ABN·AMRO

Thesis

Een onderzoek naar patchmanagement t.b.v. third-party software

ABN AMRO Hypotheken Groep

HOGESCHOOL UTRECHT

Thesis

Een onderzoek naar patchmanagement t.b.v.
third-party software

N. Boers

ABN AMRO Hypotheken Groep
Amersfoort, 01-08-2013

Afstudeerder:
Niels Boers
1587222

Bedrijfsbegeleider:
drs. Dhr. O.G.A.C.M. Hamelers

Docentbegeleider/1ste examinator:
Dhr. R.C. van der Ploeg

'We didn't install the [Code Red] patch on those DMZ systems because they were only used for development and testing'.

-Anonymous client, shortly after spending 48 continuous hours removing 2001's Code Red worm from internal corporate servers (Graff & van Wyk, 2003, p. 116).

Colofon

Documenteigenschappen

Titel	Thesis AAHG Niels-Boers v1.2.pdf	**Status**	Definitief
Project	Afstudeerstage	**Versie**	V1.2
Auteur	Niels Boers	**Studentnr.**	1587222
Bedrijf	ABN AMRO Hypotheken Groep		

Typografische conventies

Het voorliggende document maakt gebruik van de volgende typografische conventies.

Conventie	Betekenis	Voorbeeld
AaBbCc1234	Normale tekst	Dit is een voorbeeld.
AaBbCc1234	Quotatie/motto	De missie van ICT is: *"Wij ondersteunen zorgeloos werken"*.
AaBbCc1234	Kruisreferentie in dit document	Zie hoofdstuk 2 voor meer informatie.
AaBbCc1234	Hyperlink naar website of e-mail adres	e-mail: niels.boers@aahg.nl

Revisie

Revisie	Datum vorige revisie	Samenvatting van wijzigingen	Versie
08-08-2013	N.v.t.	Initiële thesis	V0.1
25-11-2013	08-08-2013	Verwerking feedback docent	V0.2
09-12-2013	25-11-2013	Thesis naar versie 1	V1.0
13-12-2013	09-12-2013	Verwerking feedback bedrijfsbegeleider	V1.1
14-12-2013	13-12-2013	Verwerking feedback docentbegeleider	V1.2

Distributie

Naam	Rol	Datum distributie	Versie
Olaf Hamelers	Opdrachtgever/begeleider	16-12-2013	V1.2
Niels Boers	Projectleder/student	16-12-2013	V1.2
Rienk van der Ploeg	Docentbegeleider	16-12-2013	V1.2

1 Voorwoord

In het voorliggende document vind u mijn thesis van de opleiding Bachelor informatica (systeembeheer).
Via mijn broer heb ik de mogelijkheid gekregen om mijn afstudeerstage bij ABN AMRO Hypotheken Groep [AAHG] in Amersfoort te doen. Aanvankelijk was er de mogelijkheid dat ik zou kunnen werken aan een technisch project. Uiteindelijk bleken deze deel uit te maken van projecten die al gestart waren voor de aanvang van mijn afstudeerperiode, of waren ze al bezig met het afronden ervan.

De opdracht die mij vervolgens werd aangeboden was niet zozeer technisch, maar meer een procesopdracht die de gehele IT afdeling raakte.
Hoewel procesopdrachten niet mijn voorkeur hebben, had deze opdracht een security insteek. Aangezien dit een interesse van me is, ben ik akkoord gegaan met de opdracht en heb ik dan ook met plezier en volle motivatie aan deze opdracht gewerkt. Het komt niet vaak voor dat een student naar eigen inzicht een proces mag inrichten. Natuurlijk zijn er wel compromissen gemaakt en is er gelet op de eisen en behoeften van de AAHG.

2 Managementsamenvatting

In dit document is gekeken naar de reden en beste manier voor het patchen van third-party software bij ABN Amro Hypotheken Groep [AAHG]. De definitie van third-party software hierbij is: alle applicaties die niet door Microsoft aangeboden worden. Binnen AAHG is namelijk wel een proces aanwezig voor het patchen van de Windows updates, maar niet voor de overige applicaties die zijn geïnstalleerd op werkstations en servers. Gevolg hiervan is dat vele applicaties in versies ver achter lopen. Ook zijn er nog versies aanwezig die door de third-party leverancier al als End-of-Life bestempeld zijn. AAHG wil nu ook hiervoor een proces, zodat het meer controle kan uitoefenen op de omgeving. Er is dan ook een onderzoek opgezet om te bepalen, waarom het patchen van third-party software belangrijk is, en waarop gelet moet worden met het schrijven van een nieuw proces. Uit het onderzoek kwam naar voren dat sinds 2011 niet Windows maar een aantal andere third-party applicaties zoals Adobe Reader en Java Runtime Environment de top tien vulden als meest kwetsbare software.

Voor het schrijven van een nieuw proces is gekeken naar verschillende best practices en in hoeverre deze bruikbaar zijn voor het nieuwe proces. Hiervoor is gekeken naar white papers van securitybedrijven, ITIL, het informatiebeveiligingsbeleid en ISO 27002. Hieruit werd duidelijk dat met name de frequentie waarmee patches worden uitgerold en de testprocedure van belang zijn. Verder is ITIL geschikt om ook hiervoor een proces te maken. Het Windows patchproces kan hierbij dienen als voorbeeld. Dit proces is namelijk ook al op ITIL gebaseerd en heeft zich bewezen in de praktijk. Het third-party software proces moet wel afwijken bij het testen. Java is namelijk een platform-applicatie en wordt gebruikt als framework door andere applicaties. In andere woorden, ze zijn afhankelijk van Java. Hierdoor kan Java niet als een losse applicatie getest worden, maar moet worden getest via elke applicatie die gebruik maakt van Java. Om het proces te ondersteunen is er ook gekeken naar het technische aspect van patchen, namelijk patchmanagementsoftware. Door middel van een marktonderzoek is gekeken of Microsoft System Center Configuration Manager [SCCM], dat door AAHG wordt gebruikt, de beste keuze is voor het patchen van third-party software of dat een andere applicatie beter zou zijn. Op basis van criteria en de bijbehorende waardes, is van de longlist een shortlist gemaakt. Uit deze shortlist is gekozen voor Secunia Corporate Software Inspector [CSI] om verder te behandelen in een Proof of Concept. De keuze hiervoor was dat Secunia CSI integreert met Windows Server Update Services [WSUS] en SCCM, Application Virtualization [App-V] pakketten kan scannen en vele third-party leveranciers ondersteunt. Secunia CSI bevestigde in het Proof of Concept dat het hebben van patchmanagement software voor third-party applicaties zeer wenselijk is.

Aan AAHG wordt het advies gegeven om zo snel mogelijk het beschreven proces (te vinden op pagina 35) te implementeren om de systemen weer compliant te maken. Hierbij moet het proces net zoals bij de Windows patches eens in de maand worden uitgevoerd. Dit is namelijk een vereiste van het gestelde informatiebeveiligingsbeleid. Elke patch dient ook getest te worden in de acceptatieomgeving voordat deze in productie gaat. Voor het testen kan het beste gebruik gemaakt worden van een gemengde test. Dit bestaat uit een systeem test, functionele acceptatie test en een gebruikers acceptatietest. Bij de functionele acceptatie test moet onderscheid worden gemaakt tussen normale applicaties en platform applicaties. Verder is het aan te raden om patchmanagementsoftware te implementeren. Het ondersteunt het proces goed en zorgt ervoor dat systeem beheer niet meer handmatig op de hoogte moet blijven van nieuwe updates. Secunia CSI is hiervoor een geschikte kandidaat.

ABN·AMRO

Inhoudsopgave

3 Proloog

De Blaster worm, ook wel bekend als Lovesan of MSBlast, is een zichzelf vermenigvuldigend computerprogramma dat vanaf 11 augustus 2003 25 miljoen computers had geïnfecteerd via een kwetsbaarheid van het Windows besturingssysteem. Dit lek was echter al bekend bij Microsoft en 26 dagen voor de uitbraak al gepatcht (Microsoft, 2003) (2005). Toch heeft de worm binnen twee dagen 25 miljoen computers kunnen infecteren doordat de patch door veel systeembeheerders niet was geïnstalleerd.
Aaron Turner vertelt in een artikel op csoonline (2013, p. 3) over de nasleep van Blaster en dat na 10 jaar patches nog steeds te laat worden geïnstalleerd.
Een voorbeeld van Turner was zijn bezoek aan een bedrijf in 2012. Het bedrijf had naar schatting 60.000 smartphones in productie waarop 20.000 verschillende combinaties van software met verschillende versies/configuraties actief waren. De smartphones draaiden dus niet allemaal dezelfde (laatste) versie, terwijl aanvallen op smartphones juist aan populariteit winnen. Het hebben van verschillende versies maakt het dus voor kwaadwillende gemakkelijker om binnen te dringen en data te stelen.
Dit geeft goed aan dat in een wereld die niet meer zonder IT kan nog steeds weinig wordt gedaan op het gebied van patchmanagement. Met name third-party software zoals Java, Adobe Flash Player en Adobe Reader komen tegenwoordig regelmatig in het nieuws vanwege de hoeveelheid kwetsbaarheden. De term third-party software wordt gebruikt bij applicaties die niet door de leveranciers van het besturingssysteem wordt geleverd. Op een Windows besturingssysteem is software van Microsoft first-party en zijn software van andere leveranciers third-party.

Ondanks dat het patchen van third-party software nauwelijks wordt gedaan, bestaan er wel studies naar patchmanagement. Een van de meest bekende ‘best practices’ is te vinden bij ITIL. In dit document wordt gekeken hoe al bestaande software update methodieken gebruikt kunnen worden voor third-party software om zodoende meer controle te houden op de totale softwareomgeving.

4 Context afstudeeropdracht

4.1 Beschrijving bedrijf/afdeling

In 1964 is de Algemene Bank Nederland [ABN] ontstaan uit de fusie van de Nederlandsche Handel-Maatschappij (1824) en de Twentsche Bank (1861). Daarnaast ontstond ook in 1964 de Amsterdam-Rotterdam Bank [AMRO] uit de fusie van de Rotterdamsche Bank (1863) en de Amsterdamsche Bank (1871). Uiteindelijk ontstond er in 1991 uit de fusie van de ABN en AMRO de ABN AMRO Bank (ABN AMRO, z.j.).

Naast de bank zelf kent de ABN AMRO ook 16 dochterondernemingen waaronder de ABN AMRO Hypotheken Groep [AAHG].
De AAHG is gespecialiseerd in het verstrekken en beheren van hypotheken. Door hun jarenlange ervaring en voortdurende verbetering van hun producten en processen behoren ze tot de grootste gespecialiseerde hypotheekverstrekkers van Nederland (ABN AMRO, z.j.).

De missie van AAHG is: *"Wij maken zorgeloos wonen mogelijk door middel van zinvolle en begrijpelijke financiële producten en verantwoord advies"* (ABN AMRO, z.j.).

De ICT afdeling van de AAHG bestaat uit verschillende onderdelen die zich bezighouden met verschillende disciplines binnen de ICT. Deze onderdelen zijn ICT Beheer, bestaande uit de teams Infra- en Systeembeheer en Applicatiebeheer, ICT services, ICT Informatiebeveiliging en ICT Development.

De missie van ICT is: *"Wij ondersteunen zorgeloos werken".* Zij zijn verantwoordelijk voor het draaiend houden, vervangen en updaten van de IT infrastructuur, servers, workstations en applicaties. Daarnaast worden ook de eindgebruikers ondersteund in ICT gerelateerde vragen.

4.2 Positie, taken en verantwoordelijkheden student

De student zal deel uitmaken van de IT afdeling en zal zich daar bezighouden met het afstudeerproject. In het afstudeerproject is de student zowel projectleider als projectlid. Het zal aan de student liggen om het project goed te laten verlopen en contact te leggen met verschillende afdelingen binnen ICT voor informatie over de IT infrastructuur en al bestaande processen. De student werkt zelfstandig, maar is wel afhankelijk van de medewerking van verschillende personen binnen de ICT afdeling.
Het initiatief en uitvoering zal dus liggen bij de student. Daarmee komt ook het uiteindelijke succes van het project bij de student te liggen.

Naast het project zelf is de student ook verantwoordelijk voor het op tijd inleveren van afstudeerdocumenten zoals het Plan van Aanpak [PvA] en de uiteindelijke scriptie.
De student zal zich naast de verantwoordelijkheden voor het afstudeeropdracht ook proactief opstellen.

5 Definitie afstudeeropdracht

5.1 Probleemstelling

Binnen de AAHG zijn er naast de Windows-updates ook third-party software updates waaronder Java en Adobe Flash. Voor dit onderdeel is er echter binnen de AAHG geen geaccordeerd en geïmplementeerd proces.
Uitrol van de updates gebeurt momenteel onregelmatig en alleen patches van grote security lekken worden meteen doorgevoerd.
Hoewel het niet patchen van third-party software niet direct verstorend voor de productie is, bestaat er toch het gevaar dat deze kwetsbaarheden geëxploiteerd kunnen worden. Een oude of out-of-date versie van Java bijvoorbeeld geeft een hacker de mogelijkheid op afstand toegang te krijgen tot een systeem zonder dat de gebruiker zich daar bewust van is. Als een hacker eenmaal toegang heeft tot het systeem, kan hij onder andere data stelen, data verwijderen, wachtwoorden achterhalen (i.i.g. de wachtwoorden van het lokale systeem) of proberen andere systemen binnen te dringen. Het up-to-date houden van third-party software vermindert de kans op een succesvolle aanval.

5.2 Afstudeeropdracht

Voor het schrijven en implementeren van een nieuw updateproces doet de student een literatuuronderzoek naar patchmanagement en de waarde ervan. Voor het literatuuronderzoek worden o.a. bronnen zoals white papers, thesissen en andere documenten gebruikt om zodoende te komen tot nieuwe kennis die gebruikt kan worden voor het schrijven van een nieuw update proces voor AAHG.

De student heeft ook interactie met verschillende afdelingen binnen de IT om zodoende de ‘AS-IS’ situatie te inventariseren van het update proces. Ook verkrijgt de student van de verschillende afdelingen informatie die helpt bij het schrijven van het nieuwe proces. Het nieuwe proces zal dus voortkomen uit het onderzoek en de informatie verkregen van collega’s.
Het proces wordt op het einde door middel van een Proof of Concept [PoC] met minimaal één softwarepakket getest.

Naast het proces zelf wordt ook de huidige distributie software, Microsoft System Center Configuration Manager [SCCM] 2012, onder de loep genomen en wordt er gekeken naar alternatieve oplossingen om updates uit te kunnen rollen. Over deze resultaten zal de student een advies geven waaruit blijkt of SCCM de juiste keuze is of dat een ander pakket toch een betere keuze is.

5.3 Doelstellingen

Dit project kent de volgende doelstellingen:

- Een advies hoe AAHG het beste kan omgaan met third-party software patches;
- Een gedocumenteerd updateproces voor de third-party software;
- Een advies over de beste technische oplossing en met welke updatesoftware, getest middels een Proof of Concept.

5.4 Onderzoeksvragen

Hieronder de onderzoeksvragen bestaande uit een hoofdvraag en een aantal deelvragen. Deze vragen zullen in de loop van het project worden beantwoord. Deze informatie zal dan worden gebruikt om te komen tot het advies.

Hoofdvraag:

- Wat is de beste methode voor het uitrollen van third-party software updates, zowel procesmatig als technisch?

Deelvragen:

- Waarom is het nodig om third-party software regelmatig te updaten?;
- Welke 'best practices' zijn er voor patchmanagement?;
- Waaruit bestaat het huidige updateproces voor de third-party software?;
- Op welke manier is ITIL geïmplementeerd met betrekking tot change- release- en configuratiemanagement?;
- Welke softwarepakketten komen voor het te ontwerpen proces in aanmerking?;
- Wat is procesmatig de beste manier voor AAHG om third-party software patches uit te rollen?;
- Op welke manier kunnen software updates efficiënt worden getest voordat ze in productie worden genomen?''
- Wat is er technisch nodig om third-party software updates uit te rollen?;
- Wat is er technisch nodig om geautomatiseerd een melding te geven wanneer third-party software updates beschikbaar zijn?;

6 Theorie

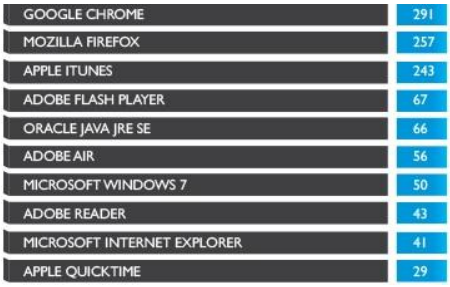
6.1 Reden tot patchen

Patchen wordt uitgevoerd om onvolkomenheden in de programmacode te verbeteren. Deze onvolkomenheden zijn fouten in de applicatie die leiden tot problemen met de functionaliteit of beveiliging van een programma (SANS, 2003, p. 6). Tot onvolkomenheden van de functionaliteit kunnen o.a. crashes, vertragingen en missende functionaliteit behoren. Met onvolkomenheden van de beveiliging wordt verstaan dat fouten in de code kunnen leiden tot o.a. mogelijkheden voor code injection, buffer overflow of arbitrary code execution. Deze kunnen door kwaadwillenden misbruikt worden om o.a. informatie te stelen en/of te wissen, wat kan leiden tot financiële- en/of imagoschade.
Hoewel beide onvolkomenheden reden genoeg is om te patchen, is het logisch dat het security aspect vanwege de impact zwaarder weegt binnen een bedrijf. Dit document zal dus de reden om te patchen met name bekijken vanuit een security standpunt.

Binnen bedrijven is de security van het IT infrastructuur een belangrijk onderdeel. Een goede manier om de veiligheid te kunnen waarborgen is het toepassen van defense in depth. Onder deze gelaagde beveiligingsstrategie denkt men voornamelijk aan firewalls, Demilitarized Zones [DMZ], Intrusion Prevention Systems [IPS], Intrusion Detection Systems [IDS], anti-virus en proxy's. Het is echter niet moeilijk om patchmanagement ook te zien als onderdeel van defense in depth. In zekere zin is een goed gepatcht systeem de laatste laag van verdediging voordat een kwaadwillende zijn doel bereikt.

Patches moeten dus gezien worden als een deel van de beveiliging en niet als iets dat alleen maar tijd vergt om te installeren en te testen. Er wordt immers wel tijd genomen om de anti-virus up-to-date te houden. Er moet worden gerealiseerd dat het patchen goed en volledig moet gebeuren. Het gezegde *"A chain is only as strong as its weakest link"* is hier ook goed van toepassing. Het niet toepassen van alle security patches laat informatiesystemen vatbaar voor one-day aanvallen.

Third-party vulnerability
De producten van Microsoft (met name Windows) zijn berucht als het aankomt op veiligheid. Jaren lang hebben de producten van Microsoft op nummer één gestaan in de top 10 van vulnerabilities. Door constante verbetering van de Windows beveiliging en Windows Update, dat sinds Windows 98 aanwezig is, is dit veranderd. In 2011 is voor het eerst geen Microsoft product in de top 10 te vinden (Kaspersky, 2011). De lijst wordt nu gevuld door de producten van Adobe en Oracle. Dit is een trend die zich in 2012 en 2013 doorzet. Zo laat een onderzoek van Secunia (Vulnerability review 2013 - The Highlights, 2013) zien dat de top 10 van meest kwetsbare applicaties met name third-party zijn, zoals te zien in figuur 1.



Figuur 1 Top 10 meest kwetsbare applicaties. Aangepast van Secunia (2013) http://secunia.com/vulnerability-review/vulnerability_update_top50.html

Kaspersky (IT Threat Evolution: Q3 2012, 2012) komt ook in 2012 tot dezelfde conclusie als in 2011. Ook in dit onderzoek komt Microsoft niet naar voren en zijn de meest voorkomende vulnerabilities te vinden in third-party software.

De top 10 van Kaspersky is te herleiden tot de volgende leveranciers:

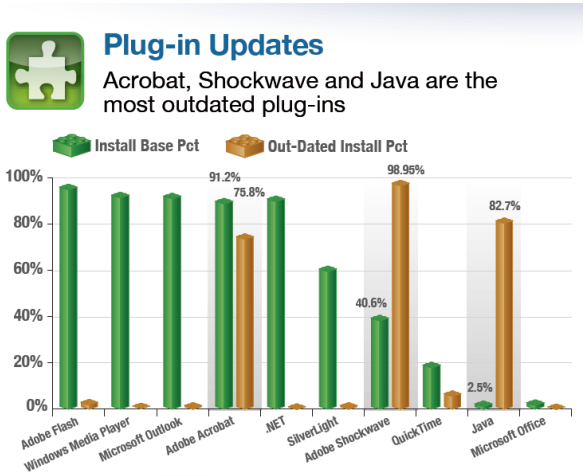
- Oracle (Java);
- Adobe (Flash, Reader, Shockwave);
- Apple (QuickTime, iTunes);
- Winamp.

Voor leveranciers is het lastig hun software zo up-to-date mogelijk te houden. Hoewel leveranciers zelf ook fouten in hun software vinden, blijft het vooral dweilen met de kraan open. Dit komt omdat de exploit window krimpt (White, 2006, p. 21). Dit is de tijd tussen de introductie van een vulnerability en het verschijnen van een exploit. Omdat het steeds gemakkelijker wordt om een exploit te maken, krimpt de exploit window. Dit is iets waar patchmanagement geen oplossing voor heeft en er dus vertrouwd moet worden op andere beveiligingsmethodieken zoals firewalls en proxy's. Het is duidelijk dat patchen van third-party applicaties hard nodig is. Iets dat volgens onderzoek van F-Secure (2013) te weinig wordt gedaan.
In het onderzoek van F-Secure komt naar voren dat op 87% van alle bedrijfscomputers o.a. Microsoft, Java en Adobe vaak niet up-to-date worden gehouden.
Het probleem is alleen dat vele bedrijven het belang van third-party patches onderschatten of zien als iets dat alleen maar tijd in beslag neemt.

Daarnaast spelen ook de updatemechanismen een rol in het achterblijven van third-party software. Microsoft biedt bedrijven structuur door alle Microsoft updates aan te bieden via Windows Update. Verder hanteert Microsoft sinds 2004 'Patch Tuesday', waarin elke tweede dinsdag van de maand nieuwe patches worden vrijgegeven.
Hierdoor kunnen bedrijven hun updatestrategie goed inrichten.
Third-party leveranciers aan de andere kant maken allemaal gebruik van hun eigen updatemethodes en kunnen patches op elke dag vrijgeven. Dit maakt het voor bedrijven lastig om met regelmaat patches voor third-party software te installeren.

In een onderzoek van ZScaler (Q3 2012 State of the web, 2012) is dit dan ook goed terug te zien. Het onderzoek werd gehouden onder zakelijke klanten en keek naar de browser plug-ins. In figuur 2 is te zien dat terwijl Microsoft plug-ins in grote getallen worden geïnstalleerd, juist deze pakketten nog redelijk up-to-date worden gehouden in vergelijking met de producten van Adobe. Adobe Flash Player wordt up-to-date

gehouden omdat updates geforceerd worden. Een gebruiker moet dus de update downloaden om de video af te kunnen spelen (Google, z.j.).
De drempel om third-party software te updaten ligt dus hoger dan die van OS updates.



Figuur 2 Install vs out-dated plugin rate. Overgenomen van ZScaler (2012) https://www.zscaler.com/thankyou_state-of-the-web-q3-2012-inforgraphic.php

If it ain't broke, don't fix it
Hoewel de focus om wel of niet te patchen ligt op het securityaspect, komen er ook geregeld patches vrij die functionaliteitsproblemen oplossen. De vraag is nu, zijn deze wel nodig? Het komt geregeld voor dat patches een bugfix bevatten voor een probleem waar een bedrijf zelf geen last van heeft. In dit geval is het dus alleen maar een risico om de patch uit te rollen. Er is namelijk altijd een kans dat een update iets breekt. Met name als er niet getest wordt.

Het changemanagement proces van ITILv3 beschrijft ook een aantal Key Performance Indicators [KPI]. Een hiervan is dat de change voordelen moet opleveren in vergelijking met de kosten. Als een patch een functioneel probleem oplost waar een bedrijf geen last van heeft, kan er gezegd worden dat de patch geen voordelen oplevert maar wel kosten met zich meebrengt. Dit is al helemaal waar wanneer de patch niet goed is en er een fall-back actie gedaan moet worden. Zo moest Microsoft in september 2013 de niet-security gerelateerde Outlook-update KB2817630 terugtrekken. De patch zorgde er voor dat de mappenstructuur aan de linker kant verdween (Security.nl, 2013), met alle gevolgen van dien.

Up-to-date ≠ veilig
Over het algemeen doen patches waar ze voor gemaakt zijn, het oplossen van een probleem. Het kan echter voorkomen dat een patch toch onverwachte bijwerkingen vertoont zoals het introduceren van een nieuwe exploit, het herintroduceren van een oude exploit, breken van de functionaliteit of zelfs de exploit niet verhelpen. Deze gebrekkigheid zorgt ervoor dat bedrijven voorzichtig zijn met patchen, iets wat geheel terecht is. Ze moeten een afweging maken, niet patchen en hopen dat het goed gaat of wel patchen met de kans dat het alsnog mis gaat (White, 2006, p. 23).

Een voorbeeld van een slechte patch is te vinden bij de SQl Slammer, ook wel Sapphire, worm.
In dit voorval had Microsoft op 24 juli 2002 een exploit gepatcht in een dll die in januari 2004 gebruikt zou worden door SQL Slammer (Microsoft security bulletin MS02-039,

2002). Na de patch in juli volgende er in oktober 2002 nog een patch die weer een oude versie van de dll gebruikte (Microsoft, 2002) (Cooper, 2003) (White, 2006, p. 29) (Bosworth, Kabay, & Whyne, 2009, p. 41). Microsoft had de exploit opnieuw geïntroduceerd. De fout werd gevonden en weer gepatcht.
Drie maanden later werd Slammer losgelaten in het 'wild' en slaagde het erin om binnen 25 minuten 67.000 computers te infecteren. Het gevolg was onder andere zeer traag internet (Tweakers, 2003). De reden dat Slammer alsnog kon toeslaan was dat ondanks dat Microsoft 3 maanden eerder een patch ervoor had uitgebracht velen de patch niet hadden geïnstalleerd. Een half jaar later op 11 augustus 2004 zou het niet patchen verhaal zich nogmaals herhalen met de Blaster worm.

Het is duidelijk dat zelfs na het uitbreken van twee wormen in een jaar er te weinig aan patchen wordt gedaan. Ook laat het zien dat patches niet altijd veiligheid garanderen. Dit wijst er weer op dat ook bedrijven de patch moeten controleren om er zeker van te zijn dat de lek daadwerkelijk gedicht is.

6.2 Update notification

Third-party software patches worden minder snel uitgevoerd omdat de drempel hoger is dan die van Windows patches.
Zo is er geen centrale plek voor update meldingen zoals bij Microsoft WSUS en worden de patches ook niet aan de hand van een schema vrijgegeven.
Om de drempel voor systeembeheerders lager te maken is het makkelijk als er een systeem geïmplementeerd is dat ook voor third-party software een notificatie kan geven als er updates beschikbaar zijn. Dit kan met verschillende methodes worden gerealiseerd:

Leverancier notifications
Leveranciers zoals Adobe (Adobe - Security Notification Service, z.j.) hebben vaak verschillende methodes om bedrijven op de hoogte te houden. Zo kunnen bedrijven zich abonneren op een mailinglijst. Hiermee krijgen bedrijven een mail als er een nieuwe CVE [Common Vulnerabilities and Exposures] aangemeld is of nieuwe update beschikbaar is. CVE is een databank van verschillende computer kwetsbaarheden. Elke keer dat er een nieuwe kwetsbaarheid gevonden is, wordt dit toegevoegd aan de databank.
Ook hebben bedrijven vaak een webpage waar deze meldingen worden gepost of is er een mogelijkheid om te abonneren op een RSS-feed zoals die van Oracle (Oracle Security Alerts, z.j.). Hiervan zijn de mailinglist en RSS-feed praktischer doordat deze naar systeembeheer opgestuurd/gepusht worden. Het nadeel van deze manier is dat er door elke leverancier een mail wordt gestuurd. Dit kan resulteren in een volle mailbox die niet erg overzichtelijk is.

Derde partij
Er zijn ook bedrijven die als derde partij een mailinglijst aanbieden (Patchmanagement, z.j.) (Shavlik, z.j.). Hiermee staat in een e-mail gelijk alle uitgekomen patches. Deze aanpak is al binnen AAHG aanwezig maar werkt niet optimaal doordat e-mails niet toegespitst zijn op de software van AAHG. Ook komen deze e-mails vaak pas binnen terwijl de patch al geïnstalleerd is.

Security sites en community
Een andere mogelijkheid is het in de gaten houden van security gerelateerde sites en andere IT communities zoals cvedetails.com, tweakers.net en security.nl. Op deze sites worden vaak nieuwe exploits en patches ter sprake gebracht. Deze sites bieden ook de mogelijkheid voor RSS-feeds. In het geval van cvedetails.com (CVE Details, z.j.) is het zelfs mogelijk een RSS-feed of widgets te creëren die alleen CVE's toont met betrekking tot een of meerdere specifieke aanvallen of aan de hand van een impact score.
Het nadeel van deze mogelijkheden is dat het niet gericht is op alleen de software binnen AAHG en ook tijd van beheerders in beslag neemt doordat ze sites in de gaten moeten houden.

Software
De laatste optie voor update notifications zijn update monitors of vulnerability management software. Dit zijn softwarepakketten die scannen naar de geïnstalleerde software, en vervolgens alleen voor deze software een update melding geven. Hiermee worden alleen update meldingen van geïnstalleerde software op een centrale plek weergegeven. Nadeel hiervan is dat niet alle software ondersteund wordt. Deze monitors ondersteunen wel veel gebruikte software. Bijkomend voordeel is dat deze software ook inzicht kan geven in de compliance van de werkstations en servers.
Verder maakt AAHG gebruik van App-V [Application Virtualization] voor third-party software. Doordat de software gevirtualiseerd is, kan het voor vele monitors moeilijk tot onmogelijk worden om de software te controleren op updates.

6.2.1 Patchsoftware
Patchsoftware kan net iets meer dan vulnerability management software. Naast het geven van update meldingen, kunnen deze pakketten ook de patch downloaden. Vaak is er ook de optie om de patch te packagen en te distribueren naar groepen. Dit kan de software ook automatisch doen, zodat er weinig omkijken naar is.
Het gebruik maken van patchsoftware is dus een goede aanvulling om een patch proces semi of volledig te automatiseren. De patchsoftware heeft echter, net zoals de vulnerability management software, het nadeel dat niet alle leveranciers worden ondersteund. Doorgaans is er alleen ondersteuning voor Microsoft en veel gebruikte third-party applicatie patches, zoals browsers, Adobe producten, Java en Apple producten.

6.3 Best practices

Voor het gecontroleerd uitrollen van patches zijn door de jaren heen verschillende studies gedaan en best practices opgezet voor patch management. ITIL is een bekend voorbeeld dat veelvuldig gebruikt wordt als richtlijn binnen de ICT. Daarnaast geven security gespecialiseerde bedrijven telkens vaker een signaal af dat bedrijven meer aan patchmanagement moeten doen. Dit gaat vaak gepaard met white papers waarin advies wordt gegeven over hoe patches op een goede manier uitgerold kunnen worden.

In een artikel van SANS (Patch Me If you Can: Patch Managements Vital Role Defense-in-Depth, 2003, pp. 7-9) worden zeven punten besproken die leiden tot effectieve patchmanagement.
De besproken punten zijn als volgt:

- **Automatiseer**
  Door het automatisch laten scannen naar missende updates en het downloaden van nieuwe updates wordt het al een stuk gemakkelijker om een up-to-date status te behouden.
- **Plannen**
  In dit onderdeel wordt beschreven dat de gehele infrastructuur niet gezien moet worden als een grote groep, maar het moet worden onderverdeeld in verschillende groepen. Door deze aanpak kan bij een release de update eerst worden geïnstalleerd op de servers waar het belang het grootst is.
- **Testen patches**
  Dit punt spreekt voor zich. Het eerst testen van patches is altijd belangrijk om er zeker van te zijn dat updates ook stabiel zijn in de eigen omgeving.
- **Ken de configuraties**
  Het is ook belangrijk te weten wat er allemaal gebruikt wordt en waar het is geïnstalleerd. Zo kunnen patches gerichter worden uitgerold.
- **Blijf up-to-date**
  Het is makkelijker een bepaald niveau te behouden dan dat je telkens een of meerdere patches achter loopt.
- **Documenteer**
  Om overzicht te behouden is het belangrijk om alles goed gedocumenteerd te hebben.
- **Communiceer**
  Door elkaar constant op de hoogte te houden van patches en exploits. Hierdoor denken meer mensen mee aan de veiligheid van de informatiesystemen en zal alles gemakkelijker verlopen.

Ook GFI (Fisher, 2011) geeft drie do's en drie don'ts aan op het gebied van patchmanagement. Samengevat zijn ze als volgt:

Do's

- **Gebruik patch software die ook third-party patches kan doen;**
  Het patchen van third-party software is even belangrijk als OS patches. Dit komt neer op een hoop patches en dus is het gewenst één systeem te hebben dat ook overweg kan met third-party software.

- **Test patches voordat ze in productie gaan;**
  Testen van de patches op een testomgeving is zeer belangrijk. De leverancier kan namelijk met een systeem hebben getest met een andere configuratie of een 'foute' patch leveren.
- **Patch regelmatig aan de hand van een schema.**
  Om de veiligheid zo hoog mogelijk te kunnen houden is het belangrijk dat er regelmatig op vaste data gepatcht wordt.

Don'ts

- **Ga er niet van uit dat je vanaf het begin op de hoogte bent van security issues;**
  Er moet gerealiseerd worden dat een aanval door middel van zero-day attacks altijd mogelijk is en dat het even kan duren voordat er hiervoor een patch beschikbaar komt. Om dit enigszins op te vangen kan er worden geabonneerd op een security-feed die het bedrijf op de hoogte houdt van alle security gerelateerde ontwikkelingen.
- **Ga er niet van uit dat patches werken;**
  Naast het testen van patches voordat ze in productie gaan, moeten patches ook na de uitrol worden getest of ze het gewenste effect hebben. Met ander woorden is het lek nu gedicht? Dit kan worden gecontroleerd door gebruik te maken van een vulnerability scanner.
- **Gebruik geen software die alleen OS patches kan uitrollen.**
  In feite is dit hetzelfde punt als een van de DO lijst. Fisher geeft hiermee aan dat het zo belangrijk is dat dit twee keer vermeld moet worden.

ISO/IEC 27002:2013 Information technology – security techniques

ISO [International Organization for Standardization] is een internationaal bedrijf dat standaarden creëert (ISO, z.j.). Deze standaarden bevatten vaak best practices en daarmee is het voor een bedrijf mogelijk om voor een standaard te certificeren. Zo heeft de ISO ook een standaard voor informatie beveiliging, de ISO/IEC 27002. In deze standaard staan ook een aantal best practices rondom patchen die goed aansluiten bij al bovengenoemde punten. De onderstaande punten komen uit de 27002 (ISO, 2013, p. 47):

- *'A timeline should be defined to react to notifications of potentially relevant technical vulnerabilities.'*
- *'Patches should be tested and evaluated before they are installed to ensure they are effective and do not result in side effects that cannot be tolerated; if no patch is available, other controls should be considered, such as:*
  - *Turning off services or capabilities related to the vulnerability;*
  - *Adapting or adding access controls, e.g. firewalls, at network borders;*
  - *Increased monitoring to detect actual attacks;*
  - *Raising awareness of the vulnerability'.*

Windows patchproces

Het Windows patchproces van AAHG kan ook dienen als een vorm van best practice. Het is al geïmplementeerd bij AAHG en heeft zichzelf ook al bewezen. Verder is het gebaseerd op ITILv3 dat verderop in dit hoofdstuk wordt besproken.

6.3.1 Informatiebeveiligingsbeleid

Het informatiebeveiligingsbeleid binnen de AAHG (ABN AMRO, 2011) bestaat uit een 9-tal richtlijnen waaraan een patchproces moet voldoen:

- **Gedocumenteerd proces;**
  Het patch proces is beschreven en geaccordeerd.
- **Betrouwbare bron;**
  Patch notes en Common Vulnerabilities and Exposures [CVE] komen uit betrouwbare en continue bron.
- **Scope van patches;**
  Alle software valt binnen de scope.
- **Prioriteit en uitrol;**

Prioriteit	Uitroldeadline na beschikbaar komen van de patch bij de leverancier
Urgent	Binnen 2 weken
Hoog	Binnen 6 weken
Midden/laag	Binnen 6 maanden
Geen	Niet van toepassing

Tabel 1 Patchdeadline met bijbehorende prioriteit

- **Getoetste patches;**
  Patches worden getest voordat ze in productie gaan. Indien niet mogelijk, dan mogen de patches naar de productieomgeving mits er een gecontroleerde fall-back is.
- **Implementatie van patches via ITIL/change management;**
  Uitrol verloopt via het ITIL/change proces.
- **Escalaties/conflicten worden via ICT management besloten;**
  Conflicten worden formeel opgelost door het ICT management.
- **Periodieke rapportage.**
  Patch status wordt maandelijks gerapporteerd aan het ICT management.
- **Controle op uitvoering;**
  Patch proces wordt getoetst door een vulnerability scanner.

6.3.2 ITILv3

ITIL is ontstaan uit een verzameling ‘best practices’ uit de IT-dienstverlening. Het is uiteindelijk uitgegroeid tot een van de meest gebruikte methodes in de IT (Bon, et al., 2007, p. 9). ITIL is geen set regels waaraan gehouden moet worden, maar een set richtlijnen die bedrijven handvaten biedt voor het beheren van processen.
Op het moment van schrijven is ITILv3 de meest recente versie. ICT had in het begin met name een ondersteunende rol, en daar speelde ITILv2 op in met het bieden van verschillende processen. Nu is ICT vaak de basis van een bedrijf, en daar wordt met ITILv3 op ingespeeld. ITILv3 is ten opzichte van ITILv2 uitgebreid met enkele processen en focust nu meer op de life-cycle (Bon, et al., 2007, pp. 14-15).
Binnen ITIL zijn voor het uitrollen van patches change-, release- en configurationmanagement van belang.

Release- en deploymanagement
Releasemanagement is verantwoordelijk voor het uitrollen van releases in de productieomgeving en daarbij dus ook patches. Het beschrijft de cyclus voor het wijzigen van CI's van het bouwen tot het uitrollen van de release. Het bouwen van de release is binnen de AAHG gelijk aan het creëren van een package voor een patch. Releasemanagement kent de volgende hoofdlijnen (Bon, et al., 2007, pp. 255-256):

- Planning;
- Voorbereiding op bouw, test en deployment;
- Bouw en test;
- Servicetesten en pilots;
- Plannen en voorbereiden van deployment;
- Transfer, deployment, uitfaseren;
- Deployment controleren;
- Early life support;
- Evalueren en afsluiten.

Daarnaast beschrijft releasemanagement ook verschillende opties voor het uitrollen:

- 'Big Bang', de wijziging in een keer naar iedereen uitrollen;
- Gefaseerd, de wijziging bij een gedeelte van de gebruikers uitrollen;

- Push, de wijziging wordt vanaf het distributiesysteem naar de gebruikers uitgerold (gepusht);
- Pull, de wijziging wordt op het distributiesysteem beschikbaar gesteld voor gebruikers, gebruikers kunnen zelf kiezen (pull);

- Geautomatiseerd, de wijziging wordt automatisch doorgevoerd;
- Handmatig, de wijziging wordt handmatig doorgevoerd.

Bij het Windows update proces wordt gebruikt gemaakt van 'Big Bang' (nadat acceptatie geslaagd is), Push en geautomatiseerd. Ondanks dat er 'Big Bang' wordt gebruikt, zal SCCM onder water de systemen gefaseerd patchen zodat het netwerk niet overbelast wordt.

Changemanagement
Zoals al vermeld, wordt via het informatiebeveiligingsbeleid gesteld dat de patches via ITIL/changemanagement worden uitgerold. Changemanagement focust op het gestructureerd wijzigen van het IT landschap. Omdat een patch wijzigingen met zich mee brengt, moet het patchproces volgens het changeproces verlopen. Change management kent de volgende hoofdlijnen (Bon, et al., 2007, pp. 238-241):

- Changeplanning en –control;
- Releaseplanning;
- Communicatie;
- Change-autorisatie;
- Herstelplannen opstellen;
- Rapporteren;
- Impact bepalen;
- Continue verbetering.

Daarnaast kent changemanagement ook nog specifieke activiteiten voor het beheren van individuele changes:

- Indienen en registeren;
- RFC beoordelen;
- Change beoordelen en evalueren;
- Change autoriseren;
- Coördineren en implementeren;
- Evalueren.

Changemanagement kent samen met releasemanagement het plannen, implementeren, valideren en evalueren van de release. Hierin kent het onderdeel coördineren en implementeren de grootste raakvlak met releasemanagement.
Afhankelijk van het uiteindelijke proces kan het zijn dat het indienen en registreren maar eenmalig gebeurt. In het geval bij de Windows updates is er sprake van een non-standard change doordat het proces maandelijks terugkomt, maar wel elke keer een andere impact kan hebben (Goktas & Tomassen, 2013).

Serviceasset- en configurationmanagement
Serviceasset- en configurationmanagement [SACM] richt zich op het leveren van een logisch model van de IT-infrastructuur. Het model toont de IT-services in relatie met de verschillende IT-componenten (Bon, et al., 2007, pp. 244 - 253).

De activiteiten die bij dit proces horen zijn als volgt:

- Management en planning;
- Configuratie-identificatie;
- Configuratiebeheer (control);
- Statusbewaking;
- Verificatie en audits.

Van het proces SACM is het configuratie gedeelte belangrijk voor het patchen. Hierin worden de verschillende configuration items [CI] bepaald en opgenomen in de Configuration Management Database [CMDB]. Enkele CI's die voor software gebruikt kan worden zijn naam en versie.
Door het goed bijhouden van de database blijft er overzicht van de software die in gebruik is. Hierdoor is er inzicht in welke versies nog in productie zijn en welke verwijderd kunnen worden. Het software inventarisatieprogramma SNOW, dat in gebruik is door AAHG, is een goed voorbeeld van een CMDB voor software. In SNOW is duidelijk te zien welke software aanwezig is met welke versies.

6.3.3 Patroon

Uit de 'Best Practices' komen bepaalde onderwerpen telkens naar voren.
Zo is duidelijk dat patchen gemakkelijker en minder problemen geeft als de patches getest, en op vaste data uitgerold worden.

Testen

Testen is een belangrijke taak in het patch proces.
Door het testen van een patch op een gevarieerd testomgeving kunnen patches die problemen opleveren worden gevonden. Hierdoor kan worden voorkomen dat de 'foute' patches in de productieomgeving komen en zo daar meer problemen veroorzaken (White, 2006, p. 57) (The Government of Hong Kong Special Administrative Region, 2008, pp. 8-9) .
In het geval van ernstige beveiligingslekken moet er alsnog de voorkeur worden gegeven om de patch eerst te testen. Hoewel daarmee bewust de window of exposure wordt vergroot, zorgt het er ook voor dat er geen problemen ontstaan nadat de patch is uitgerold in de productieomgeving.

Daarnaast moeten patches niet alleen op stabiliteit worden getest maar ook op effectiviteit. Dit kan onder andere gedaan worden door een vulnerability scanner. Zo weet een bedrijf of een patch wel doet waar het voor gemaakt is en zelf geen verdere acties hoeft te ondernemen zoals tijdelijk poorten dichtgooien of plug-ins uitschakelen. Binnen de AAHG wordt er al gebruik gemaakt van toetsing door middel van een vulnerability scanner. Zo wordt bij de Windows patches gebruik gemaakt van Microsoft Baseline Security Analyzer [MBSA]. Deze scanner kijkt echter alleen naar of de patch is geïnstalleerd en niet of de lek daadwerkelijk weg is. Daarnaast is deze tool alleen geschikt voor Microsoft software. Om echt te kunnen bepalen of het lek weg is, moet er gebruik worden gemaakt van vulnerability scanners zoals Nessus, die actief met exploits proberen een systeem binnen te komen. Omdat er met werkende exploits gewerkt worden, valt dit meer onder penetration testing en is te uitgebreid voor een maandelijkse patch ronde. Het vraagt namelijk veel tijd en kennis van de programma's om dit goed uit te kunnen voeren, en test daarnaast het gehele systeem.

Aan de andere kant hebben vele third-party applicaties een minimale impact op andere applicaties zoals Adobe Reader. Door een bedrijf kan dan gekozen worden om voor deze applicaties het testen minder intensief te maken of deze helemaal niet te testen (ACM Queue, 2005, p. 30). Het moet dan wel zeker zijn dat de applicatie geen problemen kan geven.
Verder wordt door Bouman (SmarTEST - Slim testen van informatiesystemen, 2008), beschreven dat, ondanks dat testen goed moet gebeuren, het ook zo min mogelijk tijd in beslag moet nemen. Er moet getest worden wat nodig is en niet meer. Alles testen is namelijk niet reëel.

Bij het Windows update proces van AAHG is de volgende testprocedure te vinden. Systeembeheer is verantwoordelijk voor het downloaden en installeren van de patches in de acceptatieomgeving. In de acceptatieomgeving kunnen gebruikers achter een acceptatiewerkstation gewoon hun werk doen. Deze werkstations staan door het gehele pand en zijn voorzien van een sticker zodat de gebruiker weet dat het een acceptatiemachine is. Mochten er na anderhalve week geen problemen worden gemeld, dan wordt de patch verder uitgerold in de productie omgeving. Voor de servers zijn de eigenaren van de applicaties verantwoordelijk voor het testen. Door systeembeheer

wordt gemeld als de patches klaar staan op de acceptatieomgeving. Hierbij wordt gebruik gemaakt van de testvormen: Systeemtest [ST], Functionele Acceptatie Test [FAT] en Gebruikers Acceptatie Test [GAT] ook wel een gecombineerde test genoemd. De ST test of de onderliggende systemen nog stabiel draaien. De FAT controleert of de applicatie nog wel de functionaliteit biedt die verwacht wordt. De GAT wordt onbewust gedaan door gebruikers. De gebruikers werken op een machine die voorzien is van nieuwe patches en geven aan als er problemen zijn.
Het test dus precies wat nodig is; stabiliteit van de systemen, functionaliteit en acceptatie van gebruikers.

Frequentie
De frequentie van het patchen is van belang om de systemen goed up-to-date te houden. Het is belangrijk dat er een vaste frequentie bestaat zodat de systemen goed up-to-date te houden zijn zonder de beheerders te vaak bezet te houden.
In informatiebeveiligingsbeleid wordt al vermeld dat er aan de hand van de patchcriteria een deadline gesteld wordt voor het uitrollen van patches.

Het is dus goed mogelijk en geheel haalbaar dat patches eens in de maand worden geïnstalleerd. Dit is namelijk ook al het geval met de Windows updates en het valt geheel binnen het gesteld informatiebeveiligingsbeleid. Alleen de urgente patches kunnen van deze routine afwijken als het langer dan twee weken duurt voordat de volgende patchdag aanbreekt.

Minder belangrijke software kan ook eens in het kwartaal, halfjaar of jaar worden gepatcht. Dit is echter niet wenselijk, omdat het dan op de patchdagen extra druk wordt. Zoals SANS al aangaf als best practice, is het beter en gemakkelijker om up-to-date te blijven dan meerdere patches achter te lopen.

6.4 Controle op omgeving

Applicaties patchen is de uiteindelijke actie om compliant te blijven. Maar er zijn natuurlijk ook manieren om tijdelijk de veiligheid te vergroten.

Verwijderen applicaties
Applicaties die niet worden gebruikt, verouderd zijn of niet in beheer worden genomen (exoten) dienen simpelweg verwijderd te worden. Door applicaties te verwijderen vormen ze geen gevaar meer voor de infrastructuur. Deze actie zal altijd parallel lopen met patchen omdat verouderde software altijd verwijderd moet worden.

Blokkeren poorten
Een tijdelijke manier om de veiligheid te vergroten is, als de exploit bekend is, de TCP en/of UDP poorten die het gebruikt, te blokkeren in de (lokale) firewall. Met deze actie moet rekening worden gehouden dat applicaties hierdoor mogelijk niet meer werken.

Blokkeren internet
Hoewel het een extreme maatregel is, is het wel mogelijk om systemen die niet meer compliant zijn toegang tot het internet te ontzeggen. Deze maatregel zorgt er in ieder geval voor dat het systeem niet meer direct wordt aangevallen vanwege out-of-date software.

Network Access Protection
Network Access Protection [NAP] is een techniek van Microsoft om de 'health' van systemen te controleren en maatregelen te nemen als deze niet compliant zijn aan de gestelde health policy. Als een systeem non-compliant is kan ervoor gekozen worden het systeem volledig toegang te geven met logging, of het systeem beperkte toegang te geven. In dat geval zou bijvoorbeeld de toegang tot het internet kunnen worden ontzegd.
Het systeem wordt in dit geval in een apart netwerk/VLAN geplaatst waar het toegang heeft tot de remediation server. De remediation server heeft beschikking tot de benodigdheden om een systeem weer compliant te krijgen. In het geval van patch achterstand zal de server de juiste Windows updates aanbieden.

Defense in Depth
Zoals al eerder vermeld in dit document moet patchen worden gezien als de laatste verdediging van Defense in Depth. Daarbij moet niet worden vergeten dat componenten van een Defense in Depth strategie elkaar aanvullen. Dominic White (Limiting Vulnerability Exposure through effective Patch Management - a thesis, 2006, p. 2) noemt het opvangen van patchmanagement met de overige Defense in Depth componenten als *'Buying time'*, en dit is precies wat het is. Firewalls blokkeren de poorten, anti-virus scant op signatures, en de IPS kan naast signatures ook scannen met stateful protocol analysis (NIST, 2007, pp. 17-18). Maar uiteindelijk is het de patch die het probleem daadwerkelijk weghaalt (SANS, 2003, p. 5).

ISO/IEC 27002:2013
Punt twee van het behandelde ISO/IEC 27002:2013 in het vorige hoofdstuk gaf ook een aantal mogelijkheden om tijdelijk meer controle te krijgen als een patch niet doorgevoerd kan worden (ISO, 2013, p. 47):

- *'Turning off services or capabilities related to the vulnerability;*
- *Adapting or adding access controls, e.g. firewalls, at network borders;*
- *Increased monitoring to detect actual attacks;*
- *Raising awareness of the vulnerability'.*

Een aantal van deze punten werden al genoemd.

7 Situatie AAHG

De situatie AAHG beschrijft de huidige situatie van AAHG zonder te veel in detail te treden. De huidige situatie wordt in het adviesrapport gedetailleerder besproken.
De inventarisatie van de huidige situatie ('AS-IS') was de eerste stap in het onderzoek. Door de 'AS-IS' te beschrijven is er duidelijkheid gekomen over wat er allemaal speelt. In plaats van alleen naar de implementatie te kijken van third-party software, is er ook gekeken naar het proces en de techniek van de Windows patches. Het Windows proces kan namelijk goede handvaten bieden voor een nieuw proces. Om de 'AS-IS' te beschrijven is gebruik gemaakt van interviews met collega's van systeembeheer, changemanagement en informatiebeveiliging. Verder was er ook documentatie beschikbaar die het Windows update proces en de individuele ITIL processen beschreef.

Proces Windows

Bij het inventariseren van de huidige situatie is gekeken naar het Windows update proces om zo inzicht te krijgen hoe AAHG het proces voor de Windows patches heeft ingericht. Het proces wordt in het document AAHG – Proces Patchen (ABN AMRO Hypotheken Groep, 2011) beschreven.
Systeembeheer download elke maand de Critical en High Windows updates, en rolt deze uit naar de acceptatieomgeving. De download van de patches gebeurt op de woensdag na 'Patch Tuesday'. De patches worden door middel van een Functionele Acceptatie Test [FAT] getest door applicatiebeheer alvorens ze in productie worden gebracht. Bij deze tests wordt door applicatiebeheer gecontroleerd of alle applicaties in hun beheer nog in de basis werken. Als een patch problemen geeft, wordt er een rollback uitgevoerd en de patch besproken in de Change Advisory Board [CAB].
Daarnaast heeft ook de afdeling Informatiebeveiliging een hand in het update proces. Zij stellen namelijk het informatiebeveiligingsbeleid op voor het patchen. Het patch proces moet voldoen aan het gestelde beleid.

Team	Werkzaamheden
Systeembeheer	Beoordelen patches. Indienen change. Testen patches. Uitrollen patches. Controleren van patchniveau.
Applicatiebeheer	Functioneel testen van applicaties op werkstations en applicatieservers.
Changemanagement	Voortgang change bewaken.
Informatiebeveiliging	Stellen informatiebeveiligingsbeleid.

Tabel 2 Taakverdeling Windows patch proces. Aangepast van AAHG – proces patchen (p. 3) door AAHG, 2011

Proces third-party software

Binnen AAHG is er een vraag naar een nieuw patchproces dat de third-party software onder handen moet nemen.
De third-party software is momenteel op geen enkele manier voorzien van een proces. Beheerders moeten nu zelf in de gaten houden welke applicaties nieuwe updates hebben, en deze dan met de hand downloaden en in productie brengen. Momenteel worden alleen patches gedownload als het risico kritiek is. Daarnaast worden voornamelijk alleen security updates gedownload. Verder komt het ook voor dat updates niet worden getest en direct in productie worden gebracht (Hamelers, 2013).

Techniek
voor de Windows updates wordt gebruik gemaakt van WSUS in combinatie met SCCM 2012. Hierin download WSUS de updates en worden deze met SCCM gedistribueerd. Verder maakt AAHG gebruik van App-V om software, anders dan de Windows updates, virtueel aan te bieden. Er is dus geen software aanwezig die kan notificeren als er third-party software patches beschikbaar zijn, of deze kan downloaden.

Implementatie ITIL
Binnen de AAHG wordt gebruik gemaakt van ITILv3. Het is ontstaan naar aanleiding van de behoefte voor een standaardaanpak op het gebied van IT-services, en moest onafhankelijk zijn van leveranciers. De huidige processen van AAHG, zoals die voor de Windows updates, zijn gebaseerd op ITIL. In het informatiebeveiligingsbeleid wordt het gebruik van change management op basis van ITIL ook vermeld. Het is dus voor de IT organisatie gemakkelijk als het nieuwe proces ook op ITIL gebaseerd is. De drie ITIL processen: change-, release-, en configurationmanagement die nodig zijn voor het uitrollen van patches, zijn al aanwezig binnen AAHG. Bij AAHG zijn change- en releasemanagement samengevoegd. De processen worden dus bewaakt door een team. Het changeproces beschrijft de stappen die doorlopen moeten worden om op een gecontroleerde manier een wijziging, zoals een patch, in het IT landschap door te voeren. Een change wordt eerst geanalyseerd en beoordeeld voordat de change wordt gepland en uitgevoerd. Het releaseproces is binnen AAHG met name van toepassing op nieuwe software en patches. In dit proces moet de software eerst worden gepackaged en worden getest in acceptatie voordat dit door mag naar productie. Dit loopt samen met het changeproces omdat er bij het naar productie brengen sprake is van een change. Deze processen worden ondersteund door configurationmanagement en de Configuration Management Database [CMDB]. De CMDB levert accurate en verifieerbare informatie over de componenten van de ICT-dienstverlening. Verder wordt er met configurationmanagement gezorgd dat de CMDB ten alle tijden up-to-date is. Ook software wordt opgenomen in het CMDB. Hierdoor weet AAHG welke software met welke versie nog in productie is.

7.1 Knelpunten

Het project komt voort uit de gehele ICT, aangezien de hele ICT organisatie, en uiteindelijk de hele AAHG gebruikersorganisatie, er baat bij heeft. Daarom is het duidelijk dat de ICT organisatie verantwoordelijk is voor het ontbreken van het proces. Er zijn in het verleden pogingen geweest een proces van de grond te krijgen, zonder succes. De knelpunten zijn te verdelen in een kernprobleem en vier symptomen.
Het kernprobleem is dat AAHG geen geaccordeerd en geïmplementeerd proces heeft voor het patchen van third-party software. De symptomen van het kernprobleem zijn:

- Af en toe ‘patch and pray’ stijl;
- Geen controle op de omgeving;
- Geen geautomatiseerde oplossing voor downloaden third-party software updates;
- Geen ‘echte’ duidelijkheid welke software onder third-party software valt;
- Onduidelijkheid waar de verantwoordelijkheid ligt voor third-party patchmanagement.

8 Methodes en resultaten

Dit hoofdstuk beschrijft de acties de ondernomen zijn met de gebruikte methoden en de resultaten die daaruit gekomenen zijn.

8.1 Literatuuronderzoek

Nadat de huidige situatie geïnventariseerd was, was er meer kennis vereist over het onderwerp patchen. Deze kennis zal dienen als basis voor het beantwoorden van de onderzoeksvragen. Om deze kennis te vergaren is er een literatuuronderzoek uitgevoerd. Voor het literatuuronderzoek zijn verschillende bronnen gebruikt in de vorm van white papers, thesissen en boeken. Dit resulteerde in de theorie die te vinden is in hoofdstuk 6. De kern die duidelijk werd, was dat third-party patches net zo belangrijk zijn als de patches die worden aangeboden door Microsoft.
Van de third-party applicaties zijn met name browsers, Adobe en Oracle producten kwetsbaar voor aanvallen. Dit zijn applicaties die veelvuldig gebruikt worden en dus op een grote meerderheid van de computers te vinden zijn.
Uit de resultaten van het literatuuronderzoek werd ook duidelijk dat:

- Patchen volledig moet gebeuren, alle systemen die in aanmerking komen, moeten gepatcht worden;
- Andere security componenten ondersteunen het patchen.

'Best practice'
Voor de best practices werd gekeken naar onder andere ITIL, ISO 27002 en verschillende white papers. Kenmerkend was dat iedereen het op twee punten eens is. Bij het uitrollen van patches moet er goed getest worden en patchen moet frequent gebeuren. Bij het testen komt verder naar voren dat er ook niet te veel getest moet worden. Alleen de basis is nodig.
Verder is een nieuw proces op basis van ITIL de beste manier. Het wordt al door AAHG gebruikt en ook het Windows patch proces is hier op gebaseerd.

Frequentie en testen
Voor de onderdelen testen en frequentie is verder gesproken met een van de changemanagers die ook ervaring had als testmanager.
Hieruit werd duidelijk dat voor de frequentie eens in de maand de beste actie was. Het sluit aan bij het informatie beveiligingsbeleid en biedt de beste balans tussen up-to-date en werkbelasting.
Ook is overeengekomen dat het patchen van de third-party applicaties en de Windows patches het beste gescheiden kan blijven. Bij problemen in sommige situaties wordt het troubleshooten gemakkelijker door de twee gescheiden te houden. Daarnaast is het vanuit het changeproces niet wenselijk twee changes op dezelfde systemen uit te voeren. Het testproces zal verder lijken op die van het Windows update proces.

Het testen moet gebeuren op de onderdelen die nodig zijn. Net zoals bij de Windows patches zijn dit: het onderliggende systeem, de functionaliteit van de applicatie en de gebruikers acceptatie. Nazorg zou gedaan kunnen worden met een PAT [Productie Acceptatie Test], maar is minder wenselijk bij third-party patches aangezien er dan te veel wordt getest.

In het geval van third-party applicaties moet er wel onderscheid worden gemaakt tussen normale applicaties en platformapplicaties zoals Java. Platformapplicaties ondersteunen andere applicaties en kunnen daardoor niet op zichzelf getest worden. Om een patch te testen voor een platformapplicatie moet de applicatie die gebruik maakt van de platformapplicatie getest worden. Voorbeeld hiervan is een website die gebruik maakt van Java. Java wordt hier niet getest op functionaliteit, maar de website.

Notificatie
Voor het ontvangen van notificaties zijn verschillende mogelijkheden beschikbaar. Om notificaties te ontvangen die zijn gericht op alleen de applicaties die aanwezig zijn, kan het beste software gebruikt worden. Deze software is met name verwerkt in vulnerabilitymanagementsoftware en patchmanagementsoftware.

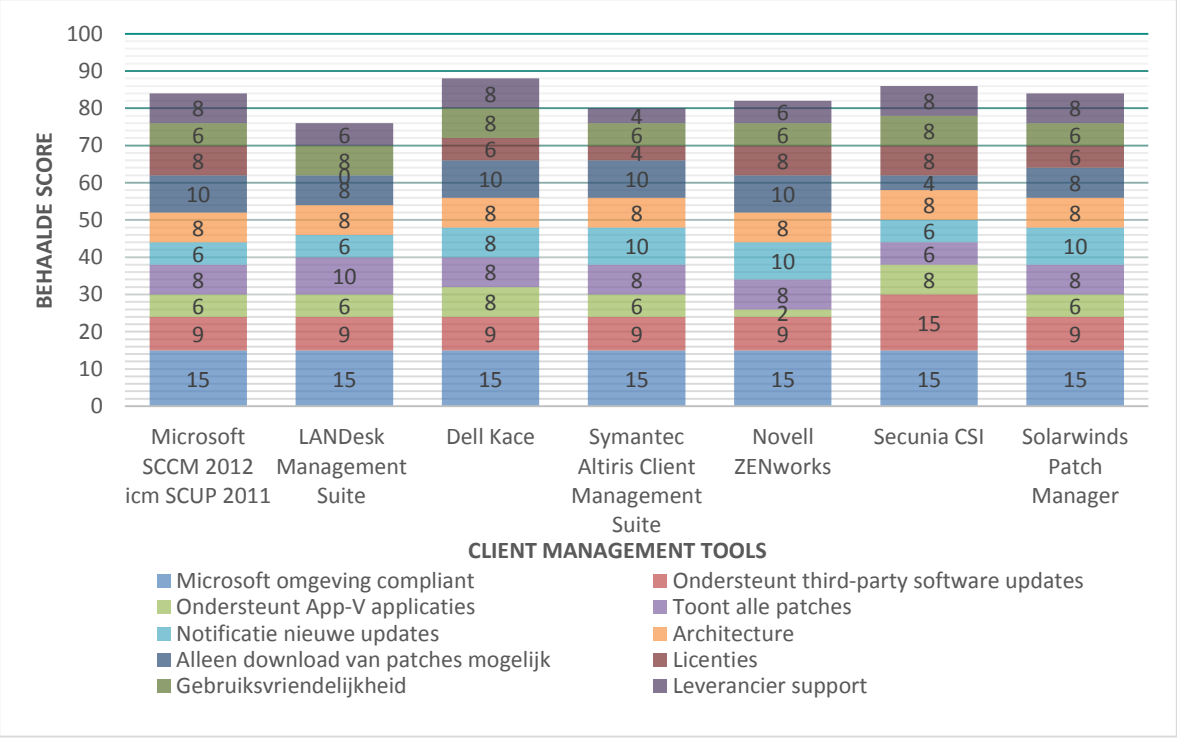
8.2 Pakketselectie

Binnen AAHG wordt gebruik gemaakt van Microsoft SCCM voor het distribueren van Windows patches. Omdat SCCM zelf geen third-party patches kan downloaden, is er een marktonderzoek gehouden naar een pakket dat SCCM kan vervangen en wel third-party patches kan downloaden. De focus van de pakketselectie lag wel op de patchmogelijkheden. Gartner heeft zelf al een onderzoek gehouden naar client management tools en uit hun Magic Quadrant zijn pakketten gekozen uit de verschillende kwadranten. Hier is bewust gekozen voor bedrijven die meer bekent zijn. Dit omwille van de tijd dat het kost om elk pakket te behandelen. Verder zijn er ook twee patchmanagement pakketten gekozen die bekend zijn. Het zijn deze pakketten waaruit de long list zal bestaan. Uit de long list worden de drie hoogst scorende pakketten gekozen voor de short list. Uit de short list wordt, omwille van de beperkte tijd, één pakket gekozen die in een PoC verder wordt getest. Om tot deze keuze te komen worden de resultaten van de pakketten uit de short list naast elkaar gehouden. Het beste allround oplossing voor AAHG wordt gekozen voor de PoC. Voor het marktonderzoek wordt er gebruik gemaakt van de COWS [Criteria, Options, Weights en Scores] methode. Deze methode is gebruikt vanwege de gewichten die aan de criteria worden gegeven om zodoende een betere uitslag te krijgen. De criteria en gewichten werden voor acceptatie voorgelegd aan Infra- & Systeembeheer. Alleen de gewichten zijn hierdoor iets bijgesteld. Informatie van de producten waren de papers die de leverancier aanboden, bevindingen van Gartner en reviews van gebruikers. De producten worden dan beoordeeld op de criteria en voorzien van een cijfer van 1 t/m 5, waarin 1 zeer slecht is en 5 zeer goed. Een nul geeft aan dat er geen informatie gevonden kon worden. De score voor elk criterium wordt als volgt berekend: $score = gewicht \times cijfer$.

Figuur 3 Magic Quadrant van gartner

Criteria	Gewicht
Microsoft omgeving compliant	3
Ondersteunt third-party software updates	3
Ondersteunt App-V applicaties	2
Toont alle patches	2
Notificatie nieuwe updates	2
Architectuur	2
Alleen download van patches mogelijk	2
Licenties	2
Gebruiksvriendelijkheid	2
Leverancier support	2

Tabel 3 Criteria en gewicht voor marktonderzoek



Tabel 4 Decision matrix met de uitslagen van het marktonderzoek

In tabel 4 is de uitslag te zien van de long list. Hierin scoorde Dell het hoogst, gevolgd door Secunia. Microsoft deelt samen met Solarwinds de derde plek. Dit is dan ook de short list. De behaalde scores van de pakketten liggen wel dicht bij elkaar aangezien alle pakketten dezelfde functionaliteit bieden maar het net anders implementeren. Daarnaast speelt de duidelijkheid van de aangeleverde documentatie ook een rol.

Uit de shortlist is gekozen voor Secunia CSI om in een PoC verder te behandelen. Secunia ondersteund vele applicaties, kan App-V pakketten scannen en integreert met WSUS en SCCM.
Dell Kace is een appliance en kan niet op korte termijn worden aangevraagd en worden geplaatst in het netwerk voor een PoC. Microsoft viel af vanwege de omslachtige manier om catalogs aan te maken. Dit kwam in verschillende reviews telkens naar voren

als de grote zwakte van SCUP (Anoop's, 2013). Solarwinds heeft geen ondersteuning voor App-V en de console kan druk overkomen.

Verder is er door de afdeling informatiebeveiliging een alternatieve oplossing genoemd, vulnerabilitymanagement software. Deze software is gericht op het inzicht geven van de compliance van systemen en kan dus geen software downloaden. Hoewel het een goed alternatief is om de patch compliance te zien, kan patchmanagementsoftware dit ook en meer.

Voor pakketselectie is ook IT Development aangesproken.
De architecten gaven aan dat het kiezen van nieuwe software een project op zich is. De bevindingen van de PoC en de voorkeur van de afdeling Infra- & Systeembeheer zullen ter advies worden aangeboden.

Voor meer details van het marktonderzoek wordt verwezen naar het adviesrapport, dat te vinden is in de bijlage.

8.3 Proof of Concept

Secunia CSI is met een Proof of Concept verder beoordeeld. Het doel van de PoC is om te zien of Secunia geschikt is als patchsoftware. Verder zullen de resultaten ook meer kunnen zeggen over patchsoftware in het algemeen. Secunia CSI wordt met de PoC getest op de volgende punten:

- Integratie;
  Het pakket werkt goed binnen de omgeving en kan ook integreren met SCCM.
- Gebruiksvriendelijkheid;
  Het pakket is overzichtelijk en gemakkelijk in gebruik. De gewenningsperiode is kort.
- Handmatige download patches;
  Patches kunnen handmatig worden gedownload.
- Handmatige packaging;
  Patches kunnen handmatig worden gepackaged.
- Ondersteunt App-V packages;
  Het pakket kan ook App-V packages scannen op versie.
- Notificatie;
  Het pakket heeft de mogelijkheid om notificaties te sturen als bijvoorbeeld nieuwe patches beschikbaar zijn.
- Informatie is daadwerkelijk versleuteld.
  Informatie dat verstuurd wordt naar de Secunia cloud is daadwerkelijk versleuteld.

Ook deze punten zijn net zoals de criteria van het marktonderzoek voorgelegd aan de afdeling Infra- & Systeembeheer.

Secunia CSI kan op verschillende manieren worden geïmplementeerd. Voor de PoC werd gebruik gemaakt van de agentless-scan in combinatie met de SCCM software inventory tool. De agentless-scan houdt in dat er op de client geen Secunia agent aanwezig hoeft te zijn om de client te kunnen scannen. Er wordt gebruik gemaakt van de Com+ System Application service in combinatie met een Remote Procedure Call om informatie te verkrijgen. Alternatief kan de software inventory agent van SCCM gebruikt worden om

informatie te vergaren. De keuze voor de agentless-scan in combinatie met de software inventory agent is dat AAHG gebruik maakt van SCCM voor de uitrol van Windows patches. Met de integratie van Secunia kan SCCM breder worden ingezet doordat patchen van third-party applicaties dan ook via SCCM loopt. Verder is het voordeel van de agent-less scan dat er geen extra agents geïnstalleerd hoeven te worden op de client. Nadelig is dat de agent-less scan minder goed kan omgaan met laptops en smartphones. Hiervoor kan beter een agent gebruik worden voor de beste resultaten.

De PoC is uitgevoerd in de testomgeving waar al een SCCM server klaar stond. Verder is er een werkstation gebruikt waar de patches op uitgerold konden worden.
Aan de hand van de technical user guide van Secunia is de PoC gestart. Zo is er eerst voor gezorgd dat de server en het werkstation voldeden aan de technische eisen die gesteld werden door Secunia. Vervolgens is Secunia CSI geconfigureerd om samen te werken met WSUS en SCCM.
Gelijktijdig met het installeren van Secunia CSI is ook Wireshark geïnstalleerd op de SCCM server. Wireshark biedt de mogelijkheid om alle netwerkpakketten die langs de server komen op te vangen voor analyse. Voor het scannen van App-V pakketten is Microsoft's SFT View geïnstalleerd. Omdat de bovengenoemde testpunten scannen, downloaden, packagen en distribueren omvatten, kon door het scannen en patchen van de werkstation alle punten een-voor-een worden behandeld.

De PoC heeft een gemengde indruk achtergelaten. Alle testpunten zijn beantwoord en is over het geheel gezien positief. Voor details van de resultaten wordt verwezen naar hoofdstuk 9.3 van het adviesrapport. Secunia CSI geeft goed weer wat de kracht is van patchmanagementsoftware. De mogelijkheid om systemen te scannen en vervolgens de juiste patches in de console te downloaden is zeker wenselijk in een bedrijfsomgeving. Verder konden patches handmatig worden gedownload en worden gepackaged. Het package systeem biedt de mogelijkheid om pre-set opties te gebruiken of om handmatig het installscript aan te passen. Het installscript wordt door PowerShell, Javascript en VBscript ondersteund. Ook de notificaties werken goed en kunnen per email of sms worden ontvangen. Met Wireshark was te zien dat alles goed beveiligd was. Er is een pakket teruggevonden met de RSA 256-bit key exchange. Vanaf dat moment waren er alleen maar HTTPS en TLSv1 naar en van Secunia te vinden.
Ook het scannen naar App-V applicaties is mogelijk als SFT View geïnstalleerd is.

Een belangrijk nadeel van Secunia is de trage console. Verder is er soms ook een erg grote vertraging tussen nieuwe scanresultaten en het updaten van de overige componenten zoals het dashboard en de aangeboden patches. Secunia CSI mag dan wel goed integreren met SCCM en WSUS, maar er wordt met name voor de distributie erg zwaar geleund op WSUS. Dit is niet wenselijk met een SCCM implementatie. De patches komen namelijk niet in de software library van SCCM terecht. Ook worden de patches aangeboden via Windows Update in plaats van SCCM software center.
Ook is de ondersteuning van verschillende applicatieversies niet optimaal. Zo werd Cisco Jabber 9.0.2 wel gevonden, maar werd er geen patch aangeboden. Na controle bij Secunia bleek dat alleen versie 8 van Jabber was opgenomen in de database van Secunia.

9 Conclusies en aanbevelingen

In dit hoofdstuk worden de uiteindelijke antwoorden op de hoofd- en deelvragen gegeven.

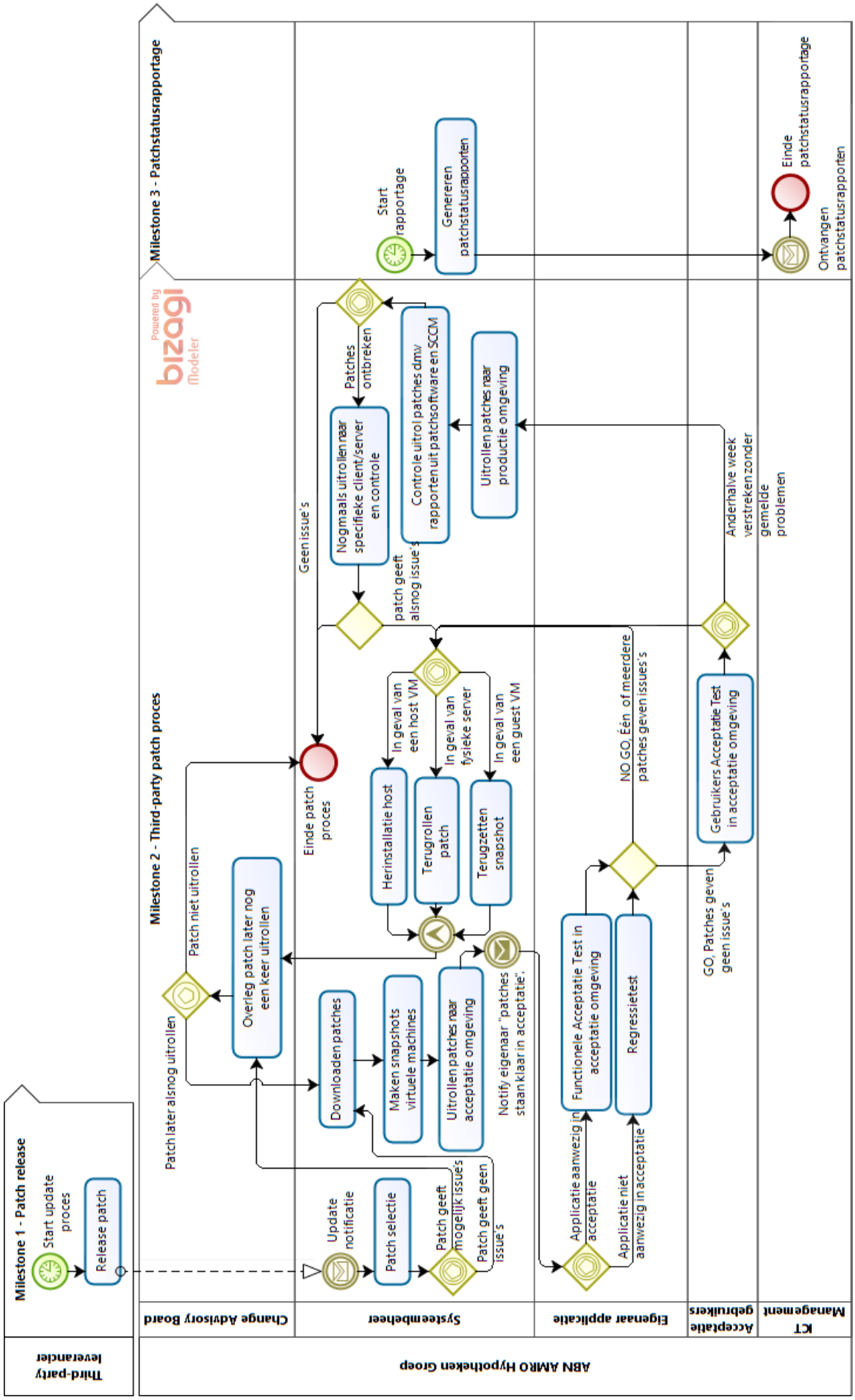
Tegenwoordig worden third-party applicaties, net zoals Microsoft producten, veelvuldig aangevallen. Met name Java en Adobe producten zijn vaak betrokken bij een aanval. Dat blijkt uit het literatuuronderzoek.
Hoewel een goede implementatie van firewalls en anti-virusscanners vele aanvallen tegen kunnen houden, is de patch de laatste lijn van verdediging en de enige manier om een aanval te voorkomen door de oorzaak van het probleem weg te halen.

Een nieuw proces is nodig. Uit de situatie van AAHG wordt duidelijk dat er momenteel geen patchproces voor third-party applicaties aanwezig is. Hierdoor lopen vele applicaties achter op patches. Als een nieuwe exploit zodanig ernstig is, dan wordt de applicatie wel gepatcht. Ook komt het voor dat de patches niet worden getest voordat ze in productie gaan. Verder moet systeembeheer zelf op de hoogte blijven van nieuwe patches en deze ook handmatig downloaden. Distributie gebeurt wel via de SCCM omgeving.

Om een proces te beschrijven zijn er 'best practices' nodig om de verschillende stappen in te vullen. In het literatuuronderzoek kwam naar voren dat ITIL, het informatiebeveiligingsbeleid en de ISO normering al goede handvaten geven voor het inrichten van een patchproces. Bij ITIL zijn dan met name change-, release- en configurationmanagement betrokken. Verder zijn er vele informationsecurity bedrijven die ook aangeven dat patchen van de third-party applicaties erg belangrijk zijn. Verder werd uit het literatuuronderzoek duidelijk met name de frequentie en goed testen van de patches van belang zijn.
Als laatste is er gekeken naar het huidige Windows patchproces. Dit proces is al gebaseerd op ITIL dat door AAHG gebruikt wordt en heeft zich al bewezen. Dit is een goede fundering voor een nieuw proces. AAHG maakt dus al gebruik van ITILv3. De drie processen die van belang zijn voor het patchen zijn ook volledig aanwezig binnen AAHG. De processen change- en releasemanagement zijn samengevoegd en worden door een team bewaakt. Configurationmanagement vervult een meer ondersteunende rol door het aanbieden van informatie vanuit de CMDB.

Het moet ook duidelijk zijn wat er precies wordt gepatcht.
De term third-party is dan ook erg generiek. Het omvat alle applicaties die op een Windows machine draaien en niet van Microsoft zijn. Third-party applicaties die momenteel aanwezig zijn en direct met het proces gepatcht moeten worden zijn Adobe Flash Player, Adobe Reader en Java RE. Uiteindelijk is het de bedoeling dat alle third-party applicaties worden gepatcht met het nieuwe proces.

Het nieuwe proces kan het beste worden gebaseerd op het Windows patch proces. Het Windows patchproces is al op ITLv3 gebaseerd en heeft zich al bewezen. Voor de third-party applicaties moet de testprocedure wel iets anders worden ingericht. Platformapplicaties moeten namelijk iets anders worden getest dan de normale applicaties. Gebaseerd op het Windows patchproces zal het nieuwe proces er als volgt uit komen te zien:



Figuur 4 Third-party patchproces

De stappen van het proces zijn als volgt:

- **Patch selectie;**
  Er wordt bij het patchen gekeken of specifieke patches problemen gaan geven. deze worden eerst niet meegenomen en in het CAB besproken. Het CAB zal bepalen of de patches alsnog wordt uitgerold of niet. Verder worden snapshots gemaakt van de VM's voor een gemakkelijke rollback.

- **Patches testen;**
  Patches worden uitgerold in de acceptatieomgeving en worden getest met drie verschillende tests; ST, FAT en GAT.

- **Patches uitrollen;**
  Als er na anderhalve week geen problemen worden gemeld, kunnen de patches worden uitgerold in de productieomgeving. Voor eventuele reboot kan het volgende worden aangehouden:

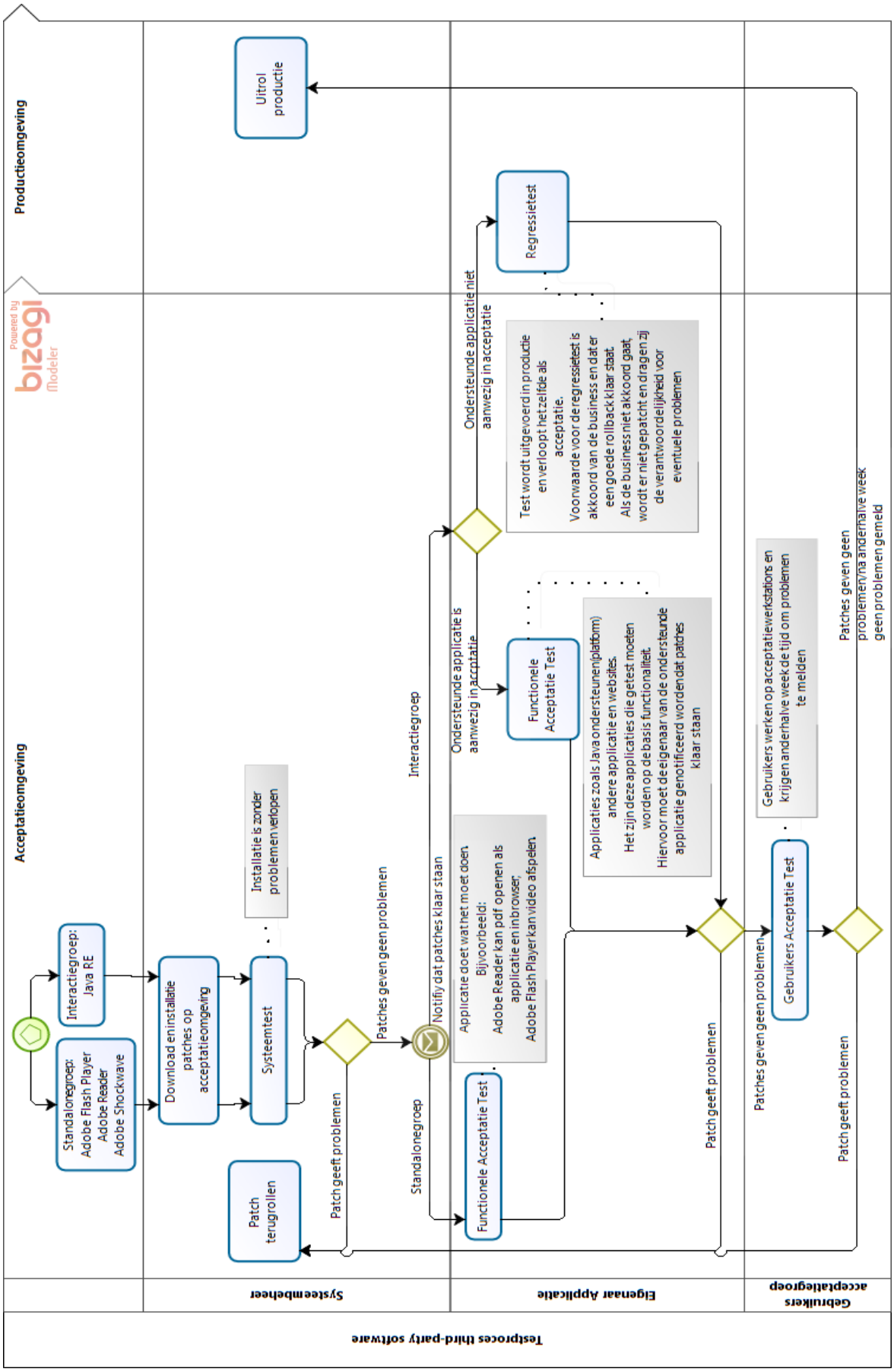
  Werkstations
  Werkstations worden in principe aan het einde van de dag afgesloten. Dit werkt dan ook als de reboot voor nieuwe updates.
  Servers
  Niet business kritieke servers, zoals beheerservers, kunnen gewoon overdag worden gereboot. Business kritieke servers worden buiten productietijd gereboot.

- **Rollback (overig);**
  Als er een rollback nodig is kan er in het geval van VMs de snapshot worden terug gezet. De host VM kan het beste opnieuw worden ingespoeld aangezien een rollback risicovol is. Op de fysieke servers kan de patch worden teruggedraaid.

- **Rapportage.**
  Nadat de patches zijn uitgerold, wordt er met SCCM en de gekozen patchsoftware een compliance report gemaakt en verzonden naar het IT management.

Het proces dekt alle punten die door ITIL's change- en releaseproces beschreven worden.
Aangezien er 6 weken de tijd is om een patch met hoge prioriteit uit te rollen, is een frequentie van een maand het beste. Het is binnen de tijd van de hoge prioriteit en makkelijker in te plannen. De vierde dinsdag in de maand (week na afronding van het Windows patchproces) is hier een goede dag voor.

Het testen moet alle vlakken dekken zonder teveel te testen. Teveel testen neemt teveel tijd in beslag. De vlakken die bij een patch getest moeten worden, zijn het systeem voor stabiliteit, de applicatie voor functionaliteit en acceptatie door gebruikers. Dit voorkomt problemen die de productieomgeving kunnen verstoren. Voor de testprocedure houdt dit in dat er getest moet worden met een ST, FAT en GAT. Omdat platformsoftware niet direct getest kan worden, moet dit getest worden via de applicaties die gebruik maken van de platformsoftware. De testprocedure komt dan als volgt eruit te zien:



Figuur 5 Testprocedure

De testprocedure gaat ervan uit dat de applicaties die getest worden aanwezig zijn in de acceptatieomgeving. Voor de applicaties die op werkstations aanwezig zijn is dit dan ook geen probleem. Wel kan het voorkomen dat applicaties die ondersteund worden door Java niet aanwezig zijn in de acceptatie omgeving. Het project OTA loopt nog en het is niet duidelijk of alle applicaties daarin vertegenwoordigd gaan worden. Voor deze applicaties kan dan geen FAT worden uitgevoerd en moet er met een regressietest de patch worden getest. De regressietest vind plaats in de productieomgeving en mag alleen worden uitgevoerd in overleg en goedkeuring van de business en moet er een rollback mogelijk zijn.
Het wordt AAHG aangeraden om het beschreven proces met de genoemde frequentie en testprocedure zo snel mogelijk te implementeren.

Het is aan te bevelen om patchmanagement software te implementeren als ondersteuning van het proces. Ondanks patchsoftware nog in volle ontwikkeling is, biedt het een goede aanvulling voor het vergemakkelijken en deels automatiseren van het patchproces. De software zorgt ervoor dat geïnstalleerde applicaties kunnen worden gescand en geëvalueerd op versie. Vervolgens biedt de software de nieuwste patch aan die dan gedownload, gepackaged en gedistribueerd kan worden.
Patchmanagement software biedt ook de mogelijkheid om notificaties te ontvangen als nieuwe patches beschikbaar zijn. Het voordeel van software die de notificaties stuurt is dat het altijd gericht is op de applicaties die aanwezig zijn.

Uit de pakketselectie komt naar voren dat Secunia CSI een goed product is voor de omgeving van AAHG. Het biedt namelijk meer ondersteuning voor verschillende applicaties en kan overweg met .sft bestanden dat door App-V wordt gebruikt. Dat blijkt uit de pakketselectie.
In de PoC liet Secunia CSI zien dat het goed integreert met WSUS en SCCM, makkelijk te bedienen is en goede informatie kan weergeven over de compliance. Het vergemakkelijkt aanzienlijk het downloaden en packagen van patches. Verder kan Secunia meldingen geven via email en sms. Notificaties konden verder op verschillende groepen worden ingesteld. Wel wordt aangeraden om de SCCM plug-in van Secunia te proberen in plaats van Secunia CSI zelf. De plug-in integreert met SCCM waardoor het patchen in een console kan gebeuren (die van SCCM). Hiervoor moet mogelijk een nieuw project worden opgestart, waarin IT Development bij wordt betrokken. Zij gaan namelijk over het aandachtsgebied ontwikkeling, dat de start is voor projecten.

9.1 Toekomstige projecten

Na de implementatie van het nieuwe proces, kan er gekeken worden naar andere projecten die de veiligheid vergroten.

Patchmanagementsoftware
Patchmanagementsoftware moet gekozen worden om het third-party patchproces te ondersteunen en deels te automatiseren. Hiervoor moet een diepgaander project worden opgezet waar ook IT Development bij betrokken wordt. Zoals in het advies al vermeld zou de SCCM plug-in van Secunia zeker overwogen moeten worden. Het heeft met de PoC veel potentie getoond.

Remote remediation
Met de komst van het nieuwe werken en Bring Your Own Device [BYOD] wordt het in stand houden van het bedrijfsbeleid omtrent de security steeds lastiger. Hoewel NAP en andere remediation oplossingen niet wenselijk zijn op kantoor, wordt er wel door vele werknemers thuisgewerkt. Hiervoor wordt gebruik gemaakt van Citrix XenDesktop. Hoewel de verbinding van XenDesktop goed beveiligd is, is dit meestal niet het geval van een thuis computer. Om ook de thuis computer te beveiligen kan er gebruik worden gemaakt van Citrix Access Gateway Endpoint Analysis. De Endpoint Analysis draait een scan voordat de client daadwerkelijk verbinding mag maken. Hier wordt de client gecontroleerd op onder andere aanwezige security software, malware, geen peer-to-peer file sharing en dat het besturingssysteem gepatcht is. Alleen als de client hieraan voldoet wordt er een verbinding opgezet met XenDesktop. Als er niet wordt voldaan, kan de client worden doorgestuurd naar een remediation server waar de problemen verholpen kunnen worden (Citrix, z.j.).

Vendor patching
Naast de Windows en Third-party patches, zijn er ook andere appliances en devices aanwezig die gepatcht moeten worden. Voorbeelden hiervan zijn de Cisco switches, Cisco Routers en Blackberries die worden gebruikt. Ook hiervoor dient een patchproces voor te zijn.
Bij het opstellen van zo'n proces moet er gelet worden op onder andere de frequentie en testmethodes. Zo zullen patches van Blackberry niet intensief getest hoeven te worden, maar die voor netwerkapparatuur wel.

10 Bibliografie

ABN AMRO. (2011, 06 08). *Patch management Informatiebeveiligingsbeleid*. Opgehaald van kennisportal.aahg.nl: http://kennisportal.aahg.nl/InformatieBeveiliging/beleid/Operationele%20Beveiligingsvoorschriften/Patch%20management.aspx

ABN AMRO Hypotheken Groep. (2011, 12 05). *AAHG - Proces Patchen V1.1.doc.* Amersfoort. Opgeroepen op 08 15, 2013, van Kennisportaal AAHG.

ABN AMRO. (z.j.). *ABN AMRO Hypotheken Groep*. Opgeroepen op mei 27, 2013, van abnamro.com: http://www.abnamro.com/nl/about-abn-amro/subsidiaries/hypotheken-groep.html

ABN AMRO. (z.j.). *ABN AMRO Hypotheken Groep*. Opgeroepen op mei 27, 2013, van abnamro.com: http://www.abnamro.com/nl/about-abn-amro/subsidiaries/hypotheken-groep.html

ABN AMRO. (z.j.). *Geschiedenis*. Opgeroepen op mei 27, 2013, van abnamro.com: http://www.abnamro.com/nl/about-abn-amro/history/index.html

ABN AMRO. (z.j.). *Missie & visie*. Opgeroepen op mei 27, 2013, van abnamro.com: http://www.abnamro.com/nl/about-abn-amro/subsidiaries/mission.html

ACM Queue. (2005, 03 01). *Understanding Software Patching.* Opgeroepen op 10 31, 2013, van queue.acm.org: http://portal.acm.org/ft_gateway.cfm?id=1053343&type=pdf

Adobe. (z.j.). *Adobe - Security Notification Service*. Opgehaald van adobe.com: http://www.adobe.com/cfusion/entitlement/index.cfm?e=szalert

Anoop's. (2013, 01 18). *ConfigMgr SCCM Patch Management Pros and Cons*. Opgeroepen op 10 11, 2013, van anoopcnair.com: http://anoopcnair.com/2013/01/18/configmgr-sccm-patch-management-pros-and-cons/

Bon, J. v., Jong, A. d., Kolthof, A., Pieper, M., Tjassing, R., Veen, A. v., & Verheijen, T. (2007). *Best Practice: Foundations van ITIL® V3.* Zaltbommel: Van Haren publishing.

Bosworth, S., Kabay, M. E., & Whyne, E. (2009). Computer Security Handbook. In S. Bosworth, M. E. Kabay, & E. Whyne, *Computer Security Handbook* (5de ed., p. 41). Hoboken, NJ, USA: John Wiley & Sons, Inc.

Bouman, E. (2008). *SmarTEST - Slim testen van informatiesystemen.* Den Haag: Sdu Uitgevers bv. Opgehaald van http://books.google.nl/books?id=63kZmb1IwA0C&pg=PA95&lpg=PA95&dq=st+fat+gat&source=bl&ots=QRqmUt1Xfw&sig=dLp23kpKLXciu7IA7kGTWb_c6CE&hl=nl&sa=X&ei=PimGUrf6M-aN4wTkvoCADg&ved=0CEcQ6AEwAw#v=onepage&q=st%20fat%20gat&f=false

Cooper, R. (2003, 01 28). *Confusion about versions*. Opgeroepen op 10 03, 2013, van archives.neohapsis.com: http://archives.neohapsis.com/archives/ntbugtraq/2003-q1/0045.html

CVE Details. (z.j.). *Vulnerability Feeds & Widgets*. Opgehaald van cvedetails.com: http://www.cvedetails.com/vulnerability-feeds-form.php

Fast Project Plans. (z.j.). Opgeroepen op augustus 6, 2013, van fastprojectplans.com: http://www.fastprojectplans.com/images/risk-management-plan-clip1.gif

Fisher, E. (2011, 03 28). *Top 3 Patch Management Do's and Don't*. Opgehaald van gfi.com: http://www.gfi.com/blog/top-3-patch-management-dos-donts/

F-Secure. (2013, 04 18). *Companies Risking Their Assets With Outdated Software*. Opgehaald van f-secure.com: http://www.f-secure.com/en/web/corporation_global/news-info/product-news-offers/view/story/915562/Companies%20Risking%20Their%20Assets%20With%20Outdated%20Software%20

Goktas, O., & Tomassen, M. (2013, 08 22). Inventarisatie AS-IS. (N. Boers, Interviewer)

Google. (z.j.). *Update Adobe Flash Player*. Opgehaald van support.youtube.com: https://support.google.com/youtube/answer/95402

Graff, M. G., & van Wyk, K. R. (2003). *Secure Coding Principles and Practices.* Sebastopol, CA, Verenigde Staten van Amerika: O'Reilly Media Inc.

Hamelers, O. (2013, 08 09). Inventarisatie AS-IS. (N. Boers, Interviewer)

Hedeman, B., Heemst, G. V., & Fredriksz, H. (2009). Projectmanagement op basis van PRINCE2™ Editie 2009. Zaltbommel: Van Haren Publishing.

ISO. (2013, 10 01). *ISO IEC 27002:2013.* Opgeroepen op 11 13, 2013, van scribd.com: http://www.scribd.com/doc/177330349/ISO-IEC-27002-2013

ISO. (z.j.). *About ISO - ISO*. Opgeroepen op 11 13, 2013, van iso.org: http://www.iso.org/iso/home/about.htm

Kaspersky. (2011, 08 11). *IT Threat Evolution: Q2 2011 - Securelist*. Opgeroepen op 10 25, 2013, van securelist.com: http://www.securelist.com/en/analysis/204792186/IT_Threat_Evolution_Q2_2011

Kaspersky. (2012, 11 01). *IT Threat Evolution: Q3 2012*. Opgeroepen op 09 03, 2013, van Securelist.com: http://www.securelist.com/en/analysis/204792250/IT_Threat_Evolution_Q3_2012

Micorsoft. (2002, 07 24). *Microsoft security bulletin MS02-039*. Opgeroepen op 09 02, 2013, van technet.microsoft.com: http://technet.microsoft.com/en-us/security/bulletin/ms02-039

Microsoft. (2002, 10 30). *FIX: Handle leak Occurs in SQL Server When Service or Application Repeatedly Connects and Disconnects with Shared Memory network Library*. Opgeroepen op 09 03, 2013, van support.microsoft.com: http://support.microsoft.com/kb/317748

Microsoft. (2003, 06 16). *Microsoft Security Bulletin MS03/026*. Opgeroepen op 08 29, 2013, van technet.microsft.com: http://technet.microsoft.com/en-us/security/bulletin/ms03-026

Microsoft. (2005, 10). *Win32/Blaster: A case study from microsoft's perspective.* Opgeroepen op 08 29, 2013, van Scribd: http://www.scribd.com/doc/65579/Blaster-Case-Study-White-Paper

NIST. (2007, 02). *Guide to Intrusion Detection and Prevention Systsems (IDPS).* Opgeroepen op 11 07, 2013, van csrc.nist.gov: http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

Oracle. (z.j.). *Oracle Security Alerts*. Opgehaald van oracle.com: http://www.oracle.com/ocom/groups/public/@otn/documents/webcontent/rss-otn-sec.xml

Patchmanagement. (z.j.). *patchmanagement.org*. Opgehaald van patchmanagement.org: http://patchmanagement.org/default.asp

SANS. (2003, 10 15). *Patch Me If you Can: Patch Managements Vital Role Defense-in-Depth*. Opgeroepen op 08 30, 2013, van giac.org: http://www.giac.org/paper/gsec/3390/patch-can-patch-managements-vital-role-defense-in-depth/105562

Secunia. (2013, 03 14). *Vulnerability review 2013 - The Highlights*. Opgeroepen op 09 03, 2013, van Secunia.com: http://www.secunia.com/vulnerability-review/vulnerability_update_top50.html

Security.nl. (2013, 09 11). *Microsoft trekt defecte Outlook-update terug*. Opgeroepen op 09 30, 2013, van security.nl: https://www.security.nl/posting/363090/Microsoft+trekt+defecte+Outlook-update+terug

Shavlik. (z.j.). *Shavlik Content Updates*. Opgehaald van shavlik.com: http://www.shavlik.com/support/xmlsubscribe/

The Government of Hong Kong Special Administrative Region. (2008, 02). *Patch management*. Opgehaald van infosec.gov.hk: http://www.infosec.gov.hk/english/technical/files/patch.pdf

Turner, A. (2013, 08 16). *Blaster worm: Lessons learned a decade later*. Opgeroepen op 108 29, 2013, van csoonline: http://www.csoonline.com/article/738210/blaster-worm-lessons-learned-a-decade-later?page=1

Tweakers. (2003, 02 06). *SQLSlammer is de snels verspreide worm ooit*. Opgeroepen op 09 03, 2003, van Tweakers.net: http://tweakers.net/nieuws/25392/sqlslammer-is-de-snelst-verspreide-worm-ooit.html

White, D. S. (2006, 07 02). *Limiting Vulnerability Exposure through effective Patch Management - a thesis.* Opgeroepen op 08 26, 2013, van http://singe.za.net/blog/archives/763-Limiting-Vulnerability-Exposure-through-effective-Patch-Management-a-thesis.html

ZScaler. (2012). *Q3 2012 State of the web*. Opgehaald van zscaler.com: https://www.zscaler.com/thankyou_state-of-the-web-q3-2012-inforgraphic.php

Plan van Aanpak

Releasemanagement t.b.v. third-party software

ABN AMRO Hypotheken Groep

Colofon

Documenteigenschappen

Titel	Plan-van-Aanpak AAHG Niels-Boers V3.3.pdf	Status	Definitief
Project	Afstudeerstage	Versie	V3.3
Auteur	Niels Boers	Klas	SV3A
Bedrijf	ABN AMRO Hypotheken Groep	Studentnr.	1587222

Typografische conventies

Conventie	Betekenis	Voorbeeld
AaBbCc1234	Normale tekst	Dit is een voorbeeld.
AaBbCc1234	Quotatie/motto	De missie van ICT is: *"Wij ondersteunen zorgeloos werken"*.
AaBbCc1234	Kruisreferentie in dit document	Zie hoofdstuk 2 voor meer informatie.
AaBbCc1234	Hyperlink naar website of e-mail adres	e-mail: niels.boers@aahg.nl

Revisie

Revisie	Vorige revisie	Samenvatting van wijzigingen	Versie
01-08-2013	N.v.t.	Initiële Plan van Aanpak	V0.1
05-08-2013	01-08-2013	Lay-out aangepast	V0.1.1
06-08-2013	05-08-2013	PvA naar V1.0	V1.0
13-08-2013	06-08-2013	Feedback bedrijfsbegeleider verwerkt	V1.0.1
19-08-2013	13-08-2013	Toevoeging paragraaf 3.4	V1.1
21-08-2013	19-08-2013	Verwerken feedback docentbegeleider	V2.0
28-08-2013	21-08-2013	Revisie onderzoeksvragen ↔ doelstelling	V2.1
11-09-2013	28-08-2013	Verwerking feedback docentbegeleider	V3.0
19-09-2013	11-09-2013	Verwerking feedback docentbegeleider	V3.1
30-09-2013	19-09-2013	Verwerking feedback docentbegeleider	V3.2
03-10-2013	30-09-2013	Wijziging KA → third-party + feedback bedrijfsbegeleider	V3.3

Distributie

Naam	Rol	Datum distributie	Versie
Olaf Hamelers	Opdrachtgever/begeleider	06-08-2013	V1.0
Niels Boers	Projectleider/student	06-08-2013	V1.0
Rienk van der Ploeg	Docentbegeleider	09-09-2013	V2.1
Niels Boers	Projectleider/student	09-09-2013	V2.1
Rienk van der Ploeg	Docentbegeleider	17-09-2013	V3.0
Niels Boers	Projectleider/student	17-09-2013	V3.0
Rienk van der Ploeg	Docentbegeleider	27-09-2013	V3.1
Niels Boers	Projectleider/student	27-09-2013	V3.1
Rienk van der Ploeg	Docentbegeleider	30-09-2013	V3.2
Niels Boers	Projectleider/student	30-09-2013	V3.2
Olaf Hamelers	Opdrachtgever/begeleider	03-10-2013	V3.3
Niels Boers	Projectleider/student	03-10-2013	V3.3
Rienk van der Ploeg	Docentbegeleider	09-10-2013	V3.3
Afstudeercommissie	Afstudeercommissie	09-10-2013	V3.3

Inhoudsopgave

1 Inleiding

In het voorliggende document wordt het daadwerkelijke Plan van Aanpak [PvA] besproken dat gebruikt gaat worden tijdens het afstudeerproject bij ABN AMRO Hypotheken Groep [AAHG]. Naast de beschrijving van het project zal het PvA ook dienen als referentie waaraan het eindresultaat tijdens de afstudeerzitting getoetst zal worden. Ook is het PvA onderdeel van het afstudeercontract.
Het PvA is gebaseerd op het afstudeervoorstel maar zal uitgebreider ingaan op het project en is voor het project ook bindend.

Het uiteindelijke doel van dit project is de AAHG voorzien van een advies voor het omgaan met third-party software patches, een advies over technisch de beste manier van patchen en een daadwerkelijk beschreven document waarin het updateproces wordt beschreven.
Het project wordt in 4 fases aangepakt te weten: analyse, onderzoek en ontwerp, realisatie en conclusie. Dit project wordt uitgevoerd van 1 augustus t/m 17 december 2013.

2 Context afstudeerproject

2.1 Beschrijving bedrijf/afdeling

De ABN AMRO Hypotheken Groep [AAHG] is gespecialiseerd in het verstrekken en beheren van hypotheken. Door hun jarenlange ervaring en voortdurende verbetering van hun producten en processen behoren ze tot de grootste gespecialiseerde hypotheekverstrekkers van Nederland (ABN AMRO, z.j.).

De ICT afdeling van de AAHG bestaat uit verschillende onderdelen die zich bezighouden met verschillende disciplines binnen de ICT. Deze onderdelen zijn ICT Beheer, bestaande uit de teams Infra- en Systeembeheer en Applicatiebeheer, ICT services, ICT Informatiebeveiliging en ICT Development.

De bedrijfsbegeleider van de student is naast teamleider Infra- en Systeembeheer ook de opdrachtgever voor dit project.

2.2 Relatie afstudeerproject met andere projecten

Het afstudeerproject is een opzichzelfstaand project en maakt geen onderdeel uit van andere projecten.

2.3 Relatie afstudeerproject met afdeling/organisatie

Het afstudeerproject komt als vraag voort vanuit de afdeling IT en kent ook met alle IT stafafdelingen en de Business een relatie.
Applicatiebeheer doet de werkelijke acceptatietest en is dan nodig om o.a. de frequentie en belasting van het patchen af te stemmen.
Infra- en Systeembeheer doen de implementatie van het technische onderdeel en zullen ook de patches downloaden.
ICT Services hebben een relatie met het project voor het functioneel beheer ervan.
ICT Development is nodig voor de afstemming van de Ontwikkel-, Test- en Acceptatieomgeving.
Ook is er afstemming met de business nodig voor de uitrol van de patches.

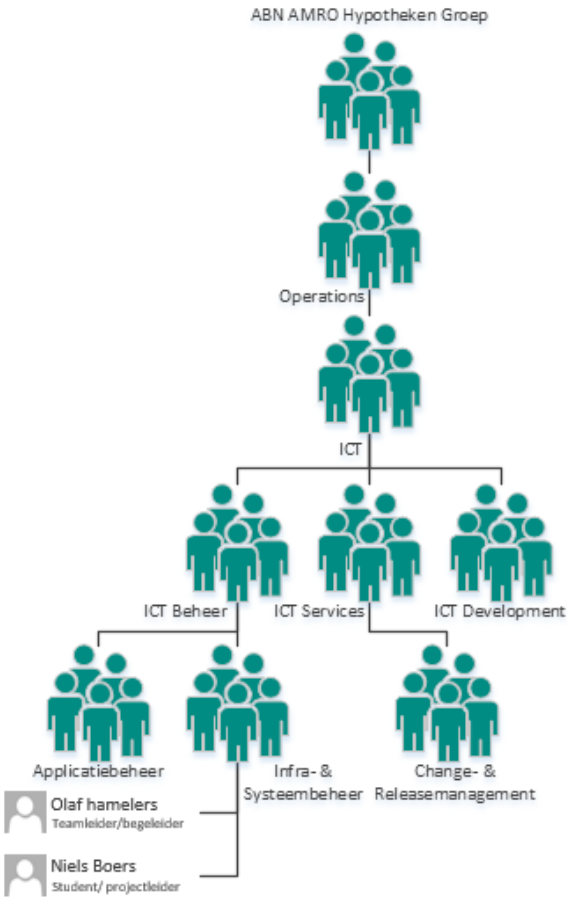
Afdeling/organisatie	Relatie met het afstudeerproject
Applicatiebeheer	Afhankelijkheden acceptatietesten
Infra- en Systeembeheer	Implementatie
ICT Services	Kantoor Automatisering Functioneel Beheer
ICT Development	Afstemming Ontwikkel, Test, Acceptatie [OTA]
Business	Uitrol

Tabel 5 Betrokken afdelingen met patchen

2.4 Positie, taken en verantwoordelijkheden student

De student zal deel uitmaken van de IT afdeling en zal zich daar bezighouden met het afstudeerproject. In het afstudeerproject is de student zowel projectleider als projectlid. Het zal aan de student liggen om het project goed te laten verlopen en contact te leggen met verschillende afdelingen binnen ICT voor informatie over de IT infrastructuur en al bestaande processen. De student werkt dus zelfstandig, maar is wel afhankelijk van de medewerking van verschillende personen binnen de ICT afdeling.
Het initiatief en uitvoering zal dus liggen bij de student. Daarmee komt ook het uiteindelijke succes van het project bij de student te liggen.

Naast het project zelf is de student ook verantwoordelijk voor het op tijd inleveren van afstudeerdocumenten zoals het Plan van Aanpak [PvA] en de uiteindelijke scriptie.
De student zal zich naast de verantwoordelijkheden voor het afstudeeropdracht ook proactief opstellen en gedragen conform de gestelde eisen van het bedrijf zelf.



Figuur 6 Projectorganisatie: Positie student en betrokken afdelingen

3 Definitie afstudeeropdracht

3.1 Probleemstelling

Binnen de AAHG zijn er naast de Windows-updates ook third-party software updates waaronder Java en Adobe Flash. Voor dit onderdeel is er echter binnen de AAHG geen geaccordeerd en geïmplementeerd proces.
Uitrol van de updates gebeurt momenteel onregelmatig en alleen patches van grote security lekken worden gelijk doorgevoerd.
Hoewel het niet patchen van de third-party software niet direct verstorend voor de productie is, bestaat er toch het gevaar van nieuwe ernstige security lekken die geëxploiteerd kunnen worden. Een oude of out-of-date versie van Java geeft bijvoorbeeld een hacker de mogelijkheid remote toegang te krijgen tot een systeem zonder dat de gebruiker zich daar bewust van is. Als een hacker eenmaal toegang heeft tot het systeem, kan hij onder andere data stelen, data verwijderen, wachtwoorden achterhalen (i.i.g. de wachtwoorden van het lokale systeem) of proberen andere systemen binnen te dringen. Door het up-to-date houden van de third-party software wordt de kans voor een aanval al een stuk minder.

3.2 Afstudeeropdracht

Voor het schrijven en implementeren van een nieuw updateproces doet de student een literatuuronderzoek naar releasemanagement en de waarde ervan. Voor het literatuuronderzoek worden o.a. wetenschappelijke bronnen zoals white papers, thesissen en andere documenten gebruikt om zodoende te komen tot nieuwe kennis die gebruikt kan worden voor het schrijven van een nieuw update proces voor AAHG.

De student heeft ook interactie met verschillende afdelingen binnen de IT om zodoende de ‘AS-IS’ situatie te inventariseren van het update proces. Ook verkrijgt de student van de verschillende afdelingen informatie, die helpt bij het schrijven van het nieuwe proces. Het nieuwe proces zal dus voortkomen uit het onderzoek en de informatie verkregen van collega’s.
Het proces wordt op het einde door middel van een PoC met minimaal één softwarepakket getest.

Naast het proces zelf wordt ook de huidige distributie software, Microsoft System Center Configuration Manager [SCCM] 2012, onder de loep genomen en wordt er gekeken naar alternatieve oplossingen om updates uit te kunnen rollen. Over deze resultaten zal de student een advies uitspreken, waaruit blijkt of SCCM de juiste keuze is of dat een ander pakket toch een betere keuze is.

3.3 Methoden

Samengevat is dit een ontwerp-/adviesopdracht. Om deze opdracht uit te kunnen voeren zal gebruik worden gemaakt van interviews, literatuuronderzoek, deskresearch, marktonderzoek en een Proof of Concept. De interviews zullen worden gehouden bij collega’s om informatie te verkrijgen over de huidige situatie en wat de visie is vanuit hun afdeling op het nieuwe proces.
Deskresearch wordt onder andere gebruikt voor de huidige situatie (al bestaande gedocumenteerde processen) en de toekomstige situatie (gebaseerd op al bestaande gedocumenteerde processen en best practices). Marktonderzoek wordt gebruikt voor het kiezen van de beste software om de updates te kunnen downloaden en uit te rollen

(informatie leverancier, wensen en eisen bedrijf en reviews van onafhankelijke partijen). Het marktonderzoek zal tevens gebruikmaken van een decision matrix.
Literatuuronderzoek wordt gebruikt om de onderzoeksvragen te kunnen beantwoorden aan de hand van white papers, thesissen en andere documenten. Als laatste wordt er een Proof of Concept uitgevoerd om het proces en de gekozen distributie software te testen.
Bepaalde beheersmechanismen worden gebaseerd op de beheermethodiek van PRINCE2.

3.4 Doelstellingen

Aan het einde van het project zijn de volgende onderdelen gerealiseerd:

- Een advies hoe AAHG het beste kan omgaan met third-party software patches;
- Een gedocumenteerd updateproces voor de third-party software;
- Een advies over technisch de beste manier van patchen en met welke updatesoftware, getest door een Proof of Concept.

3.5 Onderzoeksvragen

Dit project kent onderzoeksvragen bestaande uit een hoofdvraag en een aantal deelvragen. Deze vragen zullen in de loop van het project worden beantwoord. Deze informatie zal dan worden gebruikt om te komen tot het eindresultaat.

Hoofdvraag:

- Wat is de beste methode voor het uitrollen van third-party software updates, zowel procesmatig als technisch?

Deelvragen:

- Waarom is het nodig om third-party software regelmatig te updaten?;
- Welke ‘best practices’ zijn er voor patchmanagement?;
- Waaruit bestaat het huidige updateproces voor de third-party software?;
- Op welke manier is ITIL geïmplementeerd met betrekking tot change- release- en configuratiemanagement?;
- Welke softwarepakketten komen voor het te ontwerpen proces in aanmerking?;
- Wat is procesmatig de beste manier voor AAHG om third-party software patches uit te rollen?;
- Op welke manier kunnen software updates efficiënt worden getest voordat ze in productie worden genomen?’’
- Wat is er technisch nodig om third-party software updates uit te rollen?;
- Wat is er technisch nodig om geautomatiseerd een melding te geven wanneer third-party software updates beschikbaar zijn?;

3.6 Scope

Binnen de scope van het project vallen de volgende onderdelen:

- Inventarisatie van de huidige situatie op het gebied van updateprocessen;
- Schrijven van een proces voor de uitrol van third-party software updates;
- Het beschrijven/adviseren van de implementatie voor het updateproces van third-party software;
- Het testen van het proces voor de uitrol van third-party software.

Buiten de scope van het project vallen de volgende onderdelen:

- Software die niet onder third-party software vallen en/of al voorzien zijn van een updateproces zoals beheertools;
- Eventueel configureren van third-party software na installatie;
- Implementeren van nieuwe processen anders dan die voor de third-party software nodig zijn;
- Aanvragen offerte;
- Eventuele training collega's vanwege nieuwe softwarepakketten voor uitrol.

3.7 Randvoorwaarden

Dit project kent de volgende randvoorwaarden:

- De student is uitsluitend bezig met het afstudeerproject;
- De student heeft beschikking over de benodigde informatie betreffende het project;
- De student heeft de beschikking over een werkplek en een werkstation met tenminste Microsoft Office en internettoegang;
- De student heeft voor de PoC de beschikking over tenminste één server en workstation. Dit mag zowel virtueel als fysiek zijn.
- Collega's van de ICT afdeling zijn beschikbaar voor eventuele vragen betreffende het project.
- De bedrijfs- en docentbegeleider zijn beiden beschikbaar gedurende het project.

4 Beheersmechanismen

Om het project goed te laten verlopen, worden hieronder een aantal beheersmechanismen beschreven.

4.1 Kwaliteitsmanagementstrategie

De kwaliteitseisen voor projectdocumenten worden binnen de AAHG voor elk project bepaald door de opdrachtgever. De onderstaande kwaliteitseisen zijn van toepassing op dit project. Daarbij moet bij vermeld worden dat punt 5d t/m 5g met name van toepassing is op het Plan van Aanpak.

1. Voertaal bij AAHG is Nederlands
2. Versiebeheer
3. Distributielijst
4. Akkoord opdrachtgever en projectmanager
5. Documentstructuur met:
    a) Inhoudsopgave
    b) Managementsamenvatting
    c) Opdrachtformulering
    d) Aanpak & organisatie
    e) Projectcommunicatie & -beheersing
    f) Begroting
    g) Risico's en maatregelen ter beheersing hiervan
    h) Bijlage(n)
6. Review documentatie door projectgroep
7. Review documentatie door Teamleider(s) beheer
8. Review door opdrachtgever

Om dit te kunnen waarborgen wordt er gebruik gemaakt van een template waarin punten twee tot en met vier al in verwerkt zijn.
De bedrijfs- en docentbegeleider zullen de documenten beoordelen.
Opgeleverde documenten behouden hun concept status totdat beide begeleiders ermee akkoord gaan (punt vier).

Voor het project is het opstellen van een begroting niet nodig. Alleen bij het marktonderzoek kunnen er, mits vermeld, kosten naar voren komen. Deze kosten zullen dan in het marktonderzoek vermeld worden.

Naast de begeleiders worden documenten ook opengesteld aan collega's die het project voorzien van de nodige informatie. Ook zij kunnen vanuit hun functie het document voorzien van verdere feedback. De documenten worden via het kennisportaal van systeembeheer beschikbaar gesteld. Verkregen feedback van begeleider(s) en/of collega('s) zal, voor zover mogelijk, binnen twee werkdagen worden verwerkt.

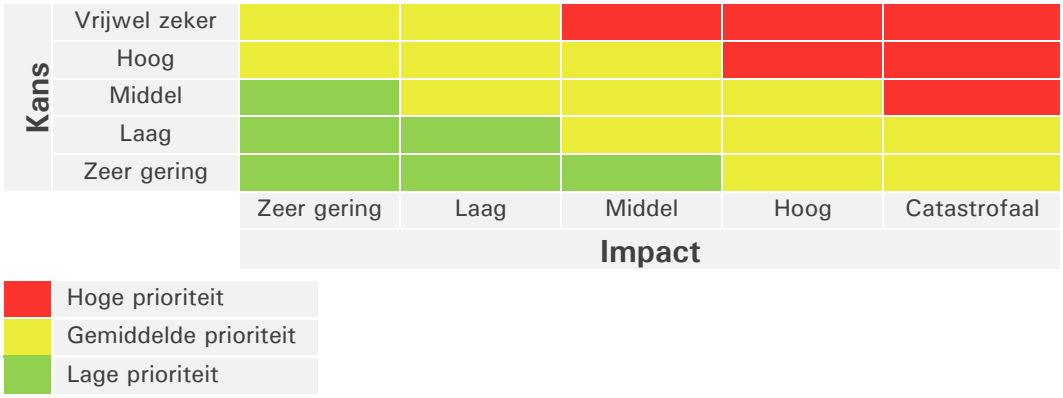
4.2 Communicatiemanagementstrategie

Voor een goede communicatie voor het project kan er gebruik gemaakt worden van e-mail, jabber en mondelinge communicatie. Het is wenselijk om grotere beslissingen over de mail te doen of te noteren. Hierdoor ontstaat er een bewijs van de plaatsgevonden beslissing. Notities van afspraken dienen digitaal beschikbaar te worden gemaakt aan alle betrokken partijen.

4.3 Risicomanagementstrategie

Risico's of issues bestaan altijd tijdens een project en kunnen gevolgen hebben voor het project.
Zoals beschreven in Projectmanagement op basis van PRINCE2 (Hedeman, Heemst, & Fredriksz, 2009, pp. 75-86) is een risico een onzekere gebeurtenis die, als deze optreedt, consequenties heeft voor het project. Het is dan bij een risico ook nodig om onzekerheden te beheersen en maatregelen te treffen voor het geval dat het daadwerkelijk optreed.
Een issue is een relevante gebeurtenis die al is opgetreden, niet gepland was en niet voorzien. Issues hebben dan ook aandacht van het management nodig.

Omdat risico's en issues altijd en uit elke hoek kunnen optreden, is het belangrijk dat het beschreven staat hoe ermee wordt omgegaan als een degelijke situatie zich voordoet.
Bij het voordoen van een risico of issue wordt er een risicoregister opgezet.
Hierin wordt het voordoende risico of issue geregistreerd, wordt aan de hand van kans en impact de prioriteit berekend (kans-effectmatrix) en worden de maatregel beschreven om het op te lossen.



Tabel 6 Kans-effect matrix voor het bepalen van de prioriteit. Aangepast van Fast Project Plans (z.j.), http://www.fastprojectplans.com/images/risk-management-plan-clip1.gif

Naast risico's die zich later in het project voor kunnen doen zijn er ook risico's die nu al aanwezig zijn.
Deze risico's zijn als volgt:

Risico	Maatregel	Kans	Impact	Prioriteit
Korte afwezigheid student (<3 dagen)	Bij aanwezigheid langere dagen maken.	Laag	Laag	Laag
Langdurige afwezigheid student (>3 dagen)	Mogelijkheid thuiswerken, begeleiders op de hoogte stellen.	Laag	Hoog	Gemiddeld
Geen beschikbare werkstation	Andere flexplek gebruiken of gebruik maken van Bring Your Own Device [BYOD].	Laag	Laag	Laag
Geen beschikbare werkplek bij systeembeheer	Flexplek gebruiken bij een andere IT afdeling.	Middel	Laag	Gemiddeld
Geen toegang tot de acceptatieomgeving	Gebruik maken van eigen virtuele omgeving op laptop.	Laag	Hoog	Gemiddeld
Onvoldoende informatie voor gestructureerd onderzoek	Voorval bespreken met begeleider(s), mogelijk gebruik maken van aannamen en eigen hypotheses.	Laag	Hoog	Gemiddeld
Tijdnood, deadline kan niet worden gehaald	Tijdnood direct melden bij de begeleiders en in overleg met hun een gepaste oplossing zoeken.	Laag	Hoog	Gemiddeld

Tabel 7 Risico's met de maatregelen, kans, impact en prioriteit

5 Projectactiviteiten

5.1 Op te leveren producten

Voor dit project worden de volgende producten met kwaliteitscriteria opgeleverd:

- Plan van Aanpak;
  Een overzichtelijke plan van aanpak die duidelijk het probleem, doelstellingen en planning beschrijft.
- Adviesrapport;
  Een bruikbaar advies dat door AAHG eenvoudig kan worden geïmplementeerd.
  - Inventarisatie 'AS-IS';
  - Rapport marktonderzoek;
  - Beschrijving 'TO-BE';
  - Procesbeschrijving;
  - Implementatieplan;
  - Testplan;
- Scriptie;
  Een duidelijke scriptie die het adviesrapport ondersteund in het advies.
  - Literatuuronderzoek;
  - Proof of Concept;
  - Reflectie en evaluatie.

De scriptie wordt conform de gestelde eisen in het afstudeerleidraad opgeleverd en zal dus o.a. de resultaten van het onderzoek en de onderbouwing ervan bevatten.
De scriptie zal waar nodig het adviesrapport ondersteunen.

5.2 Planning

Het project wordt in verschillende fases uitgevoerd en volgt voor het beheren ervan de methodologie van Prince2. De genoemde acties bij elke fase zijn de mijlpalen van het project.

Fase 1 – Analyse
De eerste fase staat in het teken van het opstarten van het project door middel van het opzetten van een PvA en het analyseren van de huidige situatie ('AS-IS').

Looptijd: 01-08-2013 t/m 13-09-2013
Uren: 232

In deze fase wordt:
- De huidige situatie geanalyseerd;
- De 'lessons learned' van de Windows-updates implementatie geanalyseerd;
- De benodigde kennis opgedaan omtrent ITIL, met name change- & releasemanagement.

Op te leveren:
- Plan van Aanpak;
- 'AS-IS' situatie releasemanagement third-party software.

Fase 2 – Onderzoek en ontwerp
De tweede fase staat in het teken van het bepalen van de toekomstige situatie ('TO-BE'), het houden van een marktonderzoek en het uitvoeren van een literatuuronderzoek.

Looptijd 16-09-2013 t/m 11-10-2013
Uren: 145

In deze fase wordt:
- De toekomstige situatie bepaald;
  - Aan welke voorwaarden moet het proces voldoen?
- Een marktonderzoek gehouden.
- Een literatuuronderzoek uitgevoerd. Hier wordt al reeds bestaande informatie verwerkt om een basis te leggen voor het nieuwe proces en om met nieuwe kennis te komen om verder te bouwen voor het nieuwe proces.

Op te leveren:
- 'TO-BE' situatie releasemanagement third-party software (functioneel ontwerp);
- Rapport marktonderzoek;
- Onderzoeksrapport.

Fase 3 – Realisatie
In de derde fase wordt het daadwerkelijke proces beschreven op basis van de verkregen informatie van fase 2. Daarnaast wordt er ook aandacht geschonken aan de implementatie en PoC.

Looptijd 14-10-2013 t/m 08-11-2013
Uren: 145

In deze fase wordt:
- Het daadwerkelijke proces beschreven;
- De implementatie beschreven;
- De PoC beschreven.

Op te leveren:
- Procesbeschrijving;
- Implementatieplan;
- Testplan;
- Proof of Concept.

Fase 4 – Conclusie en Evaluatie
De laatste fase staat in het teken van het verwerken van de bevindingen in een conclusie, het evalueren van het project en eventuele restpunten die nog opgepakt dienen te worden. De scriptie onder andere onderdelen bevatten van het literatuuronderzoek uit fase 2 en de resultaten van het PoC.

Looptijd 11-11-2013 t/m 17-12-2012
Uren: 195:45

In deze fase wordt:
- De scriptie samengevoegd;
    - Resultaten literatuuronderzoek;
- De conclusie/aanbevelingen opgesteld;
    - Lessons learned;
    - Aandachtspunten;
- Het project geëvalueerd;
- Door de student gereflecteerd.

Op te leveren:
- Scriptie;
- Eindrapport;
    - Evaluatie;
    - Reflectie.

Uren totaal: 717:45

6 Bedrijfs-/persoonsgegevens

Student

Naam:	Dhr. Niels Boers
Studentnummer:	1587222
Postcode:	Johan Fonteinpad 4
Adres:	3871 XT
Woonplaats:	Hoevelaken
E-mailadres:	niels.boers@student.hu.nl
Telefoonnr. Vast:	033-2535341
Telefoonnr. Mobiel:	06-12708721

Afstudeerbedrijf/begeleider

ABN AMRO Hypotheken Groep

Postbus:	1700, 3800 BS, Amersfoort
Naam:	drs. Dhr. Olaf G.A.C.M Hamelers
Functie:	Teamleider ICT Infra- & Systeembeheer
Adres:	Ruimtevaart 24
Postcode:	3824 MX
Plaats:	Amersfoort
E-mailadres:	olaf.hamelers@aahg.nl
Telefoonnummer:	033-7504187

School/begeleider

Hogeschool Utrecht

Postbus:	182, 3500 AD, Utrecht
Naam:	Dhr. Rienk C. van der Ploeg
Functie:	Docent Systeembeheer
Adres:	Nijenoord 1
postcode:	3552 AS
Plaats:	Utrecht
E-mailadres:	rienk.vanderploeg@hu.nl
telefoonnummer:	088-4818277

7 Stagecontract

Contract afstudeeropdracht
Instituut voor ICT
Nijenoord 1, 3552 AS, UTRECHT

NB: Dit contract dient te worden opgenomen als vast onderdeel van het plan van aanpak

Datum:

Naam student:	Niels Boers
Opleiding:	Bachelor informatica (systeembeheer)
Variant: voltijd / deeltijd / duaal	Voltijd
Adres student:	Johan Fonteinpad 4
Postcode / Woonplaats student:	3871 XT Hoevelaken
Studentnummer:	1587222
Telefoonnummer privé:	033-2535341
E-mailadres:	niels.boers@student.hu.nl
Naam bedrijf (afstuderen):	ABN AMRO Hypotheken Groep
Adres bedrijf:	Ruimtevaart 24
Postcode / Woonplaats bedrijf:	3824 MX Amersfoort
Naam bedrijfsbegeleider:	drs. Dhr. Olaf G.A.C.M. Hamelers
Telefoonnummer bedrijfsbegeleider:	033-7504187
E-mailadres bedrijfsbegeleider:	olaf.hamelers@aahg.nl
Beoogde datum van afstuderen:	Januari 2014
Geheimhouding geaccordeerd door HU op:	n.v.t.

Ondergetekenden verklaren hiermee akkoord te gaan met de inhoud van bijgesloten PvA.

Handtekeningen

Student :

Docentbegeleider :

Bedrijfsbegeleider[6] :

6 Door ondertekening van dit formulier verklaart de bedrijfsbegeleider minimaal een hbo- of vergelijkbare opleiding te hebben.

8 Bibliografie

ABN AMRO. (z.j.). *ABN AMRO Hypotheken Groep*. Opgeroepen op mei 27, 2013, van abnamro.com: http://www.abnamro.com/nl/about-abn-amro/subsidiaries/hypotheken-groep.html

Fast Project Plans. (z.j.). Opgeroepen op augustus 6, 2013, van fastprojectplans.com: http://www.fastprojectplans.com/images/risk-management-plan-clip1.gif

Hedeman, B., Heemst, G. V., & Fredriksz, H. (2009). Projectmanagement op basis van PRINCE2™ Editie 2009. Zaltbommel: Van Haren Publishing.

Appendix II Evaluatie eigen functioneren

Dit was voor mij de eerste keer dat ik zelfstandig aan een project heb gewerkt binnen een middelgroot bedrijf. Als ik terug kijk op het uiteindelijke resultaat ben ik ook tevreden wat ik bereikt heb. Een van de grootste hindernissen waar ik tegen opliep was mijn motivatie. Deze was met name gericht op een goede resultaat leveren voor AAHG. Als er een onderdeel was dat meer vanuit Hogeschool Utrecht werd verwacht, had ik al snel moeite om gefocust te blijven. Dit werd met name opgevangen door mijn doorzettingsvermogen. Hoewel mijn planning breed was opgezet kreeg ik toch te maken met tijdgebrek. Dit kwam door ziekte en mijn neiging om alles tot in de details te behandelen. Dit leidde voor mij tot veel stress waardoor het overzicht een beetje vervaagde. Hiervoor heb ik met de docentbegeleider gesproken. Er werd inderdaad geconstateerd dat ik te diep op de materie inging. Na een paar voorbeelden was voor mij duidelijk hoe ik de details kon beperken. Verder was het bijstellen van de planning nodig.

Door het bijstellen van mijn planning heb ik toch nog alles kunnen behandelen, hoewel niet helemaal zoals ik het voor ogen had. Wel heb ik de volgorde van de vier geplande fases goed afgehandeld. Dit was ook wel nodig aangezien de elke fase de informatie van de vorige fase nodig had.
Ik ben met name veel tijd kwijtgeraakt bij het marktonderzoek. Het duurde soms erg lang voordat ik informatie kon vinden. Ik had bij een aantal punten ook neer kunnen zetten dat er geen informatie gevonden kon worden. Toch heb ik doorgezet en heb na veel zoeken nog wel informatie kunnen vinden.

Op de PoC is naar mijn mening het meest bezuinigd. Vanwege de tijd heb ik uit de short list maar een pakket gekozen. Ik had liever via de PoC het beste pakket uit de shortlist gekozen. Wel heb ik bij de PoC alle punten behandeld die ik wou behandelen.

Het verwerken van de verkregen informatie in de scriptie was voor mij ook een probleem. Bij een aantal paragrafen wist ik wel wat ik wou zeggen, maar niet hoe ik dit het beste kon opschrijven.

Uiteindelijk is het me gelukt om toch nog binnen de tijd een scriptie af te leveren waar ik redelijk tevreden over ben. Ik had liever een document gemaakt in plaats van een scriptie en een adviesrapport. Hierdoor zou het document naar mijn mening overzichtelijker worden.

Ik onderschat vaak mijn geleverde werk en had bij de scriptie ook zeker het gevoel dat ik nog veel meer had kunnen behandelen (in meer detail).
Vanuit AAHG werd positief gereageerd op de opgeleverde producten. Ik was hierdoor aangenaam verrast en kan daardoor ook met trots terugkijken op mijn geleverde werk. Verder was het erg leuk werken bij AAAHG. Collega's stonden altijd voor me klaar en er hing een aangename sfeer. Ook werd er interesse getoond in mijn project. Bij de daily stand-up vertelde ik ook waar mijn project stond en gaven collega's op sommige punten tips.

Het project is voor AAHG dus met succes afgerond. Als ik het ook met succes kan afsluiten kan ik mijn schoolperiode afsluiten en de volgende stap nemen.

Appendix III Evaluatie procesgang

Het project is naar mijn mening succesvol afgerond. Hoewel ik bij het schrijven van het Plan van Aanpak een goede planning had gemaakt met veel speling qua tijd, werd ik al snel geplaagd door tijdsdruk vanwege ziekte en doordat ik te diep de materie wilde behandelen. Verder had ik bij aanvang van het project het gevoel dat het schrijven van een nieuw patch proces redelijk gemakkelijk zou zijn. Patchen op een computer thuis gaat immers ook snel. Niets bleek minder waar. Patchen in een bedrijfsomgeving kent veel haken en ogen. Ondanks dat mijn tijd daardoor beperkt werd, ben ik wel trouw gebleven aan de volgorde van mijn planning.
De volgorde was gesplitst in vier fases waarbij elke fase niet gestart kon worden als de vorige niet voltooid was. Hierin heb ik eerst gekeken naar de huidige situatie, zodat bij mijn bekend was wat er allemaal speelde. Voor de duidelijkheid heb ik het Windows patchproces uitgetekend. Vervolgens ben ik de theorie gaan onderzoeken zodat de kennis rondom patchen breder werd. Dit is verwerkt in het literatuuronderzoek en gaf mij de richtlijnen waar een nieuw proces aan moest voldoen. Voor het technische onderdeel van het project was een marktonderzoek nodig. Dit bleek wel een van de lastige onderdelen te zijn aangezien software beoordeeld werd op wat er te vinden was in de documentatie. Ik had vooraf een goed gevoel bij Secunia en was dan ook blij dat het hoog scoorde. Uiteindelijk is Secunia verder beoordeeld met een PoC en bleek het een redelijk goed product te zijn. Het bewees in ieder geval wel de kracht van patchsoftware. Uiteindelijk kon alles goed beschreven worden. Ik had met de fases wel al telkens de onderdelen verder uitgewerkt, maar nu werd alles een goed geheel. Uiteindelijk had ik besloten om het nieuwe proces te baseren op het al bestaande Windows patchproces. Dit proces is namelijk al bekend en werkt goed. Verder is de mens een gewoontedier. Door het proces te baseren op het Windows proces hoeven de beheerders minimaal bij te stellen en kan het sneller opgenomen worden dan als het compleet anders zou lopen.

De fases zijn dus met succes voltooid. Echter kan ik naar mijn mening altijd iets dieper uitwerken, en ben ik nooit echt tevreden over mijn eigen werk tenzij andere mensen er positief over zijn. Voor het project was wel veel interactie nodig met collega's uit de IT. Zij hebben me altijd te woord gestaan en boden altijd hulp in termen van feedback. Wat ik wel geleerd heb van de interactie is dat contact voor sommige onderdelen het beste ver van tevoren aangekondigd kan worden. Ondanks dat mijn collega's me best wilden helpen, was er niet altijd direct tijd voor me. Verder heb ik veel opgestoken van het literatuuronderzoek. Ik ben daarmee meer het belang gaan inzien van patchen en heb daardoor thuis zelfs 'automatic update' van Windows weer aangezet. Ook was de PoC erg fijn om uit te voeren. Ik ben technisch ingesteld en was erg blij om met de PoC even weer met servers bezig te zijn in plaats van documentatie. Met de PoC heb ik ook voor het eerst gewerkt met SCCM. Na een korte gewenningsperiode kon ik al snel zelf software pushen naar mijn eigen werkstation.

Voor de documentatie vond ik het wel jammer dat het adviesrapport en de scriptie gescheiden moesten zijn. In het laatste project van de hoofdfase hadden we de documenten tot één samengevoegd en daar was toen geen probleem mee. De reden van dit is dat er nu tweemaal dezelfde informatie verwerkt moest worden. Als ik dit in één document zou verwerken, zou het, in iedere geval voor mij, overzichtelijker zijn. Ook zou ik meer aandacht kunnen besteden waar het nodig is. Ik vind het namelijk lastig om mijn gedachten op papier te zetten en al helemaal als het twee keer in andere woorden moet. Ondanks dit ben ik nog wel tevreden met het behaalde resultaat.

ABN·AMRO

Appendix IV Adviesrapport

Adviesrapport

Third-party patchmanagement AAHG

ABN AMRO Hypotheken Groep

Colofon

Documenteigenschappen

Titel	Adviesrapport_AAHG_Niels-Boers_v1.2.pdf	**Status**	Definitief
Project	Afstudeerstage	**Versie**	V1.2
Auteur	Niels Boers	**Studentnr.**	1587222
Bedrijf	ABN AMRO Hypotheken Groep		

Typografische conventies

Het voorliggende document maakt gebruik van de volgende typografische conventies.

Conventie	Betekenis	Voorbeeld
AaBbCc1234	Normale tekst	Dit is een voorbeeld.
AaBbCc1234	Quotatie/motto	De missie van ICT is: *"Wij ondersteunen zorgeloos werken"*.
AaBbCc1234	Kruisreferentie in dit document	Zie hoofdstuk 2 voor meer informatie.
AaBbCc1234	Hyperlink naar website of e-mail adres	e-mail: niels.boers@aahg.nl

Revisie

Revisie	Datum vorige revisie	Samenvatting van wijzigingen	Versie
08-08-2013	N.v.t.	Initiële Adviesrapport	V0.1
11-12-2013	08-08-2013	Adviesrapport naar V1.0	V1.0
13-12-2013	11-12-2013	Verwerking feedback bedrijfsbegeleider	V1.1
13-12-2013	14-12-2013	Verwerking feedback docentbegeleider	V1.2

Inhoudsopgave

1 Inleiding

In het voorliggende document wordt een advies gegeven voor het patchen van third-party software. Het beschrijft de huidige situatie en de toekomstige situatie met de implementatie van de software. Tevens wordt in dit document ook de Proof of Concept [PoC] en het third-party patch proces beschreven. Door ook third-party software patches procesmatig aan te pakken, krijgt AAHG [ABN Amro Hypotheken Groep] meer controle over haar omgeving.

2 Theorie

Patchen is belangrijk voor een goede, gezonde en veilige ICT infrastructuur. Hoewel patchen in de begin jaren met name gericht was op het verbeteren van de functionaliteit, speelt tegenwoordig ook de beveiliging een grote rol.
Om ook AAHG compliant te houden is er vanuit de afdeling informatiebeveiliging een informatiebeveiligingsbeleid opgezet rondom patchen. Het beleid is van toepassing op alle software en stelt o.a. een deadline voor het uitrollen van patches op basis van de impact. Sinds 2011 is niet Microsoft maar zijn verschillende third-party applicaties de meest geëxploiteerde software (Kaspersky, 2011). Het is dus belangrijk third-party patches net zo serieus te nemen als Windows patches. In ieder geval de applicaties die vaak worden aangevallen. Voorbeelden van third-party applicaties die vaak worden misbruikt zijn browsers, Adobe Flash Player, Adobe Reader en Java Runtime Environment (Secunia, 2013).
Om ook de third-party applicaties te voorzien van een proces, kan er gekeken worden naar ‘best practices’ om zodoende het proces in te vullen.
Naast ITIL, dat met de processen change- en releasemanagement al goede handvaten biedt, zijn er ook white papers van verschillende IT (security) bedrijven die aandachtspunten beschrijven voor het goed uitrollen van patches. Twee aandachtspunten die vaak terug komen zijn: regelmatig patchen en goed testen. Deze twee punten zullen dan ook terug komen in het advies.

3 Huidige Situatie

In dit hoofdstuk wordt de huidige situatie van AAHG vermeld rondom het patchen van third-party software.

3.1 Gedefinieerde third-party software

In eerste instantie zou er een nieuw patchproces geschreven worden voor de kantoorautomatiserings- [KA] software. Echter was het onduidelijk wat allemaal geclassificeerd kon worden als KA-software, afgezien van Java, Adobe Reader en Adobe Flash. Uiteindelijk is er parallel met het uitzoeken van de exoten (ongewenste software) bepaald welke groepen software binnen AAHG aanwezig zijn. Dit zijn respectievelijk: kantoorautomatiseringssoftware, business software en infrastructuursoftware.
Door deze classificering is bepaald dat applicaties zoals Java en Adobe Flash niet meer onder KA-software vallen, maar onder infrastructuursoftware.
Daarnaast is het de wens van AAHG dat het nieuwe proces generiek is. Met andere woorden, het moet ook kunnen werken met software die misschien over drie jaar in gebruik wordt genomen. Om deze redenen spreken we nu over third-party software. Hierdoor kunnen de eerdergenoemde applicaties Java en Adobe Flash, die vaak worden aangevallen, alsnog worden voorzien van een patchproces.

Omdat third-party software een generieke term is, vallen er automatisch vele softwarepakketten onder. Om niet te veel software in een keer te behandelen en gefocust te blijven op de meest kwetsbare van de groep dat op iedere werkstation aanwezig is, behandelt dit project de onderstaande software weergegeven in tabel 8. Tabel 8 geeft daarnaast ook de verschillende versies die op het moment van schrijven aanwezig zijn binnen AAHG. De laatste kolom geeft het aantal Common Vulnerabilities and Exposures [CVE] aan voor het product. Dit zijn de geregistreerde vulnerabilities van het product.

Software	Uitgever	Versie aanwezig	Installatie	Gebruikers	CVE
Adobe Flash Player	Adobe	9	1	0	
		10	5	0	298
		11	90	5	
Adobe Reader	Adobe	7	1	0	
		8	2	0	
		9	2	0	311
		10	1.198	1.121	
		11	2	3	
Java RE	Oracle	1.4	2	0	
		1.5	33	0	397/192[1]
		6	1.223	269	
		7	83	7	

Tabel 8 Gedefinieerde third-party software

[1] Oracle nam in 2010 Sun Microsystems over waardoor CVE's voor Java RE onder SUN en Oracle staan. De cijfers zijn hier dus gescheiden voor CVE's onder SUN/Oracle.

3.2 Proces

3.2.1 Proces Windows

Een update blijft een update, of het nou Windows updates zijn of die voor third-party software zoals Java. Daarom is het belangrijk om te kijken naar het Windows update proces om zo te zien hoe dit gerealiseerd is en welke lessen eruit te halen zijn.

Het Windows update proces wordt beschreven in het document AAHG – Proces Patchen (ABN AMRO Hypotheken Groep, 2011) en speelt zich af tussen de drie afdelingen (Infra- en) Systeembeheer, Applicatiebeheer en Changemanagement. Hierin zijn de twee eerst genoemde teams de uitvoerende partijen. Changemanagement is bij het proces betrokken om de voortgang te bewaken.
Daarnaast heeft ook de afdeling Informatiebeveiliging een hand in het update proces. Zij stellen namelijk het informatiebeveiligingsbeleid op voor het patchen. Het patch proces moet voldoen aan het gestelde beleid, maar heeft daarin een zekere mate van vrijheid.

Team	Werkzaamheden
Systeembeheer	▌Beoordelen patches. ▌Indienen change. ▌Testen patches. ▌Uitrollen patches. ▌Controleren van patchniveau.
Applicatiebeheer	▌Functioneel testen van applicaties op werkstations er applicatieservers.
Changemanagement	▌Voortgang change bewaken.
Informatiebeveiliging	▌Stellen informatiebeveiligingsbeleid.

Tabel 9 Taakverdeling Windows patch proces. Aangepast van AAHG – proces patchen (p. 3) door AAHG, 2011

Elke tweede dinsdag van de maand (patch Tuesday) brengt Microsoft nieuwe patches uit. Door tijdsverschil zijn deze in Nederland de woensdag erna beschikbaar.
Het patch proces voor de Windows updates omvat alle Critical en High Windows updates met uitzondering van de Service Packs [SP]. De SP's bevatten vaak een gewijzigde functionaliteit en hebben daardoor een groter risico om tot incidenten te leiden.

Voor de uitrol van de patches wordt een non-standard change aangevraagd. Dit gaat gepaard met een lijst van de te patchen servers. Het is een non-standard change omdat dit elke maand gebeurt en de change automatisch wordt ingepland maar de impact van elke change per uitrol kan variëren (Goktas & Tomassen, 2013).

Het patch proces wordt in het document AAHG – Proces Patchen (ABN AMRO Hypotheken Groep, 2011) in drie stappen beschreven met nog een extra stap voor een eventuele rollback. De stappen zijn als volgt:

- **Patch selectie;**
- **Patches testen;**
- **Patches uitrollen;**
  Omdat patches vaak een reboot vereisen, zijn de volgende regels in acht genomen voor werkstations en servers:

  Werkstations
  Werkstations worden in principe aan het einde van de dag afgesloten. Dit werkt dan ook als de reboot voor nieuwe updates.

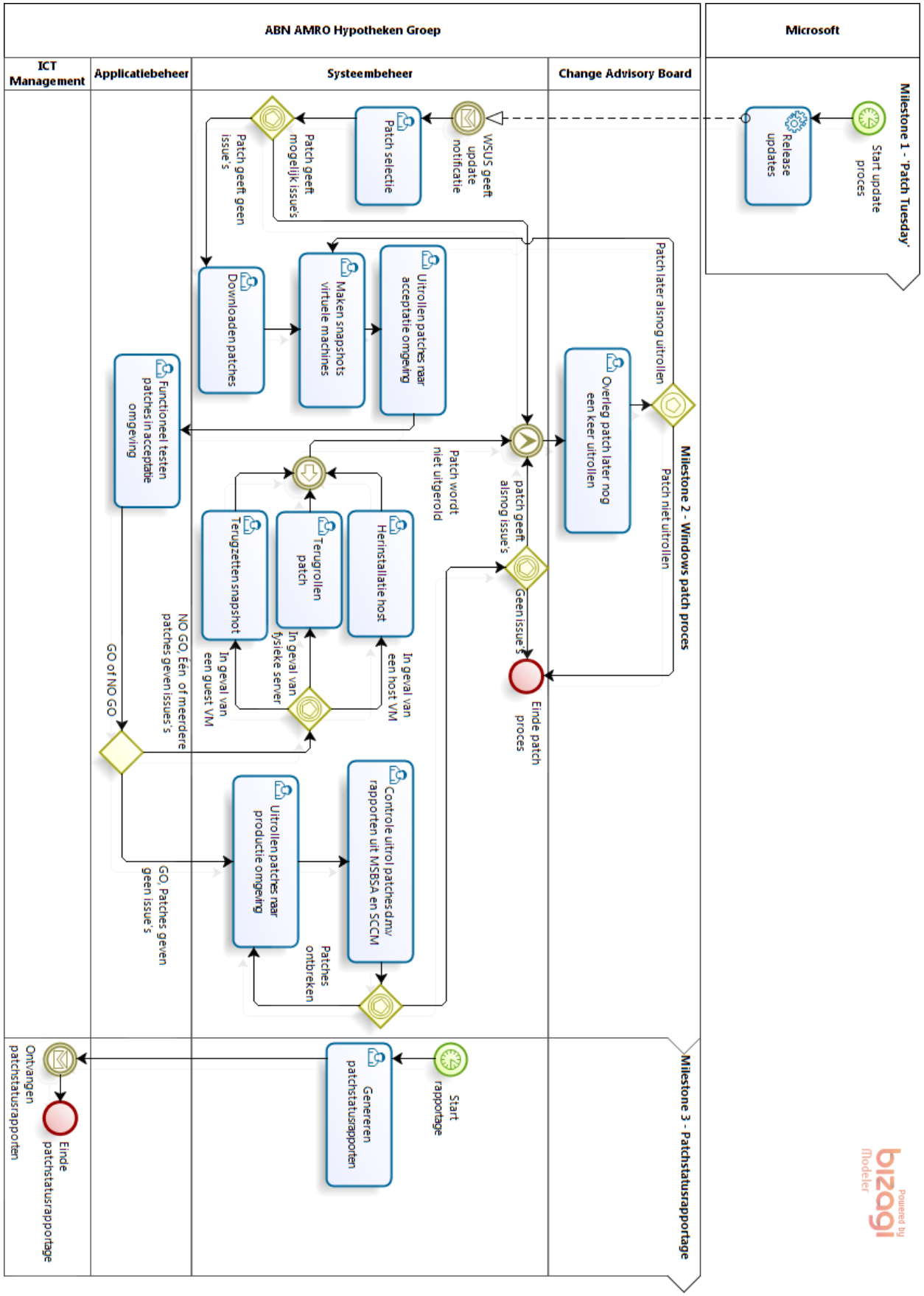
  Servers
  Niet business kritieke servers, zoals beheerservers, kunnen gewoon overdag worden gereboot.
  Business kritieke servers worden buiten productietijd gereboot.

- **Rollback (overig);**

- **Rapportage.**

Process flow
In figuur 7 zijn alle stappen van het Windows update proces te zien in een process flow. Door het proces niet alleen te beschrijven maar ook uit te tekenen ontstaat er meer duidelijkheid in hoe het proces in elkaar zit en wordt het ook makkelijker om het proces te kunnen analyseren.

Afwijking
Hoewel het proces goed beschreven is, wordt het toch niet tot op de letter nageleefd. Het onderdeel rapportage aan de IT management groep is in het begin wel uitgevoerd. Maar doordat er weinig met de rapporten werd gedaan staat dat nu stil (Berends, 2013). De plannen zijn om het weer in te voeren.



Figuur 7 Windows patchproces flow

3.2.2 Proces third-party

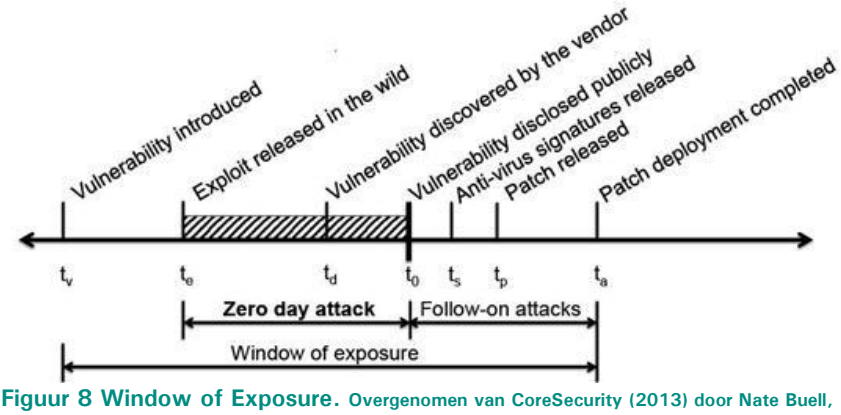
De huidige implementatie van de third-party software is momenteel onoverzichtelijk. In plaats van een geaccordeerd en geïmplementeerd proces worden updates, wanneer beschikbaar, door een beheerder gedownload en in de productieomgeving gebracht. Daarnaast zijn het veelal alleen de belangrijke securityupdates die worden gedownload en uitgerold naar de productie omgeving (Hamelers, 2013). De stijl van patchen binnen AAHG heeft dan ook wat weg van een 'patch and pray' implementatie. Patches worden in zekere mate wel gecontroleerd, maar het komt ook voor dat er zonder enige vorm van acceptatie of validatie een patch in productie wordt gebracht. De voorwaarde hiervoor is wel dat er een fall-back mogelijkheid is.

3.2.3 Proces risico's

Ten eerste bestaat het risico van het missen van bepaalde functionaliteit. Hoewel dit geen directe impact heeft op de digitale veiligheid, kan het wel een impact hebben op de productiviteit. Deze punten kunnen opgelost worden door het uitrollen van updates.

Ten tweede kan het, door het ontbreken van een proces, lastig worden om de digitale veiligheid te kunnen waarborgen. Systeembeheer wordt momenteel op de hoogte gehouden door e-mails van een derde partij. Hierin wordt vermeld of er een nieuw lek is gevonden in de software, de impact hiervan en ook of er een patch voor is vrijgegeven (Granneman, 2013). Het probleem hiermee is dat er alsnog handmatig actie moet worden ondernomen om de updates te downloaden. Dit is voor 10 verschillende softwarepakketten misschien niet zo'n probleem, maar met 50+ applicaties kan dit routine klusje veel onnodige tijd in beslag nemen om elke update telkens te downloaden, te installeren en te testen. Daarnaast zijn deze 'vulnerability reports' niet volledig en niet gericht op alleen de software binnen AAHG. Ook komt het voor dat alerts pas binnen komen als de patch al geïnstalleerd is (Berends, 2013).

Als laatste is er een risico in de tijd dat het duurt om een update uit te rollen. Exploits[2] kennen namelijk een 'window' waarin ze het effectiefst zijn, te zien in figuur 8 (CoreSecurity, 2013). Elke dag dat een update niet wordt doorgevoerd wordt de window groter, en dus ook de kans dat de exploit effect kan hebben.



Figuur 8 Window of Exposure. Overgenomen van CoreSecurity (2013) door Nate Buell, http://blog.coresecurity.com/2013/02/27/a-world-of-vulnerabilities-guest-blog-post-from-infosec-institute/

[2] Zowel zero-day als 1-day exploits

3.2.4 ITIL

Binnen AAHG wordt gebruik gemaakt van ITILv3. Het is dan ook grotendeels geïmplementeerd (Hamelers, 2013). Voor het uitrollen van patches zijn drie processen met name van belang, namelijk: changemanagement, releasemanagement en configurationmanagement. Ook is er een raakvlak met security management met betrekking tot het informatiebeveiligingsbeleid.

Changemanagement

Het change management proces staat beschreven in het document AAHG Change Management proces – V 1.1 (ABN AMRO Hypotheken Groep, 2010).
Binnen AAHG wordt onder een change iedere verandering in processen, procedures, informatie voorziening en ICT middelen verstaan. Change management wordt gebruikt voor het op gestructureerde en geplande wijze doorvoeren van een change. Dit moet er voor zorgen dat de geplande change de ICT dienstverlening in stand houdt of verbetert zonder dat het verstoringen veroorzaakt.
Ook geeft het AAHG een gedetailleerd inzicht in de nog te realiseren changes, voortgang van alle changes en resultaten van alle changes.

Het change proces is als volgt:

- Aanvragen en registreren request for change [RFC];
- Analyseren RFC;
- Beoordelen RFC;
- Inplannen RFC;
- Coördineren realisatie RFC;
- Coördineren implementatie RFC;
- Evalueren en afsluiten RFC.

Releasemanagement

In het document AAHG Release Management proces – V1.0 (ABN AMRO Hypotheken Groep, 2010) wordt het release proces beschreven binnen AAHG. Binnen AAHG wordt release management gebruikt voor het beheren en distribueren van alle hard- en software versies die in gebruik zijn en worden beheerd door de afdeling ICT.
Hiermee wordt er voor gezorgd dat alleen de juiste, geautoriseerde en geteste versies van hard- en software beschikbaar zijn, zonder dat de kwaliteit van de werkomgevingen in het geding komt.

Het release proces is als volgt:

- Releaseplanning;
- Release ontwerpen, bouwen of kopen en samenstellen;
- Release testen en accepteren;
- Uitrol plannen;
- Communiceren, voorbereiden en trainen;
- Release distribueren en implementeren.

Configurationmanagement
Binnen AAHG wordt het proces voor configuratie management beschreven in het document AAHG Configuration Management proces – V1.2 (ABN AMRO Hypotheken Groep, 2013). Configuratie management is in feite de backbone van de andere ITIL processen door het leveren van actuele, accurate en verifieerbare informatie over de componenten van de ICT-dienstverlening.
Daarnaast zorgt configuratie management er voor dat wijzigingen van componenten van de ICT-dienstverlening zodanig worden verwerkt, dat de consistentie en integriteit van deze componenten gewaarborgd blijft. Deze componenten zijn vastgelegd in de Configuration Management Database (CMDB).

Het configuration proces is als volgt:
- Configurationmanagement planning;
- CI's identificeren;
- CI's onderhouden;
- Rapportage;
- Verificatie en audits;
- Proces controle en evaluatie.

3.3 Techniek

3.3.1 Uitrol methodiek
Voor de productie omgeving worden een drietal software pakketten gebruikt voor de uitrol van software. Dit zijn respectievelijk:

- Windows Server Update Services [WSUS];
- System Center Configuration Manager 2012 [SCCM];
- Application Virtualization [App-V].

Doordat WSUS alleen overweg kan met Windows updates, worden updates voor third-party software handmatig gedownload.
Door middel van App-V wordt er van software een package gemaakt die dan weer met SCCM wordt gedistribueerd naar de gebruikers. Van Windows-updates wordt geen package gemaakt. Deze worden direct met SCCM gedistribueerd.

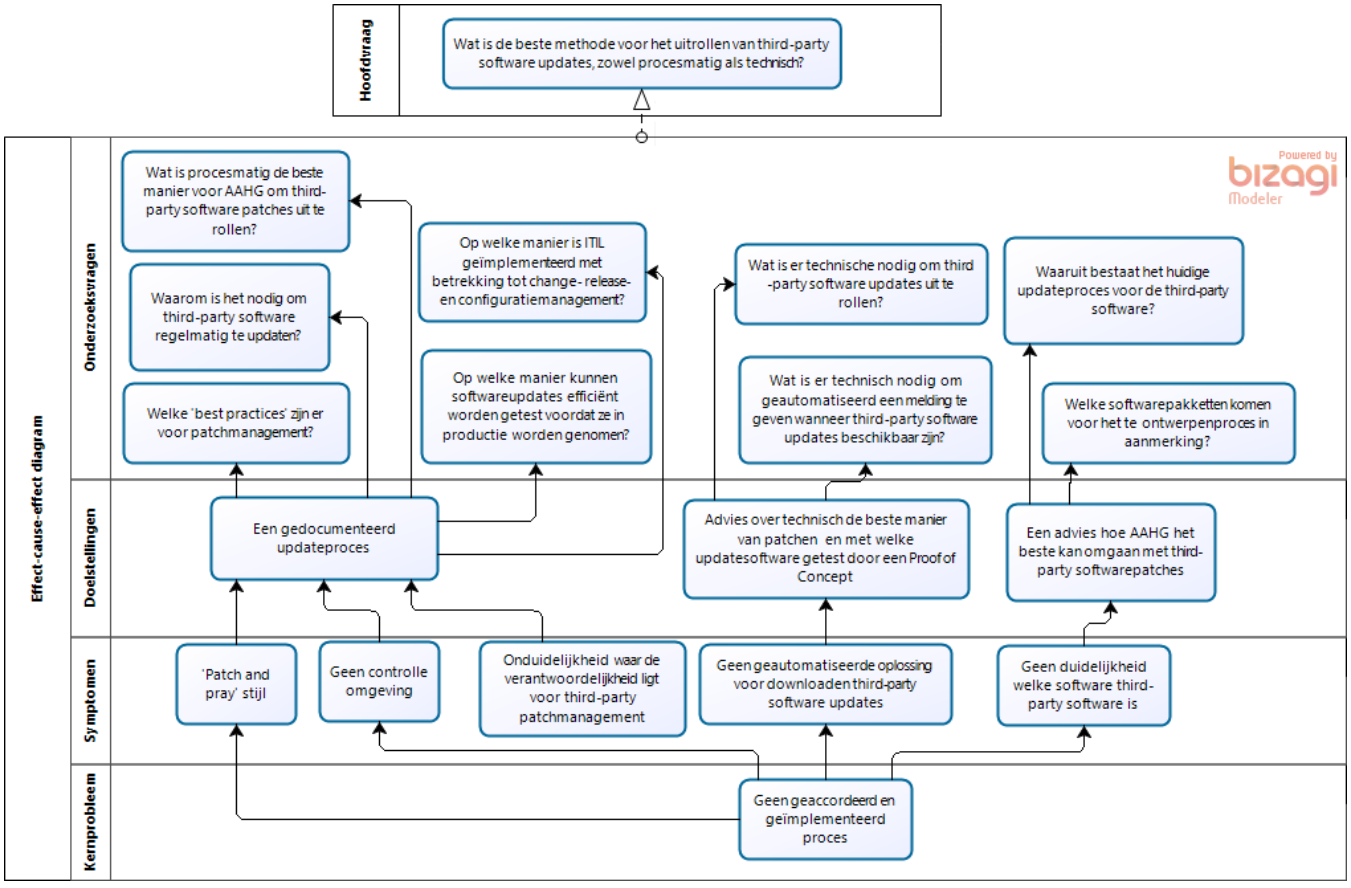
3.3.2 Technische risico's
De technische risico zit in het gebruik van App-V. Doordat App-V applicaties virtualiseert en dus in een sandbox draaien, kunnen verschillende versies naast elkaar draaien. Hierdoor ontstaat er een potentieel beveiligingsrisico omdat oudere versies niet meer worden gepatcht of helemaal geen ondersteuning hebben van de leverancier, terwijl ze nog wel aanwezig zijn in de productieomgeving.
Tabel 8 laat dit goed zien. De informatie omtrent versie, installatie en gebruikers komt uit de software inventarisatie tool SNOW. Het laat al duidelijk zien dat er binnen AAHG nog oude versies rondzwerven die niet meer worden gebruikt.

3.4 Knelpunten

Nu we zicht hebben op de huidige situatie binnen AAHG kan er een inventarisatie worden gemaakt van de knelpunten binnen AAHG:

- Geen geaccordeerd en geïmplementeerd proces;
- Af en toe 'patch and pray' stijl;
- Geen controle op de omgeving;
- Geen geautomatiseerde oplossing voor downloaden third-party software updates;
- Geen 'echte' duidelijkheid welke software onder third-party software valt;
- Onduidelijkheid waar de verantwoordelijkheid ligt voor third-party patchmanagement.

In figuur 9 zien we dat de eerstgenoemde het kernprobleem is. De andere knelpunten vloeien voort uit het kernprobleem. Deze vloeien dan weer door naar de doelstelling van het afstudeerproject die gerealiseerd moet worden door het beantwoorden van de onderzoeksvragen. De onderzoeksvragen zijn gelijk aan die in het PvA. De hoofdvraag wordt op zijn beurt weer beantwoord door de deelvragen.



Figuur 9 Effect-cause-effect third-party software AAHG

4 Toekomstige situatie

4.1 Proces

De wens van AAHG is om een patchproces te hebben voor de third-party applicaties. Hierdoor kan er meer controle worden uitgeoefend en wordt er meer voldaan aan het gestelde securitybeleid. Verder is het wenselijk dat het proces globaal wordt opgezet. Dit houdt in dat ook in de toekomst nieuwe software met dit proces gepatcht kan worden. Het proces moet alle stappen beschrijven, van selectie tot uitrol en de eventuele roll-back. In het proces wordt met name rekening gehouden met de frequentie en het testen van de patches. Doordat het Windows patchproces al beschreven is, zal het nieuwe proces hierop gebaseerd worden. Het nieuwe proces zal met name onderscheid maken in het testen. Verder zal het proces elke maand worden uitgevoerd om de compliance zo hoog mogelijk te houden.
De stappen van het proces zijn als volgt:

- **Patch selectie;**
  Er wordt bij het patchen gekeken of specifieke patches problemen gaan geven. Deze worden eerst niet meegenomen en in het CAB besproken. Het CAB zal bepalen of de patches alsnog worden uitgerold of niet. Verder worden snapshots gemaakt van de VM's voor een makkelijke rollback.

- **Patches testen;**
  Patches worden uitgerold in de acceptatieomgeving en worden getest met drie verschillende tests; ST, FAT en GAT. Voor details kan worden gerefereerd naar hoofdstuk 7.

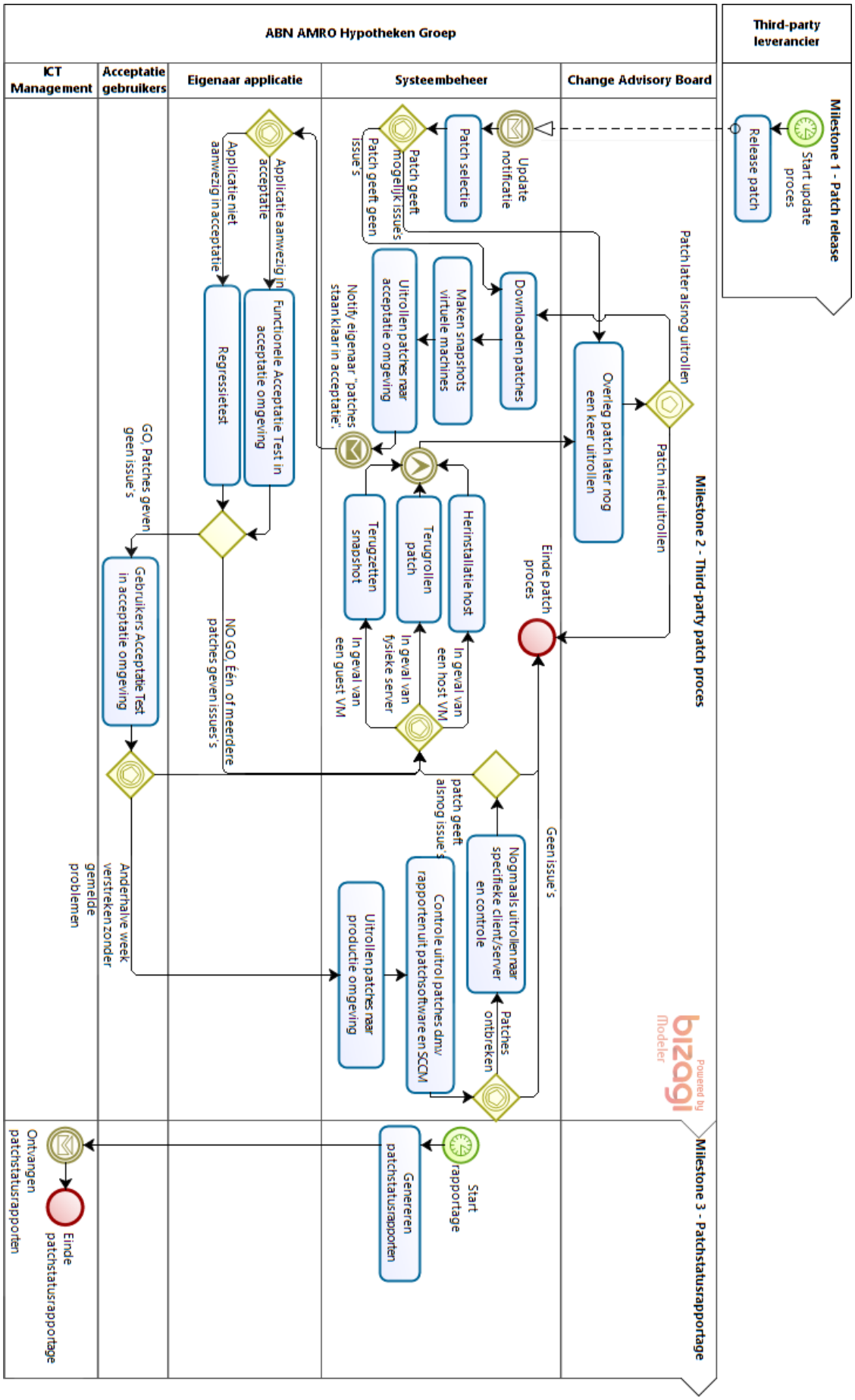
- **Patches uitrollen;**
  Als er na anderhalve week geen problemen worden gemeld kunnen de patches worden uitgerold in de productieomgeving.
  Voor eventuele reboot kan het volgende worden aangehouden:

  Werkstations
  Werkstations worden in principe aan het einde van de dag afgesloten. Dit werkt dan ook als de reboot voor nieuwe updates.

  Servers
  Niet business kritieke servers, zoals beheerservers, kunnen gewoon overdag worden gereboot.
  Business kritieke servers worden buiten productietijd gereboot.

- **Rollback (overig);**
  Als er een rollback nodig is kan er in het geval van VMs de snapshot worden terug gezet. De host VM kan het beste opnieuw worden ingespoeld aangezien een rollback risicovol is. Op de fysieke servers kan de patch worden teruggedraaid.

- **Rapportage.**
  Nadat de patches zijn uitgerold, wordt er met SCCM en de gekozen patchsoftware een compliance report gemaakt en verzonden naar het IT management.



Figuur 10 Third-party patchproces flow

De frequentie van het proces is erg belangrijk. Het bepaalt met name hoe compliant het ICT landschap blijft. Voor het proces is een balans nodig tussen zo snel mogelijk uitrollen en de tijd die nodig is om deze te testen. Als richtlijn kan gebruik worden gemaakt van het informatiebeveiligingsbeleid. In het beleid wordt de deadline gesteld vanaf het moment dat een patch beschikbaar komt in combinatie met de prioriteit. De gestelde tijd is als volgt:

Prioriteit	Uitroldeadline na beschikbaar komen van de patch bij de leverancier
Urgent	Binnen 2 weken
Hoog	Binnen 6 weken
Midden/laag	Binnen 6 maanden
Geen	Niet van toepassing

Tabel 10 Patchdeadline met bijbehorende prioriteit

Voor het Windows patchproces is dit geen probleem sinds Microsoft de patches op de tweede dinsdag van de maand vrijgeeft.
In het geval van third-party leveranciers wordt er geen vaste dag gehanteerd. De uitzondering is Adobe die tegenwoordig ook doet aan Patch Tuesday.
Aangezien er 6 weken de tijd is om een patch met hoge prioriteit uit te rollen, is een frequentie van een maand het beste. Het is binnen de tijd van de hoge prioriteit en gemakkelijker in te plannen.

Omdat er vanuit changemanagement wordt gesteld dat er geen twee changes tegelijk op dezelfde systemen mogen worden uitgevoerd, is de beste datum om te patchen de vierde dinsdag van de maand. Een bijkomend voordeel om third-party patchen gescheiden te houden van de Windows patches is dat eventuele troubleshooting wordt vergemakkelijkt.

In het geval van een patch met een urgente prioriteit moet er in het CAB [Change Advisory Board] worden overlegd wat de beste actie is: Afwijken van het proces en conform het beleid de patch uitrollen of de risico's aanvaarden en wachten tot de eerst volgende patchronde. Dit gebeurt in samenspraak en met goedkeuring van de securitymanager.

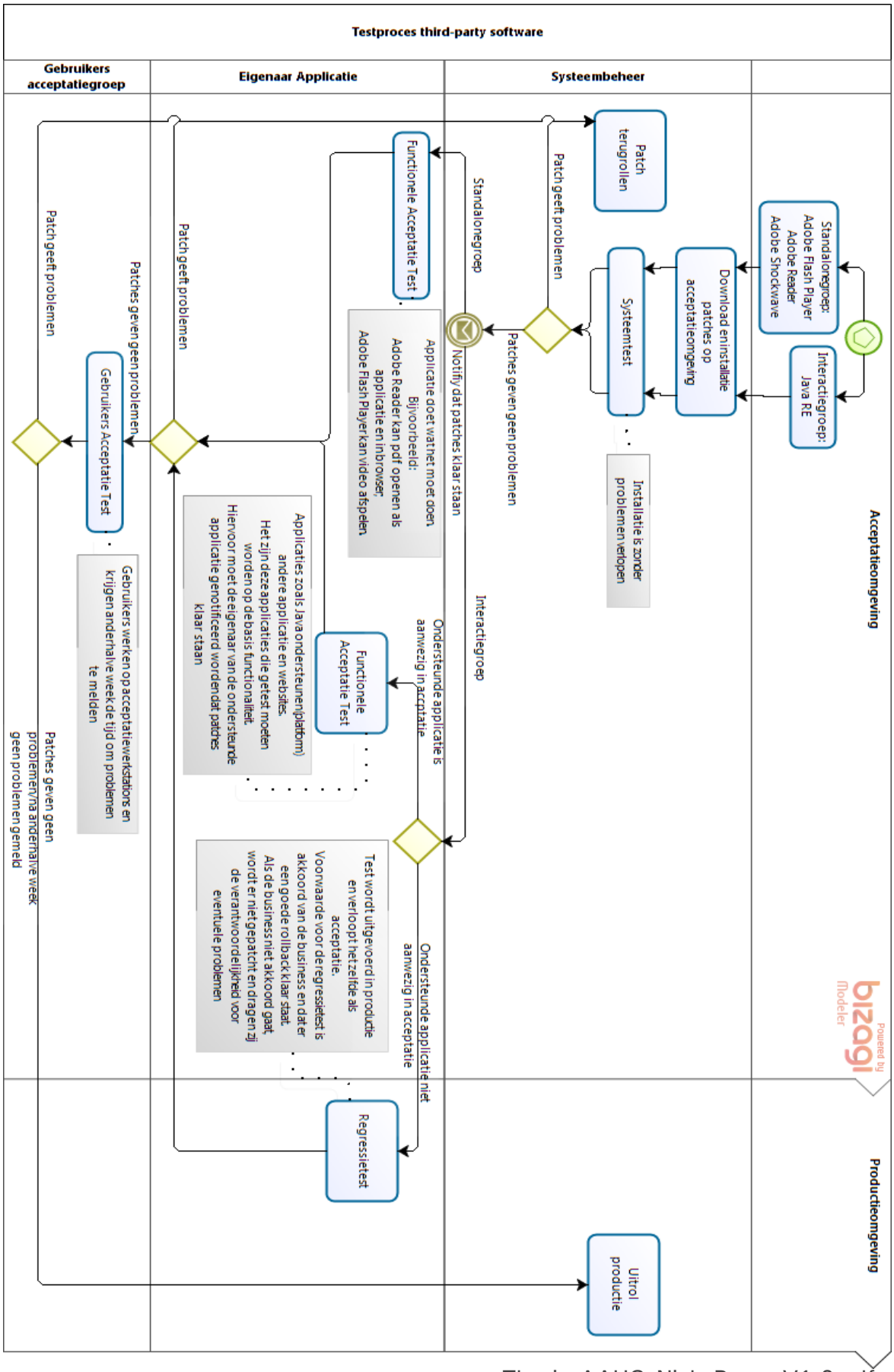
4.2 Technisch

Om het proces zo vlot mogelijk te laten verlopen is patchsoftware nodig. Voor het maken van packages en het distribueren naar de clients en servers kan gebruik worden gemaakt van SCCM. Hierdoor blijven alle packages onder een catalogus in SCCM staan. Voor het downloaden en ontvangen van notificaties bij nieuwe patches is echter wel extra patchsoftware nodig.
Bij de pakketselectie werd duidelijk dat patchmanagement software vaak alle acties uit handen (kunnen) nemen. Om nog gebruik te blijven maken van SCCM is patchmanagement software nodig dat met SCCM integreert.

De keuze voor patchmanagementsoftware moet ook lopen via ICT Development. Bij het vergaren van informatie bij een van de architecten werd aangegeven dat pakketselectie, in ieder geval voor hun, een project op zichzelf is. Het kunnen aanwijzen van de beste patchmanagement software in een korte periode is volgens hun niet mogelijk.

5 Testplan

Figuur 11 Testprocedure



Het testplan beschrijft hoe de patches efficiënt getest kunnen worden.
Het testproces, dat onderdeel is van het gehele third-party patch proces, staat beschreven in figuur 11.
Het testen wordt in drieën gesplitst en vindt plaats in de acceptatieomgeving.

Systeemtest
De systeemtest [ST] wordt uitgevoerd door systeembeheer nadat de patches gedownload en uitgerold zijn in de acceptatieomgeving. De systeemtest houdt in dat systeembeheer controleert of de patches goed zijn geïnstalleerd en dat de systemen nog stabiel zijn. Er zijn dus geen fouten opgetreden tijdens de installatie en ook de logboeken geven geen problemen aan.

Functionele Acceptatie Test
Bij de Functionele Acceptatie Test [FAT] wordt er onderscheid gemaakt tussen standalone applicaties en platformsoftware(interactie). De standaloneapplicaties zijn software die geen interactie hebben met andere applicaties. Voorbeeld hiervan is Adobe Reader die alleen ervoor zorgt dat een pdf bestand geopend kan worden.
Een voorbeeld van platformsoftware is Java RE. Java RE is voor sommige applicaties nodig om Java applets te kunnen draaien.

De FAT wordt uitgevoerd door de eigenaar van de applicatie. In het geval van de platformsoftware wordt dit gedaan door de eigenaar van de software die gebruik maakt van de platformsoftware.
De eigenaar zal dan met de FAT testen of de basis functionaliteit van de applicatie nog aan de gestelde eisen voldoet.

Omdat de Acceptatieomgeving nog niet volledig in gebruik is, zijn vele business kritieke applicaties hier nog niet aanwezig. Hierdoor wordt het testen van de platformsoftware op de business servers lastig. Onder voorwaarde dat er een rollback is en dat de business akkoord gaat, kan er een regressietest worden gedaan op de productieomgeving. Met de regressietest worden alle onderdelen van de applicatie getest of het nog juist functioneert. Als de business niet akkoord gaat met de regressietest, dan ligt bij hun de verantwoordelijkheid als er securityproblemen ontstaan.

Gebruikers Acceptatie Test [GAT]
Nadat de eigenaren klaar zijn met de FAT worden de patches gecontroleerd door de acceptatie groep. Gebruikers achter deze werkstations kunnen gewoon hun dagelijkse werkzaamheden doen. Mocht er na anderhalve week geen problemen met een gepatchte applicatie gemeld worden bij de servicedesk, dan kan de patch worden uitgerold in de productieomgeving.

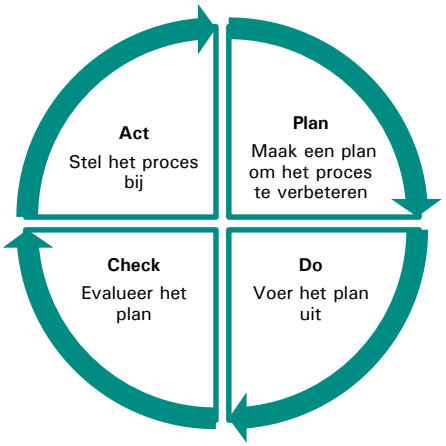
Rollback
Om in het geval van foute patches snel terug te kunnen naar een stabiele omgeving, is het nodig om een goede rollback klaar te hebben staan.
Hiervoor kan in feite dezelfde rollback worden gebruikt als bij de Windows patches.
Voor virtuele servers wordt een snapshot gemaakt voor snelle rollback. Voor de host VM is een herinstallatie het beste. Dit omdat een rollback op de host risicovol kan zijn.
Voor fysieke servers wordt de patch simpelweg teruggedraaid. Dit kan worden gedaan met SCCM.

6 Implementatieplan

Het implementatieplan beschrijft hoe het proces en de patchsoftware geïmplementeerd kan worden.

Proces

De implementatie van het proces is relatief eenvoudig aangezien het proces sterk lijkt op het Windows patchproces. Hierdoor zal de gewenningsperiode kort zijn. In de beginperiode is het wel van belang om het nieuwe proces telkens te beoordelen. Het gaat hier immers om een nieuw proces. Voor het beoordelen van het proces kan de kwaliteitscirkel van Deming uitkomst bieden. De cirkel beschrijft de vier activiteiten plan, do, check en act (Janssen, 2010, p. 34).



Figuur 12 Kwaliteitscirkel van Deming; Plan, Do, Check en Act

Evaluatie van het proces kan het beste in het CAB [Change Advisory Board] worden mee genomen.
Om het proces in gebruik te nemen moet er de volgende stappen worden ondernomen:

Inventarisatie

Er moet vooraf geïnventariseerd worden welke applicaties gebruik maken van platformsoftware zoals Java. Dit zodat de juiste testers op de hoogte gesteld kunnen worden.

Introductie

Beheerders en testers die met het proces gaan werken moeten het proces eerst doornemen zodat het duidelijk is wat de stappen zijn. Met name die zij moeten uitvoeren.

Communicatie

Afspraken met de eigenaren van applicaties en de business moeten worden gemaakt rondom het testen.

Planning

Het patchen moet vooraf gepland worden. Hiervoor moet een change worden aangevraagd. Omdat dit een nieuw proces is, is ook een impactanalyse nodig en wordt eerst in de CAB behandeld.

Uitvoeren

Het proces kan worden uitgevoerd. Na afloop moet het proces worden geëvalueerd. Dit kan gedaan worden met de bovengenoemde kwaliteitscirkel van Deming. Door gebruik te maken van de kwaliteitscirkel van Deming blijft een verbetering van het proces gewaarborgd.

Technisch

Als er gebruik gemaakt gaat worden van patchsoftware, dan ligt het aan de software hoe de implementatie gaat verlopen. In het geval van Secunia CSI [Corporate Software Inspector] met de PoC was dit redelijk eenvoudig aangezien Secunia een SaaS oplossing is. Alleen een plug-in voor Internet Explorer was nodig om het te kunnen configureren.

7 Pakketselectie

In dit hoofdstuk wordt SCCM 2012 met andere software vergeleken om zodoende de beste software te kunnen kiezen voor de notificatie en download van third-party patches. De resultaten en conclusie zijn te vinden in de gelijknamige hoofdstukken. De beste keuze zal in het Proof of Concept verder worden beoordeeld.

7.1 Pakketten

Selectie van de producten is tot stand gekomen aan de hand van het onderzoek van Gartner. Gartner heeft in hun Magic Quadrant voor client management tools verschillende pakketten onder de loop genomen. Uit het onderzoek van Gartner is bewust voor een aantal bekende bedrijven gekozen voor dit marktonderzoek. Dit omwille van de tijd dat het kost om elk pakket te behandelen. Verder zijn er twee pakketten eraan toegevoegd die ook patchsoftware leveren, en niet in de test van Gartner waren opgenomen. Het gaat om de volgende pakketten:

Microsoft SCCM in combinatie met Microsoft System Center Updates Publisher [SCUP]	LANDesk Management Suite
Dell Kace	Symantec Altiris Client Management Suite
Novell ZENworks	Secunia CSI
Solarwinds Patch Manager	

Tabel 11 Long list pakketten voor marktonderzoek

7.2 Methode

Voor het marktonderzoek wordt gebruik gemaakt van de COWS [Criteria, Options, Weights en Scores] methode. Met deze methode hebben de criteria een bepaald gewicht aan de hand van hoe belangrijk het is. Het gewicht kent waardes van 1 t/m 3.
De producten worden dan beoordeeld op de criteria en voorzien van een cijfer van 1 t/m 5, waarin 1 zeer slecht is en 5 zeer goed. Een nul geeft aan dat er geen informatie gevonden kon worden. De score voor elk criterium wordt als volgt berekend: $score = gewicht \times cijfer$. Door gebruik te maken van de COWS methode zullen de resultaten meer gericht zijn op de situatie van AAHG. De criteria en het gewicht zijn door de afdeling Infra- & Systeembeheer gekeurd. De criteria en gewicht waarop de producten worden beoordeeld, zijn als volgt:

Criteria	Gewicht
Microsoft omgeving compliant	3
Ondersteunt third-party software updates	3
Ondersteunt App-V applicaties	2
Toont alle patches	2
Notificatie nieuwe updates	2
Architectuur	2
Alleen download van patches mogelijk	2
Licenties	2
Gebruiksvriendelijkheid	2
Leverancier support	2

Tabel 12 Criteria en gewicht voor marktonderzoek

Van de zeven producten die worden onderzocht, wordt alleen de top 3 in detail beschreven.

8 Proof of Concept

In het Proof of Concept wordt het gekozen softwarepakket van de pakketselectie (Secunia CSI) getest in de acceptatieomgeving. Hiermee ontstaat inzicht in hoe het pakket werkt binnen de omgeving van AAHG en of het voldoet aan de wensen.

8.1 Doelstelling

Het doel van de PoC is om te zien of Secunia CSI geschikt is als patchsoftware voor third-party applicaties. Daarnaast kan ook door de PoC worden bekeken of patchsoftware in zijn algeheel geschikt is voor AAHG.

8.2 Werkzaamheden

Om de PoC uit te voeren is er beschikking nodig van de acceptatieomgeving. Daarbinnen is een SCCM omgeving nodig. Met andere woorden alle servers die SCCM nodig heeft. Verder is er minimaal een werkstation nodig die verbonden is met de genoemde SCCM server. Deze wordt gebruikt om de updates te ontvangen.
Secunia geeft de volgende technische eisen voor Secunia CSI.

De Secunia CSI 7.0 console (server):

- Minimale resolutie: 1024x768;
- Internet Explorer 8 of hoger;
- Internet connectie naar https://csi7.secunia.com;
- De adressen crl.verisign.net, crl.thawte.com en https://*.secunia.com moeten in de whitelist staan van de firewall/proxy;
- First-party cookies in Internet Explorer staan op zijn minst op prompt;
- Session cookies zijn toegestaan;
- Een PDF reader;
- WSUS installer;
- Visual C runtime;
- Microsoft .NET Framework runtime 4 of hoger;
- WSUS self-signed certificate voor patch deployment via WSUS of SCCM (optioneel).

Werkstation(s):

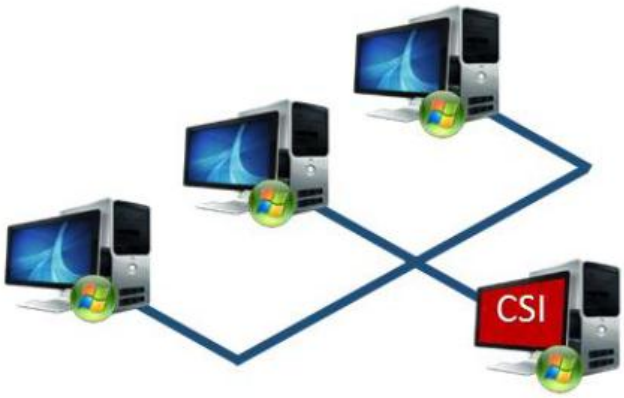
- Porten 139/TCP en 455/TCP moeten inbound open staan;
- File sharing moet enabled zijn;
- Easy/simple file sharing moet disabled staan;
- Windows Update Agent 2.0 of later moet aanwezig zijn.

Ook moeten de volgende services gestart zijn:

- Workstation service;
- Server service;
- Remote Registry service;
- COM+ services (COM+ System Application: set to automatic).

Met agent-less scans kunnen resultaten terugkomen als 'Partial'. Dit komt door de Windows firewall die RPC dynamic ports blokkeert. Een allow inbound RPC dynamic ports regel in de firewall voor de applicaties die hier gebruik van maken lost dit probleem op.
Voordat Secunia CSI wordt geïnstalleerd, moeten de servers voorzien worden van een snapshot. Dit voor een makkelijke rollback, mocht dat nodig zijn. Secunia CSI wordt op de SCCM server geïnstalleerd en zal daarna worden geconfigureerd om samen te kunnen werken met SCCM en WSUS.

De configuratie die wordt gebruikt tijdens de PoC is de agent-less configuratie.
Door voor agent-less te kiezen hoeft er geen agent te worden geïnstalleerd op de werkstations. Met agent-less is er de keuze om de systemen te scannen met Secunia zelf, of met SCCM. Secunia scant de systemen op basis van een IP range. Met SCCM worden systemen gescand die zijn verbonden met de upstream SCCM server door middel van de SCCM software inventory agent.
Scans van SCCM worden opgeslagen op de SQL server. De vergaarde data per host is 5 tot 10 MB.
Verder is er ook een plug-in voor SCCM. De plug-in integreert met WSUS, SCCM en Active Directory.



Figuur 13 Secunia agent-less scan. Overgenomen van Secunia (2013, p. 16) , http://secunia.com/?action=fetch&filename=Secunia_CSI7_Technical_User_Guide.pdf

De daadwerkelijke scan gebeurt met alle configuraties op dezelfde manier. Secunia CSI scant het systeem op metadata uit .EXE, .DLL en .OCX bestanden en stuurt deze op naar de Secunia process cloud. Data wordt via een beveiligde SSL verbinding (256-bit encryptie) verstuurd.

Een voorbeeld van de metadata die Secunia opstuurt:

c:\CD1\SETUP.EXE - PE Timestamp : 0x45d6922f
- Version : 5.2.3790.3959
- VendorName : Microsoft Corporation
- FileDescription : Welcome to Windows Server 2003
- FileVersion : 5.2.3790.3959 (srv03_sp2_rtm.070216-1710)
- InternalName : autorun
- LegalCopyright : Microsoft Corporation. All rights reserved.
- Filename : AUTORUN.EXE
- ProductName : Microsoft Windows Operating System
- ProductVersion : 5.2.3790.3959

De data wordt hier verwerkt en Secunia stuurt de applicatie naam met o.a. de versie en of de software out-of-date is terug. Voor controle kan gebruik gemaakt worden van wireshark om te zien of de pakketten daadwerkelijk versleuteld zijn.
Om de impact laag te houden, worden software pakketten gekozen die geen grote impact hebben met andere applicaties zoals Adobe Reader. Secunia moet aangeven welke patches vereist zijn en deze aanbieden.

Om App-V packages te scannen moet Microsoft Application Virtualization SFT view worden geïnstalleerd op de te scannen host. Door dit uit te voeren op de content server, moet Secunia in één keer alle App-V packages kunnen scannen.

De patch wordt dan gedownload, gepackaged en uitgerold naar de client.
Hierna volgt een controle via Secunia en een handmatige controle.

8.3 Testpunten

- Integratie;
  Het pakket werkt goed binnen de omgeving en kan ook integreren met SCCM.
- Gebruiksvriendelijkheid;
  Het pakket is overzichtelijk en gemakkelijk in gebruik. De gewenningsperiode is kort.
- Handmatige download patches;
  Patches kunnen handmatig worden gedownload.
- Handmatige packaging;
  Patches kunnen handmatig worden gepackaged.
- Ondersteunt App-V packages;
  Het pakket kan ook App-V packages scannen op versie.
- Notificatie;
  Het pakket heeft de mogelijkheid om notificaties te sturen als bijvoorbeeld nieuwe patches beschikbaar zijn.
- Informatie is daadwerkelijk versleuteld.
  Informatie dat verstuurd wordt naar de Secunia cloud is daadwerkelijk versleuteld.

8.4 Budget

Er is een keuze tussen standard en enterprise editie die zich onderscheiden in het aantal hosts binnen het netwerk en het aantal gebruikers. Verder is er ook nog verschil in de support die geleverd wordt. Voor prijzen moet echter contact worden gezocht met Secunia.

Secunia biedt de software voor 7 dagen gratis aan om te testen.

9 Resultaten

9.1 Proces

Het nieuwe patchproces is een aanpassing van het huidige Windows patchproces. Het Windows proces heeft hierin dus gediend als een 'best practice' vanuit AAHG. Het is al beschreven en werkt in de kern goed. Uit het literatuuronderzoek werd duidelijk dat frequentie en testen van belang zijn bij patchen. Het testen is het deel dat met name is aangepast aan het nieuwe proces vanwege de diversiteit van de applicaties die worden gepatcht met dit proces.

9.1.1 Te patchen software

Uit de theorie wordt duidelijk dat third-party patches net zo belangrijk zijn als de Windows patches. Een proces moet hiervoor dus worden ingericht.

9.1.2 Frequentie

Het is belangrijk dat er een vaste frequentie komt voor het patchen. Het informatiebeveiligingsbeleid geeft aan dat de deadline voor patchen tussen de twee weken en zes maanden ligt. De frequentie moet dus binnen deze tijd liggen.

Verder is het niet wenselijk om de third-party patches gelijktijdig met de Windows patches te installeren. Hierdoor wordt troubleshooting niet bemoeilijkt door twee verschillende patchprocessen. Ook is dit niet wenselijk vanuit changemanagement.

9.1.3 Testen

Het testgedeelte was het grootste onderdeel dat aangepast moest worden voor het proces. Net zoals bij Windows is er gebruik gemaakt van het gemengde test proces. Door op systeem, functioneel en gebruikers niveau te testen worden alle vlakken van een applicatie getest. Vanwege de diversiteit is de FAT gesplitst in applicatie- en platformsoftware. Dit is gedaan omdat platformsoftware niet direct getest kan worden en business kritieke applicaties kunnen ondersteunen. Door twee groepen te maken kan er meer controle worden gehouden.

Een PAT [Productie Acceptatie Test] is overwogen, maar niet geïmplementeerd. Third-party applicaties hebben doorgaans geen invloed op business applicaties waardoor het houden van een PAT als nazorg te veel van het goede kan zijn.

Het testplan (en het gehele proces) is al door een van de changemanagers bekeken, en had geen verdere op- of aanmerkingen.

9.2 Pakketselectie

Tabel 13 Decision matrix met de uitslagen van het marktonderzoek

In tabel 13 zijn de uitslagen te zien van het marktonderzoek. De scores van het marktonderzoek liggen dicht bij elkaar in de buurt. Dit is te verklaren doordat de verschillende software op papier allemaal de zelfde functionaliteit bieden, het zij wel door iedere leverancier anders geïmplementeerd. Juist door gebruik te maken van de COWS methode is de score iets verschoven, anders deelde drie pakketten een plaats. Uit het onderzoek heeft Dell Kace de hoogste score behaald.
De tweede plaats gaat naar Secunia CSI. De derde plaats wordt gedeeld door Microsoft SCCM 2012 in combinatie met SCUP 2011 en Solarwinds Patch Manager.

Microsoft SCCM 2012 in combinatie met SCUP 2011

Microsoft SCCM 2012 is de beheertool van Microsoft voor bedrijven. Het geeft bedrijven de mogelijkheid om op een centrale plek andere computers en mobiele apparaten te beheren. Zo is het onder andere in staat om software te distribueren en te inventariseren. Ook biedt het de mogelijkheid om o.a. Endpoint Protection te beheren en Windows updates te automatiseren (Microsoft, z.j.).

Gartner Magic Quadrant 2013
In de Magic Quadrant van Gartner staat SCCM bovenin bij de leaders. Volgens Gartner is het een zeer goede applicatie die goed schaalbaar is, erg slim en goed integreert met App-V. Daarnaast waarschuwt Gartner dat SCCM een zwaar server product is en geen ondersteuning heeft voor third-party software (zonder SCUP) (Gartner, 2013).

Microsoft omgeving compliant
SCCM is van Microsoft zelf en is volledig in staat om samen te werken met andere Microsoft producten zoals WSUS en App-V.

Ondersteunt third-party software
SCCM ondersteunt out-of-the-box geen third-party software. Om SCCM toch de mogelijkheid te geven om updates voor third-party software te downloaden, heeft Microsoft de gratis plug-in System Center Updates Publisher [SCUP] gemaakt (Microsoft, z.j.). SCUP is in staat om door middel van catalogs third-party software via WSUS of SCCM te downloaden.
De catalogs worden door de leveranciers van third-party software geleverd, of kunnen door een administrator zelf worden gemaakt.
Op het moment van schrijven bieden alleen Dell, HP en Adobe catalogs aan.
De support van leveranciers is dus erg mager. Verder is het zelf creëren van een catalog erg tijdintensief en moet voor elke third-party applicatie gebeuren (Anoop's, 2013). Er bestaat ook de mogelijkheid om de catalogs te kopen die door andere gemaakt zijn (Shavlik, 2013). Shavlik is momenteel in handen van LANDesk.

Ondersteunt App-V applicaties
App-V applicaties kunnen niet worden gescand op updates. Alle Microsoft updates worden direct aangeboden via WSUS of SCCM. Het zelfde geldt voor third-party applicaties, mits er gebruik wordt gemaakt van SCUP.

Toont alle patches
SCCM werkt standaard met WSUS en zal in dit geval alleen updates tonen voor Microsoft producten. Door gebruik te maken van SCUP kan er via WSUS ook alle third-party updates tonen. Ondanks dat er met SCUP alle updates getoond worden, moet er veel ingesteld worden voordat dit mogelijk is (Microsoft, 2012).

Notificatie
SCCM geeft geen ondersteuning voor notificaties als er nieuwe updates beschikbaar zijn. Wel is het mogelijk om alerts te genereren voor update compliance (Daalmans, 2012). Hiermee wordt een melding gegeven als een machines achter loopt met updates. Het missen van notificaties heeft geen grote impact als er op een vaste dag wordt gepatcht. Ook is het algemeen bekend dat Microsoft elke tweede dinsdag van de maand nieuwe updates vrijgeeft.

Architecture
SCCM is een softwarepakket dat lokaal geïnstalleerd wordt op een of meerdere servers, afhankelijk van de implementatie.
Verder is het mogelijk om distributie punten in de cloud te hebben. Dit kan bijvoorbeeld worden gerealiseerd met Windows Azure.
Op client pc's draait software center voor het pullen van software.

Alleen download van patches mogelijk
Met SCCM kan er op verschillende manieren worden omgegaan met updates. Zo kunnen er automatic deployment rules worden aangemaakt om updates geheel te automatiseren.
Verder kunnen er groepen worden aangemaakt met ieder zijn eigen update criteria. Ook kunnen updates alleen worden gedownload zodat een beheerder later zelf de deployment kan doen (Brady, 2011) (Microsoft, 2012).

Licenties
SCCM is onderdeel van de System Center en kent verschillende licenses.
De Managed Server licensing is gescheiden in de groepen Standard en Database.
Het verschil tussen deze pakketten is dat de Datacenter license meer Operating System Environments ondersteunt (Comsoft-direct, z.j.) (Microsoft, z.j., p. 4).
Voor het beheren van clients met SCCM is nog een extra Client Management license nodig per endpoint. Deze licenses zijn aanwezig in de Core en Enterprise Client Access Licensing, en blijven volgens Microsoft de meest kost efficiënte manier voor client licenses (Microsoft, z.j.).

SCUP 2011 zelf is gratis te verkrijgen.

Gebruiksvriendelijkheid
Met de komst van het Windows 8/Server 2012 laat Microsoft zien dat het zijn producten eenvoudig wilt maken. Dit is ook te zien in SCCM 2012 waar alles, ondanks de vele opties, nog duidelijk en overzichtelijk weet te blijven.
SCUP is echter nodig om third-party software te kunnen downloaden. Omdat catalogs niet goed worden ondersteund kan het erg omslachtig zijn om SCUP 2011 te gebruiken.

Leverancier support
Microsoft biedt support aan voor al zijn producten via de site TechNet. Deze site is zeer uitgebreid en de onderwerpen zijn relatief makkelijk te vinden. Verder kent Microsoft ook een actieve community op de TechNet forums.
Als laatste is er ook online support met een professional mogelijk. Het gebruik maken van deze mogelijkheid kan kosten met zich meebrengen (Microsoft, 2013) (Microsoft, z.j.).

Dell Kace

Dell Kace is de client management oplossing van Dell. Een van de vele taken die het kan verrichten is patchmanagement.

Gartner Magic Quadrant 2013
Ook Dell Kace is opgenomen in Gartners onderzoek en staat hoog bij de visionaries (bijna op de grens met de leaders). De Kace appliance is volgens Gartner zeer gemakkelijk in gebruik te nemen, goed voorzien van image en deployment tools en kent een van de grootste user communities.
De basis functionaliteit van de Kace is volgens Gartner niet zo uitgebreid vergeleken met de concurrentie. Ook kan het een uitdaging zijn om de Kace helemaal in te richten naar eigen voorkeur (Gartner, 2013).

Microsoft omgeving compliant
Dell Kace ondersteunt Windows, Mac OS X en een aantal Linux distributies. Verder is er ondersteuning voor 32-bit en 64-bit systemen. Ook ondersteunt Kace Active Directory (Dell, z.j.).

Ondersteunt third-party software
Dell Kace biedt ondersteuning voor verschillende bekende third-party software zoals Java en Flash Player. Echt veelzijdig is het dus niet, maar het zorgt wel ervoor dat in ieder geval de bekende third-party software up-to-date kan worden gehouden (Dell, 2013, p. 5).

Ondersteunt App-V applicaties
Kace ondersteunt App-V in de zin van distribueren van software. Het hebben van de App-V software is nog steeds nodig. De App-V applicaties die door Kace worden gedistribueerd, worden ook opgenomen in de inventory (Gasaway, 2012). Hiermee kan een beheerder op de hoogte blijven van de status van zowel lokaal geïnstalleerde software als App-V applicaties.

Toont alle patches
Kace toont voor de ondersteunde applicaties zowel de functionele als de security patches.

Notificatie
Beheerders kunnen met Dell Kace notificaties ontvangen als er nieuwe updates beschikbaar zijn. De Kace appliance neemt geen verdere actie zoals downloaden en installeren (Dell, z.j., p. 232).

Architecture
Dell Kace is geen software die wordt geïnstalleerd, maar een appliance. Verder maakt Kace gebruik van client agents om informatie van de workstations te krijgen.

Alleen download van patches mogelijk
Alleen downloaden van patches is mogelijk. Het downloaden staat los van de deploy schedule (Dell, 2012, p. 9).

Licenties
De totale implementatie kosten voor 1000 endpoints, tien verschillende locaties over 3 jaar bedragen voor Dell Kace $24.800,- (Dell, z.j.).

Gebruiksvriendelijkheid
De appliance is via een browser te benaderen en oogt erg minimalistisch. Hierdoor is het overzichtelijk en moet beheer geen problemen geven (Dell, z.j.).

Leverancier support
Dell biedt ook een uitgebreide support. Zo is er toegang tot een knowledge base, verschillende training programma's, Nederlandse contact support en een community. Dell host op zijn website geen community. De community van Dell is te vinden op de IT site ITNinja.com (Dell, z.j., p. 152).

Secunia CSI (SC2013 Plug-in)

Secunia is een Deens bedrijf dat zich specialiseert in security. Ze zijn met name bekend op het gebied van patchen, vinden van zero-days en het maken van security trendanalyses. Secunia Corporate Software Inspector [CSI] is de tegenhanger van de Secunia Personal Software Inspector [PSI] software. Waar PSI zich richt op particulieren, is CSI gericht op bedrijven. Secunia CSI is een stukje software dat alle applicaties inventariseert en aangeeft wanneer software out-of-date is.

Gartner Magic Quadrant 2013
Secunia CSI is een van de twee pakketten dat niet in Gartners Magic Quadrant voorkomt.
Dit komt omdat het een patchoplossing is en niet een client management tool.

Microsoft omgeving compliant
Secunia CSI werkt volledig binnen een Microsoft omgeving. Het integreert met System Center en WSUS om zodoende patchen te vergemakkelijken (Secunia, z.j.). Secunia heeft ook een plug-in beschikbaar voor SCCM. Hierdoor kan alles binnen de console van SCCM gedaan worden.

Ondersteunt third-party software
De software van Secunia is gericht op third-party applicaties. Zelf promoot Secunia dat hun software duizenden leveranciers ondersteunt en meer dan 20.000 applicaties (Secunia, z.j.). Daarnaast hanteren ze een dynamische patch catalogus waardoor support voor nieuwe applicaties alleen maar groeit (Secunia, z.j.). Mocht een applicatie niet door de scanner worden ondersteund, dan is er de mogelijkheid dit bij Secunia aan te geven. Bij voldoende animo wordt de applicatie opgenomen in hun database (Secunia, z.j., p. 5).

Ondersteunt App-V applicaties
Secunia CSI heeft ook de mogelijkheid om App-V applicaties te scannen en te voorzien van updates. Om dit mogelijk te maken moet eerst de Application Virtualization SFT viewer van Microsoft worden geïnstalleerd. Dit is een gratis tool van Microsoft. Daarnaast scant CSI niet de hosts, maar de server die alle App-V packages host (Mangan, 2011).

Toont alle patches
De producten van Secunia zijn alleen gericht op security patches. Hierdoor zullen functionele patches niet worden aangeboden door CSI.

Notificatie
Smart Group Notification geven de mogelijkheid om e-mail en SMS alerts te versturen als bepaalde events getriggerd worden. Welke opties hier allemaal voor zijn geeft Secunia niet, afgezien van een paar voorbeelden. Zo noemen ze al de mogelijkheid om een notification te krijgen als er een nieuwe critical bulletin is.

Architecture
Secunia CSI is SaaS [Software as a Service] georiënteerde software dat door middel van een browser plug-in werkt. Ook wordt er een plug-in aangeboden voor SCCM zodat het management binnen een console gedaan kan worden. Verder heeft de software toegang tot het internet nodig. De resultaten van de scan worden via een SSL verbinding (256-bit encryptie) naar Secunia gestuurd. Daar worden de resultaten met hun database vergeleken en bepaald welke software out-of-date of End-of-Life [EOL] is.
De SCCM plug-in bestaat uit twee onderdelen, de plug-in zelf en de Secunia Daemon. De daemon is verantwoordelijk voor de scheduled jobs. Scannen gebeurt op basis van agent scans. Mocht dit niet wenselijk zijn, dan kan er ook een agentless scan plaatsvinden. Deze wordt uitgevoerd door naar de hosts te kijken die verbonden zijn met SCCM. Data wordt verzameld met de SCCM software inventory agent.

Alleen download van patches mogelijk
CSI is gericht op het automatisch packagen van updates. Dit is erg makkelijk als de applicaties lokaal geïnstalleerd zijn. Voor App-V applicaties is dit echter niet mogelijk. Hoewel niet duidelijk aangegeven, geeft CSI wel de mogelijkheid om updates handmatig te downloaden. Dit gaat via URL's naar de download pagina van de leverancier.

Licenties
Er is een keuze tussen standard en enterprise editie die zich onderscheiden in het aantal hosts binnen het netwerk en het aantal gebruikers. Verder is er ook nog verschil in de support die geleverd wordt. Voor prijzen moet echter contact worden gezocht met Secunia.

Gebruiksvriendelijkheid
De console van Secunia CSI toont veel informatie en kan in het begin nog erg wennen zijn. De GUI is echter goed en overzichtelijk ingericht, en moet voor patchen geen problemen geven. Ook de plug-in variant integreert goed met SCCM.

Leverancier support
Support wordt geleverd met de gekozen licentie. Met de standard licentie wordt er alleen support geleverd voor een 'setup call'. De Enterprise licentie kent deze support niet, maar biedt wel 'full solution setup and implementation support' en telefoon support. Beide licenties bieden ook e-mail support. Ook is er een community waar vragen kan worden gesteld.

Solarwinds Patch Manager

Solarwinds is een bedrijf dat binnen de IT bekend is voor zijn grote aanbod van management producten. Zo biedt Solarwinds ook een patchmanager aan om betere controle te krijgen over de updates die uitkomen. Verder maakt AAHG al gebruik van Solarwinds om inzicht te krijgen van het netwerk.

Gartner Magic Quadrant 2013
Solarwinds Patch Manager is het andere pakket dat niet voorkomt in Gartners Magic Quadrant. Ook hiervoor geldt dat Patch Manager geen client management tool is.

Microsoft omgeving compliant
Ook Solarwinds kan overweg met een Microsoft omgeving. Het ondersteunt onder andere Active Directory, SCCM en WSUS. Patch Manager is een add-on dat via een Microsoft Management Console [MMC] wordt beheerd. Ook is er een web console aanwezig (Solarwinds, z.j.).

Ondersteunt third-party software
De ondersteuning van third-party software is bij Solarwinds ook minimaal. Net zoals andere pakketten die in dit document vergeleken zijn, biedt Solarwinds ondersteuning voor een aantal bekende third-party software zoals: Abode Flash, Adobe Reader, Citrix receiver en Oracle Java Runtime Environment (Solarwinds, z.j.).

Ondersteunt App-V applicaties
Solarwinds ondersteunt geen App-V applicaties. App-V applicaties kunnen dus niet worden gecontroleerd op updates. Doordat Patch Manager wel alleen downloads toestaat, is het wel mogelijk om de update te downloaden (mits ondersteund door Patch Manager) en de App-V package zelf te patchen.

Toont alle patches
De Patch Manager software toont zowel functionele als security patches (Solarwinds, 2012).

Notificatie
Patch Manager biedt de mogelijkheid tot het versturen van e-mail notificaties, mits het geïnstalleerd is als application server. Hierdoor kan het een e-mail sturen als er nieuwe, verlopen of aangepaste updates zijn gesynchroniseerd (Solarwinds, 2013, p. 188).

Architecture
Solarwinds wordt lokaal geïnstalleerd. Clients ontvangen hun updates door middel van de Windows Update Agent. Ook is het mogelijk updates te deployen met Update Management (Solarwinds, 2013, p. 33).

Alleen download van patches mogelijk
Omdat de updates ook zelf gepackaged kunnen worden, is het ook mogelijk om eerst alleen de updates te downloaden (Solarwinds, 2012).

Licenties
Prijzen voor Patch Manager beginnen vanaf €2.850,-. De prijzen voor licenties zijn gebaseerd op het aantal nodes dat gepatcht moeten worden. Voor 1.000 nodes bedraagt de prijs €7.330,- (Solarwinds, z.j.).

Gebruiksvriendelijkheid
Solarwinds biedt op hun site (SolarWinds Patch Manager - Embedded Interactive Demo, z.j.) de mogelijkheid om gebruik te maken van een demo. Hoewel de demo niet geheel live is, geeft het wel een beter inzicht de gebruiksvriendelijkheid dan sceenshots. De web console weet nog goed overzichtelijk te blijven. De console is echter erg vol. Er wordt veel informatie getoond en er is zeker een gewenningsperiode nodig.

Leverancier support
Ook Solarwinds geeft op vele vlakken support. Zo is er op hun site documentatie te vinden en een knowledgebase. Verder maken ze blogs en is er een community. Ook is er de mogelijkheid om Solarwinds gecertificeerd te worden. Hiervoor wordt er via de Learning Center informatie aangeboden. Achteraf moet er een examen worden afgelegd.

9.3 Proof of Concept

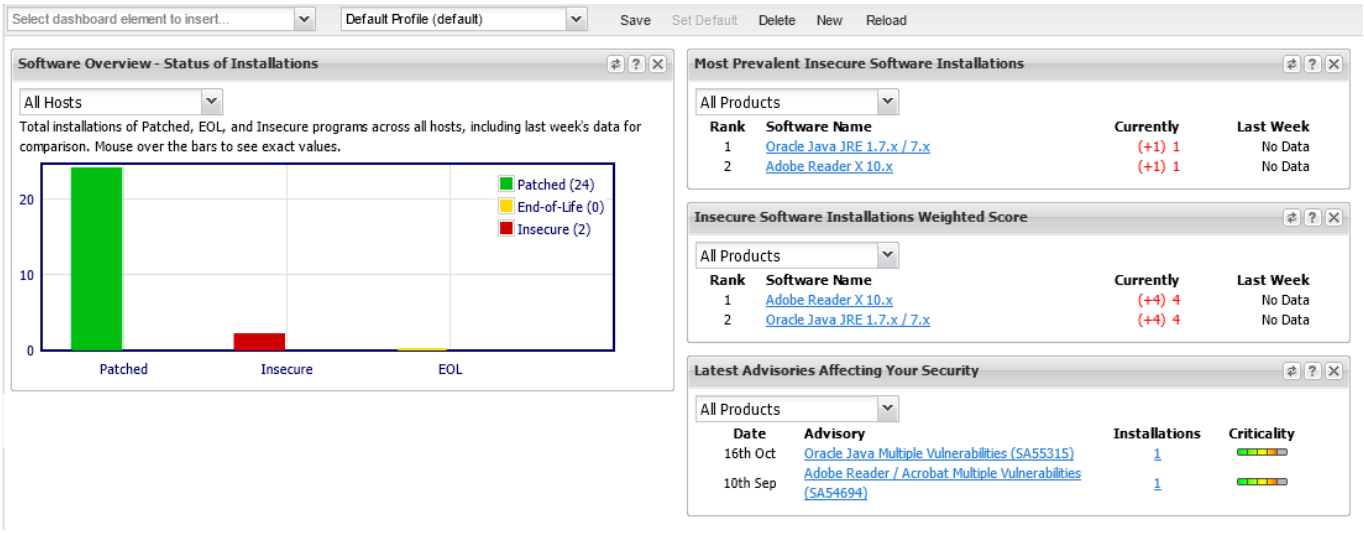
Het plan was om de PoC in de acceptatieomgeving uit te voeren om zodoende de productieomgeving niet te storen. De acceptatieomgeving was echter nog niet klaar voor gebruik (het project OTA [ontwikkel, test en acceptatie loopt nog) waardoor de PoC verplaatst is naar de testomgeving.
Voor de PoC is gebruik gemaakt van een host die via SCCM een verouderde versie van Java RE en Adobe Reader heeft ontvangen. De plug-in voor SCCM kon helaas niet geïnstalleerd worden. Om hiervoor toegang te krijgen wordt er door Secunia contact gezocht voor een speciaal account om gebruik te maken van de SCCM plug-in.

Integratie
Secunia CSI 7 is een SaaS applicatie die te benaderen is via csi7.secunia.com. Bij het eerste keer opstarten, wordt er gevraagd om een Internet Explorer [IE] plug-in te installeren. Dit is een andere plug-in dan die voor SCCM, maar zorgt er wel voor dat Secunia vanuit de browser kan communiceren met de WSUS en SCCM servers. Om verbinding te maken met WSUS en SCCM is het verder nodig dat Internet Explorer gestart wordt als administrator.
Secunia maakt contact met SCCM zodat er gebruik gemaakt kan worden van de software inventory import. Contact met WSUS wordt gezocht voor de packages die beschikbaar zijn en welke hosts verbonden zijn met de WSUS server.
Om WSUS te configureren moet er naast de genoemde technische eisen ook een Group Policy Object [GPO] worden gemaakt. Secunia kan dit zelf, maar gaf tijdens de PoC foutmeldingen. Er is handmatig een GPO aangemaakt waarin de gegenereerde self-signed certificate voor WSUS werd meegegeven voor clients. Verder zijn de volgende settings aangezet in computer configuration, administrative templates, Windows components, Windows updates:

- Configure automatic updates;
- Specify intranet Microsoft Update service location;
- Allow signed updates from an intranet Microsoft update service location.

Als Secunia goed geconfigureerd is, is er sprake van een goede integratie met WSUS en SCCM. De SaaS oplossing van Secunia leunt wel zwaar op WSUS waardoor het nut van SCCM af neemt. Zo komen de patches niet in de software library te staan en wordt er geen gebruik gemaakt van de SCCM software center.

Gebruiksvriendelijkheid
De console van Secunia went erg snel en is zeer overzichtelijk. Met name het dashboard biedt in een oogopslag de status van de hosts. Verder kan het dashboard zelf worden ingericht met de widgets.

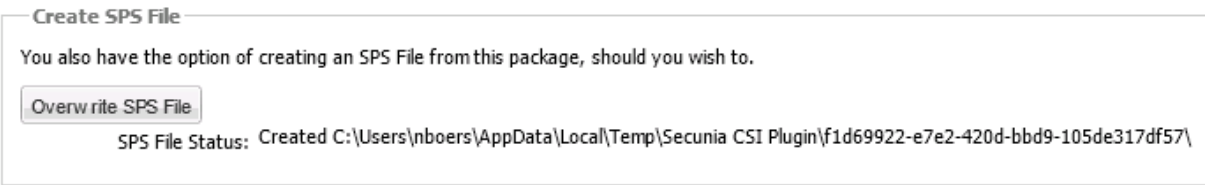


Figuur 14 Secunia CSI 7 dashboard

Minpunten van Secunia zijn dat de console traag is, wat niet fijn werkt. Ook is er een merkbare vertraging tussen de resultaten van een scan en de aangeboden patches. Zo gaf een scan aan dat er onveilige software aanwezig was, maar duurde het soms lang voordat de patches ook aangeboden werden. Verder worden de aangeboden patches (en compliance status) gebaseerd op de laatste scan. Dit betekent dat voor de meest accurate informatie alle hosts in een keer gescand moeten worden, wat dus niet ideaal is. Voor het gebruik van de software inventory tool is het mogelijk om scanschema's te maken waarmee hosts in groepen kunnen worden verdeeld en op vaste tijden gescand kunnen worden.

Handmatige download patches

Patches worden door Secunia niet automatisch gedownload. Bij het maken van een package in Secunia kan er worden gekozen om een SPS [Secunia Package System] file te maken. In dit geval zal Secunia de installer naar de Temp folder in de user profile downloaden. Voor Adobe Reader en Java RE werd een .exe gedownload. Hoewel hier ook een package van gemaakt kan worden, gaat de voorkeur bij AAHG uit naar .msi bestanden.



Figuur 15 Lokale download van patch

Handmatige packaging

Het is de opzet van Secunia dat er gebruik wordt gemaakt van de Secunia Package System [SPS]. Bij het maken van de package is onder andere de optie om het install script aan te passen in Javascript, PowerShell en VBscript. Verder kan er met SPS ook andere parameters worden meegegeven zoals het verwijderen van de EULA. Hierdoor kunnen packages sneller gemaakt worden zonder het script aan te passen. Een ander optie voor het maken van een package is de .exe downloaden en met SCCM de package bouwen. Dit is echter een omweg als het op snelheid aankomt.

Product	Vendor	Patched Version	Architecture	SAID	Criticality	Detected
Product: Adobe Reader X 10.x (1 Item)						
Adobe Reader X 10.x	Adobe Systems	10.1.8	Unspecified	SA54694		0 days, 0 hours, 13 mi...
Product: Oracle Java JRE 1.7.x / 7.x (1 Item)						
Oracle Java JRE 1.7.x...	Oracle Corporation	7u45	Unspecified	SA55315		0 days, 0 hours, 13 mi...

Figuur 16 Aangeboden patches

De package kan gedistribueerd worden naar de groepen zoals die in WSUS staan.

Ondersteund App-V applicaties

App-V maakt gebruik van .sft bestanden. Het .sft bestand kan gezien worden als een .iso. Om de .sft bestanden de lezen is er de tool Application Virtualization SFT View nodig. Deze tool plaatst een map naast de .sft waarin de inhoud van de .sft te zien is. Hierdoor kan Secunia de bestanden lezen en scannen. Het scannen is gedaan op de SCCM server waar de App-V package staat.

Overview | Scan Result | Patch Information | Patches Available

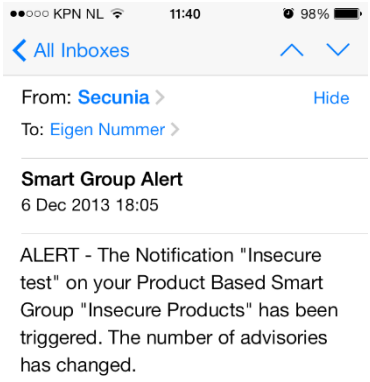
☑ Patched ☑ End of Life ☑ Insecure

Name	Version	State
Adobe Photoshop 6.x	6.0.128.0 (APP-V)	End of Life

Figuur 17 App-V scan resultaat

Notificatie

Smart-groups kunnen gebruikt worden om notificaties te krijgen. Voor de PoC is gebruik gemaakt van de build-in smartgroup dat zich richt op gescande software en advisories. De notificaties werden ingesteld zodat ze elk uur een mail stuurde. De trigger was een positieve of negatieve verandering van de insecure test groep. Een nieuwe scan werd gedraaid om zo de laatste resultaten aan te passen. Na een uur kwamen de mails netjes binnen. Erg informatief zijn ze niet. Er wordt alleen aangegeven dat er veranderingen hebben plaatsgevonden.



Figuur 18 Secunia Notificatie

Versleutelde informatie

Omdat Secunia CSI een SaaS oplossing is, is communicatie over het internet noodzakelijk. Om te controleren of Secunia daadwerkelijk de verbinding versleuteld, zoals ze beweren, is Wireshark geïnstalleerd op de SCCM server. De beveiligde verbinding wordt gemaakt bij het aanmelden op de site. Wireshark vangt vanaf dat moment HTTPS en TLSv1 pakketten. Encryptie gebeurt met een RSA 256-bit key. De hostname van de destination address is via een tracert achterhaald, en komt uit bij csi7.secunia.com.

```
⊟ Secure Sockets Layer
  ⊟ TLSv1 Record Layer: Handshake Protocol: Client Key Exchange
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 262
    ⊟ Handshake Protocol: Client Key Exchange
        Handshake Type: Client Key Exchange (16)
        Length: 258
      ⊟ RSA Encrypted PreMaster Secret
          Encrypted PreMaster length: 256
          Encrypted PreMaster: 2a59dc3b25dde822198f714db7838b405b5cb3dec5047906...
```

Figuur 19 Secunia client key exchange

Verdere bevindingen
Secunia CSI heeft een gemengde indruk achtergelaten. Hoewel het pakket doet wat het moet doen, is het op sommige momenten erg traag, duurt het soms lang voordat patches worden aangeboden en leunt het zwaar op WSUS. Zo distribueert het de nieuwe packages naar WSUS in plaats van SCCM. Waardoor de patches niet centraal in SCCM staan en er ook geen gebruik gemaakt kan worden van SCCM software center. Een ander nadeel van Secunia is dat het zoekt naar patches binnen de versie. Zo werd voor de PoC ook Cisco Jabber versie 9.0.2 geïnstalleerd op de client. Secunia detecteerde met de scan de applicatie wel maar bood geen patch aan. Op de site van Secunia (Cisco - Secunia, z.j.) is te zien dat alleen Cisco Jabber versie 8 is opgenomen in hun database.

Positieve punten van het pakket zijn onder andere het package systeem en de mogelijkheid om de patch te downloaden. Het was erg gemakkelijk om een patch te downloaden en een package te maken. De kracht van patchsoftware werd meteen duidelijk. Ook de compliance status en hoe kritiek het is om te patchen draagt hieraan bij.

10 Conclusies

10.1 'Lessons learned' Windows proces

Tijdens de inventarisatie van de huidige situatie is aan systeembeheer gevraagd naar de geleerde lessen. Hierop was geen feedback. Echter zijn na het inventariseren van het Windows proces zelf wel een aantal punten te vinden waar met het schrijven van het nieuwe proces op gelet kan worden:

- Proces moet voldoen aan gestelde eisen, beschreven in het informatiebeveiligingsbeleid;
- Er is mogelijkheid tot testen op een acceptatieomgeving;
- Rapportage naar ICT management;
- Systeembeheer en Applicatiebeheer zijn de uitvoerende partijen;
- Een vaste datum voor uitrol updates gelijktijdig met/twee weken na uitrol Windows updates mits een lage impact;
- Third-party software die impact/interactie heeft op/met business software moeten extra aandacht krijgen, bijvoorbeeld Java;

Verder is er met het literatuuronderzoek duidelijk geworden dat de frequentie van het patchen en testen van de patches erg belangrijk zijn.

10.1.1 Te patchen software

De wens van AAHG is een nieuw patchproces die de third-party software onder handen neemt. Het gaat hier niet alleen om de huidige software maar ook om software die later in gebruik worden genomen. Vanwege de kwetsbaarheid van de applicaties is het ten zeerste aan te raden om Java RE, Adobe Flash Player en Adobe Reader te patchen. Dit zijn de applicaties die aanwezig zijn en vaak worden misbruikt. Ondanks dat de andere third-party software minder snel geëxploiteerd worden, moeten ook deze gepatcht worden. Dit onder het motto *'A chain is only as strong as its weakest link'.*
Het voordeel om in het begin alleen de drie genoemde applicaties te patchen is dat overzicht bewaard kan worden en minder verandering teweeg brengt.

10.2 Frequentie

Omdat het, afgezien van Adobe, niet te zeggen is wanneer de patches uitkomen, is het lastig om de beste dag te kiezen. Dit vanwege het informatiebeveiligingsbeleid en dat het proces applicaties van verschillende leveranciers patcht. Omdat het ook niet mag botsen met het Windows proces, kan het proces het beste een week na de uitrol van de Windows patches worden uitgevoerd. Dit is de vierde dinsdag van de week en keert maandelijks terug.

10.3 Testen

Voor het testen kan het beste gebruik worden gemaakt van een gemengde test. Dit bestaat uit een ST, FAT en GAT. De third-party applicaties dienen voor de FAT gesplitst te worden.
Er is namelijk sprake van echte applicaties zoals de Adobe producten en platformsoftware zoals Java. De platformsoftware kan niet direct worden getest. Dit moet gebeuren via de applicatie die gebruik maakt van de platformsoftware.
Afgezien van de splitsing is de FAT niet uitgebreid. Met de FAT wordt gecontroleerd of de applicatie nog de functionaliteit biedt die nodig is voor dagelijkse werkzaamheden.

Voor het testen van de platformsoftware moet wel eerst worden geïnventariseerd welke applicaties en websites gebruik maken van de platformsoftware. Deze duidelijkheid is er nog niet. Het is nog niet opgenomen in de CMDB en ook applicatiebeheer heeft geen precieze aanduiding welke applicaties er allemaal gebruik van maken.

10.4 Pakketselectie

Voordat er verder op de conclusie van het marktonderzoek wordt ingegaan, moet eerst worden vermeld dat de behaalde scores zijn gebaseerd op informatie van het internet en zijn vergaard in een korte periode. Om een goed en volledig beeld te krijgen van alle mogelijkheden is het nodig om ook hands-on ervaring op te doen met de verschillende (trial) software die wordt aangeboden. Dit heeft tijd nodig die in dit onderzoek simpelweg niet aanwezig is. De PoC die uitgevoerd wordt, zal maar een product behandelen.
Ook is er maar een aspect behandeld van client management tools, en dat is third-party patching. De uitslag geeft dus alleen weer hoe sterk de pakketten zijn op het gebied van third-party patching.

De opzet van de pakketselectie was om te kijken of SCCM de beste software was voor het uitrollen van third-party patches. Hiervoor is SCCM vergeleken met andere client management tools en patchmanagement software. Hieruit komt SCCM sterk naar voren. Het is samen met Dell de enige client management tool die de shortlist heeft gehaald. De andere twee pakketten in de shortlist zijn patchmanagement software.

Ondanks dat Dell Kace het hoogst scoort, betekent het niet dat dit ook de beste keus is voor AAHG. Het gaat hier om een appliance en is in ieder geval niet geschikt voor een PoC in dit onderzoek. Dit omdat het een appliance is en er onvoldoende tijd is om dit aan te vragen en te testen in een PoC.
Verder is Dell Kace een complete vervanging van SCCM. Hoewel Dell third-party patchmanagement beter heeft geïmplementeerd, is het onnodig om SCCM compleet te vervangen. Dit omdat SCCM bij AAHG o.a. op het gebied van Windows patching en uitrol van software zijn werk goed doet.

Secunia CSI staat op de tweede plek en is geen appliance. Hoewel Secunia goede integratie kent met SCCM en veel leveranciers ondersteunt, zijn er nog wel vraagtekens bij de manier van patchen. Het stuurt namelijk niet-persoonlijke informatie naar Secunia om zo te bepalen welke software out-of-date of EOL is. Het uploaden van data, ondanks dat het niet-persoonlijke data is, kan een reden zijn om toch geen gebruik te maken van Secunia.
Dit is voorgelegd bij de afdeling informatiebeveiliging, en die zagen geen problemen erin.

SCUP 2011 deelt de derde plek met Solarwinds. Ook deze pakketten hebben zo nog hun nadelen. Zo kan SCUP nog erg lastig en tijdsintensief zijn om update catalogs te maken. Verder zijn er maar drie leveranciers die catalogs leveren. Solarwinds zit in vergelijking met SCUP beter in elkaar. Echter biedt het net zoals vele andere patch software (met uitzondering van Secunia) niet voor alle applicaties patches. Alleen bekende third-party wordt ondersteund.

Verder kwam er tijdens het marktonderzoek vanuit informatiebeveiliging nog een andere optie, vulnerability managementsoftware zoals Qualys.

Deze software wordt door een derde partij gebruik voor de jaarlijkse vulnerability scan bij AAHG. Het verschil tussen deze software en de andere twee is dat vulnerability managementsoftware geen patches kan downloaden. Het biedt alleen inzicht in compliance.
Hoewel dit een goed alternatief is aangezien de compliance van de systemen gecontroleerd kan worden, moet niet worden vergeten dat het proces globaal is opgezet en de te patchen software kan groeien. Als er toch voor software gekozen wordt, kan het beter een compleet pakket zijn.

Met het markonderzoek is wel duidelijk geworden dat patchsoftware nog erg weinig third-party software ondersteund en in zekere zin nog in de kinderschoenen staat.
Het advies luidt dan toch om een grotere PoC te houden met Secunia CSI. Het integreert goed met SCCM waardoor SCCM niet vervangen hoeft te worden en ondersteunt vele leveranciers en third-party software, in tegenstelling tot de meeste andere pakketten.

10.5 Proof of Concept

Secunia CSI heeft een gemengde indruk achter gelaten. Aan de ene kant werd de kracht van patchmanagement software duidelijk en aan de andere kant werkte het niet vloeiend. Verder leunde het erg veel op WSUS.
De positieve indruk is echter genoeg om te adviseren om patchmanagement software verder te onderzoeken en uiteindelijk te implementeren. Met name de SCCM plug-in van Secunia kan nog veel goed maken als het vloeiender draait en SCCM meer betrekt met het patchen.

11 Advies

Het advies is onderverdeeld in het advies voor het proces en de techniek (software) die het proces eventueel kan ondersteunen.

11.1 Proces

Het proces dient zo snel mogelijk worden ingevoerd. Daarbij zijn de onderstaande punten van belang. Voor de implementatie kan worden gerefereerd naar het implementatie plan.

11.1.1 Te patchen software

Op den duur moeten alle third-party applicaties worden gepatcht. Vanwege het uitzoeken van de exoten en de introductie van een nieuwe proces, kan begonnen worden met het patchen van Adobe Flash Player, Adobe Reader en Java RE. Deze applicaties zijn de grootste constante dreiging voor de veiligheid bij AAHG.

11.1.2 Frequentie

Er dient maandelijks gepatcht te worden als er patches beschikbaar zijn. Het proces start in de week na de Windows updates. Specifiek is dit de vierde dinsdag van de maand.

11.1.3 Testen

Testen moet goed gebeuren om de productieomgeving zo min mogelijk te storen. De patches zullen met een gemengde test worden gecontroleerd op stabiliteit. De gemengde test bestaat uit een ST, FAT en GAT. De FAT dient opgedeeld te worden in twee groepen, de standalone applicaties en de platform applicaties. Dit vanwege de aard van de platform software. Details voor het testen zijn te vinden in het testplan.

11.1.4 Exoten

De exoten zijn de ongewenste software die aanwezig zijn binnen AAHG. Hoewel het uitzoeken van de exoten nog loopt, is het wel aan te raden om zoveel mogelijk software en verschillende versies op te ruimen. In tabel 8, te vinden in hoofdstuk 3 van het adviesrapport, is te zien dat er verschillende versies van een applicatie aanwezig zijn. Het bevat een extract van de inventarisatietool SNOW. In de tabel is te zien dat sommige versies niet meer gebruikt worden. Voor de veiligheid van de informatiesystemen moeten deze verouderde versies worden verwijderd.

11.2 Technisch

Het advies met betrekking tot de software is om toch patchmanagement software te implementeren als aanvulling voor SCCM. Met voorkeur een die ook met SCCM integreert om zo beter overzicht te houden in de console en die een goed de compliance kan tonen.

Het advies wordt verstrekt door de PoC, waarin de kracht van patchsoftware duidelijk werd.
Aangeraden wordt om een project te starten voor het in gebruik nemen van patchmanagement software. De plug-in voor SCCM van Secunia zou hier zeker in meegenomen moeten worden. De plug-in zou meer gebruik maken van SCCM, waardoor SCCM weer tot zijn recht komt.

11.3 Toekomstige projecten

Na de implementatie van het nieuwe proces, kan er gekeken worden naar andere projecten die de veiligheid vergroten.

Patchmanagementsoftware

Patchmanagementsoftware moet gekozen worden om het third-party patchproces te ondersteunen en deels te automatiseren. Hiervoor moet een diepgaander project worden opgezet waar ook IT Development bij betrokken wordt. Zoals in het advies al vermeld zou de SCCM plug-in van Secunia zeker overwogen moeten worden. Secunia CSI heeft met de PoC al veel potentie getoond.

Remote remediation

Met de komst van het nieuwe werken en BYOD wordt het in stand houden van het bedrijfsbeleid omtrent de security steeds lastiger. Hoewel NAP en andere remediation oplossingen niet wenselijk zijn op kantoor, wordt er wel door vele werknemers thuisgewerkt. Hiervoor wordt gebruik gemaakt van Citrix XenDesktop. Hoewel de verbinding van XenDesktop goed beveiligd is, is dit meestal niet het geval van een thuis computer. Om ook de thuis computer te beveiligen kan er gebruik worden gemaakt van Citrix Access Gateway Endpoint Analysis. De Endpoint Analysis draait een scan voordat de client daadwerkelijk verbinding mag maken. Hier wordt de client gecontroleerd op onder andere aanwezige security software, malware, geen peer-to-peer file sharing en dat het besturingssysteem gepatcht is. Alleen als de client hieraan voldoet wordt er een verbinding opgezet met XenDesktop. Als er niet wordt voldaan, kan de client worden doorgestuurd naar een remediation server waar de problemen verholpen kunnen worden (Citrix, z.j.).

Vendor patching

Naast de Windows en Third-party patches, zijn er ook andere appliances en devices aanwezig die gepatcht moeten worden. Voorbeelden hiervan zijn de Cisco switches, Cisco Routers en Blackberries die worden gebruikt. Ook hiervoor dient een patchproces voor te zijn.
Bij het opstellen van zo'n proces moet er gelet worden op onder andere de frequentie en testmethodes. Zo zullen patches van Blackberry niet intensief getest hoeven te worden, maar die voor netwerkapparatuur wel.

12 Bibliografie

ABN AMRO Hypotheken Groep. (2010). *AAHG Change Management proces - V1.1.doc.* Amersfoort.

ABN AMRO Hypotheken Groep. (2010). *AAHG Release Management proces - V1.0.doc.* Amersfoort.

ABN AMRO Hypotheken Groep. (2011, 12 05). *AAHG - Proces Patchen V1.1.doc.* Amersfoort. Opgeroepen op 08 15, 2013, van Kennisportaal AAHG.

ABN AMRO Hypotheken Groep. (2013). *AAHG Configuration Management proces - V1.2.doc.* Amersfoort.

Anoop's. (2013, 01 18). *ConfigMgr SCCM Patch Management Pros and Cons*. Opgeroepen op 10 11, 2013, van anoopcnair.com: http://anoopcnair.com/2013/01/18/configmgr-sccm-patch-management-pros-and-cons/

Berends, K.-J. (2013, 09 11). Inventarisatie AS-IS. (N. Boers, Interviewer)

Brady, N. C. (2011, 09 12). *using SCCM 2012 beta 2 in a LAB – Part 11. Deploying Software Updates*. Opgeroepen op 10 17, 2013, van niallbrady: http://www.niallbrady.com/2011/09/12/using-sccm-2012-beta-2-in-a-lab-part-11-deploying-software-updates/

Citrix. (z.j.). *Endpoint Analysis.* Opgehaald van citrix.com: http://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/citrix-access-gateway-endpoint-analysis.pdf.

Comsoft-direct. (z.j.). *Microsoft System Center 2012*. Opgeroepen op 10 14, 2013, van comsoft-direct.nl: http://www.comsoft-direct.nl/microsoft-system-center-2012

CoreSecurity. (2013, 02 27). *A World of Vulnerabilities – Blog Post from InfoSec Institute.* Opgeroepen op 08 26, 2013, van http://blog.coresecurity.com/2013/02/27/a-world-of-vulnerabilities-guest-blog-post-from-infosec-institute/

Daalmans, P. (2012, 02 17). *Monotoring Configuration Manager 2012 via alerts*. Opgeroepen op 10 14, 2013, van configmgrblog.com: http://configmgrblog.com/2012/02/17/monitoring-via-alerting-in-configuration-manager-2012/

Dell. (2012, 10). *Dell Kace K1000 System Management Appliance version 5.4.* Opgeroepen op 10 21, 2013, van kace.com: http://www.kace.com/support/resources...ion/K1000/v54/K1000-Patching-v54.ashx

Dell. (2013, 09). *Best Practices in Lifecycle Managament: Comparing Suites from Dell, LANDesk, Microsoft, and Symantec.* Opgeroepen op 10 21, 2013, van kace.com: http://www.kace.com/~/media/ED66BD3E5DF845AD8D63A848490037E5.pdf

Dell. (z.j.). *Dell KACE K1000 Management Appliance - Desktop Management Solutions - Dell KACE™*. Opgeroepen op 10 21, 2013, van kace.com: http://www.kace.com/products/systems-management-appliance

Dell. (z.j.). *Dell Kace K1000 Systems management Appliance.* Opgeroepen op 10 21, 2013, van kace.com: http://www.kace.com/products/systems-management-appliance/screenshots/home%20page

Dell. (z.j.). *Flash Demo - Dell Kace.* Opgeroepen op 10 17, 2013, van kace.com: http://www.kace.com/~/media/ED66BD3E5DF845AD8D63A848490037E5.pdf

Dell. (z.j.). *K1000 Administrator Guide.* Opgeroepen op 10 21, 2013, van kace.com: http://www.kace.com/support/resources.../K1000/v54/K1000-Admin-Guide-v54.ashx

Gartner. (2013, 04 09). *Magic Quadrant for Client Management Tools*. Opgeroepen op 10 11, 2013, van gartner.com: http://www.gartner.com/DisplayDocument?doc_cd=247238

Gasaway, C. (2012, 09 04). *KACE: Microsoft App-V integration scripts for the K1000 now available!* Opgeroepen op 10 17, 2013, van itninja.com: http://www.itninja.com/blog/view/kace-microsoft-app-v-integration-scripts-for-the-k1000-now-available

Goktas, O., & Tomassen, M. (2013, 08 22). Inventarisatie AS-IS. (N. Boers, Interviewer)

Granneman, G. (2013, 09 10). Inventarisatie AS-IS. (N. Boers, Interviewer)

Hamelers, O. (2013, 08 09). Inventarisatie AS-IS. (N. Boers, Interviewer)

Janssen, P. (2010). *IT-servicemanagement volgens ITIL.* Amsterdam: Pearson Education.

Kaspersky. (2011, 08 11). *IT Threat Evolution: Q2 2011 - Securelist*. Opgeroepen op 10 25, 2013, van securelist.com: http://www.securelist.com/en/analysis/204792186/IT_Threat_Evolution_Q2_2011

Mangan, T. (2011, 11 01). *How do you know if App-v apps need security updates?* Opgeroepen op 10 14, 2013, van tmurgent.com: http://www.tmurgent.com/TmBlog/?p=705

Microsoft. (2012, 01 04). *How to install SCUP and configure - Sudheesh Blog on System Center..... - Site Home - TechNet Blogs*. Opgeroepen op 10 21, 2013, van microsoft.com: http://blogs.technet.com/b/sudheesn/archive/2012/01/05/how-to-install-scup-and-configure.aspx

Microsoft. (2013, 07 25). *Support for Microsoft System Center*. Opgeroepen op 10 14, 2013, van microsoft.com: http://support.microsoft.com/ph/16340/en-us

Microsoft. (z.j.). *Microsoft System Center 2012.* Opgeroepen op 10 14, 2013, van microsoft.com: http://www.microsoft.com/en-us/server-cloud/system-center/default.aspx

Microsoft. (z.j.). *Microsoft System Center 2012*. Opgeroepen op 10 14, 2013, van microsoft.com: http://www.microsoft.com/en-us/server-cloud/system-center/default.aspx

Microsoft. (z.j.). *Microsoft Volume Licensing*. Opgeroepen op 10 14, 2013, van microsoft.com: http://www.microsoft.com/licensing/about-licensing/client-access-license.aspx#tab=3

Microsoft. (z.j.). *System Center Configuration Manager 2012*. Opgeroepen op 10 21, 2013, van micorosoft.com: http://www.microsoft.com/nl-nl/server-cloud/system-center/configuration-manager-2012.aspx

Microsoft. (z.j.). *System Center Updates Publisher*. Opgeroepen op 10 21, 2013, van microsoft.com: http://technet.microsoft.com/en-us/systemcenter/bb741049

Secunia. (2013, 03 14). *Vulnerability review 2013 - The Highlights*. Opgeroepen op 09 03, 2013, van Secunia.com: http://www.secunia.com/vulnerability-review/vulnerability_update_top50.html

Secunia. (2013, 09 03). *Secunia – Technical User Guide*. Opgeroepen op 09 03, 2013, van Secunia.com: http://secunia.com/?action=fetch&filename=Secunia_CSI7_Technical_User_Guide.pdf

Secunia. (z.j.). *Cisco - Secunia*. Opgehaald van secunia.com: http://secunia.com/advisories/vendor/5/

Secunia. (z.j.). *Patch Management Software - Corporate Software Inspector (CSI) - Secunia*. Opgeroepen op 10 21, 2013, van secunia.com: http://secunia.com/vulnerability_scanning/?utm_expid=629622-11.zihhfXJXSjKqe9sajQFQrQ.0&utm_referrer=http%3A%2F%2Fsecunia.com%2Fvulnerability_scanning%2Fcorporate%2Fsystem_requirements%2F

Secunia. (z.j.). *Secunia Advisories by Product*. Opgeroepen op 10 16, 2013, van secunia.com: http://secunia.com/community/advisories/product/

Secunia. (z.j.). *Secunia Whitepaper - Managing non-Microsoft updates With Microsoft's System Center Configuration Manager.* Opgeroepen op 10 14, 2013, van secunia.com: http://secunia.com/vulnerability_scanning/corporate/sc2012_plugin/sc2012_whitepaper/

Secunia. (z.j.). *Security Software Comparison - Secunia*. Opgeroepen op 10 14, 2013, van secunia.com: http://secunia.com/products/corporate/compare/

Shavlik. (2013). *Shavlik SCUPdates*. Opgeroepen op 10 11, 2013, van shavlik.com: http://www.shavlik.com/products/scupdates/datasheet/

Solarwinds. (2012, 10 31). *Using WSUS or SCCM to Roll Out 3rd Party Patches - YouTube*. Opgeroepen op 10 22, 2013, van youtube.com: http://www.youtube.com/watch?v=k0szmwLEj0o

Solarwinds. (2013, 05 21). *Solarwinds Patch Manager Administration Guide.* Opgeroepen op 10 22, 2013, van solarwinds.com: http://www.solarwinds.com/documentation/patchman/docs/PatchManagerAdministratorGuide.pdf

Solarwinds. (z.j.). *Generate an Online Quote in 2 minutes.* Opgeroepen op 10 22, 2013, van solarwinds.com: http://www.solarwinds.com/onlinequote/?licences=7081:121&quantity=1

Solarwinds. (z.j.). *SolarWinds Knowledge Base :: How to install the Patch Manager web console server on a WSUS*. Opgeroepen op 10 22, 2013, van knowledgebase.solarwinds.com: http://knowledgebase.solarwinds.com/kb/questions/4065/How+to+install+the+Patch+Manager+web+console+server+on+a+WSUS+server

Solarwinds. (z.j.). *SolarWinds Patch Manager - Embedded Interactive Demo*. Opgeroepen op 10 22, 2013, van systems.demo.solarwinds.com: http://systems.demo.solarwinds.com/Orion/External.aspx?Title=SolarWinds%20Orion%20Demo&URL=http://demo.solarwinds.com/flashdemo/spm/orion-demo-embedded.aspx

Solarwinds. (z.j.). *Supported Apps | Patch Manager | SolarWinds*. Opgeroepen op 10 22, 2013, van solarwinds.com: http://www.solarwinds.com/patch-manager/supported-apps.aspx

Appendix V Begrippenlijst

AAHG	ABN AMRO Hypotheken Groep
ABN	Algemene Bank Nederland
AMRO	Amsterdam-Rotterdam Bank
App-V	Application Virtualization
BYOD	Bring Your Own Device
CMDB	Configuration Management Database
COWS	Criteria, Options, Weights, Scores
CSI	Corporate Software Inspector
CVE	Common Vulnerabilities and Exposures
DMZ	Demilitarized Zone
EOL	End-of-life
FAT	Functionele Acceptatie Test
GAT	Gebruikers Acceptatie Test
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
KA	Kantoor Automatisering
KPI	Key Performance Indicator
MMC	Microsoft Management Console
PAT	Productie Acceptatie Test
PoC	Proof of Concept
PSI	Personal Software Inspector
PvA	Plan van Aanpak
RFC	Request for Change
SaaS	Software as a Service
SCCM	System Center Configuration Manager
SCUP	System Center Update Publisher
SP	Service Pack
SPS	Secunia Package System
ST	Systeemtest
WSUS	Windows Server Update Services

Appendix VI Glossarium

Arbitrary Code Execution	De mogelijkheid om commando's uit te voeren op een vatbare machine of in een proces
Buffer Overflow	De programma schrijft meer data weg naar het geheugen dan dat is toegekend. Dit kan een applicatie crash veroorzaken of een hacker kan het programma hijacken.
Code Injection	Het misbruiken van een bug waardoor er verkeerde data verwerkt wordt. Een goed voorbeeld is SQL Injection.
One-day attack	Een aanval dat misbruik maakt van een vulnerability die openbaar/bij de leverancier bekend is. Een patch is beschikbaar of wordt gemaakt.
Zero-day attack	Een aanval dat misbruik maakt van een vulnerability die nog niet openbaar/bij de leverancier bekend is. Er is geen patch beschikbaar.