TNO Informatie- en Communicatietechnologie

Nederlandse Organisatie voor
toegepast-natuurwetenschappelijk
onderzoek / Netherlands Organisation
for Applied Scientific Research

www.tno.nl

T 015-2857076
F 015-2857382

TNO-rapport

35263

Plugwise security analyse

Datum	2 juli 2010
Auteur	Sander Degen, Ron van Paassen
Aantal pagina's	17
Aantal bijlagen	0
Opdrachtgever	Plugwise B.V.
Projectnaam	Security analyse Plugwise
Projectnummer	035.33350

Inhoudsopgave

1 Inleiding

Plugwise is een oplossing die is gericht op het verlagen van energieverbruik, door inzichtelijk te maken wat het huidige verbruik is en door elektriciteit uit te schakelen op momenten dat er geen behoefte is.

Bij toepassing van Plugwise in een zakelijke omgeving wordt de Plugwise oplossing vaak aangesloten op de bestaande IT-infrastructuur van de klant. Dit zou beveiligingsrisico's met zich mee kunnen brengen voor de IT-infrastructuur. De doelstelling van dit document is het in kaart brengen van deze risico's, en het doen van aanbevelingen over hoe ze kunnen worden verlaagd.

1.1 Leeswijzer

In hoofdstuk 2 wordt ingegaan op de security analyse. Aan de hand van risico's worden de beveiligingseigenschappen van een drietal scenario's in kaart gebracht. Deze scenario's zijn de meest waarschijnlijke implementaties van de Plugwise-oplossing, en zijn voorzien van de beveiligingmaatregelen die in de praktijk vaak gekozen zullen worden.

Aan de hand van de risico's krijgt een organisatie inzicht in de beveiligingsimpact van het invoeren van de Plugwise-oplossing. Daarmee kan zij besluiten om voor een bepaald scenario te kiezen en om extra maatregelen te treffen, of de risico's te accepteren.

1.2 Doelgroep

De beoogde lezersgroep voor dit document is de klant van Plugwise die inzicht wil krijgen in de informatiebeveiligingsrisico's op het bedrijfsnetwerk die de implementatie van een Plugwise-oplossing met zich meebrengt.

2 Risicoanalyse

De methodiek voor het uitvoeren van de risicoanalyse gaat over dreigingen, kans, impact en risico's. De dreiging is een ongewenste, beveiligingsgerelateerde gebeurtenis die zich voor kan doen. Aan het optreden van deze gebeurtenis is een kans gekoppeld; aan het resultaat een impact. Wanneer de kans en de impact van een dreiging met elkaar worden gerelateerd, wordt een maat voor het risico verkregen.

Concreet wordt de kans geschat op een schaal van 1 tot en met 5, uitgaande van een doorsnee MKB bedrijf:

Niveau	Kans
1	1x per 10 jaar, of minder vaak
2	1x per 5 jaar
3	1x per jaar
4	1x per maand
5	1x per week

De impact van de dreiging wordt op dezelfde manier (een schaal van 1 tot en met 5) beschreven. Omdat de analyse is gericht op de beveiliging van het interne netwerk, wordt met de impact aangegeven hoeveel schade een dreiging op het interne netwerk aan kan richten.

Normaliter wordt de impact uitgedrukt in bijvoorbeeld financiële schade of aantal verloren klanten, maar omdat de impact sterk afhankelijk is van de klantsituatie[1], is er in dit geval geen concrete waarde aan te koppelen. Daarom is gekozen om de impact een indicatie te laten zijn van de expertise die nodig is om de aanval succesvol uit te voeren.

Niveau	Impact
1	Inbraak technisch (vrijwel) onmogelijk
2	Inbraak vereist expertise en/of kennis van ongepubliceerde zwakheden
3	Inbraak vereist diepgaande kennis
4	Inbraak vereist basiskennis
5	Inbraak vereist geen speciale kennis

Een voorbeeld ter illustratie:
Stel dat een Source-computer (het computersysteem van de Plugwise-afnemer waarop de Source-applicatie is geïnstalleerd) is afgeschermd met een firewall die alleen webverkeer toestaat, en alle uitgaande verbindingen vanaf de Source-computer blokkeert. De kans dat een installateur kwaadaardige software op de Source-computer heeft gezet is naar schatting niveau 2 (eens per 5 jaar). De impact van een dergelijke dreiging is laag omdat de firewall alle inbraakpogingen zal tegenhouden, en is dus

[1] Het is niet vooraf duidelijk hoe kritisch het bedrijfsnetwerk is, en hoe gevoelig de informatie is die zich in het netwerk bevindt.

niveau 1. Als er geen firewall wordt gebruikt, is de impact veel hoger (niveau 4) omdat het veel eenvoudiger is om het interne bedrijfsnetwerk aan te vallen.

Normaliter wordt bij een risicoanalyse aangegeven op welke beveiligingsaspecten de dreiging van toepassing is. De drie beveiligingsaspecten zijn:

- Vertrouwelijkheid (ongeautoriseerde inzage in informatie)
- Integriteit (ongeautoriseerde wijziging van informatie/systemen)
- Beschikbaarheid (het niet beschikbaar zijn van informatie/systemen)

Omdat deze security analyse echter is gericht op de algemene beveiliging van het interne bedrijfsnetwerk is het niet mogelijk om dit onderscheid in dreigingen te maken. Een dreiging betekent dat het bedrijfsnetwerk kan worden aangevallen, het soort aanval dat een aanvaller vervolgens gebruikt is minder relevant en zal vaak heel specifiek zijn voor het gestelde doel en afhankelijk van de organisatie.

2.1 Het belang

In een risicoanalyse worden maatregelen afgewogen tegen het te beschermen belang. Net als in de fysieke wereld een juwelier strengere beveiligingsmaatregelen neemt dan een bakker, moet bij informatiebeveiliging ook gekeken worden naar de waarde van de informatie die beschermd moet worden.

Vanzelfsprekend is de gebruiker van de Plugwise oplossing als enige in staat is om in te schatten wat de waarde is van de informatie op zijn bedrijfsnetwerk, of van zijn bedrijfsmiddelen. Hij of zij is dus ook degene die de afweging kan maken welke maatregelen passend zijn.

2.2 Scope

Zoals eerder gesteld wordt bij deze risicoanalyse uitgegaan van een doorsnee bedrijf, het doel is ook om de relevante dreigingen te identificeren die voor een gemiddeld bedrijf gelden. Indien de klant speciale beveiligingseisen heeft (bijvoorbeeld qua beschikbaarheid van zijn netwerk of de gevoeligheid van de informatie) is het raadzaam om een specifieke risicoanalyse uit te voeren op die situatie.

De security analyse is gericht op risico’s op de IT-infrastructuur die de Plugwise-oplossing met zich mee zou kunnen brengen. Risico’s die betrekking hebben op de vertrouwelijkheid, integriteit of beschikbaarheid van de gegevens in het Plugwise systeem zelf worden niet beschouwd. Zo wordt bijvoorbeeld het risico dat een derde bewust het ZigBee netwerk stoort, waardoor het Plugwise systeem (tijdelijk) geen gegevens kan verzamelen, niet meegenomen.

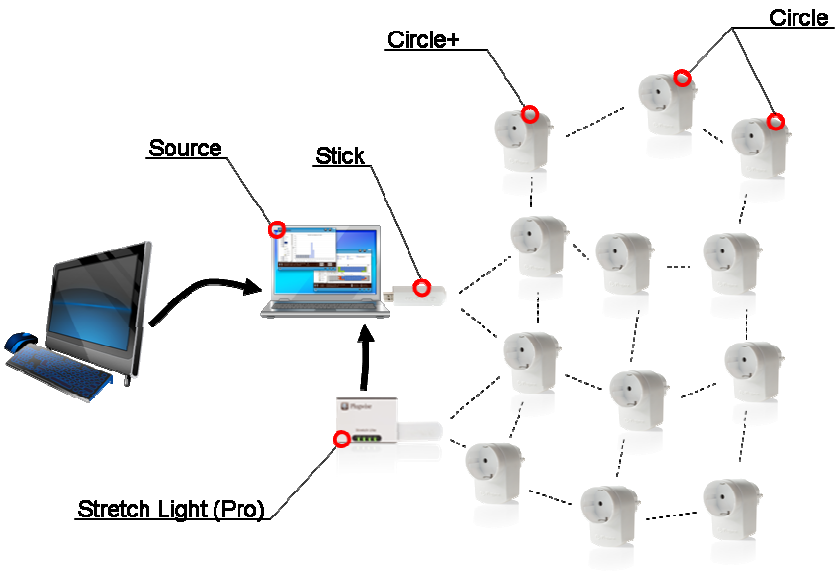
Het uitgangspunt voor deze security analyse is de informatie die door Plugwise ter beschikking is gesteld. De documenten die gebruikt zijn bij totstandkoming van dit onderzoek zijn opgenomen in bijlage I. Er is door TNO geen onderzoek gedaan naar de kwaliteit of veiligheid van de afzonderlijke producten. Voor deze risicoanalyse is het uitgangspunt dat de Plugwise producten een normaal dreigingsprofiel hebben, dat wil zeggen dat ze vergelijkbare kans hebben op kwetsbaarheden en beveiligingsproblemen dan vergelijkbare ICT-producten (bijvoorbeeld WLAN access-points of switches).

2.3 Plugwise product

De Plugwise oplossing bestaat uit een aantal kerndelen:

1. Circles
2. Source (software)
3. Koppeling tussen Circles en Source (Stick of Stretch/Stretch Light)

Zie ook de schematische weergave in Figuur 1.



Figuur 1: Belangrijkste onderdelen van Plugwise oplossing

2.3.1 Circles / Circle+

De Circles zijn de intelligente stopcontactmodules waarop elektrische apparatuur wordt aangesloten. Een Circle kan worden geprogrammeerd om bijvoorbeeld op bepaalde tijden wel of geen elektriciteit door te laten, en hij kan het verbruik bijhouden. Meerdere Circles communiceren met elkaar zoals in een mesh-netwerk, waarbij communicatiepaden automatisch worden opgebouwd. Dit gebeurt door middel van ZigBee.

De Circle+ vervult een netwerkcoördinator rol en houdt bij welke Circles toegang tot het netwerk willen krijgen, en zorgt tevens voor het periodiek verversen van de netwerksleutel. Er is één Circle+ per netwerk.

2.3.2 Source

Source is een applicatie waarmee inzichtelijk wordt wat het verbruik is, wat de besparingen zijn, etc. Ook kan door middel van Source elke Circle worden geconfigureerd. Source wordt geïnstalleerd op een systeem (de Source-computer), vervolgens kan de applicatie zowel lokaal worden gebruikt als vanaf een ander systeem door middel van de webinterface. Vooral bij zakelijk gebruik zal de toegang via de webinterface plaatsvinden; hiervoor kan een willekeurige werkplek worden gebruikt.

2.3.3 Koppeling tussen Circles en Source

De koppeling tussen de Circles en de Source applicatie kan op verschillende manieren worden gerealiseerd. Als de **Stick** (een USB stick waarmee ZigBee 'gepraat' kan worden) in de Source-computer wordt ingevoerd is er een directe koppeling. Voor het overbruggen van grotere afstanden is het ook mogelijk om over een IP-netwerk te communiceren, daarbij is een conversie van ZigBee naar IP nodig: dit kan met de zogenaamde Stretch. Hier zijn drie varianten van:

Stretch Light: Deze zorgt voor een (onbeveiligde) USB-tunnel tussen de Source-computer en de Stick die in de Stretch Light zit. De USB-tunnel zorgt voor extra dataverkeer door de overhead van het USB protocol, en voor broadcasts-meldingen op het netwerk. Omdat de Stretch Light geen authenticatiemogelijkheden heeft is het van belang dat alleen vertrouwde systemen netwerktoegang tot de Stretch Light hebben.

Stretch Light Pro: Hierbij is er geen USB tunnel maar worden alleen relevante berichten doorgestuurd via een SSH verbinding tussen de Source-computer en de Stretch Light Pro. De Stretch Light Pro kan alleen worden beheerd door middel van een gebruikersnaam en wachtwoord en kan daardoor zonder problemen in een onveilig netwerksegment worden geplaatst.

Stretch: Dit systeem realiseert een communicatiekanaal tussen de Circles en een Internetversie van Source. Dit betekent dat er geen lokale Source-applicatie nodig is maar dat de configuratie en inzage van de Plugwise oplossing via de website van Plugwise plaatsvindt.

Voor deze security analyse wordt uitgegaan van drie verschillende scenario's, dit komt overeen met de hierboven genoemde koppelingsmanieren waarbij de Stretch Light en de Stretch Light Pro zijn samengevoegd.

2.4 Reeds genomen maatregelen en uitgangspunten

De genomen beveiligingsmaatregelen in de Plugwise producten zijn:

Circles

- Circles communiceren via ZigBee, een netwerkprotocol dat de gegevens versleutelt met 128 bit AES encryptie
- Elk ZigBee Circle-netwerk heeft haar eigen netwerksleutel die periodiek wordt ververst, afhankelijk van het netwerkverkeer maar ongeveer eens per maand
- Als een nieuwe Circle toegang wil krijgen tot het netwerk geeft de Circle+ dit door aan de Source-applicatie, waarin de gebruiker al dan niet toestemming kan geven voor het verlenen van toegang

Source

- De applicatie heeft geen admin rechten nodig waardoor een kwetsbaarheid in de applicatie tot een lagere impact leidt
- Toegang tot de webinterface is afgeschermd met een gebruikersnaam en wachtwoord. Directe toegang tot de source-applicatie is afhankelijk van de gebruikte systeemauthenticatie (om bijv. toegang tot Windows te krijgen)
- Vanuit de applicatie kunnen nieuwe Circles aan het netwerk worden toegevoegd
- Vanuit de applicatie kan een Stretch Light (Pro) worden aangestuurd, hiervoor moet de gebruiker het IP-adres van de Stretch Light (Pro) in de Source-applicatie invoeren

- De Source-applicatie is ook via een webbrowser (via http) te gebruiken, hiervoor moet de webserver worden aangezet en een gebruikersnaam en wachtwoord worden opgegeven
- De Source-applicatie kan periodiek controleren op updates wanneer de gebruiker daarvoor kiest

Stretch Light (Pro)
- De Stretch Light Pro wordt door middel van SSH aangestuurd, hiervoor moet de Source-applicatie gebruik maken van een geldige gebruikersnaam en wachtwoord

Stretch
- De Stretch communiceert met de webserver over https door middel van een self-signed certificaat, waarmee client side authenticatie wordt uitgevoerd

Plugwise webserver
- Communicatie tussen de Source-applicatie en de centrale Plugwise update server is beveiligd door middel van https
- Communicatie tussen de Stretch en de centrale Plugwise server is beveiligd door middel van https

Uitgangspunten:
Van de volgende standaardmaatregelen wordt verwacht dat ze door de afnemer van een Plugwise product worden toegepast:
- Systemen en applicaties worden regelmatig voorzien van beveiligingsupdates en -patches
- De werkplekken maken gebruik van antivirussoftware
- De Source-computer maakt gebruik van antivirussoftware
- De servers zijn fysiek afgeschermd en alleen voor beheerders e.d. toegankelijk
- De Stretch Light / Stretch Light Pro apparatuur is fysiek afgeschermd

Door regelmatig (afhankelijk van de aard en noodzaak van de updates is er geen vaste tijdsperiode te noemen) beveiligingspatches en -updates te installeren op systemen en applicaties wordt de tijd dat kwetsbaarheden te misbruiken zijn ingeperkt. Daarmee wordt ook het risico van misbruik verlaagd en dus het beveiligingsniveau verhoogd.

Antivirusmaatregelen op de werkplekken en de Source-computer zelf kunnen kwaadaardige programma's ontdekken voordat ze schade aan kunnen richten. Hiermee wordt de inbreng van deze malware niet voorkomen, maar (in veel gevallen) wel de schade die anders aangericht had kunnen worden.

Een aantal dreigingen kunnen alleen ontstaan wanneer iemand fysieke toegang heeft tot een systeem. Voor deze security analyse wordt uitgegaan van fysieke afscherming van de servers zodat deze dreigingen niet relevant zijn.

Eventuele extra maatregelen

Om bepaalde risico's te verlagen zijn de volgende maatregelen te overwegen:
- Toepassen van een application level firewall
- Toepassen van een IDS/IPS

Een application level firewall kan het verkeer van/naar de Source-applicatie nauwkeuriger controleren dan een firewall die alleen naar IP-adressen en poorten kijkt. De application level firewall kan het verkeer analyseren en niet-http verkeer tegenhouden.

Een Intrusion Detection System of Intrusion Prevention System gaat zelfs een stap verder en kan aanvallen detecteren. Deze detectie kan aan de hand van ‘signatures’ gebeuren, d.w.z. kenmerken van bekende aanvallen waaraan het verkeer voldoet, of via afwijkingen ten opzichte van het normale netwerkverkeer. Hiermee kunnen aanvallen vanuit de Source-computer worden ontdekt en (in het geval van een Intrusion Prevention System) worden gestopt.

2.5 De standaard systeemopzet

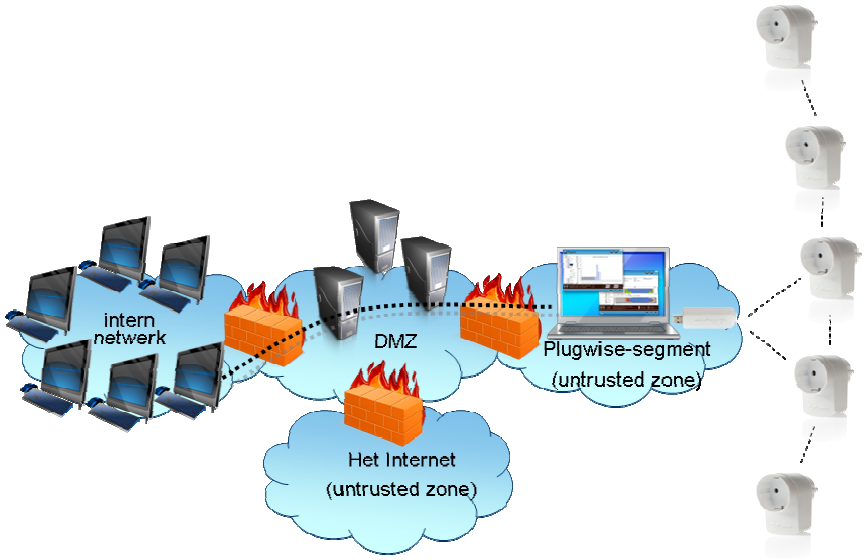
In het allereenvoudigste scenario wordt een PC aangewezen waarop de Source-applicatie draait en waarop de Stick wordt aangesloten. Deze PC is niet aangesloten op het bedrijfsnetwerk. Omdat er geen verbinding is tussen het Plugwise systeem en het interne bedrijfsnetwerk, is er ook geen dreiging denkbaar tegenover de gegevens op het bedrijfsnetwerk. Daar staat tegenover dat de Source-applicatie ook niet via het netwerk bereikbaar is, maar alleen lokaal door de bediener van de PC.

Eén stap verder is het scenario waar een PC op het interne netwerk aangewezen wordt als de PC waarop de Source-applicatie geïnstalleerd wordt. Op deze PC wordt een Stick aangesloten die de communicatie met de Circles verzorgt. Met deze opstelling wordt het mogelijk dat gebruikers via het netwerk de Source-applicatie bedienen. Hierbij heeft de Plugwise-apparatuur toegang tot het interne bedrijfsnetwerk en bestaat de kans dat aanvallen worden uitgevoerd en gevoelige informatie via een Internetverbinding uitlekt.

Als de Plugwise-apparatuur door de gebruiker wordt vertrouwd, of als de impact van aanvallen verwaarloosbaar is (bijvoorbeeld omdat het netwerk geen vertrouwelijke informatie bevat en dat er een goed backup-beleid is), dan zijn er geen extra maatregelen nodig.

2.6 Scenario 1: Stick op PC die in “untrusted zone” wordt geplaatst

In deze configuratie is een Source-computer voorzien van de Stick: een USB-ZigBee-device waarmee de Source-computer met de Circles kan communiceren. De server is neergezet in een apart netwerksegment dat als “untrusted” wordt gekwalificeerd. De firewalls zijn zodanig ingesteld dat de Source-computer van buitenaf niet te benaderen is, en van binnenuit het interne netwerk wel.



Figuur 2: Schematische weergave van scenario waarin Plugwise Source in een apart "untrusted" netwerksegment geplaatst wordt.

De Source-computer is afgeschermd van het interne netwerk door middel van twee logische firewalls; één voor het afschermen van verkeer van/naar de DMZ (DMZ-firewall), en één voor het afschermen van verkeer van/naar de Source-computer (Source-firewall). Deze twee firewalls kunnen fysiek hetzelfde apparaat zijn.

De Source-firewall hoeft alleen inkomend netwerkverkeer op de gebruikte webserver-poort (standaard is dit poort 8080) toe te staan, en geen uitgaande verbindingen. Hiermee worden zowel het interne netwerk als de systemen in de DMZ beschermd tegen aanvalspogingen vanuit het Plugwise-segment. De DMZ-firewall moet uiteraard ook zo zijn geconfigureerd dat werkplekken via de browser met de Source-computer kunnen communiceren. Vanaf werkplekken kan dan de Source-applicatie via een browser benaderd worden, dit is in bovenstaande figuur aangegeven met de gestippelde lijn.

2.6.1 *Analyse van de Dreigingen:*

In bovenstaand scenario bestaat slechts één plaats vanwaar het bedrijfsnetwerk kan worden aangevallen: via de Source-applicatie die vanuit het bedrijfsnetwerk benaderd wordt door gebruikers.

Wanneer de Source applicatie gecompromitteerd zou worden, zouden gebruikers van de applicatie via een kwetsbaarheid in de webbrowser geïnfecteerd kunnen raken met malware. Dit zou ertoe kunnen leiden dat gegevens op het bedrijfsnetwerk aan kwaadwillenden bekend zou raken. Dit vereist wel dat de webbrowsers of één van de gebruikte plugins een specifieke kwetsbaarheid bevatten die benut kan worden door een aanvaller.

Het gecompromitteerd raken van de Source-applicatie is in bovenstaande set-up niet heel waarschijnlijk. Mogelijke scenario's hiervoor zouden kunnen zijn: het aanvallen van de Zigbee stack via de draadloze Zigbee communicatie, het verwerken van malware in de sourcecode van de Source-applicatie, of een kwaadwillende gebruiker of systeembeheerder die de malware op de Source-applicatie zet. Merk op dat in al deze

gevallen er meer voor de hand liggende methoden zijn om het interne bedrijfsnetwerk aan te vallen.

Het mag duidelijk zijn dat het uitvoeren van deze aanval niet eenvoudig is, en specifieke kennis vereist van de aanvaller:
- Kwetsbaarheid in de gebruikte webbrowser van Source-gebruikers
- Trojan die niet door de gebruikte virusscanners wordt herkend

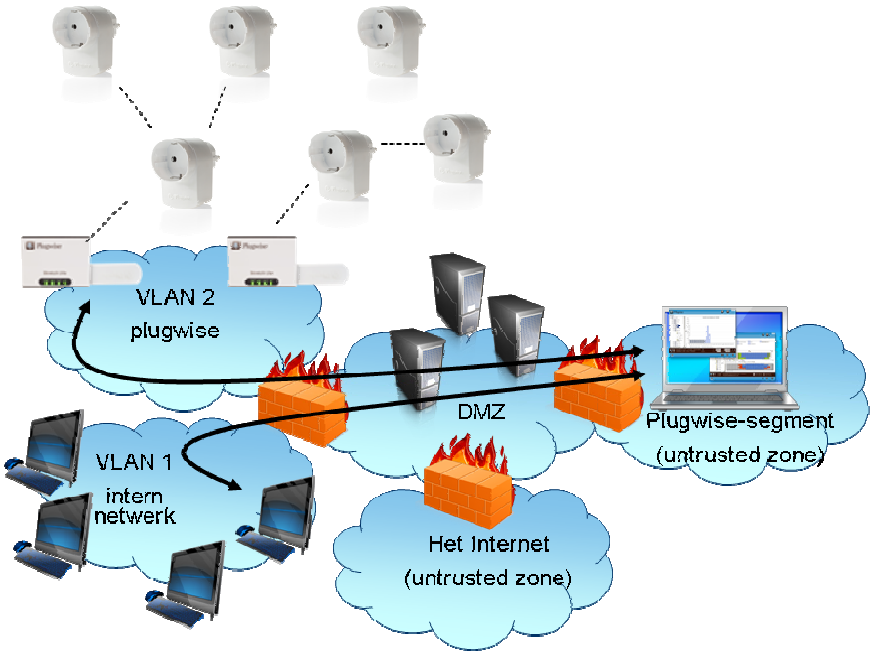
Vandaar dat de kans voor deze dreigingen op niveau 2 (*Inbraak vereist expertise en/of kennis van ongepubliceerde zwakheden*) is geschat.

Samengevat:

ID	Beschrijving dreiging	Kans	Impact	Risico
Zigbee:				
1.A	Inbraak via het ZigBee-protocol, van daaruit wordt de Source-computer aangevallen	1	2	**2**
Circle:				
1.B	Inbraak via kwaadaardige Circle (+), van daaruit wordt de Source-computer aangevallen	1	2	**2**
Source:				
1.C	Een gebruiker breekt in op de Source-applicatie	2	2	**4**
1.D	De Source-applicatie bevat kwaadaardige code, doordat de broncode is aangepast door een aanvaller	2	2	**4**
1.E	De Source-applicatie bevat kwaadaardige code, doordat misbruik is gemaakt van een kwetsbaarheid bij de communicatie met de Plugwise server over Internet	2	2	**4**

2.7 Scenario 2: Stretch Light / Stretch Light Pro

De configuratie in dit scenario zal voornamelijk voorkomen bij systemen waarbij grotere afstanden overbrugd moeten worden. Door het gebruik van een Stretch Light of een Stretch Light Pro hoeft de Source-computer niet binnen het bereik van de Circles te staan. De Stretch Light (Pro) zorgt dat het ZigBee signaal over het bedrijfsnetwerk (via IP) naar de Source-computer wordt getransporteerd, en andersom, dat de informatie van de Source-computer als een ZigBee signaal naar de Circles gaat.



Figuur 3: Scheiding van Plugwise en intern netwerk door middel van een VLAN

De firewall die de Source-computer afschermt van de DMZ dient inkomend verkeer toe te staan naar de webserver toe, en uitgaand verkeer naar de Stretch Light (Pro)'s, en eventueel naar de Plugwise-Internetwebserver indien men toestaat om statistische informatie te verzenden. De firewall tussen het interne netwerk en de DMZ dient inkomend verkeer van het Plugwise segment naar het interne netwerk toe te staan voor:
TCP: poort 22 (Stretch Light Pro),
TCP en UDP poorten: 7303, 7305, 20005, 30201, 30202, 30203 (Stretch Light).

Door het gebruik van VLAN is het mogelijk om verkeersstromen van elkaar te scheiden door in de switch aan te geven welke poorten met elkaar verbonden zijn. VLANs zijn een drempel die het moeilijk maakt om informatie naar het bedrijfsnetwerk te sturen, maar vaak niet onmogelijk. Oude of onjuist geconfigureerde switches kunnen kwetsbaar zijn voor aanvallen waarbij het mogelijk is om 'uit een VLAN te breken'[2]. Desondanks is het gebruik van VLAN aantrekkelijk doordat deze functionaliteit vaak al beschikbaar is en het toch een aanvullend niveau van beveiliging biedt.

2.7.1 Analyse van de dreigingen

Voor dit scenario gelden dezelfde dreigingen als die in de vorige paragraaf, met een aantal aanvullende mogelijke dreigingen omdat in dit scenario de Plugwise Circles en Stretch apparatuur communiceren over het interne vertrouwde bedrijfsnetwerk, en de Stretch Light (Pro) apparatuur aangesloten wordt op het interne netwerk.

Hiermee kunnen aanvullende dreigingen geïntroduceerd worden die verband houden met het aansluiten op het netwerk van de Stretch Light (Pro). Mogelijke nieuwe dreigingen zijn:

- de Stretch Light (Pro) bevat kwaadaardige software die netwerkverkeer aftapt en uitzendt via Zigbee[3];

[2] Zie bijv. http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/prodlit/vlnwp_wp.pdf
[3] Nota bene: dit werkt vaak niet als het netwerk geswitcht is, wat tegenwoordig vaak het geval is.

- de Stretch Light (Pro) bevat kwaadaardige software waarmee een aanvaller een backdoor verkrijgt naar het interne netwerk;
- de Stretch Light (Pro) bevat een kwetsbaarheid in de Zigbee protocol stack waarvan misbruik kan worden gemaakt door een aanvaller om een backdoor te verkrijgen naar het interne netwerk.

Wanneer dit verkeer echter niet vertrouwd wordt, kan ervoor gekozen worden om het Plugwise sensor IP verkeer gescheiden te houden van het IP verkeer in het reguliere bedrijfsnetwerk. Dit kan door gebruik te maken van VLANs of van VPN.

Als een organisatie niet wil vertrouwen op VLAN technieken en toch de verkeersstromen wil scheiden, is het alternatief om VPN tunnels op te zetten tussen de Stretch Light (Pro)'s en de Source-computer. Dat betekent dat de organisatie een VPN gateway bij de Source-computer zal moeten plaatsen en VPN endpoints bij elke Stretch Light (Pro). Omdat Plugwise in deze een onvertrouwde partij is (qua beveiliging) is het aan te raden dat de afnemende organisatie dit zelf implementeert. Het gebruik van VPN is echter een relatief kostbare maatregel die ook grote beheersinspanningen vergt.

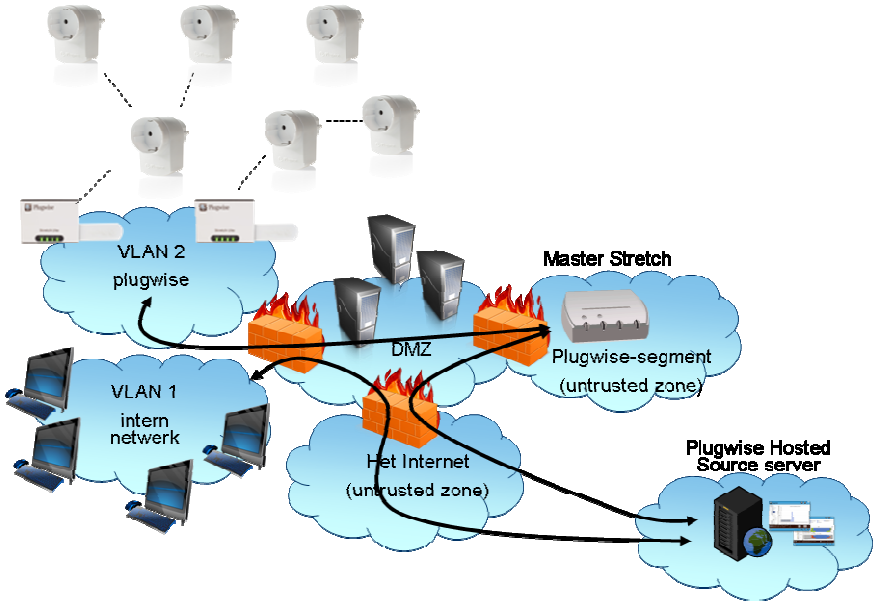
Samengevat:

ID	Beschrijving dreiging	Kans	Impact	Risico
Zigbee:				
2.A	Inbraak via kwetsbaarheid in ZigBee-implementatie van de Stretch Light (Pro), van daaruit wordt het netwerk aangevallen	1	3	**3**
2.B	Inbraak via kwetsbaarheid in ZigBee-implementatie van de Stretch Light (Pro), van daaruit wordt de Source-computer aangevallen	1	2	**2**
Circle:				
2.C	Inbraak via kwaadaardige Circle (+), van daaruit wordt het netwerk aangevallen	1	3	**3**
2.D	Inbraak via kwaadaardige Circle (+), van daaruit wordt de Source-computer aangevallen	1	2	**2**
Stretch Light (Pro):				
2.E	De netwerkinstellingen van een Stretch Light worden ongeautoriseerd gewijzigd	2	3	**6**
2.F	De netwerkinstellingen van een Stretch Light Pro worden ongeautoriseerd gewijzigd	1	3	**3**
2.G	Het bedrijfsnetwerk wordt aangevallen doordat een ander apparaat (bijv. een laptop) op de netwerkpoort van de Stretch Light (Pro) wordt aangesloten	2	4	**8**
2.H	De Stretch Light (Pro) bevat kwaadaardige code en valt het bedrijfsnetwerk aan	2	3	**6**
Source:				
2.I	Een gebruiker breekt in op de Source-applicatie en valt daarvandaan andere gebruikers aan	2	2	**4**
2.J	De Source-applicatie bevat kwaadaardige code, doordat de broncode is aangepast	2	2	**4**
2.K	De Source-applicatie bevat kwaadaardige code, doordat misbruik is gemaakt van een kwetsbaarheid bij de communicatie met de Plugwise server over Internet	2	2	**4**

2.8 Scenario 3: Stretch

In dit scenario wordt geen gebruik gemaakt van een lokale Source-computer, maar in plaats daarvan is een vergelijkbare gehoste Source-applicatie op de Plugwise-website te gebruiken voor het collecteren van, en de inzage in verbruiksgegevens en aansturing van de Circles.

Elk ZigBee-netwerk is verbonden met een Stretch, en deze Stretches communiceren met een Master Stretch. Deze Master Stretch communiceert via Internet (HTTPS met een self-signed certificaat voor client authenticatie) met een Plugwise systeem waarop een gehoste Source-applicatie actief is.



Figuur 4: Opzet met Plugwise Stretch

De Master Stretch kan afgeschermd worden van het interne netwerk door middel van een firewall en kan ofwel in een aparte untrusted zone ofwel in de DMZ opgenomen worden (in het plaatje is hij geplaatst in een aparte untrusted zone). Uitgaande verbindingen naar de Stretches en naar de Plugwise-webserver zijn hierbij toegestaan. Het toestaan van inkomende netwerkverbindingen is niet nodig.

Werkplekken kunnen direct de Plugwise-website benaderen voor het gebruik van de op Internet gehoste Source-applicatie.

Evenals in het vorige scenario wordt ook hier gebruik gemaakt van VLAN-technologie om de verkeersstromen te scheiden.

2.8.1 *Analyse van de dreigingen:*

De dreigingen in dit derde scenario komen overeen met de dreigingen die genoemd zijn in scenario 2, met daarbij een aantal aanvullende mogelijke dreigingen die een consequentie zijn van het additionele verkeer over het internet naar de hosted Plugwise Source-applicatie.

Dreigingen tegen het interne netwerk die geïntroduceerd kunnen worden door gebruik te maken van een externe hosted service zijn vergelijkbaar met de dreigingen van het gebruik maken van een interne Source-applicatie, met het verschil dat er minder controle over de Source-applicatie is omdat het beheer ervan door een derde partij wordt uitgevoerd. Daarnaast kan de Source-applicatie benaderd worden via Internet wat de kans op aanvallen sterk verhoogt.

Samengevat:

ID	Beschrijving dreiging	Kans	Impact	Risico
Zigbee:				
3.A	Inbraak via kwetsbaarheid in ZigBee-implementatie van de Stretch, van daaruit wordt het netwerk aangevallen	1	3	**3**
3.B	Inbraak via kwetsbaarheid in ZigBee-implementatie van de Stretch, van daaruit wordt de Master Stretch aangevallen	1	2	**2**
Circle:				
3.C	Inbraak via kwaadaardige Circle (+), van daaruit wordt het netwerk aangevallen	1	3	**3**
3.D	Inbraak via kwaadaardige Circle (+), van daaruit wordt de Master Stretch aangevallen	1	2	**2**
Stretch:				
3.E	De netwerkinstellingen van een Stretch worden ongeautoriseerd gewijzigd	1	3	**3**
3.F	Het bedrijfsnetwerk wordt aangevallen doordat een ander apparaat (bijv. een laptop) op de netwerkpoort van de Stretch wordt aangesloten.	2	4	**8**
3.G	De Stretch bevat kwaadaardige code en valt het bedrijfsnetwerk aan	2	3	**6**
Master Stretch:				
3.H	De netwerkinstellingen van een Master Stretch worden ongeautoriseerd gewijzigd	1	3	**3**
3.I	De Master Stretch bevat kwaadaardige code en valt het bedrijfsnetwerk aan	2	3	**6**
Hosted Source:				
3.J	Een gebruiker breekt in op de gehoste Source-applicatie en valt daarvandaan andere gebruikers aan	2	2	**4**
3.K	De gehoste Source-applicatie bevat kwaadaardige code, doordat de broncode is aangepast vanuit Plugwise	2	2	**4**
3.L	De gehoste Source-applicatie bevat kwaadaardige code, doordat een aanvaller misbruik heeft gemaakt van een kwetsbaarheid in de Source-computer	2	2	**4**

3 Conclusie en aanbevelingen

De Plugwise oplossing bestaat uit een aantal componenten waarmee een systeem opgebouwd kan worden dat is aangepast aan de wensen van de klant.

In dit document is voor een aantal scenario's aangegeven wat de daarmee gepaard gaande dreigingen kunnen zijn die implementatie van Plugwise voor het interne ICT netwerk met zich mee kan brengen. Voor die dreigingen is aangegeven welke maatregelen genomen zouden kunnen worden om die dreigingen weg te nemen of te verminderen.

Of het wenselijk is om een bepaalde dreiging weg te nemen of te verminderen, is aan de eigenaar van het bedrijfsnetwerk c.q. de eigenaar van de informatie op dat bedrijfsnetwerk. Alleen de eigenaar kan de afweging maken tussen de extra kosten en de daarmee gepaard gaande extra veiligheid.

Vanuit een optiek van informatiebeveiliging is de meest eenvoudige aanpak het installeren van de Plugwise Source-applicatie op een stand-alone systeem. De nadelen zijn echter:

- een beperkte toepasbaarheid van de Circles (de Source-computer moet binnen een straal van 10 meter van een Circle staan);
- dat gebruikers geen toegang tot Source hebben vanaf hun werkplek.

Als netwerktoegang gewenst is, kan de Source-computer in de DMZ van het bedrijf geplaatst worden, of in een apart "untrusted" netwerksegment aan de DMZ. Het systeem is dan niet bereikbaar vanaf Internet, maar wel voor de medewerkers van het bedrijf (uiteraard afhankelijk van de firewall configuratie). Als de Plugwise Source-computer gecompromitteerd zou raken, hoeft dat geen impact te hebben op de veiligheid van het interne bedrijfsnetwerk door de genomen beveiligingsmaatregelen.

Voor het aansturen van een groter Circle-dekkingsgebied kan gebruik gemaakt worden van Stretch Light (Pro)'s. Dit zijn apparaten die de informatiestroom tussen de Circles en de Source-applicatie verzorgen via een IP-netwerk. Wanneer gebruik gemaakt wordt van de Stretch Light (Pro)'s kan de wens bestaan om deze af te scheiden van het interne netwerk, als deze apparaten niet vertrouwd worden door de netwerkeigenaar. Daarvoor kan een VLAN gebruikt worden. Een duurder en complexer alternatief is het gebruik van VPN gateways om tunnels op te zetten tussen de Stretch Light (Pro)'s en de Source-applicatie.

Als alternatief kan gebruik gemaakt worden van een hosted Source-oplossing, waarbij de Source-applicatie via een Internet-server wordt aangeboden. Dit betekent wel dat er een extra apparaat in het bedrijfsnetwerk komt te staan (de zogenaamde Master Stretch) die voor de communicatie met de Source-applicatie zorgt, en door deze externe koppeling open staat voor externe aanvallen.

Geconcludeerd kan worden dat er voor alle genoemde scenario's beveiligingsmaatregelen te nemen zijn waarmee de risico's beperkt kunnen worden. Elke Plugwise gebruiker zal zelf moeten bepalen welke risico's acceptabel zijn. Voor de overige risico's zullen extra maatregelen moeten worden getroffen.

Bijlage 1: Overzicht van gebruikte documentatie

Referentie	Document	Versie/datum
1	Installatie binnen de zakelijke omgeving	08-09-2009
2	Plugwise Zakelijk	27-05-2009
3	Email van Theo Vroege	27-01-2010