THOMAS MORE

VERDER UITROLLEN VAN CLEARPASS

Realisatie document

Stijn Luyts

2024 - 2025

Inhoud

1. Inleiding

Dit realisatiedocument heeft als doel om toe te lichten wat mijn stageopdracht inhield en wat ervan werd verwacht. In dit document worden de verschillende oplossingen besproken die tijdens de opdracht zijn onderzocht, welke oplossingen effectief zijn toegepast, en waarom sommige mogelijkheden uiteindelijk niet zijn gebruikt. Daarnaast wordt er ingegaan op de uitdagingen en moeilijkheden die tijdens de uitvoering van de opdracht naar voren zijn gekomen.

De stageopdracht die door de Politiezone Geel-Laakdal-Meerhout werd aangeboden, bestond uit het verder implementeren van ClearPass Network Access Control (NAC). ClearPass NAC zorgt ervoor dat een apparaat dat verbinding maakt met het netwerk eerst een authenticatieproces doorloopt. Op basis van deze authenticatie wordt bepaald tot welk netwerk het apparaat toegang krijgt en welke rechten het binnen dat netwerk heeft.

Deze oplossing is noodzakelijk omdat het hoofdgebouw van de politiezone, gelegen in het Veiligheidshuis Ter Stokt, gedeeld wordt met andere organisaties zoals de brandweer en het Rode Kruis van Geel. Aangezien er gedeelde ruimtes zijn die door alle diensten gebruikt worden, is het essentieel dat de NAC ervoor zorgt dat bijvoorbeeld een laptop van de brandweer geen toegang kan krijgen tot de interne systemen van de politie. Dit wordt gerealiseerd door gebruik te maken van Microsoft Intune, waarin alle gebruikersapparaten beheerd worden. Via Intune kunnen de nodige configuraties worden uitgerold zodat apparaten in staat zijn zich correct te authenticeren en de juiste toegangsrechten te verkrijgen.

Het document begint met een analyse van de stageopdracht. Er wordt een projectplan toegelicht dat als leidraad diende bij de uitvoering van de opdracht. Dit projectplan vormde een logisch stappenplan dat werd gevolgd tijdens het traject. Het plan startte met een onderzoeksfase waarin informatie werd verzameld over alle noodzakelijke onderdelen, met name Microsoft Intune en Aruba ClearPass. Vervolgens werd er getest op kleine schaal, met één laptop die verbonden was met een vooraf geconfigureerde switchinterface. Na deze test werd het project verder uitgerold over de andere kantoren. Tijdens de uitrol werd er zowel actief als passief gemonitord om na te gaan of zich eventuele problemen voordeden. In de laatste fase werd alles gedocumenteerd: wat er precies is uitgevoerd en hoe de volledige configuratie tot stand is gekomen.

Aansluitend worden de gebruikte technologieën opgesomd, met uitleg over hun functie en de reden waarom deze werden ingezet. De belangrijkste tools die gebruikt werden, zijn Microsoft Intune, Aruba ClearPass, Aruba-switches, Windows PowerShell en de IntuneWinAppUtil-tool.

Daarna gaat het document in op de configuratie van de gebruikersapparaten. Dit deel beschrijft wat er allemaal werd gedaan om ervoor te zorgen dat een apparaat zich succesvol kon authenticeren via ClearPass. Dit gedeelte is opgedeeld in twee delen: handmatige configuratie en automatische uitrol via Intune. In het handmatige deel wordt toegelicht welke stappen er manueel zijn uitgevoerd, hoe dit werd aangepakt, en vooral waarom dit aanvankelijk noodzakelijk was. Voor het Intune-gedeelte wordt uitgelegd hoe de filters werden ingesteld en waarom deze van belang waren voor de opdracht. Verder wordt beschreven hoe apparaatconfiguraties werden aangemaakt, waarvoor ze dienden en welk doel ze dienden te bereiken. Tot slot wordt ingegaan op de configuraties die via een Win32-app werden uitgerold naar de gebruikersapparaten.

Vervolgens wordt in het derde hoofdstuk dieper ingegaan op ClearPass, het onderdeel waar de andere stukken van mijn stageopdracht uiteindelijk aan verbonden zijn. De ClearPass-server was al vóór de start van mijn stage geïnstalleerd en deels geconfigureerd. Daarom wordt eerst besproken wat er reeds vooraf was ingesteld op de ClearPass-server en waarom deze configuraties zijn toegepast.
De bestaande configuraties omvatten onder andere het opzetten van een ClearPass-cluster. Hierdoor werd redundantie en load balancing mogelijk gemaakt, en werd het beheer van beide servers vereenvoudigd doordat wijzigingen op de master automatisch werden overgenomen door de secundaire server. Daarnaast waren er enforcement profiles aangemaakt die door de switches worden gebruikt om via poortrollen het juiste VLAN toe te wijzen op basis van het profiel dat een apparaat krijgt na authenticatie. Verder waren ook

de enforcement policies geconfigureerd. Deze bepalen welke voorwaarden moeten vervuld zijn voor een bepaalde vorm van authenticatie en welke acties hieraan gekoppeld zijn. Ten slotte werden er services aangemaakt op basis van de eerdergenoemde profiles en policies, zodat ClearPass deze correct kan toepassen tijdens het authenticatieproces.
Naast deze vooraf geconfigureerde onderdelen, werd er tijdens mijn stage ook nog een bijkomende configuratie uitgevoerd, namelijk de authenticatie van printers. Aangezien printers niet over certificaten beschikken en dus geen gebruik kunnen maken van 802.1X-authenticatie, werd gekozen voor MAC Authentication Bypass (MAB). Door het MAC-adres van de printers als vertrouwd te markeren in ClearPass, konden ze correct geauthentiseerd worden en toegang krijgen tot het juiste netwerksegment.

In het vierde hoofdstuk komt de configuratie van de Aruba-switches aan bod. Eerst werd de communicatie tussen de switch en ClearPass tot stand gebracht. Vervolgens werden de noodzakelijke authenticatiemethoden zoals MAC-authenticatie en 802.1X ingeschakeld. Daarna werd ingesteld dat ClearPass wijzigingen aan de switch mag doorvoeren op basis van de ontvangen authenticatie-informatie. Er werden ook poortrollen gedefinieerd, zodat de switch op basis van het toegewezen profiel van ClearPass een VLAN kon toewijzen aan een specifieke poort. Verder wordt toegelicht hoe de bekabeling werd aangepakt en waarom het essentieel is om te weten welke kabel op welk patchpaneel en op welke switchinterface is aangesloten. Tot slot zijn ook de individuele switchpoorten geconfigureerd zodat ze deelnemen aan het authenticatieproces. Al deze stappen worden in dit hoofdstuk uitgelegd aan de hand van de gebruikte commando’s, inclusief toelichting over hun werking en het doel ervan.

Het vijfde hoofdstuk gaat over de documentatie die tijdens de stage werd opgeleverd. Er zijn drie verschillende documenten opgesteld. Het eerste is dit realisatiedocument, waarin beschreven wordt wat de stageopdracht inhoudt, welke taken uitgevoerd zijn, en hoe dit werd aangepakt. Het tweede document is de handleiding, bedoeld voor intern gebruik. Deze handleiding bevat gedetailleerde informatie over alle configuraties en is opgesteld vanuit het perspectief dat nog niets vooraf geconfigureerd is. Het dient dus als leidraad om het systeem opnieuw op te bouwen indien nodig. De handleiding bespreekt ook hoe men verder kan bouwen op de bestaande configuratie en bevat mogelijke problemen met bijhorende oplossingen, evenals suggesties voor vervolgstappen in het project. Het derde document is het Rollout-bestand, een Excel-bestand waarin wordt bijgehouden welke apparaten al zijn geconfigureerd, welke configuraties nog ontbreken, en hoe de bekabeling is opgezet. Dit bestand toont ook welke kabel naar welk patchpaneel en vervolgens naar welke switchinterface loopt.

Het zesde en voorlaatste hoofdstuk behandelt de problemen die tijdens de stageopdracht zijn opgetreden en de oplossingen die daarvoor gevonden zijn. Een eerste uitdaging was dat tijdens de opleiding aan Thomas More geen specifieke kennis over Microsoft Intune werd aangeboden, wat betekende dat dit terrein volledig nieuw was voor mij. Bovendien ging het om een reeds bestaande Intune-omgeving, waardoor ik moest uitzoeken welke bestaande groepen ik kon gebruiken. Een tweede probleem was het ontbreken van administratorrechten tijdens de stage. Hierdoor moest ik bij elke wijziging of test telkens een ICT-medewerker vragen om in te loggen op de laptop, Intune-omgeving of op de Aruba-switches. Een derde probleem had betrekking op de manier waarop configuraties via Intune uitgerold moesten worden. Er werd gekozen om dit te doen via een Win32-app in plaats van via een herstelscript of een apparaatconfiguratie, en in dit hoofdstuk wordt uitgelegd waarom deze keuze werd gemaakt. Vervolgens was er een probleem met de authenticatie van IP-telefonen, die aanvankelijk niet correct wilden authenticeren of waarbij de netwerkicoon in Windows verkeerd weergegeven werd. Daarnaast was er de uitdaging van printerauthenticatie, omdat printers geen gebruik kunnen maken van 802.1X-authenticatie maar toch toegang nodig hebben tot het administratief netwerk. Tot slot vormde het feit dat alles binnen een actieve productieomgeving moest gebeuren een extra moeilijkheid. Dit vereiste een voorzichtige aanpak om te voorkomen dat netwerkproblemen zouden ontstaan tijdens het testen of implementeren van wijzigingen.

Het laatste hoofdstuk bevat het besluit van de stageperiode. Hierin wordt het belangrijkste nog eens kort samengevat en benadrukt. Er wordt ook een blik geworpen op de toekomst, waarbij mogelijke vervolgstappen en aandachtspunten besproken worden om het project verder uit te bouwen op een veilige en efficiënte manier.

2. Analyse

De uitvoering van de stageopdracht bij Politiezone Geel-Laakdal-Meerhout vereiste een doordachte aanpak en het gebruik van specifieke technologieën. In dit hoofdstuk wordt het opgestelde projectplan toegelicht, gevolgd door een overzicht van de gebruikte tools en technologieën. Beide onderdelen speelden een cruciale rol in het succesvol configureren van netwerktoegang via ClearPass en Microsoft Intune binnen een productieomgeving.

2.1. Projectplan

Het projectplan begon met een onderzoeksfase naar Microsoft Intune, de bestaande netwerkstructuur en Aruba ClearPass. Deze fase was van groot belang, aangezien mijn beschikbare kennis over deze technologieën beperkt was. Microsoft Intune is een technologie die steeds belangrijker wordt, maar binnen het onderwijs nog weinig aan bod komt. Aruba ClearPass was bovendien volledig onbekend terrein. De netwerkstructuur speelde een centrale rol in de stageopdracht en vereiste daarom een grondig begrip.
De informatie over Microsoft Intune werd voornamelijk verkregen via officiële Microsoft-documentatie. Deze documentatie is doorgaans diepgaand, maar dekt niet alle praktische scenario's. Daarom werden aanvullend ook instructievideo's geraadpleegd, waarin specifieke toepassingen aan bod kwamen. Voor Aruba ClearPass bleken vooral video's waardevol, aangezien relevante en volledige documentatie moeilijk te vinden was. Wat betreft de netwerkstructuur was er geen directe toegang tot de benodigde informatie, waardoor extra informatie via collega's werd verzameld.
Na de onderzoeksfase werd gestart met het testen op zeer kleine schaal. Dit was essentieel, aangezien de verdere uitrol van ClearPass in een productieomgeving plaatsvond. Een verkeerde configuratie zou impact kunnen hebben op het volledige kantoor. Om dit risico te beperken, werd de eerste test uitgevoerd met één laptop en één switchpoort die authenticatie via ClearPass uitvoerde. Hierdoor bleef de testomgeving beheersbaar.
De verdere uitrol naar de verschillende kantoren werd stapsgewijs uitgevoerd. Deze gefaseerde aanpak maakte het mogelijk om snel in te grijpen bij eventuele fouten. Voor de configuratie werd gebruikgemaakt van Microsoft Intune, waarbij filters werden toegepast voor gerichte uitrol. Een nadere toelichting op dit proces volgt in het hoofdstuk *Configuratie van client device*. Daarnaast werden enkel de nodige switches en switchinterfaces aangepast. Door het gebruik van checkpoint-commando's op de switches konden wijzigingen snel ongedaan worden gemaakt. Dit aspect wordt verder besproken in het hoofdstuk *Configureren van de switch*.
Tijdens de uitrol vond actieve en passieve monitoring plaats om eventuele fouten tijdig op te sporen. Dit was cruciaal om snel correctieve maatregelen te kunnen nemen. Monitoring werd uitgevoerd via Aruba-switches en ClearPass, alsook via feedback van eindgebruikers. Via de switches werd, met behulp van show-commando's, nagegaan welke authenticatiemethode was toegepast en welke rol aan het apparaat was toegekend. Als de authenticatie faalde, kon in ClearPass de oorzaak worden achterhaald. Aanvullend werd monitoring uitgevoerd via medewerkers, zowel actief door navraag te doen, als passief door meldingen af te wachten. Ondanks een correcte authenticatie op systeemniveau, kon het immers voorkomen dat gebruikers toch hinder ondervonden. Daarom werd ook deze vorm van monitoring als waardevol beschouwd.
Tot slot werd er documentatie opgesteld en afgeleverd. Deze documentatie stelt de organisatie in staat om na afloop van de stage zelfstandig verder te werken met de implementatie, en om eventuele problemen te kunnen oplossen. In het hoofdstuk *Documentatie* wordt hier dieper op ingegaan.
Wegens het fait dat de stage bij de Politiezone Geel-Laakdal-Meerhout was ga de inhoud van scripts en sommige configuraties niet getoond worden maar er gaat wel uitgelegd worden wat ze doen.

2.2. Gebruikte technologie

Tijdens Tijdens de uitvoering van de stageopdracht werden verschillende technologieën en tools ingezet om de doelstellingen te realiseren. Hieronder volgt een overzicht van de gebruikte middelen, inclusief hun functie, het gebruik en de reden van inzet.

- **Microsoft Intune**
  Intune is een cloudgebaseerde service van Microsoft waarmee organisaties centraal apparaten kunnen beheren en configureren. De dienst biedt mogelijkheden voor het uitrollen van configuraties, het installeren van applicaties en het beveiligen van apparaten. In tegenstelling tot Windows Active Directory (AD), dat enkel lokaal ("on-premise") werkt en zich richt op Windows-systemen, ondersteunt Intune ook Linux- en mobiele apparaten. Intune werd gebruikt binnen de stageopdracht omdat de betrokken apparaten reeds gekoppeld waren aan deze service. Configuraties werden uitgerold via Intune-apparaatconfiguraties en applicaties via de Intune-appdistributie.

- **Aruba ClearPass**
  ClearPass is een netwerkbeveiligingsoplossing die zorgt voor toegangscontrole (Network Access Control, NAC). Het systeem bepaalt op basis van authenticatie wie toegang krijgt tot het netwerk, zowel bekabeld als draadloos. ClearPass stuurt een "challenge" naar het apparaat dat verbinding wil maken. Afhankelijk van het resultaat krijgt het apparaat een rol toegewezen, waarop de switch een VLAN instelt. De ClearPass-server was reeds operationeel voor de start van de stage en werd daarom binnen de opdracht gebruikt. De authenticatie verliep via 802.1X met MAC Authentication Bypass (MAB) als fallback.

- **Aruba-switches**
  De Aruba-switches verzorgen de netwerkcommunicatie binnen het politiekantoor en zorgen voor netwerksegmentatie via VLAN’s. Ze spelen een sleutelrol in het authenticatieproces tussen de apparaten en de ClearPass-server. De switches werden zodanig geconfigureerd dat ze wisten waar de ClearPass-server zich bevond en welke authenticatiemethoden moesten worden toegepast. Vervolgens gaven de switches de uitdagingen en resultaten van de ClearPass-authenticatie correct door. Op basis van de toegekende rol werd de VLAN-configuratie aangepast voor de desbetreffende poort.

- **Windows PowerShell**
  PowerShell is een scripttaal die voornamelijk gebruikt wordt op Windows-systemen om taken te automatiseren en configuraties te beheren. Binnen deze stageopdracht werden uitsluitend Windows-apparaten geconfigureerd, waardoor PowerShell de aangewezen tool was. De scripttaal werd ingezet om de nodige instellingen op de apparaten toe te passen. Verdere details hierover worden toegelicht in het volgende hoofdstuk.

- **IntuneWinAppUtil-tool**
  De IntuneWinAppUtil-tool is een hulpmiddel van Microsoft dat gebruikt wordt om installatiebestanden en bijbehorende scripts om te zetten naar het *.intunewin*-formaat. Dit formaat is vereist voor het uploaden en distribueren van toepassingen via Microsoft Intune. Binnen de stageopdracht werd deze tool gebruikt om een taakplanner-script (Task Scheduler) in het juiste formaat aan te leveren, zodat het automatisch kon worden uitgerold naar de gewenste apparaten. De IntuneWinAppUtil-tool werd lokaal uitgevoerd en nam als input een installatiemap met daarin het script en eventuele aanvullende bestanden.

3. Configuratie van client device

In dit hoofdstuk wordt beschreven hoe de netwerkconfiguratie op clientapparaten werd opgezet, beginnend met een handmatige benadering om inzicht te krijgen in de noodzakelijke instellingen en om configuratiebestanden te genereren voor verdere automatisering. Deze configuraties zijn vervolgens ingezet via Microsoft Intune. Zowel de handmatige aanpak als de geautomatiseerde uitrol via Intune worden uitgebreid toegelicht, inclusief de gebruikte scripts, XML-bestanden, taakplannerinstellingen en het gebruik van de IntuneWinAppUtil-tool.

3.1. Handmatig

De eerste stap in de configuratie van clientapparaten bestond uit een handmatige aanpak. Dit was noodzakelijk om volledig inzicht te verkrijgen in de benodigde instellingen voor netwerkverificatie en om configuraties te exporteren naar XML-bestanden. Deze bestanden zijn later gebruikt voor de geautomatiseerde uitrol via Intune.
Allereerst moest de Windows-service "Wired AutoConfig" worden geactiveerd. Zonder deze service zou de ethernetinterface geen netwerkverificatie uitvoeren. Dit werd gerealiseerd door de service handmatig te starten via de toepassing "Services" en in te stellen op automatisch opstarten.
Zodra de service actief is, verschijnt er in de eigenschappen van de ethernetverbinding een extra tabblad genaamd "Authenticatie". In dit tabblad wordt de gewenste methode voor netwerkverificatie geconfigureerd. De exacte gebruikte methode wordt in dit document niet toegelicht vanwege vertrouwelijkheid.
Na het configureren van de netwerkauthenticatie werd het profiel geëxporteerd met het volgende PowerShell-commando:

```
netsh lan export profile folder=. interface="interface_naam"
```

Hierbij wordt "interface_naam" vervangen door de naam van de ethernetinterface. Het geëxporteerde bestand (bijvoorbeeld ethernet.xml) werd vervolgens gebruikt in een PowerShell-script dat wordt aangeroepen via een Taakplanner-taak.
De reden voor het gebruik van de Windows Taakplanner in plaats van directe uitrol via Intune, is te wijten aan het gebruik van dockingstations. Indien de configuratie via Intune wordt gepusht terwijl het apparaat niet is aangesloten op een dockingstation, wordt de ethernetinterface van dat dockingstation niet meegenomen in de configuratie. Door gebruik te maken van een trigger in Taakplanner, wordt de configuratie toegepast telkens wanneer een nieuwe netwerkverbinding wordt gedetecteerd.
De taak in Taakplanner werd als volgt ingesteld:

- Algemeen: Uitvoeren als gebruiker SYSTEM, met de optie "Met hoogste bevoegdheden uitvoeren" ingeschakeld.
- Trigger: Een nieuwe gebeurtenis, gebaseerd op de volgende instellingen:
  - Logboek: Microsoft-Windows-NetworkProfile/Operational
  - Bron: NetworkProfile
  - Gebeurtenis-ID: 10000 (nieuwe netwerkverbinding gedetecteerd)
- Actie: Starten van het programma powershell.exe met als argument:

```
-ExecutionPolicy Bypass -File "pad_naar_script"
```

Het PowerShell-script (ethernet_detect.ps1) voerde de volgende acties uit:

1. Start de service Wired AutoConfig en stel deze in op automatisch.
2. Laad de geëxporteerde XML-configuratie op alle ethernetinterfaces.
3. Herstart de service Wired AutoConfig om de configuratie toe te passen.

Tot slot werd deze taak geëxporteerd naar een XML-bestand (ethernet_verbinding_detectie.xml) voor latere uitrol via Intune.

3.2. Automatisering via Intune

Na de handmatige uitvoering werden alle configuraties geautomatiseerd via Microsoft Intune. Hiervoor zijn drie componenten ingericht: een filter, een apparaatconfiguratie en een Win32-app.

3.2.1. Aanmaken van een filter

Om gecontroleerd te kunnen testen en gefaseerd uit te rollen, werd een filter aangemaakt binnen Intune. Deze filter bepaalt welke apparaten in aanmerking komen voor configuratie. De filter is gebaseerd op apparaatgegevens, zoals de apparaatsnaam, en wordt toegepast op een specifieke groep binnen Intune. Zodra de uitrol stabiel verloopt, kan de filter eventueel worden verwijderd of aangepast.

3.2.2. Aanmaken van een apparaatconfiguratie voor het uitrollen van het certificaat

Vervolgens werd een apparaatconfiguratie opgezet voor het uitrollen van een vertrouwd certificaat. Dit certificaat is noodzakelijk voor netwerkverificatie en moet geplaatst worden in het computerarchief en niet in het gebruikersarchief. Dit is noodzakelijk omdat de netwerk-authenticatie plaatsvindt op computerniveau, en dus niet afhankelijk mag zijn van een specifieke gebruiker die is ingelogd.
Het verschil tussen het gebruikersarchief en het computerarchief is dat het gebruikersarchief uniek is per gebruiker. Wanneer een gebruiker zich op een ander apparaat aanmeldt, wordt zijn gebruikerscertificaat op dat apparaat geladen (indien roaming-profielen of profielsynchro actief zijn). Daarentegen is het computerarchief gekoppeld aan het apparaat zelf, onafhankelijk van wie erop inlogt. Elk account dat op het toestel wordt gebruikt, kan dus toegang hebben tot de certificaten in het computerarchief.
Een praktisch voordeel van het computerarchief is dat het apparaat zich kan authentiseren op het netwerk nog voordat een gebruiker is aangemeld — bijvoorbeeld tijdens de opstart of aanmeldfase. Dit is vooral belangrijk bij 802.1X-authenticatie of netwerktoegang via NAC-oplossingen zoals ClearPass, waarbij connectiviteit vereist is voordat er interactie met de gebruiker plaatsvindt.
Via het sjabloon "Vertrouwde certificaten" in Intune werd het certificaat toegevoegd en toegewezen aan de juiste groep. Hierbij werd opnieuw gebruikgemaakt van de eerder aangemaakte filter. De succesvolle plaatsing van het certificaat kan worden gecontroleerd in het lokale certificaatarchief van het apparaat, onder “Vertrouwde basiscertificeringsinstanties”.

3.2.3. Aanmaken van een app voor het configureren van Wired AutoConfig

Voor het automatisch toepassen van de Wired AutoConfig-instellingen werd een Win32-app gecreëerd in Intune. Deze app zorgt ervoor dat de eerdergenoemde taakplannerinstellingen worden toegepast, inclusief de juiste service-instellingen en het inladen van de netwerkinstellingen.
Hiervoor werd een PowerShell-installatiescript (installtask.ps1) geschreven met de volgende stappen:

1. Controle op het bestaan van een lokale map, en indien nodig aanmaken.
2. Kopiëren van de drie benodigde bestanden (ethernet.xml, ethernet_verbinding_detectie.xml en ethernet_detect.ps1) naar deze map.
3. Importeren van de taakplanner-XML om de taak aan te maken.

Alle bestanden werden vervolgens verpakt met behulp van de IntuneWinAppUtil-tool in een .intunewin-bestand. Deze tool, beschikbaar via GitHub, vraagt om:

- De map waarin de bestanden staan
- Het installatiebestand (in dit geval installtask.ps1)
- De outputlocatie van de .intunewin-file

Na het genereren van het pakket werd een Win32-app aangemaakt in Intune:

- App-type: Windows app (Win32)
- Installatieopdracht:

```
powershell.exe -executionpolicy bypass -file .\installtask.ps1
```

- Detectieregel: Controle of de drie configuratiebestanden aanwezig zijn in de doelmap. Indien aanwezig, wordt de app als succesvol uitgerold beschouwd.

De keuze voor deze aanpak boven andere opties zoals apparaatconfiguraties of herstelscripts wordt verder toegelicht in het hoofdstuk "Problemen, aandachtspunten en geprobeerde oplossingen".

4. ClearPass

In dit hoofdstuk geef ik een overzicht van de ClearPass-configuratie die gebruikt werd tijdens mijn stage. Aangezien de initiële opzet van de ClearPass-omgeving voorafgaand aan mijn stage werd uitgevoerd door een extern bedrijf, was er weinig nood aan fundamentele wijzigingen. Toch heb ik tijdens mijn stage verschillende elementen moeten begrijpen, controleren en waar nodig aanpassen. Deze configuratie-inzichten zijn gebaseerd op mijn eigen bevindingen, testen en de documentatie die door het externe bedrijf werd aangeleverd. Daarnaast behandel ik in dit hoofdstuk ook de specifieke uitdaging rond de authenticatie van printers en de toepassing van MAC Authentication Bypass (MAB) als oplossing.

4.1. Bestaande ClearPass-configuratie

De opzetting van de ClearPass server was gedaan voor de stageperiode door een extern bedrijf, daarom gaat dit eerste deel heel vaag kunnen zijn wegens de reden dat er weinig aan verandert moest worden waardoor het gedeelte dat hier gaat besproken worden gebaseerd is op de bevindingen dat tijdens mijn stage opdracht genomen zijn en ook op de documentatie/handleiding van dat externe bedrijf.

4.1.1. ClearPass-cluster

De ClearPass-omgeving is opgezet als een cluster met twee servers achter één virtueel IP-adres (VIP). Deze opstelling biedt redundantie: als één van de twee servers uitvalt, blijft de andere beschikbaar voor authenticatieverzoeken. Dankzij het gebruik van een VIP hoeven de configuraties op de switches niet aangepast te worden wanneer een server uitvalt.
Daarnaast maakt de cluster gebruik van load balancing, zodat beide ClearPass-servers actief gebruikt worden in plaats van dat alle verzoeken naar één server gaan. Ten slotte is er binnen de cluster één "master"-server aanwezig; configuraties die hierop worden aangebracht, worden automatisch gesynchroniseerd met de tweede server.

4.1.2. Enforcement Profiles

De *enforcement profiles* bepalen welke netwerktoegang een apparaat krijgt na succesvolle authenticatie. Deze profielen worden toegewezen door de *enforcement policies* (zie volgend onderdeel) en zorgen ervoor dat de switch weet in welke VLAN het apparaat geplaatst moet worden. De configuratie van deze profielen is essentieel voor correcte netwerksegmentatie en wordt verder toegelicht in het hoofdstuk over de switchconfiguratie.

4.1.3. Enforcement Policies

Enforcement policies zijn de regels die bepalen hoe ClearPass omgaat met binnenkomende authenticatieverzoeken. Elke policy bestaat uit één of meerdere condities en bijbehorende acties. Als een apparaat aan een conditie voldoet, wordt de gekoppelde actie uitgevoerd — meestal het toewijzen van een specifiek *enforcement profile*.
ClearPass werkt volgens het principe "deny by default": als geen enkele conditie wordt gehaald, wordt de toegang geweigerd. Daarom is een correcte en volledige configuratie van deze policies cruciaal. ClearPass past het "first hit"-principe toe: zodra een conditie overeenkomt, wordt de bijbehorende actie uitgevoerd en worden latere regels niet meer geëvalueerd.
Aanvankelijk waren er slechts drie condities geconfigureerd. Tijdens mijn stage heb ik een vierde toegevoegd om ondersteuning te bieden voor de authenticatie van printers via MAB. Meer details hierover worden besproken in sectie 4.2.

4.1.4. Services

Tot slot zijn er *services* aangemaakt in ClearPass. Deze services maken gebruik van de eerder genoemde *enforcement policies*. Een service bepaalt:

- **Wanneer** deze actief wordt (via condities),
- **Waar** de authenticatie-informatie vandaan komt (zoals een authenticatiebron of database),
- En **welke policy** wordt toegepast bij succesvolle matching.

Zonder deze services kan ClearPass de juiste policies niet koppelen aan een authenticatieverzoek.

4.2. Authenticatie van printers en MAB

Een onverwachte uitdaging tijdens de implementatie was de authenticatie van printers. In tegenstelling tot laptops en andere netwerkapparaten, kunnen printers geen certificaten gebruiken. Hierdoor was een alternatieve methode nodig om hen toegang te geven tot het admin-netwerk.
De oplossing was het toepassen van MAC Authentication Bypass (MAB). Hiervoor heb ik in ClearPass een extra regel toegevoegd waarin toestellen met de status “Known” toegang krijgen tot het gewenste netwerksegment. Vervolgens heb ik de MAC-adressen van alle printers als vertrouwd gemarkeerd in ClearPass, zodat deze correct geauthentiseerd kunnen worden — ook zonder certificaat. Zo werd het mogelijk om printers veilig en automatisch te verbinden met het admin-netwerk.

5. Configureren van de switch

In dit hoofdstuk wordt toegelicht hoe de netwerkapparatuur, in het bijzonder de switches, wordt geconfigureerd om netwerktoegang via authenticatie mogelijk te maken. De focus ligt op de integratie met de ClearPass-server, het instellen van authenticatiemethoden, het correct patchen van bekabeling, en het configureren van individuele switchpoorten. Deze stappen zijn essentieel voor een correcte implementatie van 802.1X en MAC-authenticatie, waarbij apparaten dynamisch worden toegewezen aan netwerken op basis van hun authenticatiestatus en -rol. Een foutloze implementatie van deze configuraties zorgt ervoor dat enkel geautoriseerde apparaten toegang krijgen tot het netwerk en dat deze apparaten in de juiste VLAN terechtkomen op basis van hun rol.

5.1. Opzetten van communicatie tussen switch en ClearPass

De eerste stap in de configuratie is het opzetten van een correcte communicatie tussen de switch en de ClearPass-server. Dit is cruciaal, aangezien de switch authenticatieverzoeken moet kunnen doorsturen naar ClearPass en ClearPass op zijn beurt rollen moet kunnen terugsturen naar de switch.

Als eerste controle wordt er een ping uitgevoerd vanaf de switch naar het IP-adres van de ClearPass-server om te verifiëren of netwerkconnectiviteit aanwezig is. Wanneer deze basisconnectiviteit werkt, wordt de RADIUS-server geconfigureerd met het volgende commando:
radius-server host <x.x.x.x> key plaintext <pre-shared key>
Hierbij vervang je <x.x.x.x> door het IP-adres van de ClearPass-server en <pre-shared key> door de vooraf afgesproken sleutel. Let op: de switch geeft op dit moment nog geen directe terugkoppeling over de status van de verbinding. Dit wordt pas zichtbaar bij een daadwerkelijke authenticatiepoging.

Om in de toekomst meerdere RADIUS-servers makkelijk te kunnen beheren, wordt er een RADIUS-servergroep aangemaakt:

```
aaa group server radius <Group-naam>
    server <x.x.x.x>
```

Daarna worden de gewenste authenticatiemethodes geactiveerd:

```
aaa authentication port-access dot1x authenticator
    radius server-group <Group-naam>
    enable
```

en

```
aaa authentication port-access mac-auth
    radius server-group <Group-naam>
    enable
```

Deze configuratie zorgt ervoor dat de switch zowel 802.1X als MAC-authenticatie uitvoert via de opgegeven RADIUS-servergroep.

Tot slot wordt Dynamic Authorization ingeschakeld. Hiermee kan ClearPass dynamisch VLAN-rollen toewijzen aan een poort:

```
radius dyn-authorization enable
radius dyn-authorization client <x.x.x.x> secret-key plaintext <pre-shared key>
```

Ook wordt RADIUS-accounting ingesteld, zodat de switch op regelmatige basis updates stuurt naar ClearPass:

```
aaa accounting port-access start-stop interim <interval> group <Group-naam>
```

Hierbij bepaalt <interval> hoe vaak deze updates worden verstuurd.

5.2. Opzetten van poort rollen

Wanneer de communicatie met ClearPass succesvol is opgezet, kunnen de poortrollen worden aangemaakt. Een poortrol dient als vertaalslag van de rol die ClearPass toewijst naar een VLAN die op de switch geconfigureerd is.

Een poortrol wordt als volgt geconfigureerd:

```
port-access role <rolnaam>
    vlan trunk allowed name <vlan-naam>
```

Stel dat ClearPass de rol “admin” toewijst, en deze rol op de switch gekoppeld is aan VLAN “admin-netwerk” (bijv. VLAN 55), dan zal de poort van het betreffende apparaat automatisch aan VLAN 55 worden toegewezen. Dit proces moet herhaald worden voor elke mogelijke rol die ClearPass kan terugsturen. Ontbreekt een rol in de configuratie, dan zal de switch geen aanpassing uitvoeren.

5.3. Patching van kabels

Voordat poorten geconfigureerd worden, is het essentieel om eerst te bepalen welke poorten daarvoor in aanmerking komen. Een fout in dit proces kan leiden tot verstoring van netwerkverbindingen, zeker als per ongeluk poorten worden geconfigureerd waarop andere switches zijn aangesloten.

De bekabeling verloopt doorgaans als volgt: van het gebruikersapparaat gaat een netwerkkabel naar een wandcontactdoos, die verbonden is met een patchpaneel. Vanuit dit patchpaneel loopt een kabel naar de patchruimte, waar de verbinding uiteindelijk eindigt in een switchpoort.

Het is dus noodzakelijk om per werkplek te documenteren welk patchnummer gekoppeld is aan welk gebruikersapparaat. Op basis hiervan kan in de patchruimte worden nagegaan op welke switch en welke poort de verbinding eindigt. Dit proces wordt verder toegelicht in het hoofdstuk Documentatie.

5.4. Configureren van de switch poorten

Wanneer duidelijk is welke poorten moeten worden geconfigureerd, kunnen deze geactiveerd worden voor authenticatie. Poorten die verbonden zijn met andere switches of routers worden hierbij niet geconfigureerd om misconfiguraties te voorkomen.

Voor elke poort wordt het volgende configuratieproces doorlopen:

```
interface <int>
    aaa authentication port-access dot1x authenticator enable
    aaa authentication port-access mac-auth enable
    port-access onboarding-method concurrent enable
    aaa authentication port-access client-limit 5
```

Hiermee wordt ingesteld dat de poort zowel 802.1X als MAC-authenticatie ondersteunt, en dat deze tegelijkertijd worden uitgevoerd voor snellere connectiviteit (concurrent onboarding). Daarnaast wordt een limiet van vijf gelijktijdige authenticerende apparaten per poort ingesteld.

6. Documentatie en Oplevering

In dit hoofdstuk wordt de opleverdocumentatie van de stageopdracht besproken. Deze documentatie is essentieel voor het correct beheren, onderhouden en eventueel uitbreiden van de implementatie na afloop van de stageperiode. Het doel is om de opgedane kennis en uitgevoerde configuraties duidelijk en gestructureerd over te dragen aan de medewerkers van Politiezone Geel-Laakdal-Meerhout. Dit gebeurt aan de hand van drie onderdelen: een realisatiedocument, een gedetailleerde handleiding voor intern gebruik, en een Excel-bestand dat de uitrol praktisch ondersteunt en opvolg baar maakt.

6.1. Realisatiedocument

Het realisatiedocument geeft een globaal overzicht van de volledige stageopdracht. Hierin wordt uiteengezet wat het doel van het project was, welke stappen zijn ondernomen om dat doel te bereiken en hoe het eindresultaat tot stand is gekomen. Het document fungeert als een samenvattend verslag van het traject en biedt lezers een duidelijk beeld van de werkzaamheden en beslissingen die gedurende de stageperiode zijn genomen.

6.2. Handleiding

De handleiding is een intern technisch document waarin uitgebreid wordt beschreven welke configuraties er zijn uitgevoerd en hoe deze zijn opgezet. Aangezien het document gevoelige informatie bevat, zoals IP-adressen, hostnamen en beveiligingsinstellingen, is het uitsluitend bedoeld voor intern gebruik.
De structuur van de handleiding is als volgt:

1. **Algemene informatie:** Een overzicht van de gebruikte namen voor de Intune-configuraties en een opsomming van de kantoren die tijdens de opdracht zijn behandeld.
2. **Intune-configuraties:** Stap-voor-stap instructies voor het opzetten van filters, het uitrollen van certificaten, het aanmaken en exporteren van benodigde bestanden, het installeren van deze bestanden via een Win32-app en hoe nieuwe apparaten kunnen worden toegevoegd. De uitleg is geschreven vanuit het perspectief van iemand die de configuratie volledig opnieuw moet opzetten, bijvoorbeeld na gegevensverlies.
3. **Switchconfiguratie:** Beschrijving van de configuraties op de switches, inclusief instructies over hoe deze uitgevoerd en gemonitord kunnen worden.
4. **Aanpassingen in ClearPass:** Een overzicht van de wijzigingen die tijdens de stage aan de ClearPass-configuratie zijn doorgevoerd, met vermelding van de redenen hiervoor. De basisconfiguratie van ClearPass wordt niet verder behandeld, aangezien dit systeem door Securitas is opgezet en zij hun eigen handleiding hebben aangeleverd.
5. **Handmatige installatie:** Instructies voor het handmatig toevoegen van apparaten aan het netwerk in situaties waarin Intune niet gebruikt kan of mag worden, met als doel deze alsnog toegang te geven tot het admin-netwerk.
6. **Problemen en oplossingen:** Beschrijving van problemen die tijdens het project zijn opgedoken, mogelijke toekomstige uitdagingen en de oplossingen of aanbevelingen die hiervoor zijn geformuleerd.
7. **Toekomstige uitbreidingen:** Suggesties voor verdere ontwikkeling van het systeem als de politiezone in de toekomst verder wil bouwen op deze opdracht.

Het doel van deze handleiding is om de overdracht van de opdracht naar de organisatie zo vlot en duurzaam mogelijk te laten verlopen.

6.3. Rollout Excel-bestand

Naast de handleiding is er een Excel-document opgesteld dat het uitrolproces van de apparaten overzichtelijk maakt. In dit bestand worden de apparaten die in Intune onder een specifieke filter vallen, geregistreerd. Voor elk apparaat wordt aangeduid of het correct geconfigureerd is. Als een apparaat niet binnen de filter valt, wordt de reden hiervan vermeld.

Verder wordt er in het bestand bijgehouden welke interfaces van de switches geconfigureerd zijn, naar welke patchnummers deze lopen, en uiteindelijk naar welke tafel en in welk kantoor het apparaat zich bevindt. Dit zorgt voor een duidelijke en efficiënte opvolging van de netwerkinfrastructuur en vereenvoudigt toekomstig onderhoud of uitbreiding.

7. Problemen en oplossingen

In dit hoofdstuk bespreek ik de verschillende obstakels die ik ben tegengekomen tijdens mijn stage, en hoe ik hiermee ben omgegaan. Niet elke poging tot een oplossing bleek succesvol; daarom leg ik uit welke benaderingen ik geprobeerd heb, waarom bepaalde methoden niet werkten, en welke alternatieven uiteindelijk wel effectief waren. Daarnaast behandel ik enkele structurele beperkingen, zoals het ontbreken van administratorrechten en beperkte voorkennis van Microsoft Intune. Tot slot geef ik ook een overzicht van nog bestaande problemen en mogelijke aandachtspunten voor de toekomst.

7.1. Intune

Aangezien Microsoft Intune geen onderdeel was van de opleiding, had ik bij aanvang van mijn stage weinig ervaring met het platform. Ik wist niet precies welke mogelijkheden het bood of hoe configuraties correct opgezet moesten worden. Daarom heb ik in de beginfase veel tijd geïnvesteerd in zelfstudie en testen.

De situatie werd bemoeilijkt doordat ik werkte in een reeds bestaande en deels afgesloten Intune-omgeving. Ondanks dat ik toegang had via een beheerdersaccount, kon ik niet overal bij. Hierdoor moest ik zelf achterhalen welke groepen bruikbaar waren en hoe ik filters correct kon instellen. Dankzij deze inspanning kon ik uiteindelijk wel een succesvolle configuratie en uitrol realiseren.

7.2. Gebrek aan administratorrechten

Een van de grootste knelpunten tijdens mijn stage was het ontbreken van administratorrechten. Omdat ik stagiair was, mocht ik geen beheerdersacties uitvoeren zonder tussenkomst van een ICT-medewerker. Bij elke aanpassing of test waarvoor adminrechten nodig waren, moest ik iemand vragen om in te loggen.

Dit werd al snel een belemmering in mijn workflow, vooral wanneer ik meerdere keren op korte tijd hulp nodig had. Het gebeurde regelmatig dat ik 15 minuten niets kon doen, simpelweg omdat er niemand beschikbaar was. Deze afhankelijkheid had een duidelijke impact op mijn efficiëntie en zelfstandigheid.

7.3. Intune-configuratieproblemen

Voor het uitrollen van de *Wired AutoConfig*-instellingen probeerde ik in eerste instantie gebruik te maken van standaard apparaatconfiguraties binnen Intune. Deze methode leidde ertoe dat de instellingen wel werden opgepikt, maar niet correct toegepast. De oorzaak was dat de service ‘Wired AutoConfig’ pas opnieuw moest worden opgestart om de instellingen effectief toe te passen.

Een script om de service te herstarten bood geen oplossing, omdat het script vaak werd uitgevoerd voordat de configuraties volledig geladen waren. Daarom heb ik een herstelscript ontwikkeld dat eerst controleert of de configuratie actief is, en zo niet, dan pas de juiste instellingen toepast en de service herstart. Dit werkte goed, totdat ik het testte op een toestel dat met een dockingstation werkte. Omdat het apparaat tijdens de uitrol geen actieve ethernetverbinding had, werden de instellingen niet op de juiste interface toegepast.

De definitieve oplossing was het gebruik van de Windows Taakplanner. Hierdoor worden de instellingen telkens opnieuw toegepast wanneer er een nieuwe netwerkverbinding wordt gedetecteerd, wat betrouwbaar bleek, ook bij dockingstations.

7.4. Authenticatieproblemen

Tijdens de uitrol van de switchconfiguraties stootte ik op twee problemen:

7.4.1. IP-telefoon authenticatie

Door de opstelling van de werkplekken (laptop → dockingstation → IP-telefoon → patchpaneel → switch) kwam het voor dat de IP-telefoon zich niet correct authenticeerde bij ClearPass. Dit gebeurde vooral als de laptop al aangesloten was op het dockingstation op het moment dat de switchinterface werd geconfigureerd.
De oplossing was om:

- De switchinterface tijdelijk te resetten.
- De laptop los te koppelen van het dockingstation.
- De juiste configuratie opnieuw toe te passen op de switchinterface.
- Daarna de IP-telefoon opnieuw aan te sluiten zodat deze zich correct kon authenticeren.
- Vervolgens kon de laptop opnieuw worden aangesloten, die zich dan ook correct authentiseerde.

7.4.2. Verkeerd netwerkicoon in Windows

Een kleiner maar hinderlijk probleem was dat Windows na het configureren van de switchinterfaces soms het verkeerde netwerkicoon toonde (bijvoorbeeld: Wi-Fi in plaats van Ethernet). Dit werd opgelost door het apparaat eenvoudigweg opnieuw op te starten.

7.5. Printers en authenticatie

Een onverwacht probleem was de authenticatie van printers. Omdat printers geen certificaten kunnen gebruiken zoals andere apparaten, moesten ze op een andere manier toegang krijgen tot het netwerk. De oplossing hiervoor was het toepassen van *MAC Authentication Bypass (MAB)*.

In ClearPass heb ik een regel toegevoegd die toestaat dat apparaten met de status “Known” toegang krijgen tot het admin-netwerk. Door de MAC-adressen van de printers in ClearPass als vertrouwd in te stellen, konden deze zonder certificaat correct worden geauthentiseerd en verbonden met het juiste netwerksegment.

7.6. Werken in een productieomgeving

Alle configuraties en testen moesten worden uitgevoerd in een actieve productieomgeving. Dit vereiste uiterste voorzichtigheid, omdat een fout direct impact kon hebben op het werk van collega’s. Om risico’s te beperken, werkte ik met checkpoints en voerde ik wijzigingen gefaseerd door. Vaak moest ik wachten om te controleren of een wijziging geen onvoorziene gevolgen had, wat het tempo van de werkzaamheden beïnvloedde, maar de stabiliteit van de omgeving waarborgde.

8. Besluit

Mijn stageopdracht bij Politiezone Geel-Laakdal-Meerhout was op het eerste gezicht vrij rechtlijnig: zorgen dat de nodige configuraties uitgerold worden via Microsoft Intune, de switches configureren voor netwerk-authenticatie via Aruba ClearPass en uiteindelijk alles correct laten doorkomen in ClearPass. Hoewel deze opdracht eenvoudig leek, bleek ze in de praktijk een stuk complexer.

Een goed voorbeeld hiervan was het werken met Intune, een platform waarmee we op school weinig tot geen ervaring hebben opgedaan. Dit werd echter het centrale punt van mijn opdracht. Het technische aspect van Intune was op zich geen onoverkomelijk obstakel met voldoende opzoekwerk en documentatie vond ik mijn weg. De grootste uitdaging was dat deze Intune-omgeving voor de volledige politiezone werd gebruikt, waardoor ik niet zomaar configuraties kon aanpassen. Ik heb bijna twee weken moeten zoeken om uit te vinden op welke groepen ik de nodige rechten had om te kunnen filteren.

Een tweede uitdaging was dat alles moest gebeuren in een actieve productieomgeving. Elk foutje had potentieel directe impact op de werking van collega's binnen de organisatie. Daarom moest ik steeds zeer zorgvuldig te werk gaan en zorgen dat ik bij problemen onmiddellijk kon terugkeren naar een werkende configuratie. Hoewel dit een lastige werkomgeving was, heeft het mij waardevolle ervaring opgeleverd situaties zoals deze zal ik ook later in mijn carrière tegenkomen.

Wat voor mij persoonlijk het grootste pijnpunt was, was het gebrek aan adminrechten. Als stagiair kreeg ik deze rechten niet, wat betekende dat ik steeds afhankelijk was van anderen om iets met administratorrechten uit te voeren. Dit zorgde niet alleen voor vertragingen, maar ook voor frustratie op momenten waarop snelle actie vereist was. Tegelijkertijd leerde dit mij om beter te plannen: ik dacht altijd vooraf na over welke tools, rechten of acties ik nodig had zodat, zodra iemand mij kon inloggen, ik meteen efficiënt aan de slag kon.

Naast technische vaardigheden zoals het werken met Microsoft Intune en ClearPass, heb ik ook mijn soft skills aanzienlijk kunnen ontwikkelen. Zo heb ik geleerd om geduldig te werken, om vooraf risico's in te schatten en om problemen gestructureerd aan te pakken. In tegenstelling tot het tempo op school, waar we snel taken afwerken en nadien testen, moest ik nu trager en zorgvuldiger te werk gaan om problemen onmiddellijk te kunnen lokaliseren en oplossen.

Ik ben trots op het resultaat van mijn stageopdracht. De laptops binnen de afdelingen die ik kon beheren, zijn correct geconfigureerd via Intune. De switches voeren nu netwerk-authenticatie uit met behulp van ClearPass. Daarnaast heb ik een uitgebreide interne handleiding opgesteld, waarin alle configuratiestappen, mogelijke problemen en bijhorende oplossingen duidelijk zijn gedocumenteerd.

Mijn project werd succesvol uitgerold op de volledige bovenverdieping. Bovendien heb ik duidelijke en bruikbare documentatie achtergelaten, zodat de organisatie het project zelfstandig verder kan uitrollen in de rest van de omgeving.

Mijn advies voor de toekomst is dan ook om dit project niet op de lange baan te schuiven, maar het zo snel mogelijk verder op te nemen. Het is belangrijk om niet alleen de uitrol af te werken, maar ook verder te bouwen op de bestaande configuratie om zo de netwerkbeveiliging nog verder te versterken.

Tegelijk wil ik wel een belangrijke waarschuwing meegeven: het is relatief eenvoudig om per ongeluk een fout te maken zonder dat je het meteen doorhebt. Omdat alles zich in een productieomgeving afspeelt, kunnen dergelijke fouten ernstige gevolgen hebben, zoals netwerkuitval. Daarom is het essentieel om eerst grondig onderzoek te doen en goed na te denken over de mogelijke risico's en impact voordat verdere stappen worden gezet.

Tot slot wil ik benadrukken dat ik deze stage als zeer waardevol heb ervaren. Ik heb altijd respectvol en professioneel gewerkt, opdrachten meteen aangepakt en goed samengewerkt met het team. De sfeer

binnen het ICT-team was aangenaam en de taken zelfs degene waarvoor ik zelf geen rechten had vond ik erg interessant. Ik zie mezelf in de toekomst zeker werken in een gelijkaardige omgeving.

Met dit besluit rond ik mijn realisatiedocument af. Ik hoop dat dit document een duidelijk beeld geeft van mijn stageopdracht, mijn aanpak en de geleverde resultaten.

THOMAS MORE