BETAALDE ANTIVIRUS VERSUS GRATIS VARIANTEN, NUT OF NUTTELOOS?

Boudewijn van Silfhout en Bart Dekker

HOGESCHOOL UTRECHT

Versiebeheer

Versie	Datum	Wijzigingen	Status
0.1	13-10-2016	Opzet skelet van het onderzoek	Gereed
0.5	12-12-2016	Gereed vorming eerste concept voor feedback	Gereed
0.9	5-1-2017	Gereed vorming laatste concept	Gereed
1.0	17-01-2017	Feedback Ander de Keijzer verwerkt. Scriptie definitief.	Gereed

Distributielijst

Functie	Naam	Organisatie	Datum
Begeleider	Ander de Keijzer	Hogeschool Utrecht	
Organisator	Leo Moergestel	Hogeschool Utrecht	
Organisator	Esther van der Stappen	Hogeschool Utrecht	
Examinator	Tim Jansma	Hogeschool Utrecht	

Goedkeuringen

Naam	Functie	Handtekening	Datum

Auteur

Naam	Initialen	Student-nummer	Telefoon	E-mail
Boudewijn van Silfhout	B.			
Bart Dekker	B.J.M.			

Voorwoord

Deze scriptie is door Bart Dekker en Boudewijn van Silfhout geschreven. Het onderwerp is gekozen vanwege de persoonlijke interesse in security en alles wat daarbij komt kijken.

Bij het opzetten van de casus voor het onderzoek, rees bij ons beiden de vraag op: betalen wij onnodig voor antiviruspakketten en alles wat deze te bieden hebben, en is een gratis alternatief even goed? Daarnaast werden wij ook nieuwsgierig hoe goed betaalde en gratis pakketten optreden tegen een actieve aanval via openbare wifi, bijvoorbeeld in een café of in de StarBucks. In deze setting moet men namelijk op de beveiligingsproducten op de laptop vertrouwen en hopen dat zijn of haar systeem niet gecompromitteerd wordt. Daarnaast bleken bijna alle vergelijkingssites voor het scoren van antivirusproducten niet te testen voor actieve aanvallen via wifi.

Vanwege deze vragen hebben wij dit onderzoek opgezet om te achterhalen of er een verschil is tussen de bescherming van de antiviruspakketten tijdens een actieve aanval. Daarnaast bood dit onderzoek een kans om de mogelijkheden te ontdekken van het aanvallen van een beveiligd systeem, iets wat geen van ons eerder gedaan had.

Wij wensen u veel leesplezier tijdens het doornemen van onze scriptie.

Utrecht, 5 januari 2017.

Managementsamenvatting

Uit persoonlijke interesse is onderzoek gedaan naar de weerbaarheid van een computersysteem tegen een actieve aanval op een wifi-netwerk. In de media is veel geschreven over computerveiligheid en ook geven bedrijven vaak tips hierover. Eén van deze tips is het installeren van een consumentenbeveiligingsproduct; hiervan zijn zowel gratis als betaalde varianten op de markt.

De onderzoekers vroegen zich af of een betaald consumentenbeveiligingsproduct beter weerstand biedt tegen een actieve aanval dan een gratis variant. Deze vraag heeft uiteindelijk geleid tot het in dit verslag beschreven onderzoek.

Binnen de scope van dit onderzoek is het niet mogelijk gebleken een succesvolle aanval te simuleren. Dit is in principe wel mogelijk met op de zwarte markt gekochte illegale software. Wegens ethische bezwaren willen wij het kopen en testen van deze software niet aanbevelen.

Tussen de geteste consumentenbeveiligingsproducten is geen groot verschil gebleken. Het blijkt betrekkelijk eenvoudig om slecht detecteerbare virussen te genereren, maar deze virussen moeten wel door de gebruiker geactiveerd worden. Het op afstand activeren van virussen is zonder illegale software niet mogelijk gebleken. Wel is het mogelijk om via *social engineering* de gebruiker te verleiden tot het activeren van het virus.

De hoofdaanbeveling is om *social engineering* te testen in het veld met onbedachte gebruikers, opdat zowel de doorsneegebruiker als diens daadwerkelijke niveau van beveiliging getest worden. Dit om te voorkomen dat respondenten tijdens een enquête gewenste antwoorden geven of oneigenlijke alertheid vertonen.

De veldtests voor vervolgonderzoek zullen het gedragspatroon van een aanvaller verder moeten nabootsen. Een aanvaller zal uit zijn op lage kosten en een hoog rendement. Er is software voor het omzeilen van ingebouwde beveiligingen in de *Java Runtime Environment* (JRE), maar deze kost tussen de €100,-- en €200,-- ten tijde van dit onderzoek. Een aanvaller zou daarom mogelijk uitwijken naar het verstrekken van gratis besmette USB-sticks (dit valt binnen de scope van openbare evenementen) of besmette bestanden verspreiden via e-mail of *torrent*-sites.

De aard van verdere veldtests zal bepalen of deze al dan niet verantwoord zijn. Daarom adviseren de onderzoekers tenslotte om voorafgaand aan het uitvoeren de veldtests juridisch advies in te winnen.

Inhoudsopgave

1. Inleiding

Tegenwoordig is het bijna overal wel mogelijk om gratis gebruik te maken van een wifi-netwerk, onder andere bij de Starbucks, McDonald's en zelfs de Albert Heijn. Vaak zijn deze openbare wifi-netwerken zonder wachtwoord beveiligd of het wachtwoord wordt vrij verstrekt. Dit feit maakt het gebruik van dit netwerk een stuk onveiliger dan in de eerste instantie verwacht zou worden. Deze gevaren worden vaak aangestipt door bedrijven, waaronder Kaspersky Lab US ("Public Wi-Fi Security," n.d.), maar ook door media die een algemene, niet technische inslag hebben zoals het Trouw en het NOS-journaal.

Tips die vaak gegeven worden om veilig gebruik te kunnen maken van het netwerk zijn:

- Controleer of je device niet automatisch verbinding maakt met een wifi-netwerk;
- Pas je surfgedrag aan op het openbare netwerk (voorbeeld: controleer dus geen bankzaken);
- Controleer de naam van het wifi-netwerk;
- Vul alleen inloggegevens of bankgegevens in op websites die met SSL beveiligd zijn (herkenbaar aan het groene slotje);
- Verander wachtwoorden regelmatig;
- Gebruik, indien mogelijk, een Virtual Private Network (VPN);
- Schakel de firewall van je systeem in;
- Zorg dat je besturingssysteem, programma's en antivirus up-to-date zijn.

Deze tips zijn al vaak gegeven en worden ook vaak opgevolgd, maar zijn deze ook voldoende om beschermd te zijn tegen kwaadwillenden? In hoeverre kan het consumentenbeveiligingsproduct op een particuliere laptop aanvallen tegengaan? Voegen de betaalde pakketten van consumentenbeveiligingsproducten daadwerkelijk iets toe, of is gratis goed genoeg? Tijdens dit onderzoek hebben de onderzoekers Bart Dekker en Boudewijn van Silfhout getracht antwoord te geven op deze vragen. Hiervoor hebben zij verschillende aanvalstechnieken onderzocht en in een gecontroleerde en persoonlijke omgeving getest. Deze aanvalstechnieken zijn in deze scriptie beschreven ten einde de lezer een antwoord te geven op voorgenoemde vragen.

2. De onderzoeksorganisatie

Dit onderzoek is uitgevoerd tijdens het onderzoeksemester van de Hogeschool Utrecht op de opleiding *System and Network Engineering* (SNE). De studenten Bart Dekker en Boudewijn van Silfhout hebben dit als onderdeel van hun studie uitgevoerd. Dit onderzoek is niet in opdracht van een bedrijf uitgevoerd, maar komt voort uit de interesse van Bart Dekker en Boudewijn van Silfhout en hun scriptiebegeleider Ander de Keijzer van de Hogeschool Utrecht. De Hogeschool Utrecht geeft voorgenoemde studenten de mogelijkheden voor dit onderzoek, waaronder 25 studiepunten per student en begeleiding waarbij de overige investeringen voor eigen rekening van voorgenoemde studenten is. Dit onderzoek heeft dan ook plaatsgevonden op eigen systemen en het eigen woonadres van de studenten. Aan de hand van contact met Ander de Keijzer is de inhoud en koers van het onderzoek bewaakt.

3. Opdrachtbeschrijving

Voor het onderzoek naar de gevaren van openbare Wi-Fi hotspots en de effectiviteit van consumentenbeveiligingsproducten, moet naar verscheidende aspecten gekeken worden. Deze luiden als volgt:

- Marktaanbod van consumentenbeveiligingsproducten;
- Marktaandeel van besturingssystemen.
- Bestendigheid van consumentenbeveiligingsproducten tegen aanvallen op een openbaar netwerk.

Aan de hand van de informatie die uit deze aspecten zal voortvloeien, kan een testplan opgesteld worden om consumentenbeveiligingsproducten te testen op actieve aanvallen op een openbaar wifi-netwerk. De praktijktest zal plaatsvinden in een testomgeving met het meest gebruikte besturingssysteem en de door een Nederlandse consumentenorganisatie als best geteste consumentenbeveiligingsproducten: één gratis en één betaald pakket. Tijdens de praktijktest zal een gecontroleerde omgeving opgezet worden die bestaat uit één of meerdere cliëntsystemen en een aanvalssysteem. Het aanvalssysteem zal gebruik maken van Kali, gezien dit besturingssysteem de meest voor de hand liggende tools bevat voor het uitvoeren van netwerkaanvallen en wordt gebruikt door professionele pentesters.

3.1 Probleemstelling

Er zijn steeds meer openbare wifi-netwerken en gebruikers controleren steeds vaker even hun e-mail of het nieuws tijdens het nuttigen van een consumptie, bijvoorbeeld bij horecagelegenheden. Daarom is het interessant om na te gaan in hoeverre de beveiliging daadwerkelijk voldoet, zoals de media beweren, om tegen aanvallers ofwel hackers te beschermen. De onderzoeksgroep gaat dit controleren door na te gaan wat het meest gebruikte besturingssysteem is en welke consumentenbeveiligingsproducten op de markt zijn. Uit dit onderzoek moet blijken of er een verschil is tussen een door een Nederlandse consumentenorganisatie als best getest gratis beschikbaar consumentenbeveiligingsproduct en het betaalde alternatief.

3.2 Doelstelling

Het doel van het onderzoek is om een vergelijking tussen het beste betaalde en gratis consumentenbeveiligingsproduct op te stellen met betrekking tot actieve aanvallen op een plat, openbaar wifi-netwerk. Om tot een realistisch testplan te komen is het van belang om vanuit betrouwbare bronnen het meest gebruikte besturingssysteem en de door een Nederlandse consumentenorganisatie als beste geteste gratis en betaalde consumentenbeveiligingsproducten te vernemen.

Uit deze productvergelijking moet blijken of een betaald consumentenbeveiligingsproduct een gebruiker beter tegen een actieve aanval beschermd dan een gratis variant, naast bescherming tegen de in het wild aanwezige virussen en andere dreigingen op het internet. Uit de vergelijking moet ook blijken of betaalde beveiligingsproducten meerwaarde hebben ten opzichte van de gratis varianten, met name de actieve beveiliging die de fabrikanten van deze beveiligingsproducten aanbieden bij de betaalde licenties of bijvoorbeeld wachtwoordbeheer.

3.3 Afbakening en randvoorwaarden

Dit onderzoek is uitgevoerd door studenten aan de Hogeschool Utrecht (HU). De HU kent per student 25 *European Credits* (EC) toe aan ieder onderzoekslid bij succesvolle afronding van dit onderzoek. Deze 25 EC staan gelijk aan 700 studielasturen. Gezien dit onderzoek door twee studenten wordt uitgevoerd staat het totaal studielasturen gelijk aan 1400 uur.

Het onderzoek is beperkt gebleven tot het meest gebruikte besturingssysteem voor computers. *portables* en *wearables* zijn buiten de scope van het onderzoek gevallen. Daarnaast heeft de onderzoeksgroep zich gelimiteerd tot de door een Nederlandse consumentenorganisatie als best geteste gratis en betaalde consumentenbeveiligingsproducten. Dit is gedaan gezien de onderzoeksgroep geen bestaande kennis en kunde had van het uitvoeren van hackaanvallen en deze kennis eerst moest gaan opbouwen. Indien meer platformen en consumentenbeveiligingsproducten getest zouden worden, was er niet voldoende tijd beschikbaar voor het grondig uitvoeren van het onderzoek.

De volgende randvoorwaarden waren van toepassing op dit onderzoek:

- Aanwezigheid van de onderzoeksleden bij de gegeven lessen en bijeenkomsten;
- Beschikbaarheid van een geschikte werkomgeving, zowel thuis als op de Hogeschool Utrecht;
- Geschikte laptops en netwerkapparatuur voor het uitvoeren van het opgestelde testplan;
- Kennis van Kali en de bijbehorende tools;
- Beschikbaarheid en bereikbaarheid van de begeleider.

4. Onderzoeksvraag en deelvragen

De voor dit onderzoek gedefinieerde onderzoeksvraag luidt als volgt:

In hoeverre is er een verschil aanwezig in detectie en daaropvolgende preventiemaatregelen tussen betaalde en gratis beschikbare consumentenbeveiligingsproducten, zodra gepoogd wordt een systeem met daarop aanwezig volledig bijgewerkte versie van het meest gebruikte besturingssysteem te compromitteren tijdens een actieve aanval via een openbaar wifi-netwerk?

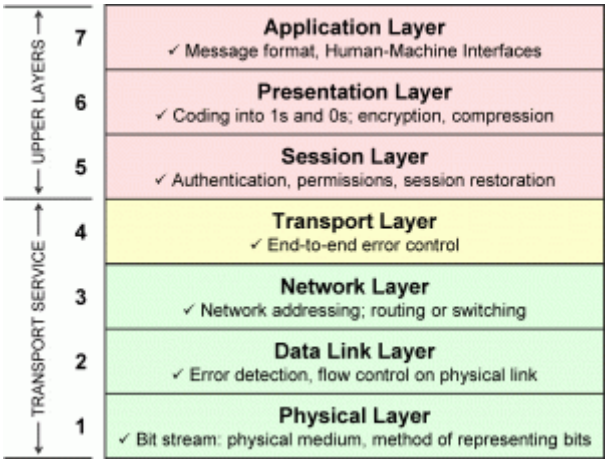
Ter beantwoording van de hierboven genoemde onderzoeksvraag zijn de volgende deelvragen gedefinieerd:

1) Wat zijn de basisparameters voor het testsysteem ter beantwoording van de hoofdvraag?
   a) Welk besturingssysteem, bijbehorend versienummer, wordt het meest gebruikt en vormt daarmee het grootste doelwit?
   b) Welk consumentenbeveiligingsproduct wordt aanbevolen door een onafhankelijke Nederlandse consumentenorganisatie?
2) In hoeverre zijn volledig bijgewerkte systemen, welke beschikken over de onder deelvraag 1a en 1b gespecificeerde combinatie, vatbaar voor een actieve aanval op een openbaar wifi-netwerk ongeacht de benodigde aaneengesloten aanvalstijd?
3) In hoeverre is het mogelijk om een computersysteem te compromitteren in de tijd waarin de gebruiker zich tijdens het nuttigen van een of meerdere consumpties op een openbaar wifi-netwerk bevindt?
4) Welke verschillen zijn te meten, tussen een door een onafhankelijke Nederlandse consumentenorganisatie aanbevolen gratis en betaald consumentenbeveiligingsproduct, bij het detecteren en eventueel reageren op een actieve aanval zoals bij de in deelvraag drie beschreven aanval?
5) Bij welke systeemconfiguraties van systemen op een openbaar wifi-netwerk of het openbare wifi-netwerk zelf loont het voor een aanvaller niet langer om willekeurige systemen op openbare wifi-netwerken aan te vallen, en zal deze doelwitten zorgvuldiger kiezen?

4.1 OSI-Model

Het *Open Systems Interconnection* model (OSI-model) staat centraal in de uitleg hoe een netwerk werkt. Dit onderzoek baseert de casus op basis van een openbaar wifi-netwerk, wat plaatsvindt op laag 2 van het OSI-Model.

Het OSI-model is een gestandaardiseerd referentiemodel voor datacommunicatiestandaarden opgesteld door de *International Organization for Standardization* (ISO). Zij definiëren het OSI-model zoals weergegeven in afbeelding 1. Deze gehele paragraaf is gebaseerd op: (“PSTN Tutorial,” n.d.-a)



Afbeelding 1: OSI-Model (“PSTN Tutorial,” n.d.-b)

Zoals te zien is in afbeelding 1, bestaat het OSI-model uit 7 lagen, namelijk:

1. De eerste laag is de fysieke laag, deze definieert de elektronische manier waarop de bits verstuurd worden tussen apparaten;
2. De tweede laag is de data link laag, hier wordt de data gecontroleerd op fouten en flow control op de fysieke link;
3. De derde laag is de netwerk laag, in deze laag wordt er gerouteerd op basis van netwerkadressering;
4. De vierde laag is *end-to-end error control*, hier wordt de connectie tussen twee apparaten opgezet en gecontroleerd op fouten;
5. De vijfde laag is de sessielaag, hier wordt er gekeken naar permissies en authenticatie. Verder wordt er gekeken of de sessie hersteld kan worden als die verbroken is;
6. De zesde laag is de presentatielaag, zorgt ervoor dat de data geconverteerd wordt zodat de applicatie er mee overweg kan. Er wordt op deze laag ook versleuteld en gecomprimeerd;
7. De zevende laag is de applicatielaag, deze laag communiceert direct met de applicatie en geeft opdrachten aan de zesde laag van het OSI-model.

4.2 Actieve aanvallen

Onder de term actieve aanval kunnen verscheidene technieken geschaard worden, namelijk:

- Gebruik van *exploits* om toegang te verkrijgen tot een systeem;
- Session-relay-aanvallen, waarbij de aanvaller door het stelen van het sessie-ID toegang krijgt tot een account van de gedupeerde;
- Man-in-the-middle-aanval, waarbij de aanvaller zich voordoet als de router om het internet op te gaan, en alle informatie van de gedupeerde door het systeem van de aanvaller leidt;
- Spoofing-aanval, waarbij een aanvaller zich door middel van ARP, DNS, MAC en/of *IP spoofing* voor kan doen als een ander systeem of verkeer om kan leiden naar een website met malafide software.

Tijdens het onderzoek zal gekeken worden welke aanval het beste uit te voeren is op een openbaar wifi-netwerk en of de consumentenbeveiligingsproducten hier voldoende tegen beschermen.

4.3 Besturingssystemen ten behoeve van internetbrowsen

Een besturingssysteem is een softwarelaag tussen de computer hardware en de gebruiker en stelt daarmee de gebruiker in staat om bijvoorbeeld eigen software uit te voeren (Silberschatz, Galvin, & Gagne, 1994). Aangezien een internetbrowser ook weer een apart stuk software is, is daarmee een besturingssysteem nodig om op internet rond te kunnen kijken. Onderstaande lijst geeft in alfabetische volgorde alle besturingssystemen weer die in de praktijk gebruikt worden om op het internet te surfen (Netmarketshare, 2016):

- Linux
- Mac OS X
- Windows

Van voorgenoemde besturingssystemen heeft Windows het grootste marktaandeel (89,34%), en de meest gebruikte versie daarvan is Windows 7 met 47,25% (Netmarketshare, 2016). Daarmee vormt Windows 7 door zijn grote marktaandeel een aantrekkelijk doelwit voor cybercriminelen, omdat een eenmaal ontwikkelde aanval van toepassing is op 47,25% van de internetgebruikers (Netmarketshare, 2016). Zoals in de voorgaande hoofdstukken is beschreven, zal de testomgeving gebaseerd zijn op het meest gebruikte besturingssysteem. Gezien uit voorgenoemde bron blijkt dat dit Windows 7 betreft, zal tijdens de testomgeving gebruik gemaakt worden van Windows 7.

4.4 Minimale beveiligingsfuncties bij consumentenbeveiliging

Naast het veel geadviseerde bijgewerkt houden van software, raden de media ook aan om antivirusproducten te installeren. Afgaande op advertenties op internet en in computerbladen als de PC-Active, zijn er veel verschillende aanbieders van antivirusproducten op de markt. De vraag is wat minimaal geïnstalleerd moet zijn aan consumentenbeveiligingsproducten (in deze categorie valt ook het antivirus). Voor een minimum aan veiligheid dient minimaal aanwezig te zijn: Een antimalwarepakket (“Virus, adware, spyware en Browser hijacking software” (IST MIT, 2016)) en een firewall (Larkin, 2008; Rebbapragada, 2016).

De minimaal aanbevolen firewall en antimalware kunnen los van elkaar geïnstalleerd worden, maar tevens kan gebruik gemaakt worden van een kant-en-klare oplossing (Rubenking, 2016). Onze inschatting was dat gebruikers die losse producten installeren, gebruik maken van gratis oplossingen gezien op het moment van schrijven (december 2016) maar één partij een los antimalwareproduct aanbiedt (Rubenking, 2016). Deze tweedeling sluit aan bij het scheiden van gratis en betaalde beveiligingsproducten om deze te vergelijken op het gebied van veiligheid.

5. Marktonderzoek

In dit hoofdstuk wordt uitgelegd waarom voor de desbetreffende bedrijven gekozen is bij het verzamelen van informatie. Deze keuze van bronnen is belangrijk om te voorkomen dat commerciële belangen van bedrijven het onderzoek in de basis vertroebelen.

5.1 Marktonderzoek besturingssystemen

De volgende onderzoeksbureaus geven in het openbaar informatie over de wereldwijde gebruikspercentages:

- Statcounter;
- Statista;
- Netmarketshare.

Al deze bedrijven bieden website-eigenaren een dienst aan om statistieken bij te houden over het gebruik van hun eigen website. De reden om de informatie uit meerdere bronnen te vergelijken en niet af te gaan op een enkele bron, is dat informatie over de achterliggende bronnen en meetmethoden niet beschikbaar zijn. De aangegeven percentages kunnen daarom per besturingssysteem verschillen. Zodoende is er per bedrijf gekeken welk besturingssysteem het meest gebruikt wordt en is hiermee als definitie gebruikt om de onzekerheid over de partijdigheid van meetmethoden weg te nemen.

5.2 Consumentenbeveiligingsproducten

Betaalde consumentenbeveiligingsproducten worden jaarlijks herzien en omschreven als “Internet Security <jaartal>”. Ondanks de jaarlijkse updates bieden de betaalde varianten vaak, maar niet altijd, meer functionaliteit (Rubenking, 2016). Dit onderzoek gaat, zoals beschreven in het Plan van Aanpak en de onderzoeksvragen, uit van door Nederlandse consumentenorganisaties uitgevoerde testen. Dit is gedaan om een zo realistisch mogelijke testomgeving te creëren, aangezien buitenlandse bronnen vooral geraadpleegd worden door IT’ers terwijl dit onderzoek zich richt op een breder publiek.

Eén van de bekendste Nederlandse consumentenorganisaties is waarschijnlijk de Consumentenbond met, volgens Parlement.com, een bereik van “ongeveer 600.000 leden”. Hierbij komt dat de Consumentenbond de enige brede consumentenorganisatie is, en zich daarmee niet op een specifiek aandachtspunt richt (Parlement.com, 2016).

Daarnaast zijn in Nederland ook een aantal computerbladen welke consumentenbeveiligingsproducten testen. Via twee verkoopsites van abonnementen op computerbladen is een oriënterende lijst samengesteld van computerbladen (123tijdschrift.nl, 2016; Proefabonnementen Gids, 2016):

- Computer! Totaal;
- Computer Idee;
- Tips & Trucs;
- PCM.

Voor deze computerbladen zijn vervolgens twee criteria opgesteld om vast te stellen of het blad geschikt is als bron: digitale doorzoekbaarheid en de aanwezigheid van vergelijkende tests.

Het eerste criterium is dat de voorgaande computerbladen via de website doorzoekbare artikelen moet aanbieden. Indien dit niet het geval was, werd het desbetreffende blad niet meegenomen tijdens het onderzoek. Dit is gedaan om tijdrovend handmatig bladeren te voorkomen. Omwille van de voortgang van dit onderzoek zijn bladen zonder online doorzoekbare artikelen dus niet meegenomen in het onderzoek.

Het tweede criterium is dat het blad onafhankelijke vergelijkende testen moet uitvoeren. Veel bladen uit de bovenstaande lijst bespreken een product wel afzonderlijk, maar zetten dit niet tegenover andere producten op de markt. Het ontbreken van dergelijke vergelijkende testen belemmert de objectiviteit, omdat de producten niet op hetzelfde moment getest zijn en daardoor de testvariabelen kunnen verschillen.

Afbeelding 2: Aanbieding voor korting bij aanschaf test winnaar bij TopReviews.nl (TopReviews.nl, n.d.).

Enkele consumentenpanels die wel aan het eerste criterium voldoen, moesten uiteindelijk toch worden uitgesloten op basis van het tweede criterium. Zo heeft bijvoorbeeld de Nederlandse site “TopReviews.nl” in 2016 een vergelijkende test uitgevoerd. TopReviews.nl moest echter uitgesloten worden omdat het niet te bepalen is door wie deze website betaald wordt en of deze vergelijkende test van 2016 wel onafhankelijk is. De voorgenoemde website biedt namelijk, voor het door hen als best getest consumentenbeveiligingsproduct, een kortingscode aan (afbeelding 2). Naast het feit dat er niet geconstateerd kon worden of er commerciële belangen waren bij de vergelijking, blijkt het domein te koop te staan zoals te zien in afbeelding 3 (DomainTools, 2016). Tot slot is vergelijking op TopReviews.nl alleen op basis van de door de fabrikant opgegeven functionaliteit en niet op basis van testen in een proefopstelling.

Afbeelding 3: Domein TopReviews.nl staat in de verkoop (DomainTools, 2016).

Bij het selecteren op basis van de twee criteria is gebleken dat de Consumentenbond de enige onafhankelijke organisatie is, welke voor de doelgroep van dit onderzoek vergelijkende testen van consumentenbeveiligingsproducten uitvoert. Bij de beantwoording van onderzoeksvraag 1b- "Welk consumentenbeveiligingsproduct wordt aanbevolen door een onafhankelijke Nederlandse consumentenorganisatie?" – is daarom gebruik gemaakt van de testinformatie van de Consumentenbond.

6. Meest gebruikte besturingssysteem en beste consumentenbeveiligingsproduct

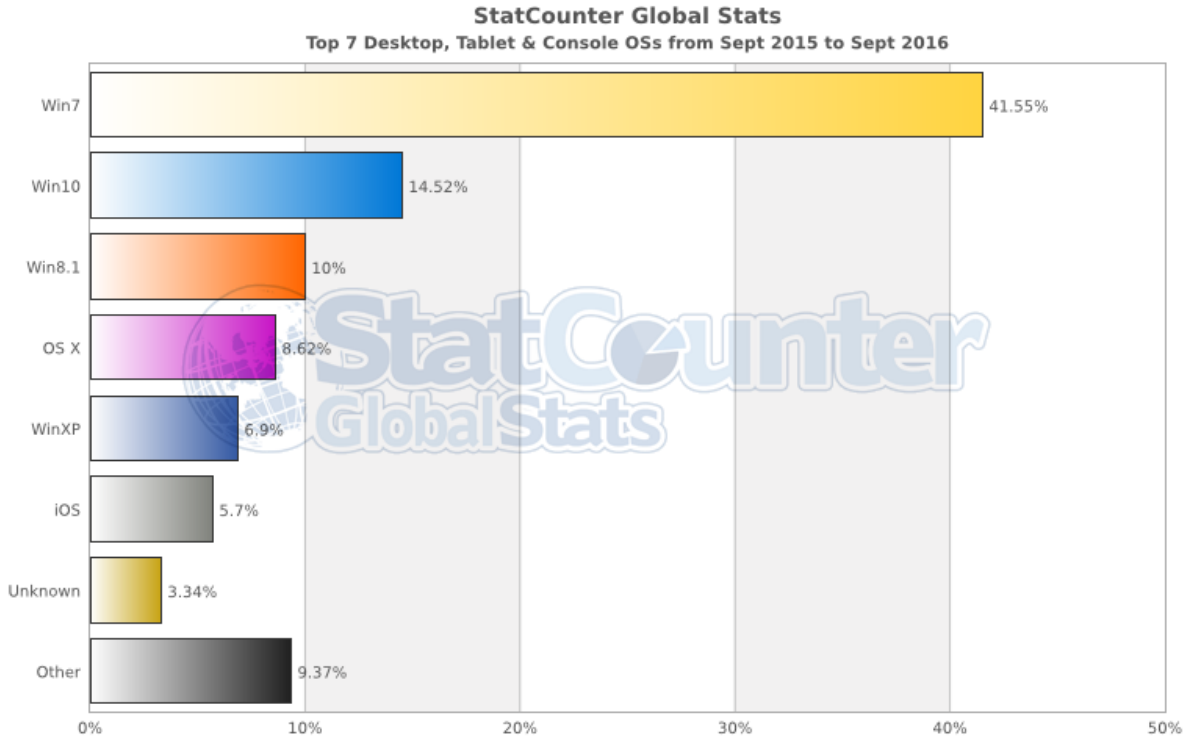
Dit hoofdstuk behandelt een analyse van de gegevens uit de hierboven besproken bronnen. Middels deze analyse wordt een besturingssysteem voor onze testomgeving geselecteerd, samen met de twee te testen consumentenbeveiligingsproducten.

6.1 Meest gebruikte besturingssysteem (OS)

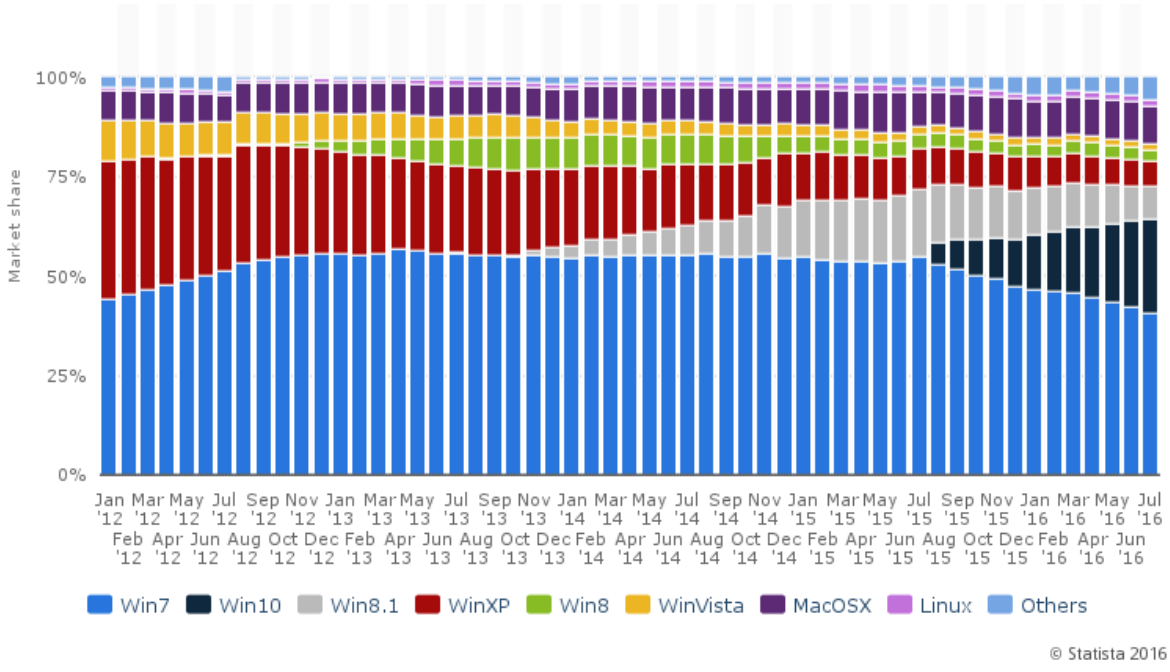
Zoals in het voorgaande hoofdstuk besproken is er gekeken naar de informatie van de volgende bedrijven:

- Statcounter
- Statista
- Netmarketshare

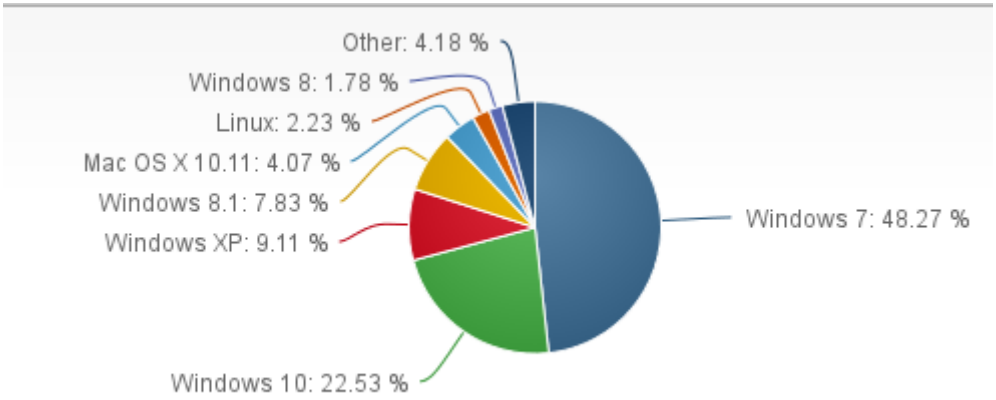
Al deze bedrijven geven aan dat in september 2016 Windows 7 het meest gebruikte besturingssysteem was. De opgegeven percentages verschillen per bedrijf, te wijten aan het feit dat ieder bedrijf zijn metingen verricht via andere websites. Verder beïnvloeden onderlinge verschillen in doelgroep en publiek ook het meest gebruikte besturingssysteem per website. Hieronder bevinden zich de afbeeldingen van de grafieken per bedrijf in combinatie met bronvermelding:



Afbeelding 4: Marktoverzicht besturingssystemen op september 2016 via Statcounter (StatCounter GlobalStats, 2016)



Afbeelding 5: Marktoverzicht besturingssystemen op september 2016 via Statista (Statista, 2016)



Afbeelding 6: Marktoverzicht besturingssystemen op september 2016 via Netmarketshare (Netmarketshare, 2016)

Afgaande op bovenstaande informatie is tijdens dit onderzoek gebruik gemaakt van Windows 7 als besturingssysteem voor de aanvallen in de testomgeving.

6.2 Beste consumentenbeveiligingsproducten

Zoals in het voorgaande hoofdstuk besproken is, De selectie aan te testen consumentenbeveiligingsproducten is gebaseerd op publicaties van de Consumentenbond. In het nummer van 5 mei 2016 is een vergelijkende test gehouden van betaalde en gratis consumentenbeveiligingsproducten.

De Consumentenbond kent de predicaten “Beste uit de test” en “Beste koop” toe. Het predicaat voor beste uit de test gaat naar het product met het hoogst behaalde rapportcijfer. Dit betreft “BullGuard Internet Security 2016” (Kamp, 2016). Het predicaat “Beste koop” gaat naar het product dat zowel een goed rapportcijfer heeft als een scherpe prijs in verhouding tot dat rapportcijfer. Het predicaat voor beste koop gaat in dit geval naar “G Data Internet Security 2016” (Kamp, 2016). Deze informatie over de predicaten is te vinden achterin iedere uitgave van de Consumentenbond.

BullGuard Internet Security 2016 is het betaalde consumentenbeveiligingsproduct dat in dit onderzoek is getest tegen actieve aanvallen. Tijdens het vooronderzoek is gebleken dat het infecteren van systemen, in de zin van dit onderzoek, de meeste kans van slagen heeft via aanvallen tijdens het surfen op het internet. Dit is de aanleiding voor het verschil in testoordeel bij beide producten, betreffende de bescherming tegen dergelijke aanvallen. Het product BullGuard beschermt volgens de Consumentbond tegen 76,72% van de aanvallen tijdens internetgebruik, tegenover 64,22% van het product van G Data (Consumentenbond, 2016a, 2016b).

Het hoogste rapportcijfer voor een gratis consumentenbeveiligingsproduct is voor “AVG AntiVirus Free 2016”, het betreft een 6,2 (Kamp, 2016). Daarom is tijdens dit onderzoek aangaande het testen van gratis consumentenbeveiligingsproducten gebruik gemaakt van AVG AntiVirus Free 2016. Aangezien de Consumentenbond geen testen van firewalls gepubliceerd heeft, is er voor het complementeren van de test gebruik gemaakt van de Windows Firewall. Om de testvariabelen gelijk te houden zijn alle consumentenbeveiligingsproducten gebruikt met de standaardinstellingen van het pakket.

7. Ethische afweging onderzoek

De keuze om in dit onderzoek een hoofdstuk over ethiek op te nemen, komt voort uit de verwachting dat de uitkomsten van dit onderzoek in verkeerde handen veel schade kunnen berokkenen. Dit hoofdstuk heeft als doel een kader te scheppen en onze afwegingen weer te geven.

Ons onderzoek bevindt zich in een grijs gebied, waarbij het grijs zowel donkerder als lichter kan worden. Het grijs is echter onherroepelijk zwart indien er buiten onze eigen testomgeving aanvallen op systemen uitgevoerd zouden worden. Denk hierbij aan het uitvoeren van aanvallen op systemen aanwezig op het openbare wifi-netwerk van bijvoorbeeld de Mc Donalds, Starbucks of Albert Heijn. In dat geval zouden wij wat onszelf betreft de grenzen van het betamelijke overtreden, aangezien onze verwachting is dat een dergelijke veldtest niet nodig is voor het kunnen beantwoorden van onze onderzoeksvraag.

Het grijze gebied blijft lichtgrijs indien aangetoond wordt dat de gevonden kwetsbaarheden niet kosteneffectief zijn bij een sleepnetmethode. In dat geval is het gros van de systemen welke zich op openbare wifi-netwerken bevinden veilig voor aanvallers. Ervan uitgaande dat de kosten voor het uitvoeren van een aanval hoog zijn, is dit onderzoek veilig te publiceren omdat gebleken is dat de aanval niet grootschalig kan worden opgezet.

Indien blijkt dat met relatief goedkope oplossingen gemakkelijk veel systemen kunnen worden gecompromitteerd, wordt het grijs een stuk donkerder. Daarmee kan ons onderzoek handvatten bieden aan gelegenheids- of beginnende aanvallers. In dit geval dient serieus overwogen te worden om het onderzoek alleen aan onze begeleider en beoordelaars van de Hogeschool Utrecht (HU) aan te bieden en niet te publiceren.

Een reden om dit onderzoek toch te doen, is om te beoordelen of gebruikers niet onnodig geld besteden aan consumentenbeveiligingsproducten. Indien namelijk uit dit onderzoek blijkt dat een gratis beveiligingsproduct afdoende is, is onze verwachting dat ons onderzoek vooral gebruikers ten goede komt.

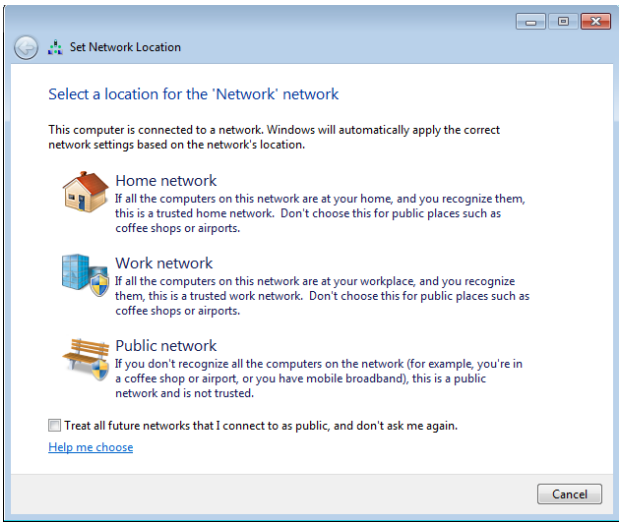
Moraal van dit betoog is dat we ons terdege bewust zijn van de mogelijke consequenties van ons onderzoek en dat uiteindelijk bij het afronden van dit onderzoek de hierboven beschreven ethische afweging gemaakt dient te worden.

8. Aanvalsdoelgroepen en aanvalsomstandigheden

In dit hoofdstuk wordt een conclusie uit voorgaande hoofdstukken herhaald, waarna de aanvalsomstandigheden en aanvalsdoelgroepen besproken worden.

8.1 Netwerkprofielen Windows 7 en hoe dit de aanval beïnvloed

Om toegang te verkrijgen tot een systeem moet een aanvaller toevlucht zoeken in Social Engineering. Uit dit onderzoek is namelijk gebleken dat een Windows 7 systeem van buitenaf goed beveiligd is, waardoor de gebruiker van binnenuit tot medewerking verleid moet worden. Indien een gebruiker na connectie met het openbare wifi-netwerk het juiste netwerkprofiel gekozen heeft, namelijk “Openbaar” of in Engelstalige edities “Public”, staan alle poorten van buiten naar binnen in de Windows Firewall dicht. Dit bemoeilijkt aanvallen, gezien het met een openbaar Windows netwerkprofiel niet mogelijk is om bestanden te delen over het openbare netwerk. Door deze maatregelen heeft Microsoft de aanvalsmogelijkheden aanzienlijk verkleind.



Afbeelding 7: Netwerkprofiel selectie dialoogvenster in Windows 7.

8.2 Aanvalsomstandigheden besproken en geanalyseerd

De beschreven aanval met SET, waarbij een door de gebruiker opgevraagde website wordt vervangen door een met een kwaadaardige *Java applet* geïnfecteerde variant, vereist nog steeds dat de gebruiker ondanks waarschuwingen op “Ja” klikt. Bedachtzame gebruikers zullen zich naar verwachting afvragen of het verstandig is om op “Ja” te klikken, aangezien een dergelijk dialoogvenster normaliter niet verschijnt. Daarom volgen nu twee scenario’s om te schatten in hoeverre het waarschijnlijk is dat de gebruiker door zal klikken en zodoende de aanval toestaat.

De eerste situatie is een dagelijkse situatie: gebruikers die in een horecagelegenheid zitten te werken of rustig het nieuws doornemen achter de laptop. Een ongehaaste gebruiker zal in de regel geen reden hebben om door te klikken. De aanval zal dan falen omdat de gebruiker het venster omzeilt of de browser anderszins afsluit. Aan de andere kant gaat het net beschreven scenario uit van een geïnformeerde gebruiker die deze correcte handelswijze paraat heeft en de hierboven beschreven gevolgtrekking kan maken. Bij gebruikers die deze kennis missen, heeft de aanval juist weer kans van slagen in de beschreven rustsituatie. Om daadwerkelijk deze gevolgtrekkingen te onderzoeken is het noodzakelijk een veldtest uit te voeren, uiteraard met inachtneming van de wettelijke kaders, in een gelegenheid zoals beschreven in het hoofdstuk Aanbevelingen. Een enquête is hiervoor niet de juiste oplossing, omdat de kans bestaat dat ofwel niet alle lagen van de digitaal actieve bevolking vertegenwoordigd zullen zijn, of dat de zelfrapportage van de respondenten een vertekend beeld zou geven van de door hen daadwerkelijk bezochte websites. Het is namelijk aannemelijk dat gebruikers een betere versie van zichzelf willen presenteren en sommige relevante websites niet zullen opgeven of gewoon vergeten.

In de voorgaande paragraaf is een scenario beschreven over bedachtzame gebruikers in een situatie van rust . Het uiterst tegenovergestelde zou een scenario zijn van publieke chaos, zoals een terroristische aanslag. Gezien de dreiging voor de eigen veiligheid of die van dierbaren, zullen vele gehaaste en zodoende minder alerte internetgebruikers snel nieuws willen opvragen, en eerder geneigd zijn om “Ja” te klikken in dialoogvenster, opdat ze bij hun nieuws komen. In dat geval is de kans groot dat een aanvaller toegang zal krijgen tot vele systemen zoals als beschreven in dit document.

8.3 Aanvalsdoelgroepen besproken en geanalyseerd

Gekeken naar de kosten voor ondertekening van de *Java applet*, noodzaakt de methode *spear phishing* een aanvaller om de juiste doelgroep te selecteren. Er zijn twee brede aanvalsdoelgroepen te onderscheiden, namelijk vermogenden en niet-vermogenden met toegang tot een (bedrijfs)vermogen. In de voorgaande paragraaf is besproken dat het alleen in uitzonderlijke omstandigheden waarschijnlijk is dat een aanval via *social engineering* veel gebruikers zal treffen. De verwachting van de onderzoekers is dat voor het beschreven sleepnet een onzekere situatie nodig is waaronder, zoals in het voorbeeld, een terroristische aanval.

Indien een aanvaller zich toespitst op een specifieke groep bijeengekomen vermogenden, vergroot het maatwerk van de aanvaller diens kans op succes Het voordeel aanvallen op bijvoorbeeld ondernemers die zich verenigen bij een Rotaryclub is dat ook bij een klein slagingspercentage het potentiële rendement hoger is dan bij een willekeurige aanval op bijvoorbeeld de Starbucks. Een aanval op systemen op het wifi-netwerk van de Rotaryclub kan namelijk als springplank dienen voor het binnendringen bij een onderneming. Zo zou een aanvaller de gemaakte kosten voor het ondertekenen van de *Java applet* aanvalssoftware snel terugverdienen.

9. Aanval op systemen zonder gebruikersinteractie

De tot nu toe besproken mogelijkheden voor het creëren van een *backdoor* binnen een systeem hebben allen betrekking op de interactie van de gebruiker. Indien de gebruiker geen actie neemt om het virus te activeren, zal de aanvaller geen toegang tot het systeem verkrijgen. Om zonder deze interactie toegang alsnog een systeem over te nemen, zijn er meer middelen nodig dan de openbaar toegankelijke.

9.1 Darkweb

Er is een markt voor het verkrijgen van *exploits* en *zero days* die nog niet gedicht zijn door fabrikant Microsoft. Dit is niet mogelijk via het standaard toegankelijke internet, maar wel op het zogeheten "*darkweb*". Het *darkweb* is een grotendeels verborgen laag binnen het internet dat anoniem via het TOR-project te bereiken is. Het browsen op het *darkweb* is anoniem doordat er gebruik wordt gemaakt van vele computers die als *relay* fungeren en daarmee het netwerkverkeer via vele versleutelde paden wordt gerouteerd. Hierdoor is het mogelijk anoniem te browsen, maar ook websites te bezoeken die alleen binnen deze *relays* te bereiken zijn, in plaats van alleen de sites die gehost worden via servers.

Een grote site is The RealDeal Market. Op deze site worden voor bedragen variërend van $1.500 tot $75.000 *exploits* verhandeld voor verscheidende besturingssystemen, netwerkrouters en firewalls.

Het kopen van deze *exploits* is een risico, gezien deze transacties anoniem gebeuren en zonder garantie dat de gekochte 'producten' daadwerkelijk functioneren zoals aangeprezen. Gezien het nader bestuderen van zulke *exploits* buiten de scope van dit onderzoek valt en dit onderzoek geen aanval op een openbaar wifi-netwerk behelst, is dit onderdeel niet meegenomen voor de resultaten van het onderzoek.

9.2 Zoeken van gaten in software

Naast het kopen van *exploits* is het uiteraard ook mogelijk om zelf op zoek te gaan naar de gaten binnen software om door middel daarvan een systeem binnen te dringen. Gezien geen enkel softwarepakket volledig waterdicht is, bestaat altijd de mogelijkheid binnen te dringen via misbruik van een manier waarop een programma iets aanroept of verwerkt. Indien zulk misbruik leidt tot het opstarten van een ander programma, of het uitvoeren van code waardoor er contact gezocht wordt het systeem van de aanvaller, is er sprake van een nuttige *exploit* voor het overnemen van een systeem. Zoals beschreven in de voorgaande paragraaf zijn deze *exploits* ook zeer lucratief om te verkopen en zullen zij die deze *exploits* kunnen opzetten deze eerder verkopen dan zelf loslaten op een openbaar wifi-netwerk.

De onderzoeksgroep heeft hiervoor niet de technische kennis om dit goed te kunnen belichten in het onderzoek en is daarbij buiten de scope van het onderzoek gebleven.

10. *Social engineering*, nut en noodzaak

Hoewel het erg makkelijk lijkt om een niet of te laat detecteerbaar virus te genereren, kan een aanvaller dit virus niet activeren zonder een zekere mate van gebruikersinteractie. Bij deze stelling is het belangrijk de reikwijdte van dit onderzoek in gedachte te houden; het is namelijk geen onderdeel van dit onderzoek om zelf systeemlekken te gaan zoeken of deze te kopen op de zwarte markt. Tijdens dit onderzoek is namelijk uitsluitend gebruik gemaakt van openbaar beschikbare informatie en technieken. Gebruik makende van deze, voor iedereen toegankelijke, technieken is het niet mogelijk om een systeem zonder medewerking van de gebruiker binnen te dringen.

Daarom is bij dit onderzoek *social engineering* betrokken. De tijdens dit onderzoek gehanteerde definitie van *social engineering* luidt als volgt: "*Any act that influences a person to take an action that may or may not be in their best interest.*" (Social Engineer, 2016b). Vertaald naar de toepassing van dit onderzoek wordt de gebruiker van een openbaar wifi-netwerk verleid tot het klikken op "ja" en daarmee tot het uitvoeren van een virus zodra deze gebruiker bijvoorbeeld een geprepareerde website bezoekt.

Een aanvaller monitort tijdens een aanval de gebruikte websites op een wifi-netwerk en voert vervolgens een ARP of DNS *spoof* uit, waarbij de gebruiker tijdelijk wordt omgeleid naar een kopie van de desbetreffende website met een virus. Op deze manier wordt de gebruiker via een dialoogvenster verleid tot het installeren van bijvoorbeeld de nieuwste Adobe Flash Player die uiteindelijk een virus blijkt te bevatten. Meer informatie over de exacte methode volgt in hoofdstuk 11.

De hierboven beschreven methode komt dicht in de buurt van *phishing*, met als belangrijk verschilpunt dat *phishing* primair gericht is op het ontfutselen van persoonlijke informatie via formulieren (Social Engineer, 2016a). Tijdens dit onderzoek is de definitie van *phishing* opgerekt naar "Het verleiden van een gebruiker tot het activeren van aanvalscode of het verstrekken van persoonlijke informatie". Deze oprekking is gedaan om deelvraag 5 beter te kunnen beantwoorden.

Waar *phishing* gebruik maakt van een sleepnetmethode, wordt bij *spear phishing* de doelgroep of doelpersoon zorgvuldig gekozen (Social Engineer, 2016a). Bij *spear phishing* creëert een aanvaller een voor de doelgroep of doelpersoon een zo effectief mogelijke vermomming van het virus, wat een betere voorbereiding vergt dan een *phishing* aanval. Deze betere voorbereiding is hiermee wegens de investering van tijd en middelen duurder. Daardoor is een goede selectie van de doelgroep of doelpersonen relevant om de kosten te laten opwegen tegen de baten.

Binnen dit onderzoek betekent *spear phishing* het selecteren van openbare wifi-netwerken wiens gebruikers een voor de aanvaller hoger rendement te bieden hebben. Een voorbeeld hierbij is het uitvoeren van een aanval op het wifi-netwerk van een club ondernemers. In een dergelijk geval kan aan de aanval ook een langere passieve voorbereidingstijd voorafgaan om bijvoorbeeld de website van de meest gebruikte bank zo goed mogelijk na te maken en zo een val voor het ontfutselen van de inloggegevens op te zetten.

De hierboven beschreven uitleg is noodzakelijk voor het begrijpen van verdere keuzes in het onderzoek, aangezien zonder s*ocial engineering* het niet mogelijk is gebleken om een systeem over te nemen. Overname van een systeem is alleen mogelijk gebleken met medewerking van de gebruiker. Het verleiden van de gebruiker tot medewerking is mogelijk via *social engineering*.

11. Opbouw van een aanval

Tijdens dit onderzoek hebben Boudewijn van Silfhout en Bart Dekker afzonderlijk van elkaar onderzoek gedaan naar mogelijke aanvallen op Windows 7 en de consumentenbeveiligingsproducten: Bullguard Internet Security 2016 en AVG Free. Alle aanvallen zijn uitgevoerd binnen de eigen omgeving; illegale aanvallen zijn niet uitgevoerd. Tijdens dit onderzoek is grotendeel gebruik gemaakt van Kali Linux, daar deze speciale distributie de mogelijkheid heeft om op een simpele manier relevante software te installeren.

11.1 Het genereren van een virus met Veil

Het Veil Framework is een softwareverzameling voor het genereren van virussen, ook wel *payloads* genoemd. Tevens biedt het Veil Framework mogelijkheden om deze virussen geautomatiseerd op systemen te zetten. Het gaat hierbij om de software Veil Catapult. Het nut van Veil Catapult is echter beperkt, omdat de aanvaller bij het gebruik van de Veil Catapult al over een gebruikersnaam en een wachtwoord moet beschikken. Als dergelijke informatie voorhanden is, beschikt de aanvaller doorgaans al over toegang tot het systeem. Daarom zal tijdens dit onderzoek verder niet gekeken worden naar Veil Catapult.

Het Veil Framework biedt ook software voor het genereren van virussen die een aanvaller op afstand toegang geven tot een systeem. Eenmaal geïnstalleerd bellen deze virussen naar huis en bieden de aanvaller op afstand toegang tot het systeem. Dit naar huis bellen wordt in vaktermen een *reverse shell* genoemd. Aanvallers maken graag gebruik van een *reverse shell*, omdat bijna alle firewalls aanvragen vanuit het vertrouwde eigen netwerk naar externe webservers doorlaten. Een aanvaller misbruikt deze firewall-instelling middels een *reverse shell* gebruik door het virus contact te laten leggen met een webserver van de aanvaller, en de aanvaller heeft daarmee geen last van een NAT firewall tussen het slachtoffer en het internet. Nadat een aanvaller middels een *reverse shell* toegang heeft gekregen tot een systeem, heeft de aanvaller het systeem volledig onder controle. Een aanvaller kan bijvoorbeeld extra virussen installeren voor het ophalen van bank- of creditcardgegevens, of gevoelige bestanden stelen.

Het probleem met het door standaard software als Veil Evasion laten genereren van virussen is dat de gegenereerde virussen op wat details zoals instellingen na gelijk aan elkaar zijn. Daardoor kunnen beveiligingsbedrijven deze gegenereerde virussen bestuderen en detectiemogelijkheden toevoegen aan hun beveiligingsproducten. De ontwikkelaars van dergelijke virusgeneratiesoftware hebben daar iets op gevonden. Doormiddel van speciale software kan een standaardvirus dusdanig gewijzigd worden dat het beveiligingsproducten misleidt. Deze misleiding gebeurd met *encoder software*, waarbij de *encoder* een virus meerdere malen aanpast en hetzelfde virus achtereenvolgens door

meerdere *encoders* aangepast wordt. Het juist instellen van deze keten van *encoders* is een proces van veel proberen en het doorlezen van de encoderdocumentatie.

Veil Evasion heeft dit hele proces in een simpele menustructuur gegoten, waardoor een aanvaller sneller komt te beschikken over een virus waarvan de kans groot is dat beveiligingsproducten het niet detecteren. Op 02-11-2016 is een door Veil Evasion gegenereerd geïnfecteerd bestand gescand door AVG Free, waarbij AVG Free het gescande bestand niet als virus detecteerde. Deze test is meerdere malen herhaald, waarna AVG Free uiteindelijk pas op 14-11-2016 het virus detecteerde. Bullguard Internet Security 2016 detecteerde daarentegen op alle testmomenten het door Veil Evasion gegenereerde virus.

11.2 Aanval op de browser met SET

In de testfase van dit onderzoek heeft elk volledig bijgewerkt Windows 7 systeem aanvallen zonder medewerking van de gebruiker succesvol afgeweerd. De gebruikte standaard software hiervoor betreft Metasploit, een veel gebruikt framework voor het verkennen en aanvallen van systemen en netwerken. Tevens is gebleken dat veel software van andere ontwikkelaars gebruik maken van Metasploit. Aanvallen die zonder medewerking van de gebruiker uitgevoerd kunnen worden, zijn bij opname in Metasploit of andere standaard software al gedicht door de desbetreffende ontwikkelaar, omdat beveiligingsonderzoekers om ethische redenen voor publicatie van een lek en Metasploit uitbreiding de desbetreffende ontwikkelaar altijd het lek laten dichten. Het zal niet verbazen dat er een zwarte markt is voor het kopen van lekken, en software die deze lekken uitbuit, om toch zonder medewerking van de gebruiker een systeem over te nemen. Het valt echter buiten dit onderzoek om op de zwarte markt lekken aan te schaffen en deze vervolgens te testen. aanschaffen

Bij het aanvallen en overnemen van een systeem is zoals hierboven beschreven een handeling van de gebruiker vereist. Een gebruikershandeling kan zijn om per abuis een met Veil Evasion gegenereerd virus te openen en daarmee een aanvaller een *reverse shell* te geven. Aangezien in de reguliere en technische media gewaarschuwd wordt tegen het openen van onbekende bestanden, is het volgens de onderzoekers onwaarschijnlijk dat een gebruiker simpelweg een onverhuld virus opent. Om een virus te vermommen, of de gebruiker te misleiden, is de Social Engineering Toolkit (SET) ontwikkeld. Middels SET is het mogelijk om een gebruiker te misleiden door het virus in een pdf-bestand te verstoppen dat zich voordoet als cv. Daarnaast is het mogelijk om een website te kopiëren en daar een aanvalscode in te verstoppen. Een aanvaller leidt vervolgens middels een ARP-spoofingaanval gebruikers naar de gekopieerde website met aanvalscode.

De volgende vormen van aanvalscode op basis van SET zijn onderzocht in combinatie met Internet Explorer, Firefox en Chrome:

- *Java applet*
- *Powershell script*

In het geval van de *Java applet*-aanval wordt de gebruiker via een dialoogvenster gevraagd om een *Java applet* uit te voeren. Deze *Java applet* downloadt en activeert een virus dat een aanvaller vervolgens toegang tot het systeem biedt. Uit het onderzoek is gebleken dat bij de laatste versie van de *Java Runtime Environment* (JRE), de software welke de *Java applet* daadwerkelijk uitvoert, de in SET ingebouwde *Java applet* niet uit wil voeren omdat de *Java applet* uit SET niet digitaal ondertekend is door een Certificaat Autoriteit (CA). De *Java applet* uit SET is namelijk *self-signed*, wat inhoudt dat de *applet* vertrouwd is door degene die het geschreven heeft maar niet door een externe partij is geverifieerd. Sinds JRE 8 is het niet mogelijk om *self-signed Java applets* uit te voeren, maar dit is nog wel mogelijk bij JRE 7 ondanks de standaardinstelling om geen *self-signed*

Java applets uit te voeren. Indien een gebruiker een verouderde versie van JRE geïnstalleerd heeft, wordt de gebruiker met veel waarschuwende teksten in de dialoogvensters afgeschrikt om de *Java applet* niet uit te voeren.

De onderzoekers achten het dan ook niet waarschijnlijk dat iemand met JRE 7 zowel de veiligheidsinstellingen verlaagd heeft als achteloos door de vele waarschuwingen heen klikt.

Voor een aanval via een *Java applet* is het daarmee noodzakelijk om een certificaat te kopen bij een CA. De kosten voor het ondertekenen van de *Java applet* blijken momenteel meer dan €100,-- te bedragen. Daarbij komt dat een CA bij misbruik de ondertekening intrekt, waardoor een nieuw certificaat gekocht dient te worden. Verder is gebleken dat alleen bij het gebruik van Internet Explorer de gebruiker prominent, en met een niet te negeren dialoogvenster verzocht wordt om de *Java applet* met het virus uit te voeren. Bij Firefox is de vraag om de *Java applet* uit te voeren slechts een kleine, eenvoudig te negeren, melding aan de bovenkant van het scherm. Binnen Chrome is het uitvoeren van *Java applets* zelfs helemaal niet mogelijk, gezien de ondersteuning hiervoor ontbreekt.

Voor het uitvoeren van de *Java applet* is zoals eerder beschreven de *Java Runtime Environment* (JRE) benodigd. Daaruit volgt dat de gebruiker reeds moet beschikken over een geïnstalleerde versie van JRE om vatbaar te zijn voor de aanval met de *Java applet.*. Om de geschatte vatbaarheid van systemen op de openbare wifi-netwerken te bepalen is gezocht naar statistieken over het marktaandeel van JRE. Er zijn verschillende bronnen voorhanden wat betreft het gebruik van JRE op servers, maar het gebruik van JRE op systemen van gebruikers is alleen onderzocht en gepubliceerd door Flexera Software. Flexera Software biedt onder andere software aan voor het detecteren van verouderde, niet bijgewerkte applicaties. Op basis van deze statistieken heeft het een document gepubliceerd over het gebruik van JRE en andere software in Nederland. JRE versie 8 is op 43% van de Nederlandse computers aanwezig, en gecombineerd met het 14% marktaandeel van JRE versie 7 komt het totale marktaandeel van JRE op 57% uit (Flexera Software, 2016).

De *Powershell script* aanval is ruwweg hetzelfde als de aanval met een *Java applet*, maar verschilt op de volgende twee punten: ondersteuning is standaard ingebouwd in Windows 7, en er is geen ondertekening van het *Powershell script* vereist. Net als de *Java applet* aanval wordt deze *Powershell script* aanval uitgevoerd door de gebruiker via ARP- of DNS-*spoofing* om te leiden naar een gekopieerde en aangepaste website. Zodra de website geopend wordt, verschijnt in Internet Explorer de vraag of het *Powershell script* uitgevoerd mag worden, middels net als bij de *Java applet*-aanval een prominent aanwezig en niet te negeren dialoogvenster. Bij Firefox en Chrome wordt alleen een bestand gedownload naar de standaard ingestelde downloadmap van de browser en wordt verder niet gevraagd of het *Powershell script* uitgevoerd moet worden. Hiermee is alleen Internet Explorer kwetsbaar voor een dergelijke aanval via een *Powershell script*.

Bij beide aanvallen wordt de gebruiker uiteindelijk naar de echte website doorgestuurd na het activeren van de *Java applet* of het *Powershell script*. Indien de *Java applet* of het *Powershell script* niet uitgevoerd wordt, en de gebruiker op een link binnen de website klikt, dan zal de aanval opnieuw gestart worden wegens de ARP- of DNS-*spoofing*. Mogelijk zal de gebruiker na enige tijd denken dat de website hapert, en deze op een ander tijdstip nogmaals proberen. Na een succesvolle aanval zal de aanvaller doorgaans de vervalste websites en de ARP of DNS-*spoofing* gericht tegen het systeem van de gebruiker staken. Als de gebruiker immers bij meerdere website te maken krijgt met de vraag om een *Java applet* of *Powershell script* uit te voeren, dan kan de gebruiker argwaan krijgen.

11.3 *Backdoor* met behulp van Shellter

Naast de mogelijkheden om een compleet nieuwe *payload* te generen met behulp van Metasploit en SET, is er ook een mogelijkheid om bestaande, uitvoerbare bestanden met de bestandsextensie .EXE te voorzien van een *backdoor*. Deze *backdoor* houdt in dat er vanaf het systeem waar het programma wordt uitgevoerd een *reverse shell* naar de sessie van de aanvaller wordt opgezet.

Het voordeel van Shellter ten opzichte van VEIL is dat Shellter bestaande programma's gebruikt en daardoor minder argwaan zal opwekken in de gebruikers. Daarnaast is tijdens praktijktesten gebleken dat zowel AVG als BullGuard deze bestanden niet detecteren als zijnde een virus. Het enige moment waarop BullGuard de aanval als zodanig geïnterpreteerd heeft, was op het moment dat de aanvaller het proces van de *reverse shell* naar een ander proces aan het migreren was. Dit werd gedaan om te zorgen dat het proces en daarmee de *reverse shell* voor langere tijd actief zou blijven dan alleen op het moment dat het originele .EXE bestand werd uitgevoerd.

Het invoegen van een *backdoor* is dankzij het Shellter project zeer eenvoudig gemaakt. Het programma is vrij toegankelijk en te downloaden op de site van Shellter. Het programma draait onder Windows en vereist slechts administratorrechten om correct te functioneren. De aanvaller kan binnen afzienbare tijd een backdoor opstellen via de menu's in Shellter.. Er wordt ook ondersteuning geboden om meerdere *backdoors* in hetzelfde programma te zetten voor het geval de firewall de poort blokkeert bij het opzetten van een *reverse shell.*

Shellter kan het programma echter niet verspreiden. De onderzoeksgroep heeft hiervoor wel een aantal mogelijkheden kunnen bedenken, namelijk:

- Een namaakwebsite opzetten, bijvoorbeeld zogenaamd voor een update van Java, waar in de setup de *backdoor* geplaatst is.
- Een populair programma wat vaak illegaal gedownload wordt, bijvoorbeeld Adobe Photoshop, Microsoft Word of Windows zelf. Bij zulke downloads worden vaak programma's meegeleverd om de volledige versie te activeren, en hier kan vervolgens een backdoor in geplaatst worden.

Deze genoemde realistische scenario's zijn wegens ethische bezwaren niet door de onderzoekgroep in werking gezet, maar het waarschuwen waard.

12. Testomgeving en resultaten

Aan de hand van het theoretisch onderzoek is er een testomgeving opgezet, gebaseerd uit de resultaten van hoofdstuk 5 en 6. Deze testomgeving is gebruikt voor het uitvoeren van de aanvallen zoals beschreven in hoofdstuk 8 en 11.

12.1 Opbouw van de testomgeving

Uit het marktonderzoek, beschreven in hoofdstuk 5 en 6, is gebleken dat het meest gebruikte besturingssysteem op het moment van schrijven Windows 7 is. Daarnaast zijn de consumentenbeveiligingsproducten “Bullguard Internet Security” en “AVG AntiVirus Free 2016” gebruikt in de testomgeving.

Voor het uitvoeren van de tests om in te dringen, of het infecteren van het systeem, is er gekozen om een tweetal machines op te zetten in VMware Workstation 12. Beide zijn voorzien van Windows 7 Ultimate en alle updates. Het enige verschil tussen de systemen was het consumentenbeveiligingsproduct wat geïnstalleerd is.

Het systeem wat gebruikt is voor het uitvoeren van de aanvallen, is de speciale VMware versie van Kali 2.0. Ook dit systeem in voorzien van de meest recente versie, van zowel het besturingssysteem als alle applicaties meegeleverd met Kali 2.0.

12.2 Testresultaten

De aanvallen zijn tweemaal uitgevoerd, tussen deze aanvallen zijn 10 dagen verstreken. Dit is gedaan om de consumentenbeveiligingsproducten de kans te geven hun *signature* database te laten updaten. Deze database is verantwoordelijk voor het detecteren van virussen. De gebruikte aanvallen zijn beschreven in hoofdstuk 8 en 11. Het gebruik van *exploits* is niet meegenomen in de resulaten, gezien deze niet succesvol uitvoerbaar waren. De beschikbare *exploits*, zoals beschreven in hoofdstuk 9, waren reeds gepatched in de Windows 7 updates, of niet van toepassing op het systeem. In de onderstaande tabel (tabel 1) is een schematische weergave van beide aanvalspogingen weergegeven.

	Bullguard Internet Security 2016		**AVG AntiVirus Free**	
	Aanval geslaagd 1e poging	**Aanval geslaagd 2e poging**	**Aanval geslaagd 1e poging**	**Aanval geslaagd 2e poging**
SET: Java applet	Ja	Ja	Ja	Ja
SET: Powershell	Ja	Ja	Ja	Ja
Veil Evasion	Nee	Nee	Ja	Nee
Shellter	Ja	Ja	Ja	Ja

Tabel 1: Overzicht van de testrondes met de verschillende werkende aanvallen.

Uit de tabel is op te maken dat “Bullguard Internet Security” wel volledige bescherming bood tegen Veil, terwijl “AVG AntiVirus Free 2016” hier een update voor nodig had. De verdere resultaten komen met elkander overeen.

Voorafgaand aan dit onderzoek werd gedacht dat een enquête over het surfgedrag van de gebruikers op een openbaar wifinetwerk op zijn plaats was. Tijdens het verloop van het praktijkonderzoek is echter gebleken dat er doormiddel van WireShark bepaald kan worden welke websites door een

gebruiker bezocht worden. Dit maakt het voor de aanvaller mogelijk om in te spelen op de websites waar zijn doelwit momenteel mee bezig is. WireShark maakt het namelijk mogelijk om de DNS-verzoeken die over het netwerk plaatsvinden in te zien. Doormiddel van deze verzoeken kan de aanvaller zeer eenvoudig zien of zijn doelwit momenteel op Facebook zit, of juist het nieuws op NU.nl zit te lezen.

13. Conclusie

Voor de conclusie op dit onderzoek zal iedere deelvraag beantwoord worden en tot slot de onderzoeksvraag.

Wat zijn de basisparameters voor het testsysteem ter beantwoording van de hoofdvraag?

De basisparameters voor het testsysteem zijn het besturingssysteem met het grootste marktaandeel en de als best aanbevolen consumentenbeveiligingsproducten: één betaald pakket en één gratis verkrijgbaar. Uit hoofdstuk 7 is gebleken dat Windows 7 het grootste marktaandeel heeft, namelijk rond de 48% afgaande op verschillende bronnen. Daarnaast zijn de consumentenbeveiligingsproducten gekozen die de Consumentenbond aanprijst als “Beste uit de test” in de categorieën betaalde en onbetaalde pakketten. Deze producten zijn respectievelijk “Bullguard Internet Security” en “AVG AntiVirus Free 2016”. Deze producten zijn op 5 mei 2016 door de Consumentenbond getest.

In hoeverre zijn volledig bijgewerkte systemen, welke beschikken over de onder deelvraag 1a en 1b gespecificeerde combinatie, vatbaar voor een actieve aanval op een openbaar wifi-netwerk ongeacht de benodigde aaneengesloten aanvalstijd?

Tijdens het onderzoek is gebleken dat het compromitteren van een volledig up-to-date systeem zeer lastig is. Dit komt alsmede de standaard firewall instellingen die Windows 7 aanhoudt op een openbaar wifi-netwerk. Hierdoor worden alle verbindingen van buitenaf die niet expliciet toegestaan zijn, geweigerd en kan er niet zomaar een verbinding geïnitieerd worden. De *exploits* om zonder gebruikersinteractie alsnog toegang te krijgen tot een systeem zijn reeds gepatcht, of zijn voor grote geldbedragen te koop op de zwarte markt. Daarentegen kan de firewall nauwelijks bescherming bieden zodra er eenmaal een virus op een systeem geplaatst en geactiveerd is. Gezien de firewall standaard alles toestaat wat vanuit het systeem zelf geïnitieerd wordt, kan er middels een vooraf geplaatst virus ook van buitenaf gecommuniceerd worden door de firewall heen.

Tot slot boden zowel “Bullguard Internet Security” als “AVG AntiVirus Free 2016” geen bescherming tegen de actieve aanvallen met ARP, DNS, MAC en/of *IP spoofing*. De pakketten hebben geen functionaliteit om deze soorten aanvallen te detecteren. Dit zou kunnen worden vastgesteld of zelfs voorkomen door het toevoegen van een *Intrusion Dectection System* (IDS) of zelfs een *Intrusion Prevention System* (IPS). Deze technieken maken het mogelijk om aanvalspogingen vast te stellen met de IDS en automatisch te blokkeren indien het een IPS is. Deze technieken voorkomen niet dat virussen zich manifesteren op een systeem, maar maakt het wel mogelijk om te voorkomen dat het netwerkverkeer omgeleid wordt zoals bij een man-in-the-middle-aanval. Indien de voorgenoemde pakketten wel over deze IDS- of IPS-functionaliteit zouden beschikken, zou het niet zomaar mogelijk zijn geweest om gebruikers een kopie van een website aan te bieden en een geïnfecteerde *Java applet* voor te schotelen. Dit zou het aanvalsvlak van SET significant verkleinen.

In hoeverre is het mogelijk om een computersysteem te compromitteren in de tijd waarin de gebruiker zich tijdens het nuttigen van een of meerdere consumpties op een openbaar wifi-netwerk bevindt?

Zodra het netwerkverkeer van de gebruiker eenmaal omgeleid werd met een *ARP spoofing attack*, was het een kwestie van enkele seconden om vast te stellen welke website bezocht werd door de gebruiker, gezien WireShark recente DNS-verzoeken toont. De websites die bezocht werden konden vervolgens in enkele seconden tot maximaal een minuut gekopieerd worden door middel van de

SET-toolkit. Bij de kopie zou vervolgens automatisch een malafide *Java applet* kunnen worden toegevoegd; dit zou in principe genoeg zijn om een systeem te compromitteren.

Het enige probleem bij deze aanval is dat sinds Java 7 update 21 gecontroleerd wordt op het certificaat waarmee de *applet* ondertekend is. Gezien SET "*self-signed certificates*" gebruikt, worden deze niet vertrouwd door Java. Hierdoor moet de gebruiker eerst zijn veiligheidsinstellingen van Java verlaagd hebben en een oudere versie dan 7 update 21 gebruiken, wat niet aannemelijk is gezien de vele waarschuwingen en notificaties die gegeven worden om Java te updaten naar de nieuwste versie(op het moment van schrijven versie 8 update 111).

Tijdens het genereren van een virus en het activeren van de *payload*, zou een aanvaller niet zozeer gehinderd worden bij het onzichtbaar maken van een virus voor de consumentenbeveiligingsproducten, maar eerder bij het plaatsen zelf. Via VEIL of Shellter kunnen aanvallers eenvoudig nieuwe virussen opzetten, of zelfs bestaande uitvoerbare programma's voorzien van een *backdoor*, maar de voor infectie benodigde gebruikersinteractie blijkt ingewikkelder. Wij verwachten dan ook dat aanvallers zullen kiezen voor verspreiding op grote schaal in plaats van op een openbaar wifi-netwerk. Hierbij kan gedacht worden aan het plaatsen van deze bestanden op illegale downloadwebsites of versturen van *phishing mails*.

Welke verschillen zijn te meten tussen een door een onafhankelijke Nederlandse consumentenorganisatie aanbevolen gratis en betaald consumentenbeveiligingsproduct, bij het detecteren en eventueel reageren op een actieve aanval zoals de in deelvraag drie beschreven aanval?

De virussen die gegeneerd zijn met VEIL en Shellter zijn meerdere keren getest met beide pakketten. De testrondes lagen 10 dagen uit elkaar om de pakketten hun *signatures* te laten updaten. Deze *signatures* worden gebruikt voor het detecteren van virussen. In tabel 2 is een overzicht opgesteld van deze aanvallen.

	Bullguard Internet Security 2016		**AVG AntiVirus Free**	
	Aanval geslaagd 1e poging	**Aanval geslaagd 2e poging**	**Aanval geslaagd 1e poging**	**Aanval geslaagd 2e poging**
SET: Java applet	Ja	Ja	Ja	Ja
SET: Powershell	Ja	Ja	Ja	Ja
Veil Evasion	Nee	Nee	Ja	Nee
Shellter	Ja	Ja	Ja	Ja

Tabel 2: Overzicht van de testrondes met de verschillende werkende aanvallen.

Het enige verschil in detectie is tussen "Bullguard Internet Security 2016" en "AVG AntiVirus Free" is dat "Bullguard Internet Security 2016" wel de eerste keer bescherming bood tegen VEIL, terwijl "AVG AntiVirus Free" het virus bij de tweede poging pas detecteerde. Bij de aanvallen met SET moet wel de eerdere kanttekening over het certificaat van de *Java applets* meegenomen worden. Tijdens het

testen is het "*self-signed certificate*" handmatig toegevoegd als zijnde een vertrouwd certificaat om op deze wijze een legitiem certificaat te simuleren. Geen van beide pakketten bood bescherming tegen een virus gemaakt met Shellter, maar dit is een lastig virus om zomaar op een systeem te krijgen, zeker in een openbare locatie.

Bij welke systeemconfiguraties van systemen op een openbaar wifi-netwerk of het openbare wifi-netwerk zelf loont het voor een aanvaller niet langer om willekeurige systemen op openbare wifi-netwerken aan te vallen, en zal deze doelwitten zorgvuldiger kiezen?

Voor het succesvol uitvoeren van een SET aanval, gebaseerd op *Java applets*, zou de aanvaller een legitiem certificaat moeten aanschaffen om de *applets* mee te ondertekenen. De kosten van dit certificaat zijn meer dan €100,-. Daarnaast is het de taak van een Certificaten Autoriteit om misbruik met certificaten te voorkomen en malafide certificaten in te trekken. Dit zou inhouden dat een aanvaller een prijzig certificaat slechts enkele keren kan gebruiken voordat deze ingetrokken wordt. Zodoende zouden aanvallen via SET niet lonend zijn om te gebruiken.

Daarnaast zijn er ook de *exploits* die gebruikt kunnen worden om een systeem binnen te dringen. De gratis beschikbare *exploits*, welke ook in MetaSploit zitten, zijn of reeds gepatcht, of dusdanig specifiek dat deze niet te gebruiken zijn op een openbaar wifi-netwerk. Om gebruik te kunnen maken van *exploits* of ongedichte *zero days* zouden aanvallers naar de zwarte markt moeten uitwijken. De kosten voor deze middelen zijn nog hoger dan een certificaat, namelijk van $1.500 tot maar liefst $75.000. Deze bedragen zijn mogelijk te hoog om te gebruiken voor aanvallen tegen consumenten en eerder bestemd voor aanvallen richting bedrijven.

De laatste mogelijkheid is het zelf zoeken van veiligheidslekken binnen de software. Dit zal veel tijd en kennis kosten van de aanvaller. Gezien het onderzoeksteam hier geen expertise in heeft, is dit buiten de scope van het onderzoek gevallen. Het is echter wel een interessant onderwerp voor een vervolgonderzoek.

Tot slot, het antwoord van het onderzoeksteam op de onderzoeksvraag:

> *In hoeverre is er een verschil aanwezig in detectie en daaropvolgende preventiemaatregelen tussen betaalde en gratis beschikbare consumentenbeveiligingsproducten, zodra gepoogd wordt een systeem met daarop aanwezig volledig bijgewerkte versie van het meest gebruikte besturingssysteem te compromitteren tijdens een actieve aanval via een openbaar wifi-netwerk?*

Het verschil tussen de detectie van de gegeneerde virussen is gering. "Bullguard Internet Security 2016" was in één geval eerder met detecteren dan "AVG AntiVirus Free". Voor de detectie van virussen zijn reeds vele andere testoverzichten beschikbaar welke een grotere scope selectie aan virussen gebruiken dan tijdens dit onderzoek gebruikt is. Daarentegen boden geen van beide pakketten bescherming tegen aanvallen die gebruik maakten van ARP, DNS, MAC en/of *IP spoofing*. Deze aanvallen konden ongestoord uitgevoerd worden. Indien een betaald pakket hier wel bescherming tegen biedt, zou dit een grote reden zijn om te kiezen voor een abonnement bij die leverancier.

De grootste stap naar een veilig systeem blijkt mogelijk niet de keuze tussen een gratis of betaald antivirus pakket, maar juist dat alle software up-to-date is, om te voorkomen dat er *exploits* gebruikt kunnen worden om toegang te verkrijgen tot het systeem. Daarnaast is het ook van belang dat de gebruiker alert is op ongewone programma's die uitgevoerd worden tijdens het bezoeken van websites. Men zou zich hierin kunnen laten steunen door het installeren van browserextensies zoals

“NoScript” die voorkomen dat websites een script opstarten zonder toestemming van de gebruiker. . Dit verkleint het aanvalsvlak nog verder en maakt het de aanvaller nog lastiger om een systeem in handen te krijgen.

Het onderzoeksteam geeft als aanbeveling mee aan de lezer: “Update nu en niet later.”

14. Aanbevelingen voor voortzetting van dit onderzoek

Gaandeweg dit onderzoek zijn wij erachter gekomen dat de scope te beperkt is om een succesvolle aanval te simuleren. Een succesvolle aanval binnen deze scope zou wel mogelijk zijn met behulp van op de zwarte markt gekochte software, maar wij vinden het moreel verwerpelijk om criminele activiteiten te ondersteunen door middel van het kopen van illegale software. Daarom gaan we niet adviseren deze software op de zwarte markt te kopen. Toch hebben wij wel een aantal aanbevelingen voor vervolgonderzoek; deze aanbevelingen betreffen verschillende veldtesten.

Een mogelijke veldtest zou kunnen zijn om, met inachtneming van de wet, daadwerkelijk aanvallen uit te gaan voeren op een openbaar wifi-netwerk. Dit omdat dan een beter beeld verkregen kan worden welke aanvallen wel en niet slagen met behulp van *social engineering*. In theorie kan dit ook middels een enquête, maar dit geeft een vertekend beeld gezien de situatie moeilijk te simuleren is. Bij de beoogde *social engineering* kan het vervolgens gaan om puur digitale aanvallen zoals elders in dit document beschreven, maar ook om het gratis verstrekken van besmette USB-sticks.

Een andere veldtest is het, met inachtneming van de wet, versturen van geïnfecteerde cv’s naar bedrijven. Hiermee kan getest worden in hoeverre bedrijven vatbaar zijn voor deze vorm van *social engineering*. Deze veldtest zou zowel de digitale beveiliging beproeven (de goede werking van beveiligingsproducten binnen de organisatie) alsmede de rol van de poortwachter, namelijk de gebruiker.

Op het internet wemelt het van de illegale software. Vaak bestaat deze illegaal te downloaden software uit een bundel van een proefversie samen met een *crack*. Een *crack* is een uitvoerbaar bestand dat een proefversie kosteloos omzet in de volledige, betaalde versie. De persoonlijke ervaring van de onderzoekers leert dat *cracks* vaak met administratorrechten gestart worden en dat meldingen van beveiligingsproducten vaak genegeerd worden. De mogelijk uit te voeren veldtest bestaat uit het, met inachtneming van de wet, verspreiden van dergelijke softwarebundels. Hierbij zou de *crack* en/of proefversie middels bijvoorbeeld Shellter geïnfecteerd zijn met een virus. Tijdens vervolgonderzoek zou dan via een speciaal opgezette server kunnen worden bijgehouden hoeveel gebruikers in deze aanval trappen en onder welke omstandigheden.

Een laatste aanbeveling is om daadwerkelijk zelf naar lekken in Windows en/of andere software te gaan zoeken. Hiermee worden moreel bezwaarlijke stappen zoals de aanschaf van aanvalssoftware op de zwarte markt vermeden, maar kan ook bekeken worden of actieve aanvallen op openbare wifi-netwerken zonder *social engineering* mogelijk zijn. De onderzoekers vinden dit echter een project dat niet door *System and Network Engineering* (SNE) uitgevoerd kan worden, omdat de benodigde kennis vanuit de opleiding ontbreekt. Dit zou wellicht beter aansluiten bij studenten Technische Informatica, al dan niet tijdens de masterfase.

Bibliografie

123tijdschrift.nl. (2016). Computerbladen op 123tijdschrift.nl. Retrieved October 24, 2016, from https://www.123tijdschrift.nl/computerbladen

Consumentenbond. (2016a). Testresultaat BullGuard Internet Security 2016. Retrieved October 25, 2016, from https://www.consumentenbond.nl/virusscanner/producten/bullguard/internet-security-2016

Consumentenbond. (2016b). Testresultaat G Data Internet Security 2016. Retrieved October 25, 2016, from https://www.consumentenbond.nl/virusscanner/producten/g-data/internet-security-2016

DomainTools. (2016). Whois Record for TopReviews.nl. Retrieved October 24, 2016, from https://whois.domaintools.com/topreviews.nl

Flexera Software. (2016). *Personal Software Inspector Country Report - Q3 2016 Netherlands*. Retrieved from https://media.flexerasoftware.com/documents/Research-SVM-NL-2016Q3.pdf

IST MIT. (2016). Viruses, Spyware, and Malware. Retrieved October 2, 2016, from https://ist.mit.edu/security/malware

Kamp, R. (2016, May). Test beveilingssoftware. *Consumentengids*, (Consumentengids 5 mei 2016), 32–35.

Larkin, E. (2008, August 26). Build Your Own Free Security Suite. Retrieved October 2, 2016, from http://www.pcworld.com/article/150204/free_security_suite.html

Netmarketshare. (2016, August). Desktop Operating System Market Share. Retrieved September 29, 2016, from https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0

Parlement.com. (2016). Consumentenorganisaties - Parlement & Politiek. Retrieved October 24, 2016, from https://www.parlement.com/id/vh8lnhrq7yb5/consumentenorganisaties

Proefabonnementen Gids. (2016). Computerbladen abonnementen. Retrieved October 24, 2016, from https://www.proefabonnementen-gids.nl/proefabonnementen/computers-internet

PSTN Tutorial. (n.d.-a). Retrieved October 2, 2016, from http://www.telecommunications-tutorials.com/tutorial-OSI-7-layer-model.htm

PSTN Tutorial. (n.d.-b). Retrieved from http://www.telecommunications-tutorials.com/tutorial-OSI-7-layer-model.htm

Public Wi-Fi Security. (n.d.). [Kaspersky Lab US]. Retrieved from https://usa.kaspersky.com/internet-security-center/internet-safety/public-wifi

Rebbapragada, N. (2016, May 25). All-in-One Security. Retrieved October 2, 2016, from https://web.archive.org/web/20101027113242/http://www.pcworld.com/article/125817-2/allinone_security.html

Rubenking, N. J. (2016, September 26). The Best Security Suites of 2016. Retrieved October 2, 2016, from http://www.pcmag.com/article2/0,2817,2369749,00.asp

Silberschatz, A., Galvin, P. B., & Gagne, G. (1994). *OPERATING SYSTEM CONCEPTS* (Vol. 4). Addison-Wesley. Retrieved from http://www.cs.du.edu/~cag/courses/CS/DU/comp3361/Lectures/tm01-05.pdf

Social Engineer. (2016a). Phishing. Retrieved December 7, 2016, from http://www.social-engineer.org/framework/general-discussion/real-world-examples/phishing/

Social Engineer. (2016b). Social Engineering Defined. Retrieved December 6, 2016, from http://www.social-engineer.org/framework/general-discussion/social-engineering-defined/

StatCounter GlobalStats. (2016, September). Top 7 Desktop, Tablet & Console OSs Sept 2015 to Sept 2016. Retrieved October 24, 2016, from http://gs.statcounter.com/#os-ww-monthly-201509-201609-bar

Statista. (2016, July). Desktop OS market share 2012-2016. Retrieved October 24, 2016, from https://www.statista.com/statistics/218089/global-market-share-of-windows-7/

TopReviews.nl. (n.d.). Beste Internet Security 2016. Retrieved October 24, 2016, from http://www.topreviews.nl/anti-virus-software/beste-internet-security/

Bijlage 1: Plan van Aanpak

Versiebeheer

Versie	Datum	Wijzigingen	Status
0.1	19-9-2016	Eerste opzet PvA	Gereed
0.2	28-9-2016	Aanvulling deelvragen en projectbeschrijving	Gereed
0.3	29-9-2016	Aanpassen onderzoeksvragen	Gereed
0.4	1-10-2016	Opzet Theoretisch Kader	Gereed
0.5	07-10-2016	Feedback Ander verwerken	Gereed
1.0	13-10-2016	Goedgekeurd door Ander de Keijzer	Gereed

Distributielijst

Functie	Naam	Organisatie	Datum
Begeleider	Ander de Keijzer	Hogeschool Utrecht	
Organisator	Leo Moergestel	Hogeschool Utrecht	
Organisator	Esther van der Stappen	Hogeschool Utrecht	

Goedkeuringen

Naam	Functie	Handtekening	Datum
Ander de Keijzer	Begeleider		13-10-2016

Auteur

Naam	Initialen	Student nummer	Telefoon	E-mail
Boudewijn van Silfhout	B.			
Bart Dekker	B.J.M.			

Voorwoord

Het document wat voor u ligt, is het Plan van Aanpak (PvA) voor het onderzoeksemester van het negende semester als gegeven door de Hogeschool Utrecht (HU). Het doel van dit project is onderzoeken wat de toegevoegde waarde van betaalde consumentenbeveiligingsproducten is ten opzichte van gratis varianten in het geval van een actieve aanval op een plat netwerk.

Dit PvA is geschreven door 4de jaars studenten van de HU. De begeleider voor dit project, vanuit de HU is Ander de Keijzer.

Het PvA is voornamelijk een plan, dat wil zeggen dat er in het verloop van het project veranderingen of wijziging kunnen plaatsvinden in deze plannen. Voor het verloop van het project zal dit PvA wel aangehouden worden.

Het doel van dit PvA is om een beeld te geven van de activiteiten waaruit het onderzoeksproject zal bestaan en de afspraken die gemaakt worden met de begeleider, Ander de Keijzer.

Utrecht, 28 september 2016.

Inhoudsopgave

1. Inleiding

Tegenwoordig is het bijna overal wel mogelijk om gratis gebruik te maken van een Wi-Fi netwerk, de Starbucks, McDonald's en zelfs de Albert Heijn. Vaak zijn deze openbare Wi-Fi netwerken zonder wachtwoord beveiligd of het wachtwoord wordt vrij verstrekt. Dit feit maakt het gebruik van dit netwerk een stuk onveiliger dan in de eerste instantie verwacht zou worden. Deze gevaren worden vaak aangestipt door bedrijven, waaronder Kaspersky Lab US ("Public Wi-Fi Security," n.d.), maar ook door media die een algemene, niet technische inslag hebben zoals het Trouw en het NOS-journaal.

Tips die vaak gegeven worden zijn:

- Controleer of je device niet automatisch verbinding maakt met een Wi-Fi netwerk;
- Pas je surfgedrag aan op het openbare netwerk; Controleer dus geen bankzaken;
- Controleer de naam van het Wi-Fi netwerk;
- Vul alleen inloggegevens of bankgegevens in op websites die met SSL beveiligd zijn (herkenbaar aan het groene slot);
- Verander wachtwoorden regelmatig;
- Gebruik, indien mogelijk, een Virtual Private Network (VPN);
- Schakel de firewall van je systeem in;
- Zorg dat je systeem en antivirus up-to-date is.

Deze tips zijn al vaak gegeven en worden ook vaak opgevolgd, maar zijn deze ook voldoende om beschermd te zijn tegen kwaadwillende? In hoeverre kan het consumentenbeveiligingsproduct op jouw laptop aanvallen tegengaan? Voegen de betaalde pakketten van consumentenbeveiligingsproductenleveranciers daadwerkelijk iets toe, of is gratis goed genoeg? Tijdens dit onderzoeksemester willen de onderzoekers, Bart Dekker en Boudewijn van Silfhout, hier antwoord op gaan geven.

2. Opdrachtbeschrijving

Voor het onderzoek naar de gevaren van openbare Wi-Fi hotspots en de effectiviteit van consumentenbeveiligingsproducten, moet naar verscheidende aspecten gekeken worden. Deze luiden als volgt:

- Gebruikerspatronen op openbare netwerken;
- Marktaanbod van consumentenbeveiligingsproducten;
- Marktaandeel van besturingssystemen.

Aan de hand van de informatie die uit deze aspecten zal voortvloeien, kan een testplan opgesteld worden om consumentenbeveiligingsproducten te testen op actieve aanvallen op een openbaar Wi-Fi netwerk. De praktijktest zal plaatsvinden in een testomgeving met het meest gebruikte besturingssysteem en de door een Nederlandse consumentenorganisatie als best getest gratis en betaald consumentenbeveiligingsproduct. Tijdens de praktijktest zal een gecontroleerde omgeving opgezet worden die bestaat uit meerdere cliëntsystemen en een aanvalssysteem. Het aanvalssysteem zal gebruik maken van Kali, gezien dit besturingssysteem de meest voor de hand liggende tools bevat voor het uitvoeren van netwerkaanvallen.

2.1 Probleemstelling

Gezien er steeds meer openbare Wi-Fi netwerken zijn en gebruikers steeds vaker even hun e-mail of het nieuws controleren tijdens het nuttigen van een consumptie, bijvoorbeeld bij de Starbucks. Is het interessant om na te gaan in hoeverre de beveiliging, zoals gesteld wordt door de media, voldoet om daadwerkelijk tegen aanvallers beschermd te zijn. De onderzoeksgroep gaat dit onderzoeken door na

te gaan wat het meest gebruikte besturingssysteem is en welke mogelijke consumentenbeveiligingsproducten op de markt zijn. Uit dit onderzoek moet blijken of er een verschil is tussen een door een Nederlandse consumentenorganisatie als best geteste gratis beschikbare consumentenbeveiligingsproduct en de betaalde opponent.

2.2 Doelstelling

Het doel van het project is om een vergelijking tussen het beste betaalde en gratis consumentenbeveiligingsproduct, op te stellen met betrekking tot actieve aanvallen op een plat, openbaar Wi-Fi netwerk. Om tot een realistisch testplan te komen is het van belang om vanuit betrouwbare bronnen het meest gebruikte besturingssysteem en de door een Nederlandse consumentenorganisatie als beste geteste gratis en betaalde consumentenbeveiligingsproducten te vernemen.

Uit deze productvergelijking moet blijken of een betaald consumentenbeveiligingsproduct een gebruiker beter tegen een actieve aanval beschermd dan een gratis variant, naast bescherming tegen de in het wild aanwezige virussen en andere dreigingen op het internet. Uit de vergelijking moet ook blijken of betaalde beveiligingsproducten meerwaarde hebben ten opzichte van de gratis varianten, met name de actieve beveiliging die de fabrikanten van deze beveiligingsproducten aanbieden bij de betaalde licenties of bijvoorbeeld wachtwoordbeheer.

2.3 Afbakening en randvoorwaarden

Dit project wordt uitgevoerd door studenten aan de Hogeschool Utrecht (HU). De HU kent per student 25 European Credit Transfer System (ECTS) toe aan ieder project lid. Deze 25 ECTS staan gelijk aan 700 studielasturen. Gezien dit project door twee studenten wordt uitgevoerd staat het totaal studielasturen gelijk aan 1400 uur.

Het onderzoek zal beperkt blijven tot het meest gebruikte besturingssysteem voor computers, portables en wearables vallen buiten de scope van het project. Daarnaast zal de onderzoeksgroep zich limiteren tot de door een Nederlandse consumentenorganisatie als best geteste gratis en betaalde consumentenbeveiligingsproducten. Dit wordt gedaan omdat de onderzoeksgroep geen bestaande kennis en kunde heeft van het uitvoeren van hackaanvallen en deze kennis en kunde eerst moet gaan opbouwen. Indien meer platformen en consumentenbeveiligingsproducten getest zouden worden, is er niet voldoende tijd beschikbaar voor het grondig uitvoeren van het onderzoek.

De volgende randvoorwaarden zijn van toepassing op dit project:

- Aanwezigheid van de projectleden bij de gegeven lessen en bijeenkomsten;
- Beschikbaarheid van een geschikte werkomgeving, zowel thuis als op de Hogeschool Utrecht;
- Geschikte laptops en netwerkapparatuur voor het uitvoeren van het opgestelde testplan;
- Kennis met betrekking tot Kali en de bijbehorende tools;
- Beschikbaarheid en bereikbaarheid van de begeleider.

3. Onderzoeksvraag en deelvragen

De voor dit onderzoek gedefinieerde onderzoeksvraag luidt als volgt:

In hoeverre is er een verschil aanwezig in detectie en daaropvolgende preventiemaatregelen tussen betaalde en gratis beschikbare consumentenbeveiligingsproducten, zodra gepoogd wordt een systeem met daarop aanwezig volledig bijgewerkte versie van het meest gebruikte besturingssysteem te compromitteren tijdens een actieve aanval via een openbaar Wi-Fi netwerk?

Ter beantwoording van de hierboven genoemde onderzoeksvraag zijn de volgende deelvragen gedefinieerd:

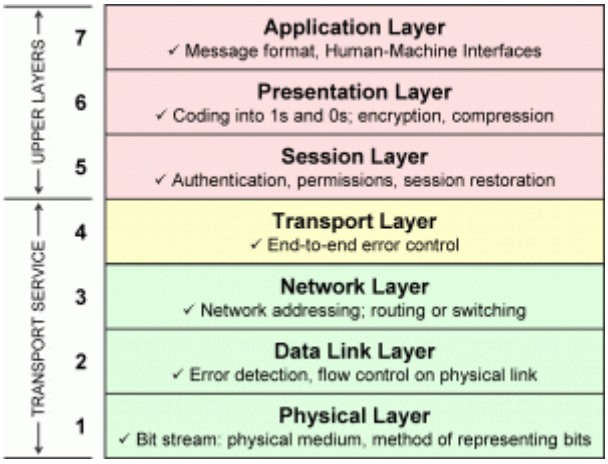
6) Wat zijn de basisparameters voor het testsysteem ter beantwoording van de hoofdvraag?
   a) Welk besturingssysteem, bijbehorend versienummer, wordt het meest gebruikt en vormt daarmee het grootste doelwit?
   b) Welk consumentenbeveiligingsproduct wordt aanbevolen door een onafhankelijke Nederlandse consumentenorganisatie?
7) In hoeverre zijn volledig bijgewerkte systemen, welke beschikken over de onder deelvraag 1a en 1b gespecificeerde combinatie, vatbaar voor een actieve aanval op een openbaar Wi-Fi netwerk ongeacht de benodigde aaneengesloten aanvalstijd?
8) In hoeverre is het mogelijk om in de tijd waarin een persoon zich tijdens het nuttigen van een of meerdere consumpties, ervan uitgaande dat de desbetreffende persoon daar geen kantoor houdt, op een openbaar Wi-Fi netwerk bevindt, het desbetreffende systeem te compromitteren?
9) Welke verschillen zijn te meten tussen een door een Nederlandse onafhankelijke consumentenorganisatie aanbevolen gratis en betaald consumentenbeveiligingsproduct, bij het detecteren en eventueel reageren op een actieve aanval bij de in deelvraag drie beschreven aanval?
10) Bij welke systeemconfiguraties van systemen op een openbaar Wi-Fi netwerk of het openbare Wi-Fi netwerk zelf, is het voor een aanvaller niet langer lonend om willekeurige systemen op openbare Wi-Fi netwerken aan te vallen maar dienen de doelwitten zorgvuldig gekozen te worden?

1. Theoretisch Kader

4.1 OSI-Model

Het Open Systems Interconnection model (OSI-model) staat centraal in de uitleg hoe een netwerk werkt. Dit onderzoek baseert de casus op basis van een openbaar Wi-Fi netwerk, wat plaatst vindt op laag 2 van het OSI-Model.

Het OSI-model is een gestandaardiseerd referentiemodel voor datacommunicatiestandaarden opgesteld door de *International Organization for Standardization* (ISO). Zij definiëren het OSI-model zoals weergegeven in afbeelding 1. Deze gehele paragraaf is gebaseerd op: (“PSTN Tutorial,” n.d.-a)



Afbeelding 1: OSI-Model (“PSTN Tutorial,” n.d.-b)

Zoals te zien is in afbeelding 1, bestaat het OSI-model uit 7 lagen, namelijk:

8. De eerste laag is de fysieke laag, deze definieert de elektronische manier waarop de bits verstuurd worden tussen apparaten;
9. De tweede laag is de data link laag, hier wordt de data gecontroleerd op fouten en flow control op de fysieke link;
10. De derde laag is de netwerk laag, in deze laag wordt er gerouteerd op basis van netwerkadressering;
11. De vierde laag is end-to-end error control, hier wordt de connectie tussen twee apparaten opgezet en gecontroleerd op fouten;
12. De vijfde laag is de sessie laag, hier wordt er gekeken naar permissies en authenticatie. Verder wordt er gekeken of de sessie hersteld kan worden als die verbroken is;
13. De zesde laag is de presentatie laag, zorgt ervoor dat de data geconverteerd wordt zodat de applicatie er mee overweg kan. Er wordt op deze laag ook versleuteld en gecomprimeerd;
14. De zevende laag is de applicatie laag, deze laag communiceert direct met de applicatie en geeft opdrachten aan de zesde laag van het OSI-model.

4.2 Actieve aanvallen

Onder de term actieve aanval kunnen verscheidene technieken geschaard worden, namelijk:

- Exploit misbruik om toegang te verkrijgen tot een systeem;
- Session relay aanvallen, door het stelen van het sessie ID krijgt de aanvaller toegang tot een account van de gedupeerde;
- Man in the Middle aanval, doordat de aanvaller zich voordoet als de router om het internet op te gaan, stroomt alle informatie van de gedupeerde door het systeem van de aanvaller;
- Spoofing aanval, door middel van ARP, DNS, MAC en/of IP spoofing aanvallen is het mogelijk voor de aanvaller om zich voor te doen als een ander systeem of verkeer om te leiden naar een website met malafide software.

Tijdens het onderzoek zal gekeken worden welke aanval het beste uit te voeren is op een openbaar Wi-Fi netwerk en of de consumenten beveiligingsproducten hier voldoende tegen beschermen.

4.3 Besturingssystemen ten behoeve van internet browsen

Een besturingssysteem is een software laag tussen de computer hardware en de gebruiker en stelt daarmee de gebruiker in staat om bijvoorbeeld eigen software uit te voeren (Silberschatz, Galvin, & Gagne, 1994). Aangezien een internetbrowser ook weer een apart stuk software is, is daarmee een besturingssysteem noodzakelijk om op internet rond te kunnen kijken. Onderstaande lijst geeft alle besturingssystemen welke in de praktijk gebruikt worden om op het internet rond te kijken in alfabetische volgorde weer (Netmarketshare, 2016):

- Linux
- Mac OS X
- Windows

Van voornoemde besturingssystemen heeft Windows het grootste marktaandeel (89,34%), waarbij de meest gebruikte Windows versie, versie 7 betreft (47,25%) (Netmarketshare, 2016). Daarmee vormt Windows 7 door zijn grote marktaandeel een aantrekkelijk doelwit voor cybercriminelen, omdat een eenmaal ontwikkelde aanval van toepassing is op 47,25% van de internetgebruikers (Netmarketshare, 2016). Zoals in de voorgaande hoofdstukken beschreven, zal de testomgeving

gebaseerd zijn op het meest gebruikte besturingssysteem, omdat uit voornoemde bron blijkt dat dit Windows 7 betreft zal tijdens de testomgeving gebruik gemaakt worden van Windows 7.

4.4 Minimale beveiligingsfuncties bij consumenten beveiliging

Naast het veel geadviseerde bijgewerkt houden van software, wordt in dezelfde media, als genoemd in de inleiding, vaak ook het installeren van antivirus producten aangeraden. Afgaande op advertenties op internet en in computerbladen als de PC-Active, zijn er veel verschillende aanbieders van antivirus producten op de markt. De vraag is nu wat minimaal geïnstalleerd moet zijn aan consumentenbeveiligingsproducten (in deze categorie valt ook het antivirus). Voor een minimum aan veiligheid dient minimaal aanwezig te zijn: Een antimalware pakket ("Virus, adware, spyware en Browser hijacking software" (IST MIT, 2016)) en een firewall (Larkin, 2008; Rebbapragada, 2016).

Zoals hierboven gesteld is een firewall in combinatie met antimalware het minimale. De combinatie van firewall en antimalware kan los geïnstalleerd worden, maar tevens kan gebruik gemaakt worden van een kant en klaar oplossing (Rubenking, 2016). Onze inschatting is dat gebruikers die losse producten installeren, gebruik maken van gratis oplossingen omdat op dit moment maar één partij een los antimalware product aanbied (Rubenking, 2016). Deze tweedeling rechtvaardigt daarmee de hoofdvraag, waarbij gepoogd wordt gratis en betaalde beveiligingsproducten op het gebied van veiligheid te vergelijken.

2. Globale Aanpak

In dit stuk zal uitgelegd worden welke methode gebruikt wordt in dit project. De theorie die gebruikt zal worden is MoSCoW en zal ook in een volgend hoofdstuk nader uitgelegd worden. De literatuur die gebruikt zal worden in dit project zal ook nog aanbod komen.

5.1 MoSCoW

De MoSCoW-methode is een techniek om prioriteiten te stellen binnen een project. De eisen van het project worden hiermee ingedeeld op basis van prioriteiten. Deze prioriteiten zijn: Must haves, Should haves, Could haves en Won't haves (ook wel Would haves) (McCabe, 2007)

M – must haves: deze eisen moeten in het eindresultaat zitten anders is het product niet bruikbaar.

S – Should haves: Deze eisen zijn gewenst maar zonder is het product ook bruikbaar.

C – Could haves: deze eisen komen aanbod als er genoeg tijd over is.

W – Won't haves: deze eisen zullen niet tijdens dit project aanbod komen, maar kunnen in de toekomst interessant zijn voor een vervolgproject.

Een project dat niet alle must haves in het eindproduct heeft zitten wordt als gefaald beschouwd Met behulp van de MoSCoW-methode zal een project realiseren overzichtelijker worden en makkelijker te realiseren zijn. (McCabe, 2007)

5.2 Literatuur

Zoals gesteld zal in gezaghebbende literatuur gezocht worden naar informatie. De literatuur die voornamelijk gebruikt zal worden zijn artikelen die gevonden zijn door middel van Google Scholar en databanken welke beschikbaar gesteld zijn door de Hogeschool Utrecht.

Voor het zoeken naar relevante artikelen zal gebruikt worden van de HUBL-cursus van de Hogeschool Utrecht.

3. Producten

Aan het einde van het project zal er door de projectgroep de volgende producten opgeleverd worden:

- Een adviesrapport, bevattend: een marktonderzoek, productvergelijking en advies;
- Een Proof of concept;
- Een testplan;
- Een logboek;
- Dit Plan van Aanpak.

4. Projectorganisatie

In de onderstaande tabel zijn de bereikbaarheidsgegevens van de onderzoeksgroep weergegeven in combinatie met de communicatieafspraken. Verder staat ook de naam van de projectbegeleider namens de HU vermeld.

Projectbegeleider	**Ander de Keijzer**			
Onderzoekers	**Bart Dekker en Boudewijn van Silfhout**			
Bereikbaarheid van de projectleden				
Naam	Studentnr.	Tel. Nr.	E-mailadres	Woonplaats
Bart Dekker				
Boudewijn v. Silfhout				
Communicatieafspraken • Alle documenten worden in de teammap op Dropbox geplaatst. • De notulen worden uiterlijk 2 dagen na de vergadering geplaatst op Dropbox • Onderlinge communicatie vindt plaats tijdens vergaderingen en via E-mail, TeamSpeak, WhatsApp of telefonisch. • Projectleden reageren zo snel mogelijk op berichten. • Ieder groepslid checkt dagelijks zijn e-mail, WhatsApp en Sharepoint. • We geven elkaar feedback door met een kritische blik te kijken naar elkaars werk. • We nemen gezamenlijke beslissingen door met elkaar in overleg te treden. • Voortgangsbewaking: middels planning • Externe communicatie naar de opdrachtgever: in de lessen of via e-mail. • Escalatie naar de begeleider: na internteam overleg • Bij consequent te laat komen: maatregelen worden getroffen. • Bij niet houden aan afspraken: treden we in overleg • Consequentie op overtreding van de regels uit het contract: Overleg met de begeleider.				

Tabel 1: de projectorganisatie.

5. Algemene Planning

Voor het verloop van het project zal de planning uit tabel 2 gehanteerd worden.

Datum	Omschrijving	Inleveren bij
05-10-2016	Inleveren concept Plan van Aanpak	Ander de Keijzer
14-10-2016	Inleveren Plan van Aanpak	Ander de Keijzer, Leo van Moergestel en Esther van der Stappen
14-10-2016	Afronden vooronderzoek	N.v.t.
18-11-2016	Eerste 5 deelvragen beantwoord en aanvragen opmerkingen bij begeleider	Ander de Keijzer
16-12-2017	Overige deelvragen beantwoord en aanvragen opmerkingen bij begeleider	Ander de Keijzer
06-01-2017	Concept scriptie afgerond en aanvragen feedback bij begeleider.	Ander de Keijzer
18-01-2017	Scriptie definitief	N.v.t.
20-01-2017	Inleveren scriptie in viervoud	Ander de Keijzer, Leo van Moergestel, Esther van der Stappen en examinatoren

Tabel 2: algemene planning.

6. Risicoanalyse

Tijdens het project zijn er een aantal risico factoren waar de projectgroep rekening mee moet houden. Met deze factoren moet rekening gehouden worden om te voorkomen dat het project op een dood spoor terechtkomt.

Reeds geïdentificeerde risico's zijn afgebeeld in tabel 4 hieronder.

Risico	Kans	Impact	Prioriteit	Risico beperkende maatregel
Ziekte teamleden, slechte samenwerking	10%	Project loopt uit, niveau 2	Laag	Communicatie op orde houden, bij vroegtijdige meldingen kan er uitval opgevangen worden. Indien het geval van slechte communicatie zal de begeleider hier de hand in nemen.

Risico	Kans	Impact	Prioriteit	Risico beperkende maatregel
Eisen zijn niet beschikbaar of kunnen niet gekwantificeerd worden tijdens de interviews	10%	Project loopt uit, niveau 3	Middel	Navragen bij de begeleider om alsnog wat mogelijke vervolgstappen kunnen zijn.
Verzamelde eisen bevatten op cruciale onderdelen onjuistheden of conflicten	10%	Securitymaatregelen kunnen niet op adequate wijze worden bepaald, niveau 4	Middel	Vergaderingen met de begeleider moeten onjuistheden vroegtijdig ontdekt worden.
Laboratorium niet beschikbaar of apparatuur niet geschikt	5%	Proof of Concept later klaar, uitstel van implementatie, niveau 2	Hoog	De projectgroep zal gebruik maken van de apparatuur op de beschikbare tijden.

Tabel 3: Geïdentificeerde Risico's.

Risico: Omschrijving van het risico
Kans: Waarschijnlijkheid dat dit risico optreedt
Impact: Impact van het risico op het project, 1= gering, 4 = hoog)
Prioriteit: Kans en impact
Maatregel: Beschrijf per risico de passende tegenmaatregelen:

Met deze voorbereiding hoopt de projectgroep onvoorziene omstandigheden zo veel mogelijk te ondervangen en voortijdig op te kunnen lossen, zonder in de problemen te komen met de gestelde deadlines van de organisatie.

7. Ethische afweging onderzoek

De reden om in dit PvA expliciet een hoofdstuk over ethiek op te nemen, komt voort uit de verwachting dat de uitkomsten van dit onderzoek in verkeerde handen veel schade kunnen berokkenen. Dit hoofdstuk heeft als doel een kader te scheppen en onze afwegingen weer te geven.

Ons onderzoek bevindt zich in een grijs gebied, waarbij het grijs zowel donkerder als lichter kan worden. Het grijs is echter onherroepelijk zwart indien we buiten onze eigen testomgeving aanvallen op systemen uit gaan voeren. Denk hierbij aan het uitvoeren van aanvallen op systemen aanwezig op het openbare Wi-Fi netwerk van bijvoorbeeld de Mc Donalds, Starbucks of Albert Heijn. In dat geval overtreden wij wat onszelf betreft de grenzen van het betamelijke, waarbij vragen gesteld kunnen worden over onze beweegredenen, aangezien onze verwachting is dat een dergelijke veldtest niet nodig is voor het kunnen beantwoorden van onze onderzoeksvraag.

Het grijze gebied blijft lichtgrijs indien aangetoond wordt dat de gevonden kwetsbaarheden niet kosteneffectief zijn bij een sleepnet methode. In dat geval is het gros van de systemen welke zich op openbare Wi-Fi netwerken bevinden veilig voor aanvallers. Ervan uitgaande dat de kosten bij het uitvoeren van een aanval hoog zijn, is het veilig ons onderzoek te publiceren omdat gebleken is dat de aanval niet grootscheeps kan worden opgezet.

Indien blijkt dat met relatief goedkope oplossingen gemakkelijk veel systemen kunnen worden gecompromitteerd, wordt het grijs een stuk donkerder. Daarmee kan ons onderzoek handvatten bieden aan gelegenheids- of beginnende aanvallers. In dit geval dient serieus overwogen te worden om het onderzoek alleen aan onze begeleider en beoordelaars van de Hogeschool Utrecht (HU) aan te bieden en niet te publiceren.

Een reden om dit onderzoek toch te doen, is om te beoordelen of gebruikers niet onnodig geld besteden aan consumentenbeveiligingsproducten. Indien namelijk uit dit onderzoek blijkt dat een gratis beveiligingsproduct afdoende is, is onze verwachting dat ons onderzoek vooral ten goede komt aan gebruikers.

Moraal van dit betoog is dat we ons terdege bewust zijn van de mogelijke consequenties van ons onderzoek en dat uiteindelijk bij het afronden van dit onderzoek de hierboven beschreven ethische afweging gemaakt dient te worden.

Bibliografie

IST MIT. (2016). Viruses, Spyware, and Malware. Retrieved October 2, 2016, from https://ist.mit.edu/security/malware

Larkin, E. (2008, August 26). Build Your Own Free Security Suite. Retrieved October 2, 2016, from http://www.pcworld.com/article/150204/free_security_suite.html

McCabe, J. D. (2007). *Network analysis, architecture, and design* (3rd ed). Amsterdan ; Boston: Elsevier/Morgan Kaufmann Publishers.

Netmarketshare. (2016, August). Desktop Operating System Market Share. Retrieved September 29, 2016, from https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0

PSTN Tutorial. (n.d.-a). Retrieved October 2, 2016, from http://www.telecommunications-tutorials.com/tutorial-OSI-7-layer-model.htm

PSTN Tutorial. (n.d.-b). Retrieved from http://www.telecommunications-tutorials.com/tutorial-OSI-7-layer-model.htm

Public Wi-Fi Security. (n.d.). [Kaspersky Lab US]. Retrieved from https://usa.kaspersky.com/internet-security-center/internet-safety/public-wifi

Rebbapragada, N. (2016, May 25). All-in-One Security. Retrieved October 2, 2016, from https://web.archive.org/web/20101027113242/http://www.pcworld.com/article/125817-2/allinone_security.html

Rubenking, N. J. (2016, September 26). The Best Security Suites of 2016. Retrieved October 2, 2016, from http://www.pcmag.com/article2/0,2817,2369749,00.asp

Silberschatz, A., Galvin, P. B., & Gagne, G. (1994). *OPERATING SYSTEM CONCEPTS* (Vol. 4). Addison-Wesley. Retrieved from http://www.cs.du.edu/~cag/courses/CS/DU/comp3361/Lectures/tm01-05.pdf