het werken met de firewall een onderdeel is van een andere functie.

Vraag 8: Wat is uw opleiding niveau / werk ervaring in dit specialistisch gebied?

Om inzicht te krijgen in hoeverre de respondenten ervaring hebben met het gebruik van een firewall.

Vraag 9: Hoe lang werkt U al in deze functie?

Om de werkervaring van de respondent te bepalen en in hoeverre de antwoorden gebaseerd zijn op werkervaring.

Risico-analyse-rapport

Vraag 10: Wat is het doel van het maken van een risico-analyse ten behoeve van een netwerk/firewall?

Om een indicatie te krijgen wat de reden is achter het maken van een risico-analyse. Is het een onderwerp wat hiërarchies is opgelegd of is het maken van een risico-analyse iets wat ondersteunt wordt door de afdeling zelf.

Vraag 11: Wordt risico-analyse effectief gebruikt binnen de organisatie?

Deze vraag is bedoelt om na te gaan in hoeverre een risico-analyse ook daadwerkelijk binnen de organisatie wordt gebruikt.

Vraag 12: Hoe vaak wordt deze risico-analyse gemaakt of bijgewerkt?

Om een indicatie te krijgen of het een eenmalig proces is of dat er structureel naar de risico-analyse wordt gekeken.

Vraag 13: Wie maakt de risico-analyse?

Vraag 14: Welke procedures en/of methodes worden hiervoor?

Vraag 15: Uit hoeveel pagina's bestaat de risico-analyse?

De bovenstaande vragen zijn bedoeld om inzicht te krijgen in het verloop van de procedure van het maken van een risico-analyse.

Vraag 16: Wat vind je persoonlijk goede en/of slechte punten van de huidige methode en/of risico-analyse?

Een algemene open vraag om meer informatie van de respondent te krijgen, is wat de respondent vindt van de risico-analyse. Dit kan anders zijn dan wat er door de organisatie gedaan wordt.

Vraag 17: Algemeen: Hoe bepaal je de kwaliteit van de risico-analyse?

Dit is de laatste vraag van de vragenlijst van de interview. Hierna kan de respondent vrijelijk praten over de risico-analyse proces.

16.4 Interviewguide presentatie

In deze paragraaf is de presentatie beschreven die als inleiding diende voor de gehouden interviews.

Verloop Interview

- Algemene punten
- Kleine presentatie / voordracht voor uw beeldvorming
- Vervolgens korte interview vragen voor mijn beeldvorming
  - Organisatie
  - Functie
  - Risico analyse document
- "Het" interview

1

Algemene Punten

- Tijdsduur interview
  - Beperkt, daarom vrij gestructureerd
- Exploratief, onderzoek van drie maanden
- Alle informatie wordt anoniem behandeld!
- Verificatie door middel van goedkeuring van het verslag.

2

Inleiding Presentatie I

- Kennismaking:
  - Wie ben ik?
- Doel van het interview
  - Waarom doe ik dit onderzoek?
- Afkadering
  - Wat wil ik precies onderzoeken?

3

Inleiding Presentatie II

- Welke case is van toepassing:
  - Case I: "de beslisser"
  - Case II "de maker"
- Classificatie
  - Raamwerk om interview te leiden
- Inleidende vragen
- Het Interview
- Afronding

4

Kennismaking

- Jasper Berlijn
  - Onderzoek voor master-scriptie
- Radboud Universiteit
  - Faculteit der Natuurwetenschappen, Wiskunde en Informatica
  - Security of Systems (SoS)
- Richting
  - Informatica/Management

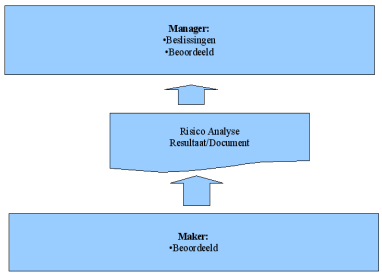
5

Waarom / Doel van Interview

- Doel:
  - Informatie verzamelen voor mijn onderzoek:
    - Kwaliteits factoren van een risico analyse ten behoeve van een firewall bepalen.
- Waarom:
  - Uit eerdere ervaringen:
    - Hoe beslis je nu of een risico-analyse resultaat met betrekking op een firewall, oftewel een risico-analyse document, van voldoende kwaliteit is.
  - Persoonlijke interesse

6

Afkadering I



Afkadering II

- Risico-analyse
  - Welke risico's loopt de digitale informatie bij het gebruik van een netwerk.
  - Quote: “Wij hebben een firewall, dus onze digitale informatie is veilig!”
- Wat bedoelen we precies met factoren?
  - Kenmerken
  - Eisen
  - Verwachtingen

8

CASE 1

- U wilt bepalen of het netwerk van een organisatie afdoende beveiligd is en, of het voldoet aan de gestelde beveiligings eisen.
- U laat een risico-analyse uitvoeren, vervolgens krijgt u een risico-analyse rapport.
- *U vraagt zich nu af of het risico-analyse rapport van voldoende kwaliteit is om er gefundeerde keuzes mee te maken.*

9

CASE 2

- U krijgt een project waarbij u voor een organisatie moet bepalen hoe veilig hun netwerk omging is.
- *U vraagt zich af wat de punten zijn die je minimaal in het rapport wilt zetten.*
- U levert een rapport op.

10

Classificatie

- Meest belangrijke
  - Moet, want ...
  - Mag, maar ...
  - Leuk, maar ...
  - Juist niet!, want ...
- Categorieën
  - Algemeen
  - IT
  - Firewall

11

Inleidende Vragen I

- Organisatie:
  - Wat doet de organisatie?
  - Hoe groot is de organisatie?
  - Hoe groot is de business unit / afdeling?
- Functie
  - Wat is uw functie beschrijving?
  - Wat is uw opleidingsniveau / werk ervaring?
  - Hoe lang werkt u al in deze functie?

12

Inleidende Vragen II

- Risico-analyse document
  - Wat is het doel van het maken ervan?
  - Hoe vaak wordt het gemaakt of bijgewerkt?
  - Wie maakt het?
  - Welke procedures worden er gebruikt?
  - Uit hoeveel pagina's bestaat het?
  - Is de risico-analyse gebruikt binnen de organisatie?

13

Het Interview

- Click to add an outline

14

Afsluiting

- Kent u mogelijke andere respondenten?
- Wat is de meest gebruikte literatuur, en wat zijn de meest gebruikte bronnen van informatie.
- Dank
- Vragen?

15

16.5 Verslaglegging interviews

In deze paragraaf worden de gehouden interviews los van elkaar uitgewerkt.

Interview I

Maker / ~~Manager~~

Organisatie

Wat doet uw organisatie?
Consulting

Uit hoeveel personeelsleden bestaat uw organisatie?
-

Wat doet uw business unit / afdeling?
Security audits en consulting

Uit hoeveel personeelsleden bestaat uw business unit / afdeling?
+/- 50 man

Functie

Wat is uw functiebeschrijving en hoe verbindt u zich met informatie beveiliging?
Manager van audit teams

Wat is uw opleidingsniveau / werkervaring in dit specifieke gebied?
Professor op de Faculteit der Natuurwetenschappen, Wiskunde en Informatica (FNWI)
afdeling
Security of Systems (SoS)

Hoe lang zit u al op deze functie?
7 Jaar

Risico-analyse document

Wat is het doel van het maken van een risico-analyse ten behoeve van een netwerk / firewall?
Of je de IT gerelateerde risico's onder controle hebt. En of CIA toegepast wordt.

Wordt risico-analyse effectief gebruikt binnen de organisatie?
Ja!

Hoe vaak wordt de risico-analyse gemaakt of bijgewerkt?
1 keer per jaar valideren, of het risicobeheer proces goed wordt toegepast.

Wie maakt de risico-analyse?
-

Welke procedures en / of methodes worden hiervoor gebruikt?
SPRINT/SARA van Information Security Forum (ISF)

SPRINT “Simplified Process for Risk Identification” en
SARA (Simple to Apply Risk Analysis for Information Systems) en vergelijkbare methodieken.

Uit hoeveel pagina's bestaat de risico-analyse?
Per object ongeveer 3 pagina's

Wat vindt u persoonlijk goede en / of slechte punten van de huidige methode en / of risico-analyse?

Hoe wordt de kwaliteit van de risico-analyse bepaald?

Andere respondenten
Wordt over nagedacht en via mail opgestuurd.

Overige

Audit: Is een 'controle' van de bestaande risico analyse “een risico-analyse van een risico-analyse”

Een risico-analyse dient intern gemaakt te worden aangezien het eigen personeel het beste de waarde van de 'assets' kan bepalen.

Een audit dient daarin tegen door een externe organisatie te worden gedaan.

Bij een audit worden de volgende punten van een risico-analyse gecontroleerd:

Beheer:

Bestaan er risico-analyse procedures?
Change management: Worden de aanpassingen, de veranderingen, toevoegingen of verwijderingen van systemen in de omgeving, bijgehouden en verwerkt volgens de bestaande procedures?
Wordt de logging, die de firewall genereert, regelmatig (afhankelijk per bedrijf, maar toch minimaal één keer per maand) gecontroleerd/geëvalueerd door de beheerder?

Configuratie:

Controle van de firewall rule set.

- Alle rules die niet gedocumenteerd zijn en niet nodig zijn dienen verwijderd te worden.
- Er dient duidelijke documentatie aanwezig te zijn van de gebruikte rule set.
- Er dient duidelijk te zijn wie verantwoordelijk is voor het gehele systeem en de 'loose' rules.

Controleren of het functioneert zoals bedoeld, hierbij wordt vaak gebruik gemaakt van penetratie testing.

Per scenario minimaal de volgende informatie: (SPRINT)

Assets
Bedreigingen
Vulnerabilities

Een risico-analyse/audit wordt gemaakt op “gevoel”.

In de praktijk bestaat een goede 'risico-analyse' bijna nooit.

Een firewall kan je eigenlijk niet als een los systeem zien. Het is een onderdeel van een groter netwerk. Je dient dus eigenlijk niet vanuit de optiek van een firewall te kijken. Deze visie is “technisch” georiënteerd terwijl er vaak vanuit een “business” perspectief gekeken wordt. Bij dit perspectief wordt de risico-analyse vanuit de applicatie opgebouwd en is de firewall een tool die gebruikt wordt om de veiligheid te kunnen garanderen. De applicatiebeheerders bepalen welke functionaliteit van de firewall nodig is en geven dit als eis door. Het risico ligt bij de applicatiebeheerder niet bij de firewall.

Er dient een tweedeling van de systemen te zijn: “kritisch” en “niet kritisch”. Alle systemen dienen aan een “baseline security” te voldoen. De “baseline security” is de minimale grens waaraan elk systeem binnen de organisatie dient te voldoen. Daarintegen dient elk kritisch systeem aan een hoge kwaliteitseis te voldoen. Per kritisch systeem dient minimaal de volgende informatie bekend te zijn:

1. Wat doet het systeem
2. Wie is verantwoordelijk voor het systeem
3. Vertrouwelijkheid
4. Integriteit
5. Beschikbaarheid

Verdeling van laag/medium/hoog is voldoende

Afhankelijk van het type organisatie, bank of kruidenierswinkel, verschilt de diepgang van de risico-analyse, oftewel het aantal scenario's dat beschreven is.

Voor de volledigheid en betrouwbaarheid dienen de scenario's gemaakt te zijn door middel van een 'workshop' van meerdere personen die de 'assets' gebruiken. De scenario's dienen niet door één persoon gedaan te worden.

CIA is zeer belangrijk. (Confidentiality, Integrity, Availability) of in het Nederlands VIB (Vertrouwelijkheid, Integriteit en Beschikbaarheid)

Elk jaar dient de risico-analyse gecontroleerd te worden op het beleid en compleetheid.

Algemene kwaliteit eis: Spelfouten / opmaak document

Opmerking: Bij de letterlijke toepassing van het Voorschrift Informatiebeveiliging Rijksdienst (VIR) dient elke systeem een volledige security assessment te krijgen. In plaats van alleen de 'belangrijke'/hoog risico systemen.

Opmerking: Bij de huidige onderzoeksvisie is vanuit technisch oogpunt gekeken en niet via een veel gebruikte organisatorische visie.

Opmerking: Risico-analyse is een algemene benaming en daardoor is moeilijk te bepalen wat er nu precies in dient te staan.

Interview II

Maker / ~~Manager~~

Organisatie

Wat doet uw organisatie?
Binnen de organisatie staat uitwisseling en overdracht van kennis centraal. Wetenschappers communiceren met collega's over de hele wereld. Er wordt onderzoek gedaan.

Uit hoeveel personeelsleden bestaat uw organisatie?
+/- 10.000

Wat doet uw business unit / afdeling?
De volgende taken worden verzorgd door de afdeling:

- Systeembeheer
- Netwerkbeheer
- Telefoniebeheer
- Werkplek ondersteuning

Voornamelijk voor een suborganisatie van bovenstaande organisatie, maar soms ook daarbuiten.

Uit hoeveel personeelsleden bestaat uw business unit / afdeling?
+/- 12 man

Functie

Wat is uw functiebeschrijving en hoe verbindt u zich met informatie beveiliging?
Facultaire Beveiligings Coördinator,
lid van bovenstaande organisatie CERT team,
Systeem/Netwerk beheerder,

Wat is uw opleidingsniveau / werkervaring in dit specifieke gebied?
Universitaire bèta opleiding (natuurkunde), daarna gepromoveerd.
Voornamelijk zelfstudie aangezien de respondent dit sneller en goedkoper vond dan cursussen te volgen.
Conferentie bezoeken zoals LISA (Large Installation System Administration Conference)
Ervaring met Solaris, routers (ACL).
Specialisatie algemeen beveiligen.

Hoe lang zit u al op deze functie?
+/- 20 Jaar

Risico-analyse document

Wat is het doel van het maken van een risico-analyse ten behoeve van een netwerk / firewall?
Er is geen algemeen overkoepelende risico-analyse document. De organisatie heeft wel een calamiteiten plan, maar op de afdeling die de sub-organisatie bedient wordt er per risico een oplossing bedacht. Deze oplossingen worden in een vergadering besproken en vervolgens via een actiepunten lijst uitgevoerd.

Wordt risico-analyse effectief gebruikt binnen de organisatie?

Er wordt dus geen gebruik gemaakt van een officieel document, maar door middel van 'hands on ervaring' en vergaderingen worden de risico's bepaald en actie ondernomen.

Hoe vaak wordt deze risico-analyse gemaakt of bijgewerkt?
Het eerste antwoord was 'Te weinig, eigenlijk nooit'. De risico's worden opnieuw bekeken op het moment dat er een probleem is of dat er vraag naar is ('ad-hoc' managing).

Uiteindelijk zal elke router/firewall bekeken worden, omdat gemiddeld een keer in de vijf jaar de router en/of firewall vervangen wordt.

Wie maakt de risico-analyse?
De respondent

Welke procedures en / of methodes worden hiervoor gebruikt?
Ad-hoc

Uit hoeveel pagina's bestaat de risico-analyse?
Veel regels bij de firewall / router configuratie. De informatie die bijgeschreven is bestaat uit de reden waarom deze regel geïntroduceerd is en wat precies het effect er van is.

Wat vindt u persoonlijk goede en / of slechte punten van de huidige methode en / of risico-analyse?

De risico-analyse heeft weinig prioriteit. Gezien de drukte van werkzaamheden zal de risico-analyse nooit effectief uitgevoerd worden. Het wordt teveel als overhead gezien.

Hypothetisch gezien als er genoeg tijd beschikbaar was, dan is een risico-analyse document van toegevoegde waarde.

Goede punten is dat er weinig bureaucratie is waardoor snel actie ondernomen kan worden. Tevens wordt alles in overleg met mede-beheerders gedaan.

Hoe wordt de kwaliteit van de risico-analyse bepaald?
n.v.t.

Overige
Bij een nieuwe project, wat binnen de volledige organisatie valt, zijn een aantal procedures van kracht. Alle uitzonderingen op het standaard beveiligingsniveau zullen een keer per jaar worden bekeken of deze nog steeds van toepassing zijn.

Interview III

Maker / ~~Manager~~

Organisatie

Wat doet uw organisatie?
Freelance

Uit hoeveel personeelsleden bestaat uw organisatie?
1

Wat doet uw business unit / afdeling?
Het ondersteunen van organisaties in systeem- en netwerk beheer bij problemen en beveiligings incidenten. Tevens het “auditen” van netwerken van organisaties

Uit hoeveel personeelsleden bestaat uw business unit / afdeling?
1

Functie

Wat is uw functiebeschrijving en hoe verbindt u zich met informatie beveiliging?
Consultancy

Wat is uw opleidingsniveau / werkervaring in dit spefieke gebied?
HTS en zelfstudie

Hoe lang zit u al op deze functie?
3 a 4 Jaar

Risico-analyse document

Wat is het doel van het maken van een risico-analyse ten behoeve van een netwerk / firewall?
Het bepalen in hoeverre de huidige netwerk/server omgeving veilig is ten behoeve het operationeel houden van de organisatie. Het inschatten van problemen die veroorzaakt kunnen worden door beveiligings incidenten.

Wordt risico-analyse effectief gebruikt binnen de organisatie?
Afhankelijk van de organisatie wordt er wel of geen risico-analyse gemaakt. Bij bedrijven waar wel een risico-analyse gemaakt wordt, meestal een eenvoudig overzicht van risico's, worden de grootste risico's aangepakt, mits het de huidige functionaliteit niet in gevaar brengt. Oftewel functionaliteit is belangrijker dan veiligheid.

Hoe vaak wordt de risico-analyse gemaakt of bijgewerkt?
Meestal wordt een risico-analyse gemaakt op het moment dat er een incident heeft plaats gevonden binnen de organisatie. Ook worden risico-analyses gemaakt wanneer er een 'groot' incident heeft plaats gevonden welke in het nieuws is gekomen.

Wie maakt de risico-analyse?
Dit hangt af van de organisatie. Soms gebeurt dit binnen de organisatie of anders door een externe partij.

Welke procedures en / of methodes worden hiervoor gebruikt?
Voornamelijk adhoc methodes waarbij de “Code van informatie beveiliging” als richtlijn wordt gebruikt.

Uit hoeveel pagina's bestaat de risico-analyse?
Het risico-analyse-rapport dient niet te lang te zijn aangezien deze anders niet gelezen wordt. Gemiddeld 1 a 2 A4tjes om een duidelijk beeld te krijgen. Zo`n 3 a 4 A4tjes om een duidelijke technische onderbouwing te hebben.

Wat vindt u persoonlijk goede en / of slechte punten van de huidige methode en / of risico-analyse?
Uitgaande dat er gebruik gemaakt wordt van de “Code van informatie beveiliging”:
Goed punt: het een standaard is.
Slecht punt: er is “Overhead”.

Hoe wordt de kwaliteit van de risico-analyse bepaald?
Het stuk dient inhoudelijk goed te zijn. Ook dienen de adviezen duidelijk onderbouwd te zijn zonder het een langdradig verhaal wordt.

Alle verantwoordelijke personen dienen hun fiat te geven aan het risico-analyse document.

Overige
-

Interview IV

~~Maker~~ / Manager

Organisatie

Wat doet uw organisatie?
Binnen de organisatie staat uitwisseling en overdracht van kennis centraal . Wetenschappers communiceren met collega's over de hele wereld. Er wordt onderzoek gedaan.

Uit hoeveel personeelsleden bestaat uw organisatie?
+/- 3500

Wat doet uw business unit / afdeling?
De centrale leverancier van de bovenstaande organisatie. Tevens bedient de afdeling (kleinere) derden. De volgende taken worden verzorgt door de afdeling:

- Technisch applicatie beheer
- Systeem beheer
- Netwerk beheer
- Werkplek ondersteuning
- “Algemene projecten”
- Programmering en webontwikkeling

Uit hoeveel personeelsleden bestaat uw business unit / afdeling?
+/- 175

Functie

Wat is uw functiebeschrijving en hoe verbindt u zich met informatie beveiliging?
50% Beveiligingscoördinatie voor de bovenstaande organisatie
50% Projecten

Wat is uw opleidingsniveau / werkervaring in dit specifieke gebied?
Bèta universitaire opleiding (bijvak informatica)
Door middel van omscholing en cursussen in huidige functie beland.

Hoe lang zit u al op deze functie?
3 a 4 Jaar

Risico-analyse document

Wat is het doel van het maken van een risico-analyse ten behoeve van een netwerk / firewall?
In 1999 / 2000 is een methode ontwikkeld die, door middel van de het classificeren op de aspecten BIV (Betrouwbaarheid, Integriteit en Vertrouwlijkheid) naar de niveaus Standaard / Gevoelig / Kritisch, via een website een rapport oplevert met maatregelen waaraan een systeem dient te voldoen. Hieronder valt ook de firewall/netwerk configuratie. De methode is ontwikkeld door interne en externe specialisten.

Wordt risico-analyse effectief gebruikt binnen de organisatie?
Er wordt actief geprobeerd om de bovenstaande methode te gebruiken om tot een veiligheids standaard te komen. De andere afdelingen dienen eerst overtuigd te worden van het nut van deze, in hun ogen, extra administratieve handeling.

Hoe vaak wordt de risico-analyse gemaakt of bijgewerkt?
Elk jaar wordt gekeken of de bovenstaande methode aangepast dient te worden.
Wie maakt de risico-analyse?
Interne en externe specialisten.

Welke procedures en / of methodes worden hiervoor gebruikt?
Code van informatie beveiliging is als basis gebruikt voor het ontwerp van de methode .

Uit hoeveel pagina's bestaat de risico-analyse?
De classificatie bestaat uit ongeveer 12 pagina's. De managementsamenvatting uit gemiddeld 1 a 2 A4tjes, anders wordt het niet gelezen!

Wat vindt u persoonlijk goede en / of slechte punten van de huidige methode en / of risico-analyse?
Positief:
- Snel overzicht van maatregelen om het systeem te beveiligen.
- Overzicht waar binnen het systeem naar toe gewerkt kan worden.

Negatief:
- "Technische mensen" zien dit als "administratieve" overhead.
- Moeite om het in te voeren.

Hoe wordt de kwaliteit van de risico-analyse bepaald?
Het niveau van veiligheid wordt in overleg met de klant vastgesteld. De verantwoordelijkheid ligt uiteindelijk ook bij de klant. Wel wordt door de Interne Accountants Dienst jaarlijks een audit gedaan om te kijken of de systemen ook minimaal beveiligt zijn volgens het afgesproken veiligheids niveau. Aangezien de klanten functionaliteit afnemen bij de BU (en daar ook voor betalen) gaat men er vanuit dat het goed geregeld is. Het is moeilijk om de managers ervan te overtuigen om een risico-analyse (assesment) uit te laten voeren.

Overige

De firewall wordt op dit moment alleen actief gebruikt binnen de BU en niet binnen de totale organisatie. Er wordt wel veel gedaan met ACL op routers.

Het beheer van de firewall wordt als een moeilijk proces ervaren. Vooral het bepalen van de ruleset is een belangrijk punt.

Om veranderingen door te voeren in de firewall wordt door de:
1. Netwerk- / Systeem beheerder
2. Firewall beheerder
3. Beveiligings coördinator

in overleg bepaald of de veranderingen:
- Nut hebben?
- Overeenkomen met de wensen van de aanvrager?
- Waarvoor het gewenst is?
- Geen veiligheids implicaties hebben?

Op het moment dat er blijkt dat er een groot risico gelopen wordt, dan zal er een overleg plaatsvinden met een pool van beheerders die als expertise beveiliging hebben. Dit zijn tevens de meest ervaren beheerders. Deze personen wegen de risico's af en versturen vervolgens het resultaat naar de desbetreffende personen. Maximaal 1 a 2 a4 pagina's

(Anders wordt het niet gelezen)

Interview V

Maker / ~~Manager~~

Organisatie

Wat doet uw organisatie?
Het leveren van ISP diensten voor het MKB. Onder deze diensten worden access, hosting en managed services verstaan

Uit hoeveel personeelsleden bestaat uw organisatie?
+/- 40

Wat doet uw business unit / afdeling?
Consultancy naar klanten van de organisatie, ten behoeve van internet acces en firewall systemen. In totaal worden er 65 klanten ondersteunt (45 kleine en 20 grote organisaties).

Uit hoeveel personeelsleden bestaat uw business unit / afdeling?
1

Functie

Wat is uw functiebeschrijving en hoe verbindt u zich met informatie beveiliging?
Consultancy naar klanten van de organisatie ten behoeve van internet acces en firewall systemen.

Wat is uw opleidingsniveau / werkervaring in dit specifieke gebied?
MBO, gecertificeerd in MCSE + TUNIX. Verder door middel van interne opleidingen gegroeid binnen de organisatie.

Hoe lang zit u al op deze functie?
8 Jaar

Risico-analyse document

Wat is het doel van het maken van een risico-analyse ten behoeve van een netwerk / firewall?
Er is geen vraag bij de klant voor een risico-analyse document. Wel wordt er mondeling advies gegeven aan klanten over de Internet Policies waar onder ook het risico-analyse document valt.

Wordt risico-analyse effectief gebruikt binnen de organisatie?
-

Hoe vaak wordt deze risico-analyse gemaakt of bijgewerkt?
Bij grotere klanten wordt af en toe door een derde instantie een audit op het netwerk gedaan. Voor ander klanten wordt er niet pro-actief naar de firewall gekeken. Behalve wanneer er zich problemen voordoen.

Wie maakt de risico-analyse?
De respondent

Welke procedures en / of methodes worden hiervoor gebruikt?

Er worden geen specifieke procedures of methodes gebruikt

Uit hoeveel pagina's bestaat de risico-analyse?
De risico bepalingen worden mondeling gedaan.

Wat vindt u persoonlijk goede en / of slechte punten van de huidige methode en / of risico-analyse?
Op dit moment wordt er geen echt risico-analyse proces doorlopen. Dit komt omdat de klanten hier geen behoefte aan hebben of de klanten de kosten voor een risico-analyse te hoog vinden. Zelf is de respondent een voorstander van het maken van een risico analyse. Eisen die hij aan dit document stelt zijn:

Een second opinion, zodat de risico-analyse inderdaad klopt. Dit om eventuele koepelverkopen te vermijden.
Het dient leesbaar te zijn voor niet technische mensen, oftewel managers.

Hoe wordt de kwaliteit van de risico-analyse bepaald?
-

Overige
-

16.6 Resultaten interviews

In deze paragraaf worden de resultaten van de interviews uitgewerkt. Als eerste wordt beschreven hoe de interviews zijn verlopen. Daarna worden de meest opvallende resultaten uitgewerkt. Vervolgens wordt er een reflectie op de resultaten van de interviews gegeven.

Uitwerking interviews

Zie appendix 16.5 (Verslaglegging interviews) voor de uitwerkingen van de interviews. In de rest van deze paragraaf worden de resultaten behandeld.

Alle respondenten, op de architecten na, stonden er positief tegenover om geïnterviewd te worden. Alle interviews zijn zonder problemen verlopen. Ondanks dat de beveiliging van een organisatie een kritiek punt is, waren de respondenten open in hun antwoorden. Het inwilligen van de wens om anoniem te blijven heeft hier mede aan bijgedragen. Er wordt vanuit gegaan dat de verkregen antwoorden ook eerlijke antwoorden zijn. Een belangrijk punt voor deze openheid kan gelegen zijn in het feit dat er niet naar specifieke technische implementaties gevraagd werd, maar meer naar de procesmatige uitvoering.

Als eerste een overzicht van de resultaten per gestelde vraag. De uitwerking van deze resultaten heeft als doel om inzicht te krijgen welk soort respondenten aan de interviews hebben mee gewerkt. Bij de het conceptueel model II, zie 5.3 (Conceptueel Model II), wordt de relatie met de onderzoeksvragen beschreven.

Maker / Manager

Van de vijf geïnterviewde personen is één persoon die gekozen heeft voor de manager perceptie. Twee respondenten konden geen keuze maken tussen maker of manager, aangezien zij een adviserende rol hebben. De keuze van de respondenten is uiteindelijk gevallen op maker. De andere twee respondenten waren makers.

In eerste instantie lijkt het aantal makers de overhand te hebben, maar aangezien de twee respondenten geen duidelijke voorkeur hadden, is de verhouding tussen maker en manager genuanceerder.

Organisatie

Uit hoeveel personeelsleden bestaat uw organisatie?

Afhankelijk van de grootte van de organisatie is duidelijk te herkennen dat hoe groter de organisatie is, des te meer over de risico-aspecten wordt nagedacht. Dat wil niet zeggen dat het maken van een risico-analyse niet gedaan wordt bij kleinere organisaties. Deze organisaties vinden het belangrijker dat alles naar behoren werkt, dan dat het veilig is.

Uit hoeveel personeelsleden bestaat uw organisatie?

Tussen de respondenten verschilt de organisatiegrootte. Tevens wordt er vanuit gegaan, wat ook door een respondent bevestigd is, dat kleine detacheringsbureaus met kleinere organisaties werken en grote detacheringsbureaus met grotere organisatie werken. De grootte van de organisaties lag tussen de 40 en meer dan 1000 medewerkers.

Wat doet uw business unit / afdeling?

Een drietal respondenten zit in de consultancy. De antwoorden van deze respondenten verbreden het inzicht in verschillende organisaties, aangezien deze respondenten projecten doen bij meerdere organisaties op veelal korte termijn visie. De andere twee respondenten werken binnen vaste organisaties en zorgen onder andere voor het beheren en configureren van firewall. Hierdoor wordt er kennis vergaard over lange termijn visie binnen organisaties.

Uit hoeveel personeelsleden bestaat uw business unit / afdeling?

Het antwoord op deze vraag heeft geen eenduidig resultaat aangezien afhankelijk van de hiërarchische positie binnen de organisatie het antwoord van de respondent anders is. Wel kan je uit deze antwoorden afleiden in hoeverre de respondent de mogelijkheid heeft om met collega's te kunnen praten over de risico-analyse.

Functie

Wat is uw functiebeschrijving en hoe verbindt u zich met informatiebeveiliging?

De respondenten hadden respectievelijk de volgende functiebeschrijving:

1. Manager van audit teams
2. Beveiligingscoördinatie/algemene projecten
3. Facultaire Beveiligings Coördinator, lid van lokale CERT team en Systeem/Netwerk beheerder
4. Consultant voor klanten van de organisatie ten behoeve van internet acces en firewall systemen
5. Consultant voor diverse organisaties

Alle personen hebben beveiliging als onderdeel van hun functiebeschrijving. Dit houdt in dat de respondenten verantwoordelijk zijn voor het analyseren en bepalen van de veiligheid van de digitale informatie, waaronder dus ook het bepalen van de risico's van het gebruik van een firewall.

Wat is uw opleidingsniveau / werkervaring in dit specialistische gebied?

De hoogste genoten opleiding van de respondenten zijn gesorteerd op niveau:

1. Universitair (Prof. Dr.)
2. Universitair (Dr.)
3. Universitair (Drs.)
4. HTS (Ing.)
5. MBO

De hoogst genoten opleidingen zijn divers. Niet alle opleidingen zijn direct aan informatie en/of beveiliging gerelateerd. Door omscholing en zelfontwikkeling binnen de interne organisaties hebben de respondenten hun huidige functie bereikt. De meeste respondenten doen aan zelfstudie aangezien ze dit sneller en goedkoper vinden dan cursussen volgen. Als

minpunt zien ze dat ze daardoor geen 'officieel' certificaat hebben om hun kunde te bewijzen.

Hoe lang zit U al op deze functie?

De gemiddelde werkervaring van de respondenten in het beveilingsgebied is zeven jaar. Hieruit wordt de conclusie getrokken dat de respondenten ervaring hebben in het gebied van digitale informatiebeveiliging.

Risico-analyse-rapport

Wat is het doel van het maken van een risico-analyse ten behoeve van een netwerk/firewall?

De antwoorden op deze vraag waren heel divers. De samenvatting is als volgt;

1. Het bepalen of de information technologie (IT) gerelateerde risico's onder controle heeft en of confidentiality, integrity en availability (CIA) toegepast wordt. In het Nederlands wordt de equivalente vertrouwelijkheid, integriteit en beschikbaarheid (VIB) gebruikt.

2. Het maken van een rapport dat als doel heeft om maatregelen te beschrijven waaraan systemen dienen te voldoen om een bepaald veiligheidsniveau, Standaard / Gevoelig / Kritisch, te kunnen garanderen. Dit door middel van vertrouwelijkheid, integriteit en beschikbaarheid (VIB).

3. De organisatie heeft een calamiteitenplan, maar op de afdeling die de sub-organisatie bedient wordt er per risico een oplossing bedacht. Deze oplossingen worden in een vergadering besproken en vervolgens via een actiepuntenlijst uitgevoerd.

4. Er is geen vraag bij de klant voor een risico-analyse. Wel wordt er mondeling advies gegeven aan klanten over de Internet Policies waaronder ook het risico-analyse-rapport valt.

5. Het bepalen in hoeverre de huidige netwerk/server omgeving veilig is ten behoeve van het operationeel houden van de organisatie. Het inschatten van problemen die veroorzaakt kunnen worden door beveiligingsincidenten.

De respondenten zijn het er mee eens dat het doel van een risico-analyse, ook al wordt dit niet direct genoemd, is: Het bepalen van de risico`s dat een incident plaats kan vinden en hoe deze ingeperkt kunnen worden.

Wordt risico-analyse effectief gebruikt binnen de organisatie?

Er is een respondent die daadwerkelijk “Ja!” heeft geantwoord. De rest van de respondenten was minder enthousiast om zo'n duidelijk antwoord te geven. De tweede respondent gaf aan dat er actief geprobeerd wordt om de gebruikte methode te introduceren in zijn organisatie. De andere afdelingen dienen eerst overtuigd te worden van het nut van deze, in hun ogen, extra administratieve handeling. Bij twee van de respondenten werd de risico-analyse niet gebruikt. Bij een respondent was het afhankelijk van de organisatie, maar de risico-analyse werd over het algemeen niet gebruikt.

Hoe vaak wordt deze risico-analyse gemaakt of bijgewerkt?

Bij twee respondenten wordt een keer per jaar de risico-analyse gemaakt en als het nodig is bijgewerkt. Bij drie respondenten wordt de risico-analyse ad hoc bijgewerkt of na een incident.

Wie maakt de risico-analyse?

De antwoorden waren hier afwisselend:

1. -
2. Interne en externe specialisten
3. De respondent
4. De respondent
5. Afhankelijk van de organisatie soms binnen de organisatie of anders door een externe partij.

Het valt op dat er vaak gerefereerd wordt aan een externe organisatie. Wat hier de oorzaak voor is, is onbekend. Verwacht wordt dat dit soort processen door interne mensen gedaan wordt aangezien deze veel beter de risico's kunnen inschatten op het moment dat ze bepaalde digitale informatie kwijtraken.

Welke procedures en / of methodes worden hiervoor gebruikt?

Ook bij deze vraag waren de antwoorden niet uniform:

1. SPRINT “Simplified Process for Risk Identification” en SARA (Simple to Apply Risk Analysis for Information Systems).
2. Code van informatie beveiliging is als basis gebruikt voor het ontwerp van de methode.
3. Ad-hoc worden er methodes / procedures gebruikt.
4. Er worden geen methodes / procedures gebruikt.
5. Er worden geen methodes / procedures gebruikt. Wel wordt de “Code van informatie beveiliging” als richtlijn gebruikt.

Bij een respondent wordt de SPRINT/SARA procedures gebruikt. Bij twee respondenten wordt de “Code van informatie beveiliging” als basis gebruikt. De laatste twee gebruiken geen of een Ad-hoc manier om een risico-analyse te maken.

Uit hoeveel pagina's bestaat de risico-analyse?

De antwoorden zijn als volgt:

1. Per object ongeveer 3 pagina's. Het is afhankelijk van de organisatie hoeveel objecten er beschreven dienen te worden.
2. De managementsamenvatting bestaat uit gemiddeld 1 a 2 A4tjes, anders wordt het niet gelezen! De classificatie bestaat uit ongeveer 12 pagina’s.

3. Een paar regels bij de firewall.
4. Mondeling, niks op papier.
5. 1 a 2 A4tjes.

In deze antwoorden zijn er geen overeenkomsten te herkennen.

Wat vindt u persoonlijk goede en / of slechte punten van de huidige methode en / of risico-analyse?

De antwoorden van de bovenstaande vraag waren:

1. -
2. De respondent heeft de volgende positieve / negatieve verdeling.
    1. Positief:
        1. Snel overzicht van maatregelen om het systeem te beveiligen.
        2. Overzicht waar binnen het systeem naar toegewerkt kan worden.
    2. Negatief:
        1. “Technische mensen” zien dit als “administratieve” overhead.
        2. Moeite om het in te voeren.
3. De risico-analyse heeft weinig prioriteit. Gezien de drukte van werkzaamheden wordt de risico-analyse nooit effectief uitgevoerd. Het wordt teveel als overhead gezien. Hypothetisch gezien als er genoeg tijd beschikbaar is, dan is een risico-analyse-rapport van toegevoegde waarde. Goede punten zijn dat er weinig bureaucratie is waardoor snel actie ondernomen kan worden. Tevens wordt alles in overleg met mede-beheerders gedaan.
4. Op dit moment wordt er geen risico-analyse proces doorlopen. Dit komt omdat de klanten hier geen behoefte aan hebben of de klanten de kosten voor een risico-analyse te hoog vinden. Zelf is de respondent een voorstander van het maken van een risico-analyse. Eisen die hij aan dit document stelt zijn:
    1. Een second opinion. Dit om eventuele koppelverkopen te vermijden.
    2. Het dient leesbaar te zijn voor niet-technisch onderlegde mensen.
5. Van uitgaande dat er gebruik gemaakt wordt van de “Code van informatie beveiliging”:
    1. Goed punt: het is een standaard.
    2. Slecht punt: er is “Overhead”.

Algemeen

Bij deze vraag is geen nieuwe informatie boven tafel gekomen.