# Stage Accell Group Heereveen

## Het bedrijf

Accell Group NV is een Nederlandse holding waaronder een aantal Europese fabrikanten van voornamelijk fietsen valt. Ik loop bij het IT gedeelte stage op de Locatie: Jagtlustweg 5

Heerenveen, Friesland 8444, NL. Hier hebben ze verschillende functies: helpdesk, frontend developers, devops, functioneel beheer, domain architect, product owners en tot slot privacy security officer hier loop ik stage. Mijn stagebegeleider is Fabian de Wit. Fabian ondersteunt mij tijdens deze 5 maanden.

## Mijn functies

Tijdens deze stageperiode richt ik mij vooral op het maken van scripts die bepaalde diensten kan automatiseren.

## Stageopdracht

Hieronder een beschrijving van de hoofdopdracht die ik deze stage moet voldoen.

# Stage opdrachtomschrijving

## Introductie

Accell gebruikt software voor het regelmatig scannen van asset op security-kwetsbaarheden. Deze software, genaamd Rapid7 (en vanaf nu “tool” genoemd) is onder beheer bij het security-team van Accell IT. Onder assets verstaan we in deze alle systemen binnen Accell met een netwerk-interface. Dat kan zijn ethernet of Wifi, of zelfs ook bluetooth.

## Probleemstelling

Rapid7 is het hart van security op het gebied van kwetsbaarheden-management. Het is van groot belang om een waarheidsgetrouwe set aan assets hierin te hebben, die overeenkomt met de assets die dag tot dag op het netwerk zijn aangesloten. Op dit moment is de set aan assets in Rapid7 onvolledig.

Assets kunnen op verschillende manieren worden toegevoegd aan de Rapid7 software. Grofweg zijn dit de volgende mogelijkheden:

* Handmatig
* Via een netwerkscan
* Via (centrale) installatie van de Rapid7 agent.

Momenteel wordt de laatste optie vooral gebruikt.

Dit komt neer op dat we grofweg de volgende apparaten scannen:

* Windows Laptops
* Windows servers
* Linux servers

De volgende apparaten zijn momenteel nog uitgesloten van de scan:

* Routers
* Switches
* Access points
* Scanners
* Printers
* Gast-apparaten
* Apple Macbooks (Udo had destijds aangegeven ze uit te faseren, tevens JamF opgezegd)

## Hoofddoel

Het hoofddoel van de stageopdracht is om te zorgen dat de configuratie van Rapid7 bestaat uit een compleet, waarheidsgetrouwe lijst van Assets in Rapid 7. Dit kan worden bewerkstelligd door de configuratie te vergelijken met andere configuratiedatabases. Dit moet dan op geautomatiseerde manier plaatsvinden, waarbij de afdeling CISO met enige regelmaat wordt geïnformeerd over de afwijkingen.

## Scope

* Het gaat om de laptops/desktops en servers die onder beheer zijn van Accell IT. Deze moeten allen in Rapid 7 als Asset opgenomen zijn.
* Het gaat in eerste instantie niet om apparaten in beheer bij 1 van onze andere decentrale IT-organisaties.(Dit mag later wel uitgebreid worden als er tijd is.)
* Het gaat niet om netwerk- apparaten, printers, scanners, of andere randapparatuur.
* Advies van de stagair hierover (wel/niet toevoegen) is welkom en zal worden behandeld in het team.

## Subdoelen

Gezien de omvang van het aantal configuratie databases die Accell heeft en de verschillende manieren die bestaan om informatie over assets in het netwerk te ontsluiten zijn de volgende subdoelen gedefinieerd. Dit kan gezien worden als stappenplan, omdat het een logische aanpak weergeeft.

1. Onderzoek: Onderzocht moet worden welke bronnen van informatie kunnen dienen voor het bepalen van de accuraatheid van de Rapid7-configuraties. Deze informatie kan op verschillende manieren uit de systemen gehaald worden. Verwacht wordt een rapport met daarin een overzicht van al deze systemen, en per systeem onder andere:
   1. Welke informatie van de Asset staat hierin
   2. Welke informatie zou bruikbaar kunnen zijn.
   3. de mogelijkheden tot ontsluiting (API/WMI/exportCSV/XML)
2. Freshservice.

Hierin staan assets als laptops/desktops en servers. Dit is ons primaire administratieve systeem. Er is een koppeling tussen dit systeem en SCCM (volgt later). De opdracht is als volgt: Zorg voor een vergelijk tussen dit systeem en Rapid 7. Vergelijk de resultaten handmatig en vorm door middel van gesprekken met engineers (Freshservice) en Security (Rapid7) een beeld van de betrouwbaarheid van beide systemen. Geef advies uit over je bevindingen aan CISO-office en eventueel manager Shared Services. Automatiseer vervolgens de vergelijking en zorg dat CISO-office regelmatig een bestand krijgt met de afwijkingen. Dit moet in elk geval de specifieke assets bevatten met info hiervan. (zoals naam, IP-adres, Operating system). Optioneel, en wenselijk moet dit verschil ook in metadata zichtbaar zijn, zoals aantallen laptops/desktops percentages, en bijvoorbeeld een “betrouwbaarheids-cijfer” zodat hierover naar het management gerapporteerd kan worden. Eigen inbreng of interpretatie van de stagair wordt hierbij erg op prijs gesteld en ook gestimuleerd.

1. SCCM.

SCCM is de beheerstool voor Windows devices. Dit zou een reflectie moeten zijn van de Assets uit Freshservice. De rapportage uit 1). Kan worden uitgebreid met een vergelijking van assets uit SCCM. Het doel hiervan is om ook van dit systeem een rapportage te krijgen over de verschillen tussen dit systeem en de assets uit Rapid 7. Bijkomend kan ook gerapporteerd worden over afwijkingen van dit systeem t.o.v. Freshservice. Het kan een idee zijn om ook van dit systeem een “betrouwbaarheidscijfer”vast te stellen. Als je dit dan bijvoorbeeld kunt vergelijken met de real time informatie uit het systeem uit 3) dan kunnen hiermee door CISO-office en Engineering goede conclusies getrokken worden, en management worden geadviseerd over security-risico’s op basis van deze verschillen.

1. Real time netwerk-info.

Met real time informatie wordt bedoeld informatie over apparaten die momenteel aanwezig zijn in het netwerk. Er zijn verschillende real-time informatiesystemen beschikbaar, welke laten zien wat op dit moment de aangesloten apparaten zijn op het netwerk. Informatie uit deze bronnen kan gebruikt worden voor betrouwbaarheidscijfers van de verschillende administratieve systemen. We hebben het hier over bijvoorbeeld:

* De DHCP-console
* Netwerk-routers van Cisco, (ARP-tabellen)
* De Aruba Clearpass netwerk-authenticatie server
* De Meraki console.
* Eventueel nog te installeren IP-scan tool.
* Eigen inbreng, keuze en interpretatie van de stagair wordt hierbij erg op prijs gesteld en ook gestimuleerd.

Deze real time informatie moet ook gematched worden met de informatie uit 1) en 2) , waarin het belangrijk dat het doel is om allereerst te zorgen dat Rapid 7 alle assets in het systeem heeft, welke beschreven zijn in de introductie van deze opdracht.

1. Vsphere. Dit systeem bevat alle servers die in het datacenter in Heerenveen aangesloten zitten
2. Azure. Ook hierin zitten servers, welke ook in Rapid7 zouden moeten voorkomen.