THOMAS MORE

Stage vzw De Waaiburg

Realisatiedocument

Sietse Didden
Student Bachelor in de Elektronica-ICT – Cloud & Cyber Security

2025 – 2026

Inhoud

Tabellenlijst

1. Inleiding

Dit realisatiedocument beschrijft de uitvoering van de stageopdrachten bij De Waaiburg in de periode van 23 februari tot en met 29 mei.
Het document bouwt voort op het eerder opgestelde projectplan en geeft een gedetailleerd overzicht van de analyse, de gemaakte keuzes, de gebruikte tools en de uiteindelijk opgeleverde resultaten.
De stage omvatte een breed scala aan IT-werkzaamheden, uiteenlopend van het oplossen van helpdeskproblemen tot het uitwerken van structurele verbeteringen op het vlak van netwerkbeheer, gebruikersondersteuning en beveiliging.

De kernopdrachten waren:

- Het ontwikkelen van een gebruiksvriendelijke oplossing voor het benaderen van de lokale NAS-opslag, ter vervanging van een omslachtige handmatige koppeling.
- Het voorbereiden van een netwerkrenovatie, waaronder de configuratie van nieuwe Meraki-switches en de installatie van een bijkomend accesspoint.
- Het verbeteren van de beveiliging door het opstellen van een wachtwoordbeleid.
- Het bieden van technische ondersteuning aan eindgebruikers bij diverse hardware- en softwareproblemen.

In de volgende hoofdstukken wordt eerst de analysefase toegelicht, waarin verschillende oplossingsrichtingen werden onderzocht en tegen elkaar afgewogen.
Vervolgens wordt de concrete realisatie beschreven, onderverdeeld in de belangrijkste deelprojecten. Het document sluit af met een besluit waarin de behaalde resultaten worden geëvalueerd en aanbevelingen voor de toekomst worden geformuleerd.

2. Analyse

Voorafgaand aan de uitvoering van de opdrachten werd een grondige analyse uitgevoerd om tot weloverwogen keuzes te komen. Dit hoofdstuk beschrijft de onderzochte alternatieven, de gehanteerde selectiecriteria en de uiteindelijke beslissingen.

2.1. Oplossingsrichtingen voor de NAS-toegang

Het oorspronkelijke probleem betrof een omslachtige manier van werken waarbij gebruikers handmatig een netwerkverbinding naar de NAS moesten opzetten via een batchbestand. Dit leidde tot het niet gebruiken van de methode. De doelstelling was tweeledig: het vereenvoudigen van de toegang tot de NAS en het reduceren van de nood aan manuele tussenkomst.

Er zijn verschillende opties onderzocht:
Userfr = Gebruiksvriendelijkheid
Sustain = Sustainability

Optie	Cost (w:20)	Security (w:25)	Userfr. (w:25)	Integratie (w:10)	Retrieval (w:10)	Sustain. (w:10)	Totaal (max 500)	(%)
NAS + Back-up	5 (100)	4 (100)	5 (125)	5 (50)	4 (40)	3 (30)	**445**	89%
Backblaze B2 + Web UI	4 (80)	4 (100)	4 (100)	3 (30)	5 (50)	4 (40)	**400**	80%
Proton Drive (E2EE)	2 (40)	5 (125)	4 (100)	4 (40)	4 (40)	4 (40)	**385**	77%
AWS S3 + Amplify (EU)	2 (40)	4 (100)	4 (100)	4 (40)	5 (50)	5 (50)	**380**	76%
Backblaze B2 (alleen delen)	4 (80)	3 (75)	3 (75)	5 (50)	5 (50)	4 (40)	**370**	74%
S3 Glacier (archief)	3 (60)	4 (100)	2 (50)	3 (30)	1 (10)	5 (50)	**300**	60%

Table 1 - Decision matrix voor NAS-oplossingen

Cloudalternatieven

- Amazon S3 Glacier / Backblaze B2: Zeer lage opslagkosten, maar trage toegangstijden en een complexe integratie met de bestaande werkomgeving. Bovendien zou een bijkomende webinterface noodzakelijk zijn om de gebruiksvriendelijkheid te garanderen, wat extra ontwikkelwerk met zich meebrengt. (Amazon, 2026) (AWS, 2026) (backblaze, 2026)
- Proton Drive: Interessant vanwege de end-to-end-encryptie en de ingebouwde gebruikersinterface, maar de prijs per gebruiker lag hoger dan gewenst voor een organisatie met veel occasionele gebruikers.
- AWS Amplify + S3 + Amazon Cognito: Een krachtige combinatie die een volledig beheerde webapplicatie mogelijk maakt met gebruikersauthenticatie. Deze optie vereiste echter een aanzienlijke ontwikkelinspanning en een terugkerend kostenmodel dat niet in verhouding stond tot de beperkte omvang van het probleem. (Amazon, 2026) (AWS, 2026)

Afweging en keuze
Bij de afweging werden de volgende criteria gehanteerd: kostprijs (zowel initieel als terugkerend), gebruiksgemak voor de eindgebruiker, beheersbaarheid door IT, en veiligheid.
De cloudoplossingen scoorden onvoldoende op kostprijs. De webinterface voegde een extra laag complexiteit toe zonder de gebruikerservaring fundamenteel te vereenvoudigen.
De keuze werd uiteindelijk gemaakt via een decision-matrix en aftoetsen met de stagementor.

De keuze viel op de ontwikkeling van een PowerShell-script met grafische interface. Deze aanpak maakte gebruik van bestaande infrastructuur (de NAS en het lokale netwerk), vereiste geen bijkomende licenties of abonnementen, en kon via Microsoft Intune centraal worden uitgerold naar alle werkplekken.
De gebruikerservaring zou sterk verbeteren doordat enkel een gebruikersnaam en wachtwoord in een herkenbaar venster ingevoerd dienden te worden, waarna de netwerkschijf automatisch en persistent werd gekoppeld en er een “map” op het bureaublad van de gebruiker zou komen, waardoor ze nooit File Explorer moesten openen.

2.2. Keuze voor een zelf gehoste wachtwoordmanager

Tijdens de stage viel op dat binnen de organisatie geen formeel wachtwoordbeleid bestond. Veel medewerkers bewaarden inloggegevens op papier of in onbeveiligde spreadsheets, wat een aanzienlijk beveiligingsrisico vormde. Tegelijkertijd was er behoefte aan het veilig delen van wachtwoorden voor gemeenschappelijke accounts (bijvoorbeeld voor printers of online diensten).

Factoren bij overweging:

- Geen recurrente licentiekosten, passend binnen het budget van een non-profitorganisatie.
- Dataopslag binnen de eigen infrastructuur (on-premises) omwille van privacy en controle.
- Ondersteuning voor meerdere gebruikers met de mogelijkheid om wachtwoorden te delen in teamverband.
- Verplichte multifactorauthenticatie (MFA) voor verhoogde beveiliging.
- Compatibiliteit met gangbare browsers en mobiele apparaten.

Na een vergelijking van verschillende open-source alternatieven, waaronder Passbolt en SysPass, werd Vaultwarden geselecteerd. Vaultwarden is een lichtgewicht, in Rust geschreven server die volledig compatibel is met de officiële Bitwarden-clients (browserextensie, desktop- en mobiele app). (García, 2026)

Solution	Security (25)	Control (20)	Cost (20)	Usability (20)	Team (10)	Maint (5)	Total (max 500)	(%)
Vaultwarden (self-hosted)	4 (100)	5 (100)	5 (100)	4 (80)	4 (40)	2 (10)	**430**	**86%**
Passbolt	4 (100)	4 (80)	4 (80)	3 (60)	5 (50)	4 (20)	**390**	**78%**
SysPass / Password-XL	3 (75)	4 (80)	5 (100)	3 (60)	3 (30)	3 (15)	**360**	**72%**
Bitwarden Cloud (free/paid)	4 (100)	2 (40)	3 (60)	5 (100)	3 (30)	1 (5)	**335**	**67%**
Zoho Vault (free tier)	3 (75)	2 (40)	4 (80)	4 (80)	3 (30)	1 (5)	**310**	**62%**

Table 2 - Decision matrix wachtwoordmanager

De belangrijkste voordelen zijn:

- **On-premises hosting**: De server kan als Docker-container op de bestaande NAS worden gedraaid, waardoor alle data binnen het eigen netwerk blijft.
- **Geen licentiekosten**: Vaultwarden is open-source en gratis te gebruiken.
- **End-to-end encryptie**: Alle opgeslagen wachtwoorden worden lokaal op het toestel van de gebruiker versleuteld voordat ze naar de server worden verzonden.
- **Ingebouwde MFA-ondersteuning**: TOTP (Time-based One-Time Password) kan verplicht worden gesteld voor alle accounts.
- **Gebruiksvriendelijke clients**: Medewerkers kunnen de vertrouwde Bitwarden-apps gebruiken, wat de adoptiegraad ten goede komt.

Het implementatieplan omvatte naast de technische installatie ook het opstellen van een wachtwoordbeleid en een communicatieplan naar de medewerkers.

2.3. Voorbereiding netwerkrenovatie en Meraki-configuratie

Een deel van de stageopdracht betrof het voorbereiden van de vervanging van bestaande netwerkswitches door Cisco Meraki-apparatuur.
De analysefase bestond uit:

- **Inventarisatie van de huidige configuratie**: De bestaande switchconfiguratie (Cisco IOS) werd geanalyseerd om de gebruikte VLAN's, trunkpoorten en accesspoorten in kaart te brengen. Hierbij werden enkele inconsistenties in de beschrijvingen van poorten vastgesteld en gedocumenteerd.
- **Studie van de Meraki-dashboardomgeving**: Het Meraki-clouddashboard biedt een fundamenteel andere beheerervaring dan de klassieke command-line interface. Via een testnetwerk in het dashboard werden de mogelijkheden van templates, VLAN-profielen en poortconfiguratie verkend. (Meraki, 2026)
- **Gebruik van de VLAN-structuur**: In overleg met de IT-verantwoordelijken werd de logische VLAN-indeling (onder andere voor data, voice, beheer en gasttoegang) die al reeds aanwezig was gebruikt voor de switches. Er werd rekening gehouden met best practices zoals het gebruik van een apart native VLAN voor trunks en het beperken van ongebruikte poorten.
- **Opstellen van een implementatieplan**: Er werd een stapsgewijs plan uitgewerkt voor de fysieke vervanging van de switches, waarbij de nieuwe configuratie volledig vooraf in het dashboard kon worden klaargezet om de downtime tijdens de ombouw te minimaliseren.

2.4. Analyse printerbeveiliging ('Locked Print')

De bestaande Ricoh-multifunctionals boden geen bescherming tegen het ongewenst inzien van afgedrukte documenten. Iedereen die zich fysiek bij de printer bevond, kon documenten van collega's zien liggen of meenemen. De gewenste oplossing was 'locked print' (Ricoh, 2026), waarbij een afdruktaak pas wordt uitgevoerd nadat de gebruiker een persoonlijke pincode heeft ingevoerd op het bedieningspaneel van de printer.

De analyse omvatte:

- **Onderzoek van de printerdocumentatie**: De specifieke terminologie en configuratiemogelijkheden voor locked print op Ricoh-apparaten werden bestudeerd.
- **Toegang tot de beheerinterface**: Er werd vastgesteld dat de beheerinterface van de printer enkel toegankelijk was met administratorcredentials. Deze credentials waren niet langer gekend, waardoor eerst contact moest worden opgenomen met de printerleverancier.
- **Evaluatie van uitrolmethoden**: Er werden twee pistes onderzocht om de locked print-instellingen naar alle werkplekken te distribueren:
    1. **Centrale uitrol via Intune**: Door de printerdrivers en -voorkeuren te exporteren en als Win32-app te verpakken (Microsoft, Microsoft Intune documentation, 2026), kon de configuratie in principe centraal worden afgedwongen. In de praktijk bleek dit echter complex en foutgevoelig, mede door de variatie in printermodellen en besturingssystemen.
    2. **Stappenplan voor eindgebruikers**: Een duidelijk gedocumenteerde handleiding waarmee medewerkers zelf de instelling eenmalig konden activeren.

Na overleg met de stagebegeleider werd gekozen voor de tweede optie: een stappenplan voor de eindgebruiker. Dit gaf medewerkers de vrijheid om al dan niet van de functie gebruik te maken, vermeed complexe Intune-packages die moeilijk werkend te krijgen zijn, en verhoogde de bewustwording rond printerbeveiliging doordat gebruikers actief de instelling konden doorvoeren en medecollega's het wel doen.

3. Realisatie

3.1. NAS-koppeling met PowerShell en Intune

3.1.1. Ontwikkeling van het PowerShell-script

Het script werd iteratief ontwikkeld, waarbij functionaliteit en gebruiksvriendelijkheid stap voor stap werden verbeterd. De uiteindelijke versie combineert een robuust back-end met een goede grafische interface.

- **Functionaliteit**: Het script vraagt de gebruiker om zijn of haar gebruikersnaam en wachtwoord via een Windows Forms-venster. Met behulp van cmdkey.exe worden de ingevoerde credentials veilig opgeslagen in de Windows Credential Manager (Microsoft, Net use, 2026) (Microsoft, New-PSDrive, 2026). Vervolgens wordt met het net use-commando een persistente netwerkschijf (Z:-schijf) gekoppeld aan de NAS-share.
- **Foutafhandeling**: Het script is voorzien van uitgebreide foutafhandeling. Bij onjuiste credentials of het ontbreken van een netwerkverbinding krijgt de gebruiker een duidelijke foutmelding te zien. Het script loopt niet vast en blijft responsief door het gebruik van asynchrone aanroepen en timeouts.
- **Grafische interface**: Om de gebruikerservaring te verbeteren, werd een Windows Forms GUI gebouwd met een aangepast achtergrondlogo van De Waaiburg. Tijdens het verbindingsproces wordt een voortgangsbalk getoond. Het script wordt aangeroepen via een VBScript-wrapper, wat ervoor zorgt dat er geen onnodig PowerShell-consolevenster op de achtergrond verschijnt.

3.1.2. Uitrol via Microsoft Intune

Om het script op alle werkplekken beschikbaar te maken, werd het verpakt als een Win32-applicatie in Microsoft Intune.

- **Verpakking**: Het PowerShell-script, het VBScript, de achtergrondafbeelding, het pictogram en een detectiescript werden samengevoegd tot een .intunewin-bestand met behulp van de Microsoft Win32 Content Prep Tool.
- **Detectieregel**: Een PowerShell-detectiescript controleert of de snelkoppeling naar het script reeds op het bureaublad aanwezig is. Indien niet, beschouwt Intune de applicatie als “niet geïnstalleerd” en wordt de installatie uitgevoerd.
- **Toewijzing**: De applicatie werd toegewezen aan de groep “Alle Intune-gebruikers”, met als opdracht “Vereist”. Hierdoor wordt het script automatisch op alle beheerde Windows-laptops geïnstalleerd.
- **Documentatie**: Er werden twee handleidingen opgesteld en op de SharePoint-omgeving geplaatst:
    - Een succeshandleiding met schermafbeeldingen die de werking van het script stap voor stap uitlegt.
    - Een probleemoplossingshandleiding die de meest voorkomende foutmeldingen beschrijft en de gebruiker instructies geeft om deze zelf op te lossen (bijvoorbeeld controleren van de netwerkverbinding of VPN)

3.2. Netwerkrenovatie: Meraki-switches en accesspoint

3.2.1. Meraki-configuratie

De voorbereiding en uitvoering van de Meraki-configuratie verliep in meerdere fasen:

- **Testomgeving**: In het Meraki-dashboard werd een testnetwerk opgezet om configuraties te valideren. VLAN's (10, 20, 30, 99, 999) werden aangemaakt, een trunkpoort met native VLAN 999 ingesteld, en een access-poorttemplate voor eindgebruikers gedefinieerd.
- **Omzetting legacy-configuratie**: De bestaande Cisco-configuratie werd vertaald naar Meraki. Hierbij werden foutieve poortbeschrijvingen uit de oude configuratie gecorrigeerd en ontbrekende beveiligingsinstellingen toegevoegd.
- **Automatisering via API**: Om toekomstig beheer te vereenvoudigen, werd een Python-script ontwikkeld dat via de Meraki API configuraties uit CSV-bestanden leest en pusht. Het script ondersteunt:
    - Gewone poortconfiguraties (VLAN, type, snelheid/duplex).
    - Beveiligingsinstellingen (zoals poortbeveiliging).
    - Link Aggregation (LAG): regels met meerdere poorten worden automatisch als een aggregatie behandeld. LACP-onderhandeling wordt door Meraki afgehandeld.
    - Logging van geplande wijzigingen (dry-run modus) alvorens definitief toe te passen.
- **Productiemigratie**: Na validatie werden de switches vanuit het testnetwerk gemigreerd naar het productienetwerk. De configuratie werd via het script opnieuw gepusht. Hierbij traden kleine problemen op (ontbrekende duplex-instellingen, poortvolgorde die niet logisch was), die systematisch werden hersteld.
- **Fysieke installatie**: Twee switches werden fysiek geïnstalleerd en functioneerden na configuratie meteen correct. Voor de overige switches werd de configuratie definitief klaargezet.

3.2.2. Accesspoint installatie

In een afgelegen ruimte werd een bijkomend accesspoint geïnstalleerd.

- **Materiaal en locatie**: In overleg met de technische dienst werd de optimale montageplaats boven een deur bepaald. De nodige pluggen en schroeven waren aanwezig. Een geschikte netwerkkabel werd getrokken en op een vrije poort van de switch aangesloten.
- **Activering**: Na overleg met IT werd de switchpoort op het juiste VLAN gezet en geopend. Het accesspoint werd ingeplugd en kwam onmiddellijk online in het Meraki-dashboard. De dekking in de ruimte was hierdoor verzekerd.

3.3. Configuratie MacBook Air M3 met dual monitor setup

Een gebruiker kreeg een nieuwe MacBook Air met M3-chip. De wens was om twee externe beeldschermen aan te sluiten via een dockingstation. De M3-chip ondersteunt van nature echter slechts één extern scherm naast het ingebouwde scherm.

3.3.1. Analyse en oplossing

Uit onderzoek bleek dat de beperking softwarematig omzeild kan worden door gebruik te maken van DisplayLink-technologie. (Displaylink, 2026) Hiervoor zijn twee zaken noodzakelijk: een dockingstation dat DisplayLink ondersteunt, en de bijbehorende driver op de Mac.

- **Aanschaf hardware**: Er werd een Dell D1000 dockingstation aangeschaft, dat DisplayLink over USB 3.0 ondersteunt. Omdat de MacBook enkel USB-C poorten heeft, werd een USB-C naar USB-B 3.0 kabel besteld.
- **Installatie en configuratie**: Na installatie van de DisplayLink Manager-software en het aansluiten van de dock via de correcte kabel, werden beide externe monitoren (één via HDMI, één via VGA) onmiddellijk herkend. In de macOS-beeldscherminstellingen werd de juiste opstelling (uitgebreid bureaublad) geconfigureerd.
- **Uitdagingen**: Tijdens de initiële testen werd het dock niet herkend, omdat er per ongeluk een oplaadkabel zonder datalijnen werd gebruikt. Ook werd de verkeerde USB-poort op het dock gebruikt (de downstream- in plaats van de upstream-poort). Deze problemen zijn systematisch opgelost.

3.3.2. Overige configuraties

- **VPN**: De Cisco AnyConnect VPN-client werd geïnstalleerd en geconfigureerd voor externe toegang.
- **NAS connectie**: Meerdere scripts werden geschreven op de Mac om een SMB share te leggen bij opstart zodra de het juiste wifi-netwerk connected is.
- **eID**: De Belgische eID-middleware werd succesvol geïnstalleerd en werkt met de aanwezige kaartlezer.
- **Bestandsoverdracht**: Gegevens van de oude Windows-laptop werden overgezet met een USB-stick, nadat een poging met de Windows Migration Assistant faalde.
- **Printer**: Een specifieke Ricoh-printerdriver werd handmatig geïnstalleerd en de printer werd toegevoegd via Systeeminstellingen.
- **PDF-software**: Het oorspronkelijke plan om Adobe Acrobat aan te schaffen werd verlaten ten gunste van Foxit PDF Editor (Software, 2026). De ondertekeningsfunctionaliteit met eID bleef echter problematisch, ondanks uitgebreide troubleshooting en contact met de leverancier. Een definitieve oplossing kon niet binnen de stageperiode worden bereikt.
- **USB-C hub**: Voor een andere Mac-gebruiker werd een geschikte USB-C hub (Melerink) aangeschaft en geconfigureerd.

3.3.3. Bijkomende zaken

Na de initiële configuratie deden zich nog enkele gebruikersproblemen voor:

- Een lege bureaublad- en documentenmap (alle scripts en IT files weg) bleek veroorzaakt door een verkeerd iCloud-account. Via Automator konden de ontbrekende scripts en snelkoppelingen worden hersteld. De nodige bestanden werden opnieuw lokaal geplaatst en nieuwe snelkoppelingen naar de NAS-share en VPN werden aangemaakt.
- Outlook-problemen (zoekfunctie voor ontvangers, emoji-reacties) werden verholpen door een systeemherstel.
- De proefperiode van Foxit verliep; een nieuwe trial kon niet meteen worden geactiveerd omdat het probleem niet aan de software lag. De helpdesk van Foxit werd voorzien van de nodige screenshots voor verder onderzoek.

De MacBook bleef verder functioneel en voldeed aan de gebruikerswensen.

3.4. Wachtwoordbeleid, Vaultwarden & awareness

3.4.1. Wachtwoordbeleidsdocument

Er werd een formeel, maar niet-afdwingbaar, wachtwoordbeleid op schrift gesteld. De kernpunten:

- Alle werkgerelateerde wachtwoorden dienen te worden opgeslagen in een goedgekeurde wachtwoordmanager. Opslag op papier of in spreadsheets is niet langer toegestaan.
- Het hoofdwachtwoord (master password) van de wachtwoordmanager moet een wachtwoordzin zijn van minimaal 14 tekens zonder logische woorden.
- MFA is verplicht voor de wachtwoordmanager en voor alle bedrijfskritische systemen waar dit wordt ondersteund.
- Lichtere richtlijnen (zoals niet hergebruiken van wachtwoorden) werden aangevuld met strengere voorschriften en voorzien van verduidelijkende voorbeelden.

3.4.2. Vaultwarden-voorstel

Oorspronkelijk werd een uitgewerkt implementatieplan voor Vaultwarden (een lichtgewicht, Bitwarden-compatibele server) opgesteld.
Het voorstel omvatte:

- Docker-deployment op de bestaande NAS.
- Beveiliging via Argon2id, Fail2Ban en interne HTTPS.
- Verplichte MFA en end-to-end encryptie.
- Collecties voor het delen van teamwachtwoorden.

Uit feedback bleek dat een dergelijke oplossing in het verleden reeds was overwogen, maar om organisatorische redenen niet was doorgevoerd. Er is daarom een bijkomend argumentatiedocument opgesteld waarin de voordelen (geen licentiekosten, volledige controle, verhoogde beveiliging) nogmaals onderbouwd werden en vergeleken met de risico's van de huidige papieren werkwijze. Dit document is overhandigd aan de IT, maar de uiteindelijke conclusie is dat dit de attack-surface alleen maar vergroot en het moeilijk afgedwongen kan worden.

3.4.3. Phishingcampagne en awareness

Om de start te creëren voor de invoering van het wachtwoordbeleid, werd een bewustwordingscampagne opgezet in de vorm van een gesimuleerde phishingmail en een begeleidende infopagina.

- **Technische uitwerking**:
  - Origineel was de bedoeling een eenvoudige, maar realistisch ogende phishingmail te ontwerpen, met een bedrijfslogo en een herkenbare afzender. Omdat een perfecte spoof technisch belemmerd werd door spamfilters, werd gekozen voor een extern Outlook-adres.
  - De mail linkt naar een via Netlify gehoste landingspagina die onder bijlage te vinden is. Deze pagina bevatte een korte, opvallende boodschap (“OEI, dit was een test!”) en interessante security-feiten, met een optionele knop om interesse in een vervolgsessie te registreren via e-mailopgave.
  - De HTML-pagina logt bezoeken, zodat kan worden gemeten hoeveel medewerkers op de link klikten.
- **Uitvoering**:
  - De mailinglijst werd gesegmenteerd via een Python-script dat door de lijst filtert.
    De mail komt succesvol aan, maar de gebruiker ziet de images en opmaak niet tot ze op vertrouwen klikken.

De campagne maakt deel uit van de voorbereiding van een kennissessie rond wachtwoorden en phishing, waarvoor reeds interesse werd geregistreerd na NAS-demonstraties.

3.5. Locked Print en bureaubladsnelkoppelingen

3.5.1. Locked Print op Ricoh-printers

Na het verkrijgen van de beheerderscredentials werd de Locked Print-functionaliteit geactiveerd. Een stappenplan met schermafbeeldingen en foto’s ter plaatse aan de printer beschrijft hoe gebruikers in de printervoorkeuren van Windows de optie ‘Locked Print’ kunnen selecteren en een pincode instellen. Het document werd op SharePoint geplaatst.

3.5.2. Snelkoppelingen naar scanfunctionaliteit

Voor diverse afdelingen werd een Intune-package ontwikkeld dat een snelkoppeling op het bureaublad plaatst naar de scaninterface van de betrokken Ricoh-printer. De snelkoppeling opent Google Chrome met het IP-adres van de printer. Initiële problemen met detectie en met .url-bestanden werden opgelost door over te schakelen naar .lnk-bestanden die rechtstreeks chrome.exe aanroepen. Het deployment verliep vervolgens succesvol over alle beoogde afdelingen.

3.6. Lessen en awarenesssessies

Om de nieuwe NAS-koppeling, het wachtwoordbeleid en veilig online gedrag te bevorderen, zijn er meerdere korte, praktijkgerichte sessies gegeven. Elke sessie had een eigen insteek en doelgroep.

3.6.1. NAS-presentatie

In aanloop naar de lessen werd een mini-presentatie van 5 tot 10 minuten ontwikkeld. Deze bevatte een live demo met een tijdelijk NAS-account, een visueel stappenplan en een verwijzing naar de uitgebreide handleiding op SharePoint. Twee afdelingen die nog niet met de nieuwe NAS-oplossing hadden gewerkt, kregen een live demo. De nadruk lag op het eenmalig invoeren van gebruikersnaam en wachtwoord, waarna de netwerkschijf automatisch verschijnt. De sessie leidde tot interesse in een vervolg over phishing en printerscan. Een eerder gemeld aanmeldprobleem op bepaalde services werd later opgelost via een handleiding op SharePoint.

3.6.2. Printeroplossing, phishing en wachtwoordbeleid

Een sessie van 30 minuten behandelde vier onderdelen: het gebruik van de printerscan-snelkoppeling, het herkennen van phishing (met live voorbeelden), het nut van een wachtwoordmanager (Bitwarden) en de kern van het nieuwe wachtwoordbeleid. De presentatie werd na evaluatie ingekort: de quiz bevatte minder vragen, overbodige voorbeelden vielen weg, en de uitleg over wachtwoordmanagers werd bondiger. Een volgende sessie voegde een live demonstratie van Bitwarden toe: het aanmaken van een vault, het gebruik van de generator en het instellen van MFA. Deelnemers konden vragen stellen over het delen van wachtwoorden in teamverband.

3.6.3. Voorbereiding van een presentatie over social engineering voor jongeren

In opdracht van de stagebegeleider werd een aparte, visueel aantrekkelijke presentatie ontwikkeld. Deze is bedoeld voor begeleiders die aan jongeren lesgeven over social engineering. De presentatie bevat pictogrammen, een Kahoot-quiz en eenvoudige taal. Eind mei is de presentatie overgedragen aan de organisatie.

3.7. Overige opgeloste problemen (MISC)

Gedurende de stageperiode werden tal van ad-hoc IT-problemen opgelost. Hieronder een overzicht van de meeste met telkens een beknopte toelichting.

- **HP-printer firmware downgrade** – Na een automatische firmware-update accepteerde de printer enkel nog dure originele HP-cartridges. Door een handmatige downgrade naar een oudere firmwareversie en het permanent uitschakelen van automatische updates werd het probleem definitief verholpen. (Save, 2026)
- **Scansnelkoppelingen hersteld** – Op een afdeling waren de snelkoppelingen naar het webportaal van de printer (scannen) verdwenen. Deze werden handmatig op meerdere laptops teruggeplaatst, zodat de vertrouwde werkwijze hersteld was.
- **Laptop freezes (meerdere toestellen)** – Verschillende laptops vertoonden onverklaarbare vastlopers, vaak tijdens periodes van inactiviteit. Logonderzoek leverde geen reproduceerbare oorzaak op. De toestellen werden geretourneerd naar de leverancier voor gespecialiseerde hardware-diagnose.
- **Terugkerende crashes bij inactiviteit** – Eén specifieke laptop bleef ondanks het wissen van testsoftware vastlopen. Omdat een hardware-oorzaak aannemelijk bleef, werd ook dit toestel teruggestuurd voor verder onderzoek.
- **IllegalTag Kernel error bij printen** – Bij het afdrukken van een specifiek document trad een 'IllegalTag'-fout op. De laptop bleek een universele printerdriver te gebruiken; na installatie van de correcte, modelspecifieke driver verdween de fout en werkte het printen normaal.
- **Word-bestanden openen niet** – Enkele oudere Word-documenten weigerden te openen of te converteren in de standaard Office-omgeving. Met behulp van LibreOffice (offline) werden ze alsnog geopend en naar PDF geëxporteerd, waardoor de inhoud opnieuw toegankelijk werd zonder dataverlies.
- **Afdrukstand "2 pagina's per ve**l" – Prints kwamen er verkleind uit doordat in de printervoorkeuren onbedoeld '2 pagina's per vel' was geselecteerd. Er werd een geïllustreerde handleiding opgesteld zodat gebruikers deze instelling voortaan zelf kunnen corrigeren.
- **Audio in meetings (laptop 1)** – Tijdens een meeting werkte het geluid niet; Bluetooth-hoofdtelefoons functioneerden wel. Na uitgebreid onderzoek bleken de rechten van de Windows Audio-service niet correct te zijn. Toevoegen van de systeemaccounts Networkservice en Localservice aan de lokale administratorsgroep en een herstart losten het probleem op.
- **Netwerkverbinding volledig weggevallen** – Een gebruiker kon opeens met geen enkel netwerk meer verbinden. Een eenvoudige systeemherstart bleek voldoende om de connectiviteit te herstellen; de oorzaak bleef onduidelijk.
- **Interne microfoon defect** – De interne microfoon van een laptop gaf geen enkel signaal, ook niet na het nalopen van drivers, privacy-instellingen, services en een sfc /scannow. Een externe microfoon werkte wél correct, waardoor een hardwaredefect van de interne module werd vastgesteld.
- **NAS-opslag tijdelijk onbereikbaar** – Een gebruiker meldde geen toegang meer te hebben tot de storage. Het probleem deed zich niet opnieuw voor en werd toegeschreven aan een tijdelijke netwerkstoring.
- **Presenterend scherm niet correct** – Tijdens een meeting lukte het niet om de schermen uit te breiden. Door de weergavemodus op 'Dupliceren' te zetten, kon de presentatie zonder onderbreking doorgaan.
- **Toegang tot TobaCube/Outlook** – Een gebruiker kon niet inloggen op TobaCube en Outlook. Het probleem werd opgelost door de browser te openen, naar de Teamsite te navigeren en vandaaruit de diensten te benaderen.
- **Verkeerde wifi-netwerkverbinding (printers onvindbaar)** – Meermaals konden gebruikers hun netwerkprinter niet vinden. Telkens bleek de laptop automatisch verbonden te zijn met een

verkeerd wifi-netwerk. Door het juiste netwerk in te stellen en het foute netwerk te ‘vergeten’, werd het euvel definitief verholpen.

- **Laptop gevallen** – Een gebruiker meldde een laptop die na een val niet meer opstartte. Met behulp van de oplader werd getracht te bepalen of het moederbord dan wel enkel het scherm defect was. Omdat fysieke reparatie ter plaatse niet mogelijk was, werd de gebruiker doorverwezen.
- **NAS-verbinding verbroken door opgeslagen oude credentials** – De stagementor kon plots niet meer bij de opslag. De oorzaak bleken verouderde, in de Windows Credential Manager opgeslagen aanmeldgegevens te zijn. Na het wissen ervan was de verbinding hersteld.
- **Retourlaptops: onvoldoende rechten** – De voor Remarkt klaargezette lokale accounts bleken geen administratorrechten te hebben. In overleg werd besloten de betreffende laptops te formatteren naar een standaard Windows-installatie, wat meteen een schone oplossing bood.
- **Azure AD-accounts van inlogscherm verwijderen** – Op een gedeelde laptop bleven oude Azure AD-gebruikers zichtbaar op het inlogscherm. Lokale methodes (register, PowerShell, groepsbeleid) konden enkel het profiel wissen, niet het account. Afdoende verwijdering bleek enkel mogelijk via centraal beleid (Entra ID / Intune).
- **Toetsenbord valt kortstondig uit** – Tijdens het oplossen van een ander probleem stopte het interne toetsenbord even met werken. Een herstart verhielp dit; de precieze oorzaak werd niet achterhaald.
- **Trage laptop door dockingstation** – Een laptop functioneerde uitzonderlijk traag (CPU 95 %) en liep herhaaldelijk vast. De doorbraak kwam toen tijdens een vastgelopen herstart de dockkabel werd ontkoppeld: het systeem startte meteen weer vlot en bleef stabiel. De oorzaak werd herleid naar de firmware van het Dell-dockingstation.
- **Defecte laptops voorzien van lokale admin voor retour** – Op twee defecte laptops moest een lokaal administratoraccount worden aangemaakt zodat ze correct geretourneerd konden worden. Via compmgmt.msc en een tijdelijke verlaging van de minimale wachtwoordlengte lukte dit alsnog.
- **PDF-/DOCX-bestand opent niet** – Bij het openen van een DOCX-/PDF-bestand verscheen een pop-up die enkel ‘Read-Only’ toestond, wat niet werkte. Het bestand werd uiteindelijk met Google Chrome geopend, waardoor de inhoud zonder problemen zichtbaar was.
- **Aanmelden met authenticator-app lukt niet** – De optie om met de authenticator-app in te loggen verscheen niet op het aanmeldscherm. Nadat de gebruiker opnieuw inlogde in de app en de laptop herstartte via een persoonlijke hotspot, verscheen de optie alsnog en kon correct worden ingelogd.
- **USB-C oplaadpoort defect** – De bovenste USB-C-poort van een laptop bleek geen stroom door te geven; opladen lukte enkel via de onderste poort. De gebruiker werd hiervan op de hoogte gebracht.
- **Afdrukprobleem vanuit Chrome** – Bij het printen vanuit Chrome werden de randen van het document afgesneden. In de printinstellingen werd de optie ‘Aanpassen aan afdrukgebied’ ingeschakeld, waarna het volledige document correct werd afgedrukt.
- **Dataoverdracht telefoon naar NAS** – Een gebruiker wilde foto’s van een smartphone naar de NAS overzetten, maar beschikte enkel over oplaadkabels. Na zoeken werd alsnog de originele USB-datakabel gevonden, waarmee de overdracht rechtstreeks en veilig kon plaatsvinden.
- **Telefoon zonder IP-adres na switch-migratie** – Een Yealink-telefoon kreeg geen IP, ook niet na factory reset. Oorzaak: de switch gaf een voice-VLAN (35) dat tevens het native VLAN was, waardoor getagd verkeer werd geweigerd. Oplossing: voice-VLAN leeg laten, zodat de telefoon ongetagd in VLAN 35 werkte.
- **Phishingcampagne als awareness-tool** – Er werd een realistische phishingmail opgesteld (extern adres, bedrijfslogo) met een link naar een Netlify-landingspagina die bezoeken logde. Na uitrol via een gesegmenteerde mailinglijst klikten 13+ medewerkers op de link – een duidelijke aanwijzing dat interne mails minder wantrouwig worden bekeken. De resultaten zijn gebruikt in de lessen.
- **Intune-deploy van printerscan mislukt (INVALID_FUNCTION)** – De Win32-app gaf fout 0x87D1041C of bleef hangen op “0 installaties”. Oorzaak: detectiescript dat niet werkte met .url-bestanden. Oplossing: overgeschakeld naar .lnk-bestanden die rechtstreeks chrome.exe aanroepen, met een marker-file als detectie.

- **Oude NAS als back-up ingericht (QNAP)** – Een tweede NAS werd operationeel gemaakt met een gereset admin-wachtwoord. Via rsync (Hybrid Back-up Sync) werd een dagelijkse/weekelijkse back-up van de Synology naar de QNAP gezet. Hardening: ongebruikte services (NFS, WebDAV, AFP, Telnet, SSH) uitgezet, UPnP uit. Leermoment: eerst stabiliteit aantonen, dan pas extra isolatie (VLAN, ACL's).
- **Mac-gebruiker: leeg bureaublad en documenten** – De gebruiker was met een verkeerd iCloud-account ingelogd, waardoor lokale mappen niet zichtbaar waren. Via Automator en terminal werden de scripts en snelkoppelingen teruggezet en de juiste iCloud-synchronisatie hersteld.
- **Mac: Outlook-zoekfunctie werkte niet** – Automatische zoek naar ontvangers en emoji-reacties faalden. Een eenvoudige herstart van het systeem loste het probleem op; oorzaak onbekend.
- **Foxit proefperiode op Mac verlopen, geen definitieve oplossing** – De proefversie van Foxit PDF Editor kon niet worden verlengd omdat het ondertekeningsprobleem met eID bleef bestaan (certificaat niet herkend). Screenshots naar Foxit support gestuurd; binnen stageperiode niet opgelost.
- **Laptop extreem traag (95% CPU) door Dell-dockingstation** – Appmodel-proces en Background Task Host veroorzaakten vastlopers. Na loskoppelen van de dock startte de laptop vlot door en bleef stabiel. Conclusie: firmwarefout in het dock.
- **Azure AD-account niet van inlogscherm te verwijderen** – Op een gedeelde laptop bleef een oud AzureAD-account zichtbaar. Lokale methodes (register, PowerShell, groepsbeleid) kunnen enkel het profiel wissen, niet het account. Enige oplossing: centraal via Intune / Entra ID (Deny local logon-beleid).
- **GenoPro werkte niet op laptop** – Er stonden twee versies (Beta en oud). Beide verwijderd, synchronisatie via Bedrijfsportaal, waarna de juiste package correct werkte.
- **USB-C poort defect (opladen onmogelijk)** – De bovenste USB-C poort van een laptop gaf geen stroom meer. De onderste werkte wel. Gebruiker geïnformeerd en geadviseerd enkel de onderste poort te gebruiken.
- **Printen vanuit Chrome sneed randen af** – Oplossing: in de printinstellingen van Chrome "Aanpassen aan afdrukgebied" inschakelen.
- **Bitwarden** – Volledig stappenplan voor Bitwarden in browser, op pc, op telefoon met Bitwarden authenticator opgesteld en afgeleverd.
- **Meeting volgen en noteren** – Heb een meeting meegedaan rond digitalisering, heb actief deelgenomen waar het kon in het gesprek, heb notities genomen en deze afgeleverd aan mijn stagementor

4. Besluit

Terugkijkend op de afgelopen stageperiode kan gesteld worden dat alle vooropgestelde doelstellingen uit het projectplan succesvol zijn gerealiseerd.

De NAS-oplossing is van een concept uitgegroeid tot een robuust, gebruiksvriendelijk en centraal beheerd script dat via Intune op alle werkplekken is uitgerold. De gegeven demonstraties stellen gebruikers in staat om zelfstandig eventuele problemen op te lossen, wat de druk op de IT-support naar verwachting significant zal verlagen.

De MacBook-configuratie werd ondanks technische uitdagingen met succes afgerond. De gebruiker beschikt nu over een volledig functionele werkplek met twee externe beeldschermen. Blijvende ondersteuning voor PDF-ondertekening blijft een aandachtspunt.

De netwerkrenovatie is goed gevorderd. De Meraki-configuratie is via een herbruikbaar Python-script uitgewerkt en in productie gebracht. Twee switches zijn fysiek vervangen en het extra accesspoint is operationeel. De overige switches zijn volledig voorbereid.

De ingevoerde Locked Print-functionaliteit en de bureaubladsnelkoppelingen naar de scans dragen bij aan een vlottere en veiligere afdrukervaring. Het uitgewerkte wachtwoordbeleid, het Vaultwarden-voorstel en de voorbereide phishingcampagne bieden een stevige basis om het beheer van inloggegevens en de algemene security-awareness binnen de organisatie naar een hoger niveau te tillen.

De stage was bijzonder leerzaam. De combinatie van projectmatig werk en het oplossen van uiteenlopende helpdeskproblemen gaf een realistisch beeld van het brede takenpakket van een IT-professional in een KMO-omgeving. De feedback van de stagebegeleider om proactiever te communiceren over de dagelijkse voortgang en een duidelijk plan van aanpak te hebben alvorens te starten, is een waardevol leermoment dat zal meegenomen worden voor de toekomst.

Als aanbeveling voor de toekomst wordt meegeven dat de implementatie van Vaultwarden een relatief kleine inspanning vergt die een grote impact kan hebben op de algehele informatiebeveiliging. Daarnaast is het aan te raden om de Meraki-configuratie periodiek te herzien en ongebruikte poorten standaard uit te schakelen, conform de best practices die tijdens de voorbereiding zijn toegepast.

5. Verklarende woordenlijst

Term	Uitleg
API	Application Programming Interface: zorgt voor communicatie tussen programma's
Argon2id	Algoritme voor veilig hashen
Azure AD / Entra ID	Microsoft-clouddienst voor identiteitsbeheer
Credential Manager	Slaat inloggegevens versleuteld op in Windows
CSV	Comma-Separated Values: bestandsformaat voor opslag van tabellen
DisplayLink	Technologie voor beeldschermen aan te sluiten via USB
Docker	Software om containers te draaien
eID	Belgische elektronische identiteitskaart
Fail2Ban	Tool voor het blokkeren van IP-adressen na een verkeerde inlogpoging
GUI	Graphical User Interface: grafische gebruikersomgeving
HTTPS	Hypertext Transfer Protocol Secure: protocol voor veilige webcommunicatie
Intune	Microsoft-cloudservice voor centraal beheer
LAG / LACP	Bundelen van netwerkpoorten
Locked print	Instelling die zorgt dat pincode nodig is voor te printen
MFA	Multifactor authenticatie: inloggen met verificatiemethode
NAS	Network Attached Storage: een bestandsserver in het netwerk
PowerShell	Microsoft-scriptlanguage
SMB	Server Message Block: protocol voor bestandsdeling
TOTP	Time-based One-Time Password: code die om de 30 seconden verandert.
VBScript	Visual Basic Scripting Edition: Microsoft scripttaal
VLAN	Virtual Local Area Network: gescheiden netwerk binnen een fysiek netwerk
VPN	Virtual Private Network: veilige verbinding over publiek netwerk
Win32	Windows 32-bit: architectuur voor programma's op Windows

6. Bibliografie

Amazon, A. (2026, februari 24). *AWS Documentation*. Opgehaald van docs aws amazon: https://docs.aws.amazon.com/

AWS. (2026, februari 24). *AWS Pricing Calculator*. Opgehaald van calculator aws: https://calculator.aws/#/

backblaze. (2026, februari 24). *Backblaze Documentation*. Opgehaald van backblaze: https://www.backblaze.com/docs

Displaylink. (2026, maart 10). *Support & Knowledge Base*. Opgehaald van Displaylink Support: https://support.displaylink.com/

García, D. (2026, april 1). *vaultwarden*. Opgehaald van github.com: https://github.com/dani-garcia/vaultwarden

Meraki, C. (2026, maart 15). *MS - Switches*. Opgehaald van documentation meraki: https://documentation.meraki.com/Switching/MS_-_Switches

Microsoft. (2026, maart 28). *Microsoft Intune documentation*. Opgehaald van learn microsoft: https://learn.microsoft.com/en-us/intune/

Microsoft. (2026, februari 25). *Net use*. Opgehaald van learn microsoft: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/gg651155(v=ws.11)

Microsoft. (2026, maart 3). *New-PSDrive*. Opgehaald van learn microsoft: https://learn.microsoft.com/nl-nl/powershell/module/microsoft.powershell.management/new-psdrive?view=powershell-7.6

Ricoh. (2026, april 2). *Support & Downloads*. Opgehaald van ricoh: https://www.ricoh.com/support

Save, C. a. (2026, februari 26). *HP Printer Firmware Downgrade Guide*. Opgehaald van compandsave: https://www.compandsave.com/hp-printer-firmware-downgrade?srsltid=AfmBOoq9fRdg7tgZXIlvYeGSkac38EMjZSyacV7atOuW3MAQbeNs6h1S

Software, F. (2026, maart 20). *Foxit Resource Hub*. Opgehaald van Foxit: https://www.foxit.com/resource-hub/

Synology. (2026, februari 25). *NAS & SAN*. Opgehaald van synology: https://kb.synology.com/en-global/DSM

Bijlagen

Netlify website