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.