Afstudeerscriptie

PCI Nederland

Onderzoek life cycle management van gebruikersaccounts

All to keep **you** going

Project naam:	Onderzoek gebruikers life cycle management
Auteur:	Jorick Benjamins
Studentnummer:	453565
E-mailadres:	453565@student.saxion.nl / Jorick.Benjamins@pci-it.nl
Onderwijsinstelling:	Hogeschool Saxion te Deventer
Opleiding:	Information Technology & Service Management (ITSM)
Opdrachtgever:	PCI Nederland
Bedrijfsbegeleider:	David Krabbenborg
Begeleider Saxion:	Erik van der Arend
Datum:	16 januari 2022
Document nummer:	1.0

Voorwoord

Mijn naam is Jorick Benjamins en momenteel volg ik de opleiding HBO-ICT bij Hogeschool Saxion te Deventer. Ik heb het uitstroom profiel Information Technology & Service Management (ITSM) gekozen. Op 1 september 2021 ben ik begonnen aan mijn afstudeertraject bij PCI IT. Voor u ligt mijn afstudeerscriptie waarin ik onderzoek doe naar de life cycle management van gebruikersaccounts.

Het schrijven van deze afstudeerscriptie heb ik als enorm leerzaam ervaren. PCI IT heeft in samenspraak op korte termijn een mooie afstudeeropdracht kunnen realiseren en deze heb ik met beide handen aangepakt.

De scriptie is geschreven voor PCI IT om advies te geven hoe accounts uit verschillende applicatielandschappen op één plek beheert kunnen worden en de life cycle management van gebruikersaccounts efficiënter ingericht kan worden. Naast dat de scriptie geschreven is voor PCI IT is de scriptie geschreven voor de afstudeerbegeleider van het Saxion, namelijk Erik van der Arend. Naast de directe doelgroep is deze scriptie publiekelijk toegankelijk en voor eenieder die geïnteresseerd is naar het verloop van mijn afstudeerperiode bij PCI IT.

Via deze weg wil ik mijn afstudeerbegeleider David Krabbenborg bedanken voor de begeleiding tijdens mijn afstudeerperiode.

Ook wil ik mijn afstudeerbegeleider van het Saxion, Erik van der Arend bedanken voor zijn inzet tijdens de afstudeerperiode.

Tot slot wil ik Eva-Linde Kool, Lydia Eilander en Sandra Roording bedanken voor het sparren en kritisch beoordelen van mijn scriptie.

Jorick Benjamins
Vorden, 16 januari 2022.

Versiegeschiedenis

In onderstaande tabel zijn de gemaakte wijzigingen in dit document opgenomen.

Status	Datum	Veranderingen	Auteurs
Concept	3-11-2021	Opzet Scriptie document	Jorick Benjamins
Concept	4-11-2021	Indeling hoofdstukken	Jorick Benjamins
Concept	5-11-2021	Achtergrond en Deelvraag 1	Jorick Benjamins
Concept	12-11-2021	Deelvraag 2	Jorick Benjamins
Concept	19-11-2021	Deelvraag 3	Jorick Benjamins
Concept	26-11-2021	Deelvraag 4	Jorick Benjamins
Concept	6-12-2021	6 W-vragen en Context analyse	Jorick Benjamins
Concept	9-12-2021	Deelvraag 5	Jorick Benjamins
Concept	12-12-2021	Deelvraag 6	Jorick Benjamins
Concept	13-12-2021	Theoretisch kader, deelvragen	Jorick Benjamins
Concept	16-12-2021	Deelvraag 7	Jorick Benjamins
Concept	17-12-2021	Voorwoord en Conclusie	Jorick Benjamins
Concept	4-1-2022	Aanpak en methoden	Jorick Benjamins
Concept	7-1-2022	Ontwerp	Jorick Benjamins
Concept	11-1-2022	Conclusie en Ontwerp	Jorick Benjamins
Concept	15-1-2022	Managementsamenvatting	Jorick Benjamins

Tabel 1 Versie beheer

Distributielijst

In de tabel hieronder worden de distributies van dit document bijgehouden.

Naam	Rol	Datum	Versie
David Krabbenborg, Erik van der Arend	Bedrijfsbegeleider, begeleider Saxion	3-11-2021	0.1
David Krabbenborg, Erik van der Arend	Bedrijfsbegeleider, begeleider Saxion	26-11-2021	0.2
David Krabbenborg, Erik van der Arend	Bedrijfsbegeleider, begeleider Saxion	6-12-2021	0.3
David Krabbenborg	Bedrijfsbegeleider	17-12-2021	0.5
Erik van der Arend	Begeleider Saxion	19-12-2021	0.5
Erik van der Arend, David Krabbenborg	Begeleider Saxion, bedrijfsbegeleider	16-1-2021	1.0

Tabel 2 Distributie beheer

Managementsamenvatting

Door de versplintering van het applicatielandschap naar de clouddiensten, zoals SaaS, IaaS of andere hosting oplossingen zijn er ook meer accounts om te beheren. Deze accounts sluiten niet altijd aan op de gewenste provisioning en daardoor ontstaan verschillende accounts waar geen overzicht en beheer over is.
Vanuit PCI IT rijst de vraag of het mogelijk is om de life cycle van gebruikersaccounts in verschillende applicatielandschappen op één plek kan beheren en deze oplossing aan te bieden als dienst voor haar klanten. In samenspraak met David Krabbenborg, de opdrachtgever vanuit PCI IT, is een opdracht gedefinieerd gerelateerd aan de life cycle management van gebruikersaccounts.
Het project is gefocust op het onderzoeken van een passende oplossing om de life cycle van gebruikersaccounts in verschillende applicatielandschappen beter te kunnen beheren. Hier komen diverse zaken bij kijken, zoals de huidige situatie van het aanvragen-, wijzigen- en opheffen van een gebruikersaccount bij zowel PCI IT intern als een voorbeeldklant.
Naast het probleem van de versplintering van de gebruikersaccounts bij cloudapplicaties, zijn interne medewerkers veel tijd kwijt aan het aanvragen, aanmaken, administreren en opzeggen van gebruikersaccounts. Het vinden van een geautomatiseerde oplossing voor bovenstaande problemen zou veel tijd besparen en helpen om deze processen efficiënter in te richten.
Tot slot kunnen applicaties als HRM- en CRM-pakketten vaak niet aan elkaar worden gekoppeld, waardoor er geen informatie uitgewisseld kan worden. Het zou een mooie oplossing zijn als informatie tussen verschillende applicaties te synchroniseren zijn, zodat werkprocessen geautomatiseerd kunnen worden.

Om tot een passende oplossing te komen voor PCI IT is er gekeken naar de huidige situatie van de life cycle van gebruikersaccounts. Hierin is naar voren gekomen dat de processen handmatig uitgevoerd worden en hierdoor een lange doorlooptijd hebben.
De wens vanuit PCI IT is om de life cycle van gebruikersaccounts in verschillende omgeving op één plek te beheren, waardoor onderhoud eenvoudiger wordt. PCI IT wil deze oplossing inzetten als MSP waardoor het mogelijk dient te zijn om meerdere klanten te koppelen aan het systeem. Om de life cycle van gebruikersaccounts minder foutgevoelig en efficiënter in te richten, is gekeken naar de mogelijkheid om processen te automatiseren. Daarnaast is er gekeken naar de mogelijkheid om producten en diensten te koppelen aan een Self-service portaal. De wens is om eindgebruikers zelf producten en diensten aan te laten vragen. Op deze wijze kunnen de aanvragen direct worden aangemaakt en automatische doorgang vinden. Hierdoor is het proces minder foutgevoelig en efficiënter.
Met al deze wensen is er gekeken naar een passende oplossing voor PCI IT. Door gebruik te maken van een Multicriteria-analyse is het softwarepakket HelloID gekozen als beste oplossing. HelloID heeft drie verschillende modules die alle eisen en wensen mogelijk maken.
De module Provisioning is met 4,5 werkdag te implementeren waarmee er een koppeling beschikbaar wordt gemaakt tussen de HR-applicatie en de Active Directory. Hiermee kunnen personen uit de HR-applicatie worden gekoppeld aan de gebruikersaccounts van de Active Directory.
Voor de implementatie is kennis benodigd voor HelloID, de koppelingen die gemaakt moeten worden en het dagelijks beheer. De kennis kan op worden gedaan door gratis cursussen te volgend van Tools4ever, de softwareleverancier van HelloID.
De prijs voor alle drie de modules op basis van 500 gebruikers is €3,56 per gebruiker per maand.

Inhoud

Figurenlijst

Tabellenlijst

Begrippenlijst

SaaS	=	Software as a Service
IaaS	=	Infrastructure as a Service
IAM	=	Identity Access Management
PAM	=	Priviliged Access Management
MSP	=	Managed Service Provider
AD	=	Active Directory
AAD	=	Azure Active Directory
ADFS	=	Active Directory Federation Service
SSO	=	Single Sign On
B2B2C	=	Business to Business to Consumer
B2B2E	=	Business to Business to Everyone
OOB	=	Out-of-the-box

1. Inleiding

Sinds het werken in de cloud populairder wordt, is er een trend gaande waar steeds meer bedrijven gebruik maken van applicaties die via het web te benaderen zijn. Hierdoor vindt er een versplintering plaats van het applicatielandschap naar verschillende omgevingen. Door deze versplintering zijn er ook meer accounts te beheren. Zo ook bij PCI IT en haar klanten. In deze afstudeerscriptie wordt er onderzocht hoe PCI IT de lifecycle management van gebruikersaccounts in verschillende omgevingen op een eenvoudigere en minder foutgevoelige wijze kan beheren.

Het doel voor deze afstudeerscriptie is om voor PCI IT een advies te geven op welke wijze zij op één plek de verschillende gebruikersaccounts kunnen beheren, waardoor onderhoud eenvoudiger wordt. PCI IT wil deze oplossing inzetten als MSP waardoor het mogelijk is om meerdere klanten te koppelen aan het systeem.

De afstudeerscriptie is gebaseerd op een onderzoek bestaande uit een hoofdvraag en 7 deelvragen. De hoofd- en deelvragen geven structuur aan het onderzoek en bepalen de scope van het onderzoek. Voor een gedetailleerde beschrijven van de onderzoek aanpak zie 3 Aanpak en methoden.

In het onderzoek is een duidelijke structuur gehanteerd, eerst wordt de afstudeerorganisatie en de opdracht definitie beschreven. Vervolgens worden de aanpak en methodes beschreven, hierbij wordt een overzicht voor alle deelvragen gecreëerd. Iedere deelvraag wordt behandeld in een eigen hoofdstuk, de structuur van deze hoofdstukken zijn onderverdeeld in proces, resultaat en eventueel een conclusie. Na alle resultaten van de deelvraag behandeld te hebben wordt er antwoord gegeven op de hoofdvraag door middel van een conclusie en aanbevelingen.

2. Achtergrond

2.1 Achtergrond PCI IT

In 1969 is de holding 'Huis van Leferink' de organisatie is destijds begonnen met het verkopen van typemachines. Hoewel de verkoop goed ging werd er gekeken naar de vraag in de markt en is besloten meer diensten aan te bieden. Vervolgens is de verkoop van kantoormeubilair en andere kantooraccessoires ook van start gegaan. Momenteel is Leferink nog steeds actief onder de naam Leferink Office Works voor het verkopen van kantoorartikelen.
Daarnaast is er een BV opgericht voor het leveren van IT-diensten, Leferink IT. Later is de naam veranderd naar ICT Spirit. ICT Spirit was een IT-dienstverlener op verschillende gebieden: bouwen, onderhouden en verbouwen van ICT-infrastructuren. Daarnaast worden er ook diensten aangeboden als: hosting, beveiliging en cloudoplossingen, ook wordt er veel aan consultancy gedaan.
Ongeveer 2 jaar geleden heeft de oud-eigenaar, Mark Leferink, aangegeven niet langer over de kennis te beschikken om ICT Spirit verder te laten groeien. Hierdoor heeft hij doen besluiten om ICT Spirit en Office Works te verkopen.

PCI Nederland heeft de afgelopen jaren al meerdere IT-partijen overgenomen en had veel interesse om ICT Spirit over te nemen. Een voorwaarde van Mark Leferink voor de overname was dat ICT Spirit een eigen organisatie zou worden binnen PCI Nederland. Daar is de naam PCI IT uit voortgekomen. Door deze overname is zowel het klantenbestand als het personeelbestand van PCI IT enorm gegroeid. Hoewel er meer personeel en kennis beschikbaar is na de overname groeit het klantenbestand in dezelfde stijgende lijn. Hierdoor is er nog steeds veel vraag naar nieuwe medewerkers binnen PCI IT.

2.2 Organisatie

PCI IT is een IT-dienstverlener die haar klanten ontzorgt op IT-gebied. Naast het projectbureau en service biedt PCI IT ook een steeds completer scala aan Managed Service Provider (MSP) oplossingen aan. PCI Nederland beschikt over ongeveer 550 FTE aan medewerkers waarvan er ongeveer 150 op de IT-afdeling werken. Momenteel beschikt PCI Nederland over twee locaties: hoofdkantoor Haaksbergen en locatie Lijnden. Daarnaast hebben ze nog op verschillende plekken in Nederland een datacenter: in Haaksbergen, Hengelo en Amsterdam.

Diensten/ producten

De diensten van PCI IT zijn op te splitsen in twee dienstencatalogussen, namelijk As a Service en Managed Security Services.

De diensten die PCI IT als As a Service aanbiedt:

- Monitoring as a Service (Maas)
- Infrastructure As A Service (IAAS)
- FG-as-a-Service (FaaS)
- Networking as a Service (NaaS)
- Device as a Service (DaaS)

De diensten die PCI IT als Managed Security Services aanbiedt:

- Managed O365 Backup
- Veaam cloud Connect Back-up
- Managed cloud Backup
- Managed Endpoint Detection & Response (EDR)
- Managed Cyber Alarm
- Managed Firewall
- Managed Security Awareness
- Managed Unified Endpoint
- Managed Patch management
- Managed Mail Security

2.3 Probleemstelling

In samenspraak met David Krabbenborg, de opdrachtgever vanuit PCI Nederland, is een opdracht gedefinieerd gerelateerd aan de life cycle management van gebruikersaccounts. Door de versplintering van het applicatielandschap naar de clouddiensten, zoals SaaS, IaaS of andere hosting oplossingen zijn er ook meer accounts om te beheren. Deze accounts sluiten niet altijd aan op de gewenste provisioning en daarom ontstaan er verschillende accounts waar geen overzicht en beheer over is.

De vraag vanuit PCI IT is of het mogelijk is om de life cycle van gebruikersaccounts in verschillende applicatielandschappen op één plek kan beheren en deze oplossing aan te bieden als dienst voor haar klanten.

Het project is gefocust op het onderzoeken van een passende oplossing om de life cycle van gebruikersaccounts in verschillende applicatielandschappen beter te kunnen beheren. Hier komen diverse zaken bij kijken, zoals de huidige situatie van het aanvragen-, wijzigen- en opheffen van een gebruikersaccount bij zowel PCI IT intern als een voorbeeldklant. S

Naast het probleem van de versplintering van de gebruikersaccounts bij cloudapplicaties, zijn interne medewerkers veel tijd kwijt aan het aanvragen, aanmaken, administreren en opzeggen van gebruikersaccounts. Het vinden van een geautomatiseerde oplossing voor bovenstaande problemen zou veel tijd besparen en helpen om deze processen efficiënter in te richten.

Tot slot kunnen applicaties als HRM- en CRM-pakketten vaak niet aan elkaar worden gekoppeld, waardoor er geen informatie uitgewisseld kan worden. Het zou een mooie oplossing zijn als informatie tussen verschillende applicaties te synchroniseren zijn, zodat werkprocessen geautomatiseerd kunnen worden.

Om het onderzoek structuur te geven zijn hoofd- en deelvragen samengesteld. Onderstaand is de hoofdvraag dikgedrukt weergegeven opvolgend door de deelvragen. Voor meer informatie over de aanpak zie hoofdstuk 3 Aanpak en methoden.

In hoeverre kan PCI IT de life cycle van gebruikersaccounts in omgevingen die bestaan uit een mix van Saas, Paas, IaaS, private cloud en on-premise op een eenvoudigere en minder foutgevoelige wijze beheren en aanbieden aan haar klanten?

1. Op welke wijze worden de gebruikersaccount in de huidige situatie aangemaakt en aangevraagd?
2. Welke mogelijkheden zijn er om in een hybride omgeving gebruikersaccounts gecentraliseerd te beheren?
3. Aan welke wensen en eisen dient een eventueel softwarepakket te voldoen?
4. Welke oplossing past het beste bij de eisen en wensen van PCI IT als MSP?
5. Hoe valt een dergelijke dienst als MSP in te zetten?
6. Hoe zou de implementatie van een dergelijk product in het dienstportfolio en dienstmanagement (dagelijks beheer) bij PCI IT eruitzien?
7. Op welke manier kan PCI IT de life cycle managementoplossing het beste inzetten als self-service oplossing voor de klanten van PCI IT?

2.4 Business requirements

In onderstaande tabel zijn de business requirements weergegeven. Hier is gebruik gemaakt van de methodiek MoSCoW**Fout! Verwijzingsbron niet gevonden.**, uitgelegd in paragraaf 3.7 REF _Ref92462649 \h Requirementsanalyse.

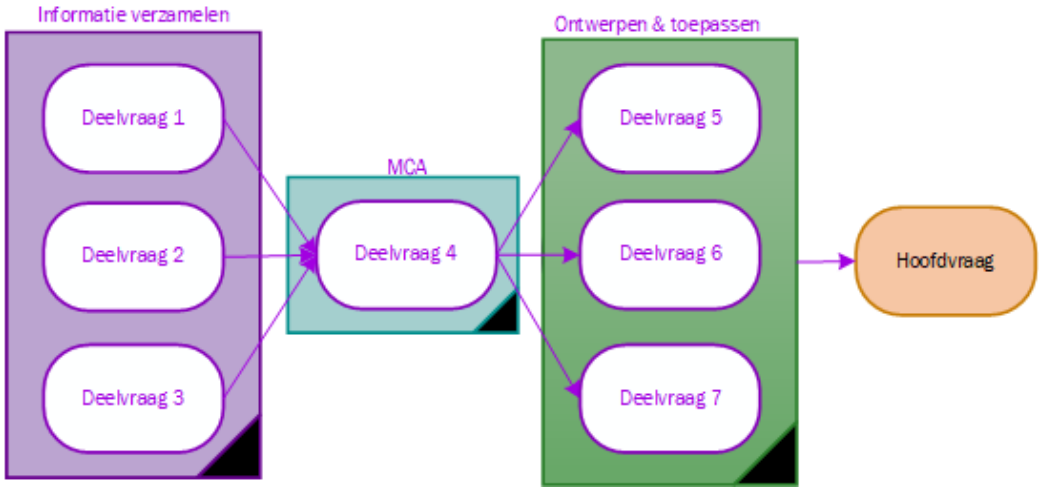
B-ID	Requirement	Prioriteit
B-01	Het product dient ingezet te kunnen worden in zowel on-premise als alle cloud omgevingen	Must
B-02	Gehele life cycle van gebruikersaccounts op een eenvoudigere wijze beheren	Must
B-03	Gehele life cycle van gebruikersaccounts op een minder foutgevoelige manier beheren	Must
B-04	Het product dient te voldoen aan de AVG eisen	Must
B-05	De nieuwe omgeving moet enkel gebaseerd worden op Microsoft Active Directory	Must
B-06	Het product dient als MSP ingezet te kunnen worden	Could
B-07	Het product dient de mogelijkheid te hebben om te betalen per gebruik	Would

Tabel 3 Business requirements

3. Aanpak en methoden

De onderzoeksaanpak is gestructureerd door middel van hoofd- en deelvragen. Er is hier voor gekozen, omdat de deelvragen voortkomen uit de opdrachtdefinitie van de opdrachtgever. De deelvragen zijn gestructureerd op een manier waarmee de antwoorden van de deelvragen de hoofdvraag beantwoorden. De deelvragen zijn op te delen in drie categorieën: informatie verzamelen, MCA en ontwerpen & toepassen.

De informatie voor het onderzoek is verkregen in deelvraag één tot en met drie (afgebeeld in de paarse kolom in Figuur 1 Diagram hoofd- en deelvragen). De deelvraag vier (afgebeeld in de blauwe kolom in Figuur 1 Diagram hoofd- en deelvragen) is bedoeld voor de multicriteria-analyse (MCA). Om deze MCA uit te voeren wordt de informatie uit deelvragen één tot en met drie gebruikt. Deelvragen vijf, zes en zeven volgen elkaar op (afgebeeld in de groene kolom in Figuur 1 Diagram hoofd- en deelvragen). De deelvragen zijn onderdelen van het systeem dat wordt ontworpen in hoofdstuk 14 Ontwerp. Daarnaast wordt er gekeken hoe het systeem toepasbaar is binnen de omgeving van PCI IT en haar klanten. Alle resultaten tezamen vormen een passend antwoord op de hoofdvraag.



Figuur 1 Diagram hoofd- en deelvragen

Per deelvraag zijn er verschillende methodieken gebruikt om tot een valide antwoord te komen. In Tabel 4 Methodieken/ Technieken per deelvraag zijn alle methodes, resultaten en fasen beschreven die worden gebruikt voor elke deelvraag. Iedere deelvraag is opgebouwd aan de hand van een vaste structuur. Deze structuur beschrijft eerst de gebruikte methodieken, welke informatie gebruikt is en waar deze informatie vandaan komt om het eindresultaat te creëren. Daarna worden de resultaten van de methodes weergegeven en waar nodig worden deze aangevuld met een conclusie. Tot slot worden de fases weergegeven, wat de fases inhouden wordt uitgelegd in paragraaf 3.1 Design thinking.

#	Deelvraag	Methodieken/ Technieken	Resultaten	Fase
1	Op welke wijze worden de gebruikersaccount in de huidige situatie aangemaakt en aangevraagd?	Bureauonderzoek; Interviews; UML-diagram	Analyse huidige processen; Knelpunten	Empathize
2	Welke mogelijkheden zijn er om in een hybride omgeving gebruikersaccounts gecentraliseerd te beheren?	Bureauonderzoek; Literatuurstudie	Literatuuronderzoek	Empathize, Define
3	Aan welke wensen en eisen dient een eventueel softwarepakket te voldoen?	Interviews; Brainstormsessie; Requirements analyse	Knelpunten; User stories; Requirements	Define
4	Welke oplossing past het beste bij de eisen en wensen van PCI IT als MSP?	Literatuurstudie; Multicriteri analyse	Multicriteri analyse	Ideate
5	Hoe valt een dergelijke dienst als MSP in te zetten?	Brainstormsessie; Interview	Literatuuronderzoek	Ideate, Prototype
6	Hoe zou de implementatie van een dergelijk product in het dienstportfolio en dienstmanagement (dagelijks beheer) bij PCI IT eruitzien?	Brainstormsessie; Interview; Literatuurstudie	Literatuuronderzoek	Ideate, Prototype
7	Op welke manier kan PCI IT de life cycle managementoplossing het beste inzetten als self-service oplossing voor de klanten van PCI IT?	Brainstormsessie; Literatuurstudie	Advies; Ontwerp	Ideate, Prototype

Tabel 4 Methodieken/ Technieken per deelvraag

3.1 Design thinking

Bij Design Thinking draait het om het begrijpen van de mensen voor wie een product of dienst ontwikkeld wordt. Design Thinking is een manier van zowel denken en werken, als een verzameling van methodes die stimuleren nieuwe alternatieven te onderzoeken om zo tot een betere oplossing te komen (Wat is Design Thinking?, 2021). Design Thinking is opgedeeld in de volgende 5 fases:

- Empathize, inleven in de gebruikers.
- Define, definiëren van het probleem.
- Ideate, meerdere mogelijke oplossingen voorleggen.
- Prototype, in deze fase wordt een ontwerp gemaakt voor de oplossing.
- Test, controleren of het voldoet aan de gestelde eisen.

In dit project wordt er geen prototype gemaakt waardoor er geen testen uitgevoerd kunnen worden. In de fase ‘Prototype’ wordt er een ontwerp gemaakt. Wel wordt en in de fase ‘Prototype’ een ontwerp gemaakt. De test fase wordt in dit project niet uitgevoerd.

3.2 APA

Om opmaak en verwijzingen in onderzoeken te structureren zijn er richtlijnen gemaakt door de American Psychological Association (ook wel bekend als: APA). De richtlijnen voor APA-verwijzing zijn regels voor de opmaak en manier van uitwerken van de bronverwijzing van een onderzoek (American Psychological Association, 2021). In dit project worden deze regels gehandhaafd.

3.3 Interviews

Om de gewenste informatie te verzamelen voor dit project worden diverse interviews uitgevoerd. Deze worden gehouden om informatie te vergaren, zoals de stakeholders en belanghebbenden in

kaart te brengen, knelpunten, eisen en wensen te verzamelen of om gedachten uit te wisselen met een collega. Daarnaast worden er gesprekken gevoerd met softwareleveranciers om duidelijkheid te verkrijgen over de producten die zij aanbieden.

3.4 Bureauonderzoek

Tijdens dit project wordt er gebruik gemaakt van bureauonderzoek (Foeke van der Zee, 2021). Bij een literatuurstudie beperkt de onderzoeker zich tot hetgeen er geschreven is. Bureauonderzoek dient breder opgevat te worden en kijkt ook naar andere informatiebronnen zoals documentatie vanuit PCI IT en oriëntatie op het internet.

3.5 Stakeholderanalyse

In de stakeholdersanalyse worden de belanghebbenden en de belangen in dit project in beeld gebracht. Door dit in kaart te brengen wordt de visie op het project en wat de belanghebbenden verwachten van dit project duidelijk. De stakeholderanalyse wordt gedaan op basis van een SIPOC en stakeholdersmatrix.

3.6 6 W-vragen

Tijdens de analyse fase wordt er gebruik gemaakt van de 6 W-vragen (Fahad, 2021). De methode beantwoord de volgende W-vragen:

- ‘Wat’ is het probleem
- ‘Wie’ ervaart het probleem
- ‘Wanneer’ is het probleem ontstaan
- ‘Waarom’ is dit een probleem
- ‘Waar’ is dit een probleem
- ‘Wat’ is de aanleiding van het probleem

3.7 Requirementsanalyse

De kwaliteit van projecten laat zich vaak uitdrukken in de mate waarin wordt voldaan aan de eisen en verwachtingen van de opdrachtgevers. In dit project wordt gebruik gemaakt van een requirementsanalyse om deze eisen en wensen duidelijk in kaart te brengen (Computable, 2021). In dit onderzoek is gekozen voor de MoSCoW methode (Vliet, 2021) om prioriteiten te stellen aan de requirements. Het is een afkorting, waarvan de letters staan voor:

M – must haves: dit zijn de requirements die minimaal in het eindresultaat terug moeten komen, zonder deze eisen is het product niet bruikbaar

S – should haves: deze eisen zijn zeer gewenst, maar zonder is het product wel bruikbaar

C – could haves: deze eisen zullen aan bod komen als er tijd genoeg is, maar zijn niet noodzakelijk of erg gewenst

W – won’t haves: deze eisen zullen in dit project wellicht niet aan bod komen, maar kunnen in de toekomst of als alle bovenstaande eisen zijn voldaan behandeld worden.

De kleine letters ‘o’ hebben in deze methode geen betekenis.

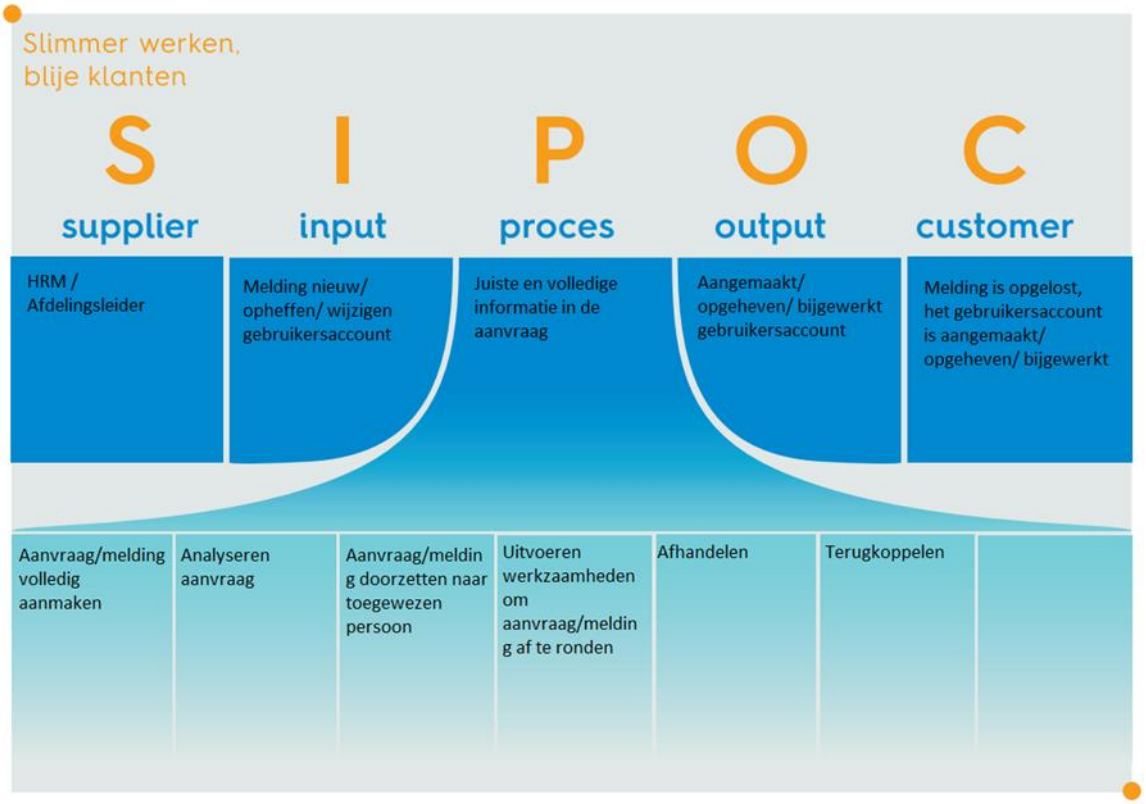
3.8 Multicriteria-analyse

Een multicriteria-analyse (MCA) (Toolshero, 2021) is een beslissingsanalyse die meerdere criteria in de besluitvorming evalueert. Binnen dit project wordt het gebruikt om een keuze te maken tussen de verschillende softwareapplicaties. Dit gebeurt door alle eisen en wensen die zijn vastgesteld in de Requirementsanalyse op rij te zetten en te vergelijken met de functionaliteiten van de softwareapplicatie.

4. Stakeholderanalyse

4.1 SIPOC

SIPOC (Bureau Tromp, 2021) is een krachtige en handige tool om een proces in kaart te brengen. Om dit proces duidelijk in kaart te brengen dienen waarden aan de SIPOC toegevoegd te worden wat uiteindelijk output aan de klant-kant oplevert. Door het gebruik van SIPOC wordt er duidelijk hoe het proces wordt gestart en wat er als output uit komt. In onderstaande figuur is de ingevulde SIPOC te zien, met als Supplier PCI IT intern.



Figuur 2 SIPOC (Bureau Tromp, 2021)

Supplier: de aanvrager van het proces is de afdeling HRM of de afdelingsmanager, dat ligt aan de vormgeving van het proces.
Input: de input kan bestaan uit 3 verschillende waarden. Namelijk een melding voor een nieuw gebruikersaccount, een gebruikersaccount opheffen of een gebruikersaccount wijzigen. Dit geldt voor zowel intern bij PCI IT of voor een klantomgeving.
Proces: in het proces gedeelte, onderste zes vlakken in Figuur 2 SIPOC, wordt het proces getoond voor een melding voor een nieuw gebruikersaccount, een gebruikersaccount opheffen of een wijziging voor een gebruikersaccount.
Output: het proces is afgerond en de output van het proces, is het aangemaakte/opgeheven of bijgewerkte gebruikersaccount door middel van het oplossen/ afronden van de aanvraag.
Customer: vervolgens vindt de terugkoppeling naar de klant plaats dat de melding is afgerond.

In bovenstaande stappen wordt bepaald hoe het proces loopt, wie erbij betrokken is en wat de output van het proces is. De volgende uitgevoerde stap is door middel van interviews bepalen wie er nog meer bij dit proces betrokken is.

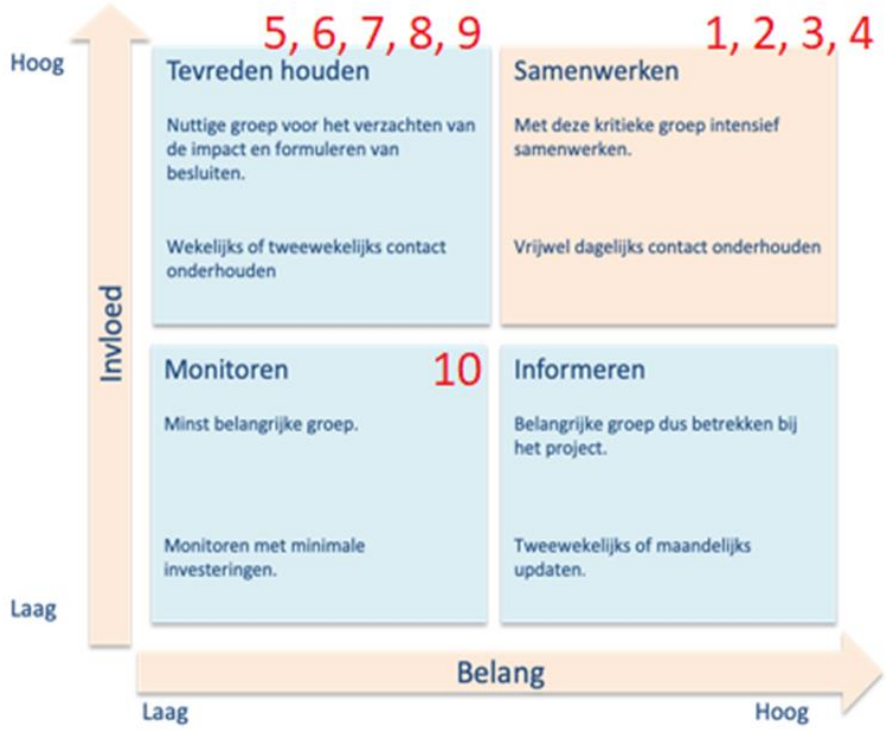
De volgende stakeholders zijn al naar voren gekomen in de SIPOC:
- Annemiek Meulenkamp – HR-functionaris
- Mitchell Kel – Medewerker ServiceDesk 2e lijn
- Sander Pot – Teamcoördinator 2e lijn
- Olaf Kornegoor - Teamcoördinator 1e lijn

Uit verschillende interviews is naar voren gekomen dat de volgende stakeholders betrokken zijn bij dit project:
- David Krabbenborg – Projectleider/ Teamcoördinator Netwerk & Security
- Bart Brevink - Technical Field Service Manager
- Roel Villerius - Security Officer
- Stephan van Hulst – Functionaris gegevensbescherming, risicomanager en kwaliteitcoördinator
- Tobias ten Brinke – 3e lijn Front-End Engineer

In het voorbeeld is de SIPOC uitgevoerd voor PCI IT intern, echter geldt ditzelfde proces voor de eindklanten van PCI IT. In dat geval doet een HR-medewerker of andere bevoegde medewerker van de eindklant de aanvraag. De input, het proces, de output en de klant zijn hetzelfde als het voorbeeld.

4.2 Stakeholdersmatrix

Na het in kaart brengen van de stakeholders is het belangrijk te bepalen welke invloed deze stakeholders hebben op het project. Om dit te bepalen is onderstaand model gebruikt, waarin de stakeholders zijn verwerkt. De getallen zijn hierin de actoren en worden onder het figuur verder uitgelegd:



Figuur 3 Impact stakeholders (Bureautromp, 2021)

1. David Krabbenborg – Teamcoördinator Netwerk & Security

David is de projectleider en heeft daarom veel invloed op het project. In overleg met hem worden de requirements besloten.

2. Bart Brevink - Technical Field Service Manager
Bart is verantwoordelijk voor het dienstenportfolio van PCI IT. Hij zou verantwoordelijk zijn voor een eventuele implementatie van het softwarepakket en is daarom belangrijk in het project.

3. Roel Villerius - Security Officer
Roel is CSO van PCI IT en is verantwoordelijk voor de beveiliging. Nieuwe producten dienen eerst goedgekeurd worden door Roel voordat ze geïmplementeerd kunnen worden. Als een nieuw product data opslaat, dient gecontroleerd te worden waar deze opgeslagen wordt in verband met de AVG-wetgeving.

4. Stephan van Hulst – Functionaris gegevensbescherming, risicomanager en kwaliteit coördinator.
Stephan is verantwoordelijk voor de gegevensbescherming van PCI IT. Stephan is verantwoordelijk voor de AVG-wetgeving en helpt meerdere bedrijven vanuit PCI IT om te voldoen aan de AVG-wetgeving.

5. Annemiek Meulenkamp – HR-functionaris
Annemiek is HR-functionaris bij PCI IT en is verantwoordelijk voor het aannemen van nieuwe medewerkers. Hierbij verzorgt ze de contracten en zorgt ze ervoor dat alles in de HR-applicatie wordt vastgelegd. Voor Annemiek geldt dat er voor het aanvragen van een gebruikersaccount veel kan gaan veranderen.

6. Aanvrager – afdelingsleider die bevoegd is om een aanvraag aan te maken.
Elke afdelingsleider kan een medewerker aandragen en een aanvraag doen voor een gebruikersaccount of wijziging. Om deze reden zijn de managers meegenomen als stakeholder.

7. Mitchell Kel – Medewerker ServiceDesk 2e lijn
Mitchell werkt op de ServiceDesk en werkt dagelijks met gebruikersaccounts. Zijn werkzaamheden bestaan onder andere uit het aanmaken, wijzigen, opheffen van gebruikersaccounts, maar ook het resetten van wachtwoorden dat volgens Olaf 25% van het werk betreft. Bij een eventuele implementatie van een softwarepakket kunnen de dagelijkse werkzaamheden van Mitchell en zijn collega's enorm veranderen. Hierdoor is Mitchell opgenomen als belangrijke stakeholder.

8. Sander Pot – Teamcoördinator 2e lijn
Sander is teamcoördinator van de ServiceDesk 2e lijn. Hij verdeelt en controleert of het werk juist uit wordt gevoerd. Voor hem verandert er indirect ook veel.

9. Olaf Kornegoor - Teamcoördinator 1e lijn
Olaf is teamcoördinator van de 1ste lijn en voor hem gaan er zaken indirect veranderen.

10. Tobias ten Brinke – 3e lijn Front-End Engineer
Tobias ten Brinke werkt op de 3e lijn als Front-End Engineer en heeft al wat ervaring met soortgelijke software. Met Tobias ten Brinke is een interview gehouden over de software. Hij is niet direct betrokken bij het project maar een 3e lijn engineer zou dit project mogelijk wel uit kunnen voeren.

5. Theoretisch kader

In de literatuurstudie komen diverse theoretische begrippen aan de orde. In deze paragraaf zijn deze begrippen uitgelegd.

SaaS

Software-as-a-Service ook wel bekend als SaaS, is een model waarbij softwaretoepassingen via internet worden aangeleverd, als een service. Hierbij zijn de licenties al geregeld. Steeds meer mensen werken graag vanaf een web-interface. Deze interfaces zijn vaak gebruikersvriendelijk en eenvoudig in gebruik. Door het Corona-virus wordt er meer thuisgewerkt waardoor er vaak voor een SaaS-oplossing vaak wordt gekozen. Bij een Saas-oplossing dient er geen hard- of software aangeschaft te worden. Er is daardoor geen onderhoud op fysieke servers. Deze kosten zijn vaak doorberekend in de kosten voor het afnemen van de applicatie (Salesforce, 2021).

IaaS

Bij Infrastructure-as-a-Service (IaaS) is de provider verantwoordelijk voor de hosting van de hardware, software, opslag en andere onderdelen van de infrastructuur. Ook hierbij geldt dat er geen fysieke servers aangeschaft hoeven te worden en er geen onderhoud is op de onderliggende virtualisatie laag.
Hierbij zijn het netwerk, de opslag, server (fysiek) en virtualisatie software bestemd voor de provider. Het operating system, de applicatie, data en dergelijke wat er vervolgens bij komt kijken is voor de afnemer (Microsoft, 2021).

PaaS

Platform-as-a-Service (PaaS) betreft, een dienst waarmee klanten een platform als een service kunnen afnemen. Een voorbeeld hiervan is een test-omgeving met Windows 11 (Microsoft, 2021).

DaaS

Desktop-as-a-Service (DaaS) staat voor het uitbesteden van de infrastructuur voor virtuele desktops aan een externe provider. Er wordt dus een dienst afgenomen voor een virtuele desktop met bepaalde resources (Citrix, 2021).

DBaaS

Bij een Database-as-a-Service (DBaaS)wordt een database online toegankelijk gemaakt, hierbij is het niet nodig om een en ander te installeren en is geen fysieke dataopslag benodigd. Dit wordt geregeld door de cloudprovider (optimadata, 2021).

Private cloud

Een aantal van bovenstaande oplossingen kunnen als Private cloud worden aangeboden, dit houdt in dat de cloud alleen voor het bedrijf beschikbaar is. Het bedrijf heeft hierdoor de mogelijkheid de cloud volledig naar eigen wens aan te passen (Microsoft, 2021)

Public cloud

Een Public cloud is een clouddienst die door iedereen afgenomen kan worden, zonder verantwoordelijkheid voor het onderhoud en de investering in hardware (KPN, 2021).

On-premises

Daarnaast is er de mogelijkheid om de servers en alle hardware zelf aan te schaffen. Dit komt vooral voor bij bedrijven die specifieke software gebruiken die nog niet naar de cloud te brengen is of veel resources nodig hebben die de oplossing in de cloud niet aantrekkelijk maken. Een voordeel van een on-premise omgeving is de mogelijkheid om de data in eigen omgeving te behouden (Dynamicsonline, 2021).

API-koppeling

Een steeds vaker voorkomend begrip is Application Programming Interface (API). Een API-koppeling is een mogelijkheid om twee of meerdere systemen te koppelen. Een API-koppeling ontwikkelen zorgt ervoor dat processen simpel en efficiënt ingericht worden.

Een organisatie gebruikt vaak meerdere applicaties zonder dat deze systemen met elkaar kunnen communiceren. Dat maakt sommige werkprocessen lastig te automatiseren of aan te passen. Daarnaast kost het overnemen van informatie of data vanuit andere pakketten tijd terwijl dit ook geautomatiseerd kan worden. Een API-koppeling kan realtime informatie doorzetten naar andere applicaties mits de applicatie API-koppelingen ondersteund (Movements, 2021).

MFA

MFA staat voor Multi-Factor Authenticatie, dit betreft een authenticatie methode waarbij de gebruiker twee stappen succesvol moet doorlopen om ergens toegang tot te krijgen. Dit soort authenticatie is ook wel bekend als Two-Factor Authenticatie (2FA) (Tools4ever, 2021).

SSO

Single sign-on (SSO) stelt eindgebruikers in staat om eenmalig in te loggen waarna automatisch toegang wordt verschaft tot meerdere applicaties en resources in het netwerk. De Nederlandse term hiervoor is eenmalig inloggen (Citrix, 2021).

Oauth 2.0

Oauth 2.0 is een veel gebruikt framework voor authenticatie. Met het gebruik van Oauth 2.0 is het mogelijk derden veilig toegang te geven tot het gebruik van bijvoorbeeld een web API en Http endpoints. Dit gebeurt dan via een toegangstoken die de derde partij (beperkt) toegang geeft tot de applicatie. Dit token bevat allerlei informatie over de aanvrager en kan dus ook rechten en claims bevatten. Vandaar de beperkte toegang (Sigma solutions, 2021).

OpenID Connect

OpenID (OIDC) is een open standaard verificatieprotocol dat gebouwd is op OAuth 2.0. OpenID Connect verzorgt verificatie voor gebruikers door een token. Met deze token zorgt OpenID Connect er voor dat systemen kunnen samenwerken om authenticatiestatus en gebruikersprofielinformatie te kunnen delen (Microsoft, 2021).

6. 6 W-vragen

Een methode die ervoor zorgt dat het probleem volledig gedefinieerd wordt, is de methode met 6W-vragen (Fahad, 2021). Met deze vragen worden verschillende aspecten van het probleem belicht.

Wat?

Het probleem binnen PCI IT is dat er steeds meer accounts ontstaan rondom verschillende applicaties die zich naar de cloud verplaatsen. Deze applicaties worden naar de cloud verplaatst om de applicatie ten alle tijden beschikbaar te stellen door middel van een SaaS-applicatie. Het nadeel aan deze transitie is dat de authenticatie vaak door de leverancier zelf wordt geregeld. Vaak sluit de provisioning van een SaaS-applicatie niet aan op de huidige infrastructuur, waardoor er een nieuw account gecreëerd dient te worden in de omgeving van de leverancier. Hierdoor verliest PCI IT grip op de verschillende accounts die zij moeten aanmaken bij een nieuwe medewerker en de daarbij horende rechten in een applicatie.

Wie?

Het probleem wordt vooral ervaren bij de security officer, aangezien deze grip verliest over de accounts en de verschillende rechten die hierin uitgedeeld worden. Echter, het probleem is niet alleen intern bij PCI IT aanwezig, maar ook bij alle klanten van PCI Nederland. Hierdoor hebben alle IT-beheerders baat bij een applicatie die hier beter inzicht in geeft, aangezien de IT-beheerders eindverantwoordelijk zijn voor de klant. Daarnaast heeft de afdeling HR baat bij een soortgelijk softwarepakket, aangezien softwareapplicaties in deze vorm (IAM/PAM) vaak samengaan met het automatiseren van werkprocessen. Hierin worden de aanvragen voor gebruikersaccounts vaak geautomatiseerd en is er minder tussenkomst van zowel HR als de IT-beheerder benodigd.

Wanneer?

Het probleem wordt vooral ervaren bij de security officer, aangezien deze grip verliest over de de SaaS-applicaties. In het beginstadium van de cloud was vooral de servers naar de cloud brengen erg populair en het daarbij horende pay-per-use (betaal per gebruik) principe. Echter werd snel duidelijk dat nog niet elke applicatie cloud-ready was, dit wil zeggen dat nog niet elke applicatie naar de cloud gebracht kon worden. Nu applicaties steeds vaker met een SaaS-abonnement aan worden geboden merken de IT-leveranciers dat de transitie naar de cloud steeds vaker voorkomt.

Waarom?

Het ontbreken van grip op de accounts en de daarbij behorende machtigingen is een probleem. Een voorbeeld van een gevolg bij het ontbreken van grip, is dat accounts bij uitdiensttreding van een medewerker blijven bestaan zonder toezicht. Het gevaar hierbij is dat deze accounts gehackt kunnen worden en de informatie die beschikbaar is op dit account wordt misbruikt.

Waar?

In dit project doet het probleem zich voor in zowel de interne organisatie, als bij de eindklanten van PCI IT. Het heeft betrekking op de afdelingen binnen de organisaties die zich bezighouden met de gebruikersaccounts.

Wat?

De aanleiding van het probleem is dat er steeds meer transitie naar de cloud is. Mede met het nieuwe ‘hybride-werken’, zowel thuis als op kantoor altijd kunnen werken, zijn applicaties in de cloud steeds populairder geworden. Ook worden webapplicaties als gemakkelijk en overzichtelijk beschouwd door eindegebruikers.

7. Deelvraag 1: Op welke wijze worden de gebruikersaccount in de huidige situatie aangemaakt en aangevraagd?

In dit hoofdstuk wordt er antwoord gegeven op deelvraag 1. Het antwoord op de eerste deelvraag geeft inzicht over de werkwijze van PCI IT intern. Er wordt onderzocht hoe het huidige proces loopt en wat voor pijnpunten er zich in dit proces voordoen.

7.1 Gebruikte methodieken

Er zijn meerdere methodieken gebruikt om antwoord te geven op deelvraag 1. Hieronder worden deze methodieken toegepast en beschreven per methode.

Bureauonderzoek

Door middel van bureauonderzoek zijn er verschillende bronnen onderzocht. Er is hier gekeken naar documenten van klantomgevingen, inrichting van de systemen en algemene globale processen van de klantomgevingen.

Dit is voornamelijk in samenspraak gegaan met collega's waar veel mondeling contact mee is geweest, over zowel de inrichting van de infrastructuur als de processen van de eindklanten. Inhoudelijk waren de processen niet altijd volledig bekend. Echter, dit heeft tot veel nieuwe inzichten geleid, aangezien een van de eindklanten zelfs al een softwareoplossing in haar omgeving heeft draaien voor het geautomatiseerd aanmaken van gebruikersaccounts.

Interviews

De informatie die is opgedaan uit de documentatie en de gesprekken op de werkvloer zijn gebruikt om de interviewvragen op te stellen. Het interview is gefocust op de details van het aanvragen, wijzigen en verwijderen van gebruikersaccounts. Daarnaast wordt er gekeken naar; wie, welke stap, in dit proces uitvoert. Om de interviews gestructureerd af te nemen is gebruik gemaakt van de volgende vragen als startpunt:

- Hoe zit het huidige proces in elkaar voor het aanvragen van een gebruikersaccount?
- Hoe worden de rechten van deze accounts bijgehouden?
- Worden eventuele wijzigingen hierin ook bijgehouden?
- Kost het proces veel tijd?
- Hoe kan een gebruiker momenteel meer rechten aanvragen voor een map of applicatie?
- Hoe tevreden ben je over dit proces?
- Heb je zelf al verbeterpunten in dit proces?

Daarnaast is er ruimte gegeven voor eigen inbreng en is er doorgevraagd naar aanleiding van de antwoorden op bovenstaande vragen.

De volgende personen worden geïnterviewd:

- Annemiek Meulenkamp – HRM
- Bart Brevink – Technical Field Service Manager
- Olaf Kornegoor – Servicedesk Teamleider
- Mitchell Kel - Servicedesk Medewerker
- Tobias ten Brinke – 3e lijn engineer
- Sander Pot - Servicedesk Teamleider
- David Krabbenborg – Projectleider/ Teamcoördinator Network & Security
- Stephan van Hulst – Functionaris gegevensbescherming, risicomanager en kwaliteitscoördinator

UML-diagram

De methodiek UML is gebruikt om een tekening te maken van de huidige situatie voor het aanvragen van gebruikersaccounts. Deze tekening helpt bij het in kaart brengen van de huidige situatie en wat er eventueel kan veranderen bij implementatie van een IAM/PAM softwareapplicatie.

7.2 Resultaten

In deze paragraaf worden bovenstaande methoden uitgewerkt en zijn de resultaten terug te lezen.

Bureauonderzoek

Tijdens het bureauonderzoek heb ik veel rondvraag gedaan over de manier van aanvragen en verwerken van gebruikersaccounts. Hierin heb ik veelal gesproken met de afdeling 3e lijn support engineers. Deze afdeling zit veelal bij klanten op locatie voor complexere vraagstukken. De 3e lijn engineers komen op locatie veel in aanraking met vraagstukken over gebruikersaccounts en het op of afschalen van licenties. Wat hierin opviel is dat elke engineer er anders mee omging en er zelfs een kleine discussie op gang kwam. De discussie ging over de licenties, over wie er verantwoordelijk is voor het doorgeven van nieuwe gebruikersaccounts en hoe deze aangemaakt worden.

De conclusie van de discussie was dat er geen duidelijkheid en correcte werkwijze is. Elke klant gaat anders met gebruikersaccounts om en PCI IT is bij elke klant op een andere manier verantwoordelijk voor de gebruikersaccounts.

Daarnaast heb ik nog de tip gekregen van Bart Brevink om eens te gaan praten met Tobias ten Brinke, 3de lijn engineer. Na een gesprek met Tobias ten Brinke bleek dat hij ondersteunende engineer is geweest bij implementatie van een softwareapplicatie die ook gebruikersaccounts geautomatiseerd kan aanmaken. Hij wist het fijne hier helaas nog niet van aangezien hij alleen de technische ondersteuning voor de implementatie heeft verricht en niet betrokken is bij de interne aanvragen van gebruikersaccounts.

Interviews

Uit de interviews (Bijlage 1: Samenvatting interviews) is veel informatie verkregen over de interne processen bij PCI IT. Uit de interviews blijkt echter dat er intern bij PCI IT nog een aantal werkprocessen niet helemaal soepel verlopen. Knelpunten die vaak naar voren kwamen:

- Onduidelijk welke formulieren ingevuld dienen te worden en door wie exact
- Onduidelijk op welke locatie de medewerker begint en welke facilitaire zaken geregeld dienen te worden
- Doorlooptijd van het aanmaken van een gebruikersaccount duurt lang
- Aanvragen van gebruikersaccounts gebeurt nog te vaak op het laatste moment
- Accounts aanmaken met de hand past niet meer bij de huidige tijd en snelheid waarop technici wordt ontwikkeld
- Geen overzicht van gebruikersaccount met welke licenties

Bovenstaande punten zijn voornamelijk interne knelpunten. Dat wil echter niet zeggen dat andere klanten met dezelfde knelpunten geconfronteerd kunnen worden.

Andere knelpunten die worden ervaren door IT-beheerders (PCI IT) maar ook door de klanten van PCI IT (denk aan managers of HR-medewerkers die bevoegd zijn om gebruikersaccounts aan te vragen/wijzigen/opheffen) zijn onderstaand kort samengevat:

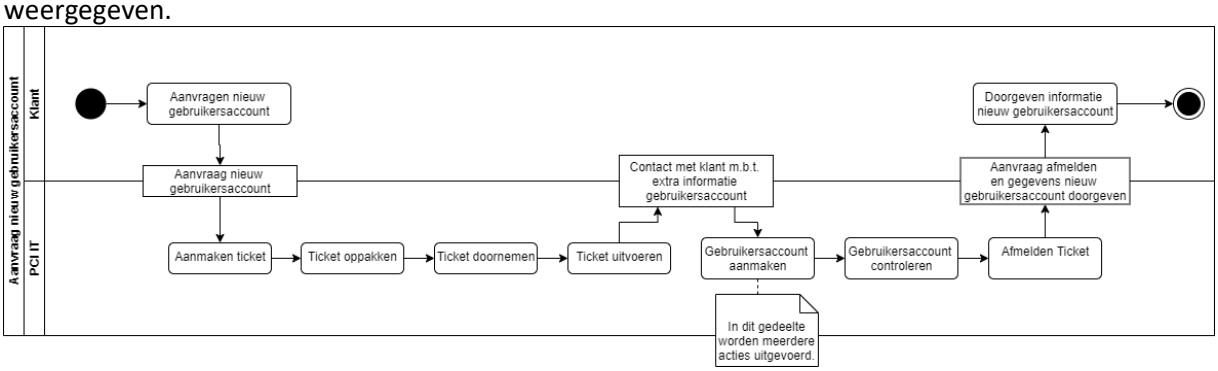
- Provisioning van gebruikersaccounts sluit niet aan op huidige infrastructuur

    - De IT-beheerder dient hierdoor bij een aanvraag van een nieuw gebruikersaccount of een opheffing van een gebruikersaccount in meerdere omgevingen in te loggen of controles uit te voeren. Dit kost extra veel tijd voor de IT-beheerder.
    - De organisatie, eindklant, heeft geen idee wat voor accounts er onder alle medewerkers bestaan.
- Accounts blijven onnodig lang bestaan
    - De IT-beheerder, krijgt de aanvraag voor het opheffen van een gebruikersaccount. De IT-beheerder zegt het AD account op, aangezien PCI IT dit account beheert. De overige accounts bij applicaties blijven echter bestaan, ook omdat dit niet in de aanvraag staat vanuit de klant.
    - De organisatie is eindverantwoordelijk om de IT-beheerder te melden welke accounts er overal opgezegd dient te worden, of de organisatie voert dit zelf uit. Echter is er geen overzicht van welke accounts er exact bestaan en dient dit eerst uitgezocht te worden. Vaak worden niet alle accounts gevonden en dus opgezegd. Dit resulteert in accounts bij leveranciers die onnodig lang blijven bestaan.
- Accounts hebben meer rechten dan nodig
    - De IT-beheerder is indirect verantwoordelijk voor het juist inrichten van de rechtenstructuur, echter is de eindverantwoording bij de klant.
    - De organisatie heeft hier de verantwoording in, maar vraagt indirect wel advies van de IT-partij. Aangezien er geen overzicht is worden de accounts éénmalig ingericht en wordt er vervolgens niet meer naar omgekeken.
- Bestaande accounts vormen een beveiligingsrisico
    - De IT-beheerder voelt zich indirect verantwoordelijk voor de juiste inrichting en voor het geven van advies. Echter blijft de verantwoordelijkheid bij de klant. Het advies van de IT-beheerder zou zijn om de rechten en applicaties alleen uit te delen indien nodig.
    - De organisatie houdt zich hier vaak weinig mee bezig, echter is het besef van de beveiligingsrisico's wel steeds meer aanwezig. Hierdoor wil de organisatie ook meer inzicht in de bestaande accounts.
- Er is geen overzicht van huidige accounts
    - De IT-beheerder weet niet in één oogopslag of het gebruikersaccount al bestaat of niet.
    - De organisatie heeft geen overzicht over alle accounts die aanwezig zijn in de infrastructuur.
- Er is geen overzicht van huidige rechtenstructuur
    - De IT-beheerder dient bij een wijziging van de rechten eerst uit te zoeken of de rechten al bestaan en kan ze vervolgens toevoegen, als er een groep of iets anders al in is gericht voor de rechten die uitgedeeld dienen te worden. Dit kost extra veel tijd.
    - De organisatie heeft geen overzicht over de huidige rechtenstructuur en geeft bij een nieuw gebruikersaccount vaak de rechten van een al bestaande medewerker. Dit resulteert vaak in dat het gebruikersaccount wordt voorzien van meer rechten dan nodig.

In deelvraag 3: 'Deelvraag 3: Aan welke eisen en wensen dient een eventueel softwarepakket te voldoen?' worden de Knelpunten in een schematisch overzicht weergegeven.

UML-diagram

In onderstaande afbeelding wordt het globale proces voor een aanvraag van een gebruikersaccount weergegeven.



Figuur 4 Aanvraag nieuw gebruikersaccount

In bovenstaande afbeelding is een overzicht gecreëerd hoe een aanvraag van een nieuw gebruikersaccount momenteel wordt uitgevoerd. Aanvragen voor het opzeggen of wijzigingen van gebruikersaccounts gebeurt op dezelfde manier, echter worden er andere acties uitgevoerd dan voor het aanmaken.

In het gedeelte waar meerdere acties aan de orde zijn, worden de volgende acties ondernomen:

- Controle welke licentie het nieuwe gebruikersaccount nodig heeft;
- Gebruikersaccount aanmaken;
- Rechten uitdelen die het nieuwe gebruikersaccount nodig heeft;
- Rechten uitdelen voor andere applicaties die het nieuwe gebruikersaccount nodig heeft.

Als deze stappen uit zijn gevoerd kan de volgende stap in het diagram uitgevoerd worden, namelijk de controle van het gebruikersaccount. Vervolgens kan het gebruikersaccount opgeleverd worden aan de eindklant.

8. Deelvraag 2: Welke mogelijkheden zijn er om in een hybride omgeving gebruikersaccounts gecentraliseerd te beheren?

In dit hoofdstuk wordt er antwoord gegeven op deelvraag 2.

8.1 Gebruikte methodieken

Er zijn meerdere methodieken gebruikt om antwoord te geven op deelvraag 2. Hieronder worden deze methodieken toegepast en beschreven per methode.

Interview

In dit proces wordt er met Bart Brevink gesproken over de transitie van de SaaS-applicaties en over de huidige omgeving van verschillende klanten. Het interview is gefocust op wat de huidige klanten set voor infrastructuur heeft.

Literatuurstudie

Een literatuurstudie wordt gebruikt bij deze deelvraag om op een systematische en gestructureerde manier informatie uit publieke bronnen te verzamelen. Hierdoor kan er gekeken worden naar de verschillende mogelijkheden van het gecentraliseerd beheren van gebruikersaccounts.

8.2 Resultaten

In deze paragraaf worden bovenstaande methoden uitgewerkt en zijn de resultaten terug te lezen.

Interview

Bart Brevink – Technical Field Service Manager van PCI IT, gaf aan dat veel klanten momenteel gebruik maken van een lokale Active Directory of een hybride omgeving van lokale Active Directory en Azure Active Directory. Daarnaast maken de meeste klanten gebruik van een Citrix omgeving of een volledige Microsoft omgeving. Bart gaf ook aan dat hij een transitie ziet richting Microsoft en haar producten ten opzichte van Citrix, maar dat niet elk bedrijf hier ook klaar voor is. Aangezien er grote klanten zijn die meer dan 30 applicaties gebruiken, die simpelweg nog niet allemaal klaar zijn om naar de cloud gebracht te worden, kunnen deze bedrijven nog niet over. Hierbij gaat het bijvoorbeeld om applicaties als röntgenapparatuur en werkbanken die vaak nog op Windows 7 of oudere computers draaien. Daarnaast zou het een langdurig traject worden om alle applicaties in kaart te brengen en om beschikbaar te stellen via de SaaS of andere mogelijkheden. Een andere ontwikkeling die Bart Brevink ziet, komt door het effect van het Corona-virus, namelijk dat de meeste mensen thuis dienen te werken en infrastructuren hier niet volledig klaar voor zijn. Ook veranderen de wensen van de klant en is er meer interesse om volledig over te gaan naar Microsoft Intune in combinatie met Office 365. Aangezien Microsoft marktleider is rondom Office-producten en zich nu voornamelijk richt op het werken op onafhankelijke locaties zijn er veel bedrijven die kiezen om van Citrix af te stappen en gebruik te maken van de Microsoftproducten zoals Office365, Intune, SharePoint, Onedrive en Teams. Dit is voornamelijk voor wat kleinere bedrijven snel en gemakkelijk in te regelen aangezien zij vaak intern maar een aantal applicaties gebruiken en deze gemakkelijk naar de cloud te brengen zijn.

Door gebruik te maken van de Microsoft Producten kan er gekozen worden om de lokale Active Directory te behouden en te synchroniseren naar Azure Active Directory dat weer samen werkt met producten als Office 365. Hierdoor is het mogelijk alle Microsoftaccounts en groepen op 1 plek te beheren namelijk bij Azure Active Directory.

Literatuurstudie

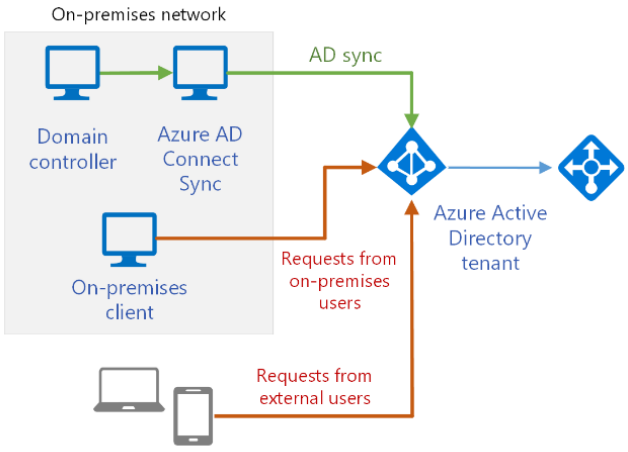
In deze paragraaf wordt verder ingegaan op wat exact een hybride omgevingen inhoudt en wat er mogelijk is in de verschillende Active Directories. Aangezien er binnen PCI IT en haar klantenkring geen gebruik wordt gemaakt van Linux wordt dit buiten het onderzoek gehouden.

Lokale Active Directory

Een Active Directory (AD) is een Windows-domein waaraan verschillende apparaten en gebruikersaccounts te koppelen zijn. Bij een lokale installatie op een fysieke server is er sprake van een lokale Active Directory. Het beheer hiervan is dan alleen mogelijk vanaf deze fysieke server.
De AD wordt gebruikt om gebruikersaccounts aan te maken. In 'Figuur 4 Aanvraag nieuw gebruikersaccount' wordt gebruik gemaakt van de AD om de gebruikersaccounts aan te maken voor de eindklant. Door een gebruikersaccount aan te maken kunnen medewerkers zich met het aangemaakte account authentiseren op locaties als Windows computers maar ook op fileservers van de organisatie (Panthera, 2021).

Azure Active Directory

Een andere omgeving is Azure Active Directory. AAD is de AD van Microsoft en kan worden gebruikt als plek voor authenticatie en autorisatie in de cloud van Microsoft (Microsoft, 2021). Echter, Azure AD is inmiddels uitgegroeid tot een groter platform waar ook cloud diensten als Facebook en Google aan te koppelen zijn. Voor de gebruiker is het mogelijk een account te koppelen aan het Microsoft-account, waarmee de gebruiker zich kan authentiseren bij Google en Facebook. Fysieke servers zijn vanuit kantoor niet direct te koppelen aan deze Azure AD zonder dat er gebruik wordt gemaakt van een lokale AD. Om dit te kunnen realiseren dient er een synchronisatie te zijn tussen de lokale AD en Azure AD. Op deze manier kunnen zowel de lokale servers als de servers in Azure toegevoegd worden aan de AD. Dit wordt gezien als een hybride omgeving. Het voordeel hiervan is dat gebruikers maar 1 account nodig hebben voor het authentiseren en er zowel in de lokale AD als in de Azure AD diensten gekoppeld kunnen worden. Om deze synchronisatie te kunnen maken dient er gebruik te worden gemaakt van de tool van Microsoft 'Azure AD Connect'. Als deze connectie is gemaakt dan worden de gegevens van de lokale AD naar de Azure AD gesynchroniseerd.
Door deze synchronisatie zijn er bijvoorbeeld voordelen te behalen in Office365. Hier kan gewerkt worden met groepen die zowel in de lokale als Azure AD aanwezig zijn en het toewijzen van Microsoft 365 licenties automatisch toewijzen.
In onderstaande afbeelding is de werking van de lokale AD, Azure AD Connect en Azure AD schematisch weergegeven (Microsoft, 2021).

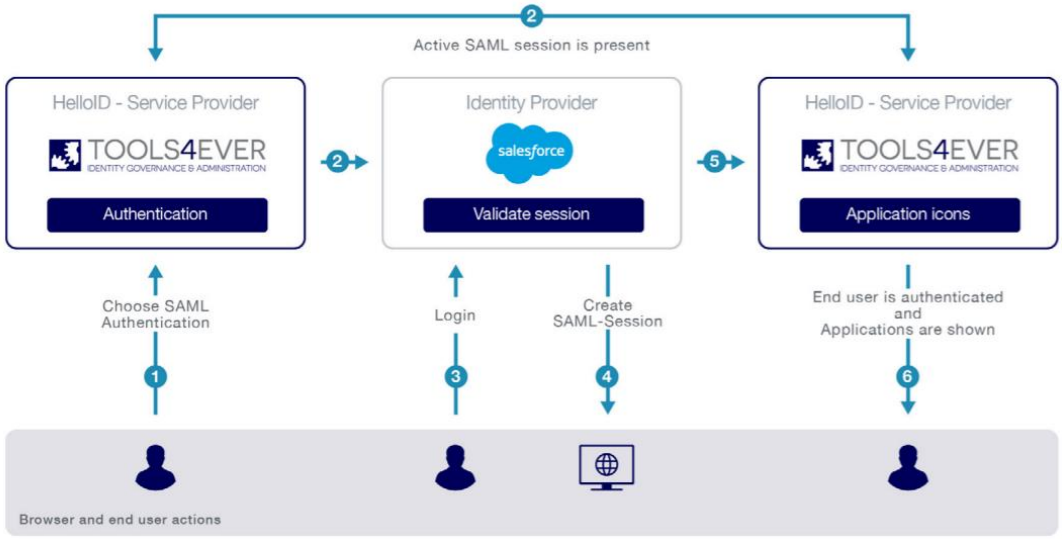


Figuur 5 lokale AD connected met Azure AD (Microsoft, 2021)

In bovenstaande afbeelding is de werking van een hybride omgeving te zien. Hierin is de DC, de tool Azure AD Connect en een on-premise client getoond. Linksboven is het 'On-premises network' gedeelte te zien, dit is het gedeelte wat lokaal bij de klant of bij PCI IT zou staan. Op de lokale AD server is de tool geïnstalleerd 'Azure AD Connect Sync' deze synchroniseert de items, die zijn gekozen bij de installatie van de tool of achteraf aan te passen, naar de Azure AD, de groene lijnen. De 2 rode lijnen zijn gebruikers die in willen loggen (authentiseren) door middel van hun Windows-account. De computer in het grijze vlak is intern aanwezig bij de klant of bij PCI IT en probeert zich te authentiseren bij de Azure Active Directory (AAD). Onder het grijze vlak staat een laptop en een mobiel getoond die zich extern (dus niet bij PCI IT of bij de eindklant op locatie) proberen te authentiseren. Ook deze aanvraag gaat via de AAD, waarbij vaak MFA benodigd is om in te kunnen loggen.
Aan de rechterkant is nu niets getoond, daar bevinden zich de overige applicaties waar de klant of PCI IT gebruik van maakt. Het gaat hier bijvoorbeeld om SaaS-applicaties en zaken als Office365.

Externe tool

Bovenstaande oplossingen zijn echter alleen gericht op (A)AD gebruikersaccounts. De accounts die bij softwareleveranciers van SaaS-applicaties zijn aangemaakt kunnen niet in deze oplossingen worden beheerd. Hiervoor dient een externe tool ingezet te worden.
In Figuur 6 Authenticatie met HelloID voor verschillende applicaties is een tool van Tools4ever getoond met de werking van haar tool HelloID. Hierin is te zien dat de gebruiker verbinding maakt met HelloID als serviceprovider en inlogt met zijn of haar gegevens van Salesforce. De gegevens worden gecontroleerd bij Salesforce en de gebruiker komt in de omgeving terecht van HelloID. In deze omgeving kunnen andere applicaties gekoppeld worden aan het bestaande account van Salesforce.



Figuur 6 Authenticatie met HelloID voor verschillende applicaties (Tools4ever, 2021)

In hoofdstuk 14 Ontwerp wordt verder ingegaan op de werking van een externe tool als serviceprovider.

9. Deelvraag 3: Aan welke eisen en wensen dient een eventueel softwarepakket te voldoen?

In dit hoofdstuk wordt er antwoord gegeven op deelvraag 3.

9.1 Gebruikte methodieken

Er zijn meerdere methodieken gebruikt om antwoord te geven op deelvraag 3. Hieronder worden deze methodieken toegepast en beschreven per methode.

Interviews

De uitgevoerde interviews uit eerdere hoofdstukken worden gebruikt om de eisen en wensen op te stellen.

Brainstromsessie

Op verschillende momenten door het project heen is er gesproken met de teamleden over de eventuele mogelijkheden van het nieuwe systeem. Op deze manier is er creatieve input verkregen vanuit verschillende afdelingen, welke wordt gebruikt voor het opstellen van verschillende eisen.

Requirementsanalyse

De requirementsanalyse is gebruikt voor het opstellen van de requirements. De voorafgaande informatie is gebruikt voor het vaststellen van een set aan requirements.

9.2 Resultaten

In deze paragraaf worden de resultaten van bovenstaande methodieken weergegeven.

Interviews

De informatie uit de interviews bij deelvraag 1 zijn meegenomen als achtergrondinformatie, aangezien hier een aantal belangrijke knelpunten zijn benoemd die relevant zijn voor de requirementsanalyse.

De knelpunten zijn terug te vinden onder 7.2 Resultaten in de paragraaf Interviews.

Brainstormsessie (met David Krabbenborg)

De brainstormsessie geldt als aanvulling op de huidige achtergrondinformatie. Hier is voornamelijk ingegaan op de werking van het product. Dit is uiteindelijk vertaald naar welke functionaliteiten het pakket dient te ondersteunen. Ook zijn zaken doordacht als beveiliging en een MFA bij het aanvragen van gebruikersaccounts. Al deze punten zijn terug te vinden in de requirements analayse.

Requirementsanalyse

De requirements zijn bepaald naar aanleiding van de informatie die uit voorgaande hoofdstukken zijn vergaard. Naar aanleiding van een conceptversie van de requirements zijn deze verder uitgewerkt en is er een volledige lijst met requirements opgesteld.

Knelpunten

De benoemde knelpunten uit paragraaf 7.2 Resultaten, zijn in onderstaande overzicht in een tabelweergave weergegeven:

K-ID	Knelpunt	Samengevat	Vanuit afdeling
K-01	De huidige aanvragen van accounts gaan traag aangezien het veel tijd (manuren) in beslag neemt.	Traag proces	Servicedesk
K-02	Het is gevaarlijk om geen overzicht te hebben welke accounts een medewerker allemaal heeft. Hierdoor blijven accounts rondzweven en kan het lijden tot een beveiligingsincident. Voorbeeld hiervan is een data lek.	Accounts blijven bestaan beveiligingsrisico	Servicedesk
K-03	Accounts handmatig aanmaken past niet meer bij de tijd van nu.	Ouderwets proces	Servicedesk
K-04	Aanvraag wordt vaak op het laatste moment gedaan (dag van tevoren).	Aanvraag komt te laat binnen.	Servicedesk & HRM
K-05	Momenteel worden gebruikersaccount aanvragen gedaan via een checklist die in Excel ingevuld dient te worden. Deze wordt niet altijd juist en volledig ingevuld.	Aanvraag niet volledig.	Servicedesk & HRM
K-06	Vaak wordt er een account aangevraagd door middel van een kopie van een bestaande gebruiker. Dit is een beveiliging probleem aangezien deze gebruiker meerdere rechten toegewezen zou kunnen hebben gekregen, op deze manier krijgt de nieuwe medewerker meer rechten dan de bedoeling is.	Nieuwe gebruiker krijgt meer rechten dan bedoelt	Servicedesk
K-07	Accounts blijven te lang bestaan doordat er geen pakket is die zorgt voor gebruikersbeheer. Niemand neemt de verantwoording voor de gebruikersaccount, ook is niet duidelijk waar de gebruiker toegang tot had.	Account wordt niet opgeheven/ beveiligingsrisico	Servicedesk/ HR externe klant

Tabel 5 Knelpunten

User stories

In onderstaand tabel zijn de knelpunten vertaald naar user stories en de eisen van David Krabbenborg (projectleider) toegevoegd. De user stories zijn opgesteld vanuit het oogpunt PCI IT, echter gelden alle user stories ook voor de eindklanten.

US-ID	User story	Gekoppeld aan
US-01	Als projectleider wil ik dat eindgebruikers (HR-medewerker of manager extern bedrijf) een aanvraag voor een gebruikersaccount kunnen doen.	K-03
US-02	Als projectleider wil ik dat cruciale wijzigingen (zoals aanvragen van nieuwe accounts) niet direct zonder goedkeuring vanuit PCI IT doorgevoerd kunnen worden (4-ogen principe).	
US-03	Als projectleider wil ik meerdere verschillende klanten (eindgebruikers) kunnen koppelen aan één ingericht systeem.	
US-04	Als HR-medewerker wil ik gebruik maken van functieprofielen in plaats van gebruikersgroepen.	K-03, K-06
US-05	Als HR-medewerker wil ik gebruik maken van functieprofielen in plaats van een kopie van gebruikersaccounts.	K-03, K-06
US-06	Als HR-medewerker wil ik een gebruikersaccount voor een nieuwe medewerker aan kunnen vragen.	K-03
US-07	Als manager van een afdeling wil ik een gebruikersaccount voor een nieuwe medewerker binnen mijn afdeling aan kunnen vragen.	K-03
US-08	Als HR-medewerker wil ik een gebruikersaccount op kunnen heffen zodra de medewerker uit dienst gaat.	K-02, K-07
US-09	Als manager van een afdeling wil ik een gebruikersaccount voor een uit dienst getreden medewerker binnen mijn afdeling op kunnen heffen.	K-02, K-07
US-10	Als aanvrager van een nieuw gebruikersaccount wil ik een einddatum voor het gebruikersaccount in kunnen stellen zodat het gebruikersaccount automatisch opgeheven wordt.	K-02, K-05, K-07
US-11	Als HR-medewerker wil ik een overzicht hebben van welke gebruikers welke rechten hebben.	K-06, K-07
US-12	Als manager van een afdeling wil ik een overzicht hebben van welke gebruikers binnen mijn afdeling welke rechten hebben.	K-06, K-07
US-13	Als projectleider wil ik dat gebruikersaccounts niet langer handmatig aangemaakt dienen te worden.	K-01, K-03
US-14	Als projectleider wil ik dat een aanvrager van een nieuw gebruikersaccount verplicht alle benodigde velden in dient te vullen.	K-05
US-15	Als HR-medewerker wil ik na de tijd extra rechten toe kunnen voegen aan een al bestaand gebruikersaccount.	K-06
US-16	Als manager van een afdeling wil ik na de tijd extra rechten toe kunnen voegen aan een gebruiker binnen mijn afdeling.	K-06
US-17	Als HR-medewerker wil ik functieprofielen aan kunnen passen.	K-06
US-18	Als HR-medewerker wil ik in kunnen zien wat de status van mijn aanvraag van een gebruikersaccount is.	

Tabel 6 User stories

Requirements

In vorig paragraaf zijn de user stories gedefinieerd. Deze worden in deze paragraaf verwerkt tot requirements. In de onderstaande tabellen is een overzicht gecreëerd van de must have requirements, de lijst met volledige requirements is terug te vinden in de bijlage.

User requirements

In onderstaande tabel zijn de user requirements vermeld en is in het veld 'Gekoppeld aan' te zien aan welke user story de user requirement is gekoppeld.

U-ID	Requirement	Prioriteit	Gekoppeld aan	Gekoppeld aan
U-01	Een bevoegde HR-medewerker dient binnen 10 minuten een overzicht te kunnen creëren van welke gebruikersaccounts welke rechten hebben.	Must	US11	K-06, K-07
U-02	Een gebruikersaanvraag die door een bevoegde eindgebruiker is ingediend dient ten alle tijden goedgekeurd te worden door een andere bevoegde medewerker (4-ogen principe).	Must	US02	
U-03	Er dient ten alle tijden een 4-ogen controle te zijn bij een aanvraag van een nieuwe gebruiker van zowel een bevoegde eindgebruiker als een HR-medewerker.	Must	US02	

Tabel 7 Must have user requirements

System requirements

In onderstaande tabel zijn de system requirements vermeld.

S-ID	Requirement	Prioriteit	(Niet) Functioneel
S-01	Het product dient een koppeling te kunnen maken met meerdere applicaties door middel van een API-koppeling.	Must	Functioneel
S-02	Er dienen meerdere klanten gekoppeld te kunnen worden aan het product.	Must	Functioneel
S-03	Het product dient een koppeling te hebben met Azure Active Directory	Must	Functioneel
S-04	Het product moet een koppeling kunnen maken met Active Directory	Must	Functioneel
S-05	Het product moet, als er data opgeslagen wordt, data opslaan binnen de Europese Economische Ruimte (EER)	Must	Functioneel
S-06	Het product dient MFA te ondersteunen.	Must	Functioneel

Tabel 8 Must have system requirements

10. Deelvraag 4: Welke oplossing past het beste bij de eisen en wensen van PCI IT als MSP?

In dit hoofdstuk wordt antwoord gegeven op deelvraag 4.

10.1 Gebruikte methodieken

In deze paragraaf wordt er gekeken naar de aanpak van deelvraag 4.

Literatuurstudie

In publieke bronnen wordt er gekeken naar de mogelijkheden om een dergelijke dienst als IAM/PAM in te zetten als MSP. Hierbij worden meerdere applicaties met elkaar vergeleken en bekeken.

Multicriteri analyse

Door middel van een multicriteria-analyse wordt er een keuze gemaakt welke applicatie er volgens de eisen en wensen het beste past bij PCI IT als MSP.

10.2 Resultaten

In deze paragraaf worden de resultaten van bovenstaande aanpak uitgewerkt.

Literatuurstudie

Als vervolg op de brainstormsessies en de gemaakte eisen en wensen kan er verder gezocht worden naar de verschillende applicaties die gewenste de functionaliteiten ondersteunen. Tijdens het zoeken naar de verschillende IAM-applicaties is gebruik gemaakt van de volgende lijst van Gartner die een vergelijking heeft gemaakt van alle Acces Management softwareapplicaties, daarnaast is er research gedaan naar softwareapplicaties die niet in de lijst van Gartner staan. Om te waarborgen dat alle beschikbare producten in de longlist meegenomen worden is de lijst van Gartner vergeleken met de website van G2 (G2, 2021) en het onderzoek van BeyondTrust (BeyondTrust, 2021).

Figuur 7 Magic Quadrant for Access Management (Gartner, 2021)

Student: Jorick Benjamins (453565)

Magic Quadrant for Access Management

In deze paragraaf wordt vermeld waarom toegangsbeheer belangrijk is en waar het Magic Quadrant for Access Management van Gartner naar heeft gekeken tijdens het onderzoek.

Toegangsbeheer is de bron van vertrouwen geworden door identiteitsbeveiliging. Door de grotere afhankelijkheid van identiteiten om overal en altijd toegang te krijgen, moet Access Management betrouwbaarder en gemakkelijker te adopteren zijn. Identiteit software, IAM en SaaS-applicaties zullen in 2022 toenemen.

Gartner (Gartner, 2021) neemt een kijk op de markt en op transformationele technologieën die voldoen aan de toekomstige behoeften van eindgebruikers. Om op de Quadrant for Access Management te komen dient het softwarepakket aan een aantal mogelijkheden te voldoen:

- Identiteitsbeheer van interne en externe identiteiten, inclusief directory- en identiteitsynchronisatiediensten:
    - De directe vraag vanuit PCI IT is om interne en externe identiteiten te kunnen koppelen. De volgende system requirements zijn van toepassing: S-01, S-03, S-04, S-08, S-09, S-10, S-11 en S-14.
- Self-service voor gebruikers, inclusief eindgebruikers- en beheerinterfaces voor gebruikersregistratie, wachtwoordbeheer, profielbeheer en gedelegeerd beheer:
    - Een wens vanuit PCI IT is dat eindgebruikers zelf bepaalde diensten uit kunnen voeren zoals het resetten van hun wachtwoord. De volgende system requirements zijn hierop van toepassing: S-02, S-08, S-11, S-12 en S-14. De volgende user requirements zijn ook van toepassing: U-04, U-06, U-07, U-08, U-09, U-10, U-11, U-13, U-14 en U-15.
- Een startpunt voor personeel van applicaties of applicatiegalerij voor eenmalige aanmelding (SSO):
    - De wens voor een applicatiegalerij is niet besproken.
- Autorisatie en adaptieve toegang, en ondersteuning voor moderne identiteitsprotocollen zoals OAuth 2.0:
    - Een harde eis in dit project is, dat het product koppelingen dient te hebben met meerdere applicaties door middel van een API-koppeling (S-01).
- Sessiebeheer:
    - De functionaliteit voor sessiebeheer is niet besproken in dit project.
- Methoden voor gebruikersauthenticatie, waaronder MFA en SSO:
    - Een harde eis in dit project is om meerdere wegen authenticatie voor gebruikers toe te kunnen passen (S-06).
- Breng je eigen (openbare)identiteit (BYOI)-integratie mee om openbare identiteiten, zoals sociale media-accounts, te gebruiken voor toegang:
    - BYOI is niet besproken met de opdrachtgever.
- API-toegangscontrole voor het afhandelen van authenticatie en autorisatie naar API-doelen:
    - Een harde eis in dit project is om verschillende applicaties te kunnen koppelen door middel van een API-koppeling (S-01).
- Standaard applicatie inschakeling, inclusief mogelijkheden voor het aanzetten van rapid access, SSO en MFA naar SaaS en andere standaard webapplicaties die moderne autorisatie protocolen gebruiken zoals SAML en OpenID Connect:
    - Een eis in dit project is om meerdere webapplicaties te koppelen met de mogelijkheid om meerdere wegen voor authenticatie te kunnen forceren voor gebruikers (S-06).
- Niet-standaard applicatie ondersteuning, inclusief de mogelijkheden om de autorisatie uit handen te nemen van deze apps. En voor applicaties die verouderd zijn, de mogelijkheid biedt om diensten als SSO en MFA te gebruiken:

    - Een wens van PCI IT is om de mogelijkheid te hebben om niet-standaard applicaties zelf te kunnen koppelen door middel van scripting (S-07).
- Analytische mogelijkheden, inclusief geschiedenis, logs en en uitgevoerde administratieve acties:
    - Een wens van PCI IT is om de IAM-applicatie te gebruiken voor analytische doeleinden. Met deze functionaliteit is het mogelijk om een risicoanalyse uit te voeren voor het uitdelen van rechten.

Multicriteria-analyse

Op de volgende pagina is Tabel 9 Multicriteria-analyse longlist te vinden. In deze tabel is er op basis van zes verschillende eisen onderzoek gedaan naar 19 verschillende applicaties. De eisen zijn terug te vinden op de Y-as en op X-as zijn de verschillende IAM-softwarepakketten af te lezen.
De eisen zijn samengesteld in overleg met David Krabbenborg. Dit is gedaan door nogmaals door de Requirements heen te lopen en de belangrijkste te noteren op de Y-as. In paragraaf 10.3 Shortlist wordt toegelicht waarom er gekozen is voor deze eisen.
De applicaties die op de X-as zichtbaar zijn, vormen samen de longlist van de multicriteria-analyse. Om de longlist te creëren is er research gedaan naar de verschillende IAM-applicaties die beschikbaar zijn op de markt. Hier is meteen gekeken naar de belangrijkste twee eisen om verschillende klanten te kunnen koppelen en applicaties te kunnen koppel op basis van een API-koppeling. Als het softwarepakket deze functionaliteit niet ondersteunde is deze niet opgenomen in de longlist. De longlist is vervolgens gevuld met 19 verschillende softwareapplicaties en 6 eisen.
De rode vlakken betekent dat de functionaliteit niet aanwezig is bij het softwarepakket. De gele vlakken geven aan dat de informatie over de functionaliteit lastig te achterhalen was en niet met zekerheid gezegd kan worden of het wordt ondersteund. De groene vlakken zijn functionaliteiten waar het softwarepakket over beschikt. Nu de longlist compleet ingevuld is wordt, is er gekeken naar welke applicaties niet aan alle eisen voldoen en dus niet in de shortlist opgenomen worden.
In de shortlist, zie Tabel 10 Multicriteria-analyse shortlist, zijn de 3 applicaties opgenomen, die aan de meeste eisen voldoen. Om een keuze te kunnen maken tussen deze verschillende applicaties zijn er 4 eisen toegevoegd namelijk: self-service password reset, implementatiegemak, de missie en visie en de prijs.
In paragraaf 10.3 Shortlist wordt de shortlist verder toegelicht.

Opties	Vooraf gekoppelde apps o.b.v. API	Multi-tenancy	MFA	Scripting	Auditing report	Automation
Onelogin						
Okta						
Auth0 (Okta)						
SailPoint (IAM)						
Omada						
Centrify Identity Service						
Oracle						
IBM (lifecycle management)						
JumpCloud						
Pulseway						
HelloID						
M365 Manager plus						
Cloudaware						
CyberArk						
SecureAuth						
Ilantus						
Micro Focus						
Microsoft Azure AD						
ForgeRock						

Tabel 9 Multicriteria-analyse longlist

Opties	Vooraf gekoppelde apps o.b.v. API	Multi-tenancy	MFA	Scripting	Auditing report	Automation	Self-service PW reset	Implementatiegemak	Missie/Visie	Prijs
Okta										
HelloID										
SecureAuth										

Tabel 10 Multicriteria-analyse shortlist

10.3 Shortlist

In deze paragraaf worden de voor- en nadelen van de applicaties verder toegelicht. Onderstaande informatie is verkregen door gebruik te maken van openbare bronnen, websites en er is getracht contact te krijgen met de leveranciers.

Softwareapplicaties

Okta (Okta, 2021) is op de shortlist gekomen, aangezien het product erg veel functionaliteiten heeft die gewenst zijn. Auth0 (Auth0, 2021) is recent overgenomen door Okta, een andere IAM-applicatie leverancier. De nadelen aan Okta:

- missie en visie zijn onduidelijk
- implementatiegemak is laag
- vooraf gekoppelde applicaties op basis van API-koppelingen is beperkt
- scripting is aanwezig, maar de mogelijkheden zijn minimaal
- geen reactie op diverse berichten, slechte communicatie

SecureAuth (Secureauth, 2021) is op de shortlist gekomen, door de vele functionaliteiten die het softwarepakket aanbiedt. SecureAuth lijkt goed in te spelen op overzicht en gebruikersgemak. De nadelen aan het softwarepakket zijn:

- missie en visie zijn onduidelijk
- weinig informatie bekend
- geen reactie op diverse contactpogingen
- scripting mogelijkheden zijn onduidelijk

HelloID (Tools4ever, 2021) – is van de Nederlandse leverancier Tools4ever. Tools4ever beschikt over alle functionaliteiten die geëist worden vanuit PCI IT. De voordelen van HelloID zijn:

- missie en visie zijn duidelijk inzichtelijk
- snelle communicatie
- scripting mogelijkheden d.m.v. PowerShell
- veel informatie beschikbaar

Een nadeel van HelloID:

- geen beschikbare koppeling voor ConnectWise

Requirements

In deze paragraaf worden de eisen op de short- en longlist verder toegelicht en wordt kort besproken waarom dit een eis is van PCI IT.

API-koppeling

In de longlist zijn de applicaties met een rood vlak afgevallen aangezien er geen API-koppelingen beschikbaar waren. Op basis van API-koppelingen zijn de verschillende SaaS-applicaties, maar ook Active Directory's te koppelen aan de softwareapplicatie. Dit is de belangrijkste requirement aangezien dit het probleem van dit onderzoek is.

Multi tenancy

Uit de longlist blijkt dat veel van deze applicaties niet ingezet kunnen worden als multi tenancy applicatie. Dit is wel een van de grootste wensen van PCI IT aangezien veel van haar klanten dezelfde problemen ervaren en de werkzaamheden hiervan door PCI IT zelf uitgevoerd dienen te worden. Om deze reden wil PCI IT deze oplossing als dienst aanbieden aan haar klanten.

MFA

MFA is een veel besproken onderwerp deze tijd en biedt enorm veel extra beveiliging. Om de beveiliging te kunnen blijven waarborgen dient het softwarepakket een mogelijkheid te hebben voor MFA.

Scripting

Scripting kan worden gebruikt om niet bestaande koppelingen zelf te maken of data te achterhalen uit softwareapplicaties die wel gewenst zijn. Aangezien PCI IT veel verschillende klanten heeft met diverse applicaties is deze requirement van belang, een overzicht van de verschillende applicaties is terug te vinden in 13.3 Voorbeeldklant. In de longlist is te zien dat er bij deze eis behoorlijk veel gele vlakken zijn, hier is dan ook een grote slag gemaakt met applicaties die af zijn gevallen.

Auditing report

Met een auditing report kan er een overzicht worden gecreëerd welke gebruikers, wat voor rechten hebben in de gekoppelde applicaties, mappen en andere gebruikeraccounts.
Auditing report is een could have system requirement en dus niet een van de belangrijkste eisen. Echter, dit is wel een functionaliteit die PCI IT in de nabije toekomst wil gaan aanbieden en is daarom in de longlist opgenomen. De meeste applicaties voldoen aan deze eis.

Automation

Automation is net als auditing report een functionaliteit die PCI IT graag in de nabije toekomst voor haar klanten aan wil bieden. Het is geen harde eis aan de softwareapplicatie maar is wel opgenomen in de multicriteria-analyse aangezien het wel gewenst is.
Met automation wordt bedoeld dat er processen geautomatiseerd kunnen worden. Bijvoorbeeld het aanmaken van gebruikersaccounts.

Self-service password reset

Met selfservice password reset kunnen de klanten direct hun eigen wachtwoord resetten zonder tussenkomst van een medewerker van PCI IT.
Deze eis is niet opgenomen in de longlist aangezien het geen must have is voor PCI IT. Het is wel een functionaliteit die veel tijd kan besparen en een efficiënte toevoeging zou zijn aan de huidige dienstverlening. Daarom is deze eis opgenomen in de shortlist.

Implementatiegemak

Een volgende eis die op is genomen in de shortlist is het implementatiegemak.
De eis is opgenomen aangezien het softwarepakket geïmplementeerd dient te worden in een bestaande omgeving.

Missie/ Visie

De missie en visie van de softwareleveranciers is de volgende eis in de shortlist. Deze is van belang aangezien IAM/PAM applicaties naar verwachting in de toekomst steeds meer gebruikt gaan worden. Om te bepalen of de applicatie door wil blijven ontwikkelen en mogelijk nieuwe functionaliteiten beschikbaar zou gaan stellen is gekeken naar de missie en visie.

Prijs

Een van de business requirements is dat betalen per gebruik een wens is en de kosten niet te hoog zijn. Als de kosten te hoog zijn is het niet aantrekkelijk voor klanten van PCI IT om een dergelijke dienst af te nemen. Voor PCI IT als MSP is het wenselijk om snel op en af te kunnen schalen met de kosten voor een uitrol van een nieuwe klant.

10.4 Conclusie

Het product voldoet aan de gestelde eisen zoals te zien is in de shortlist. Een nadeel van HelloID is dat het nog geen beschikbare API-koppeling heeft met ConnectWise, het ERP-systeem van PCI IT. Echter, aangezien er in dit project niet alleen gekeken wordt naar de beste oplossing voor PCI IT, maar ook voor haar klanten is het geen harde eis dat intern gebruikte applicaties vooraf gekoppeld kunnen worden. Daarnaast is er rekening gehouden met scripting om deze wens eventueel zelf mogelijk te maken. Alomvattend kan worden gesteld dat HelloID het beste past bij de eisen en wensen van PCI IT als MSP.

11. Deelvraag 5: Hoe valt een dergelijke dienst als MSP in te zetten?

In dit hoofdstuk wordt er antwoord gegeven op deelvraag 5.

11.1 Gebruikte methodieken

In deze paragraaf wordt er gekeken naar de aanpak van deelvraag 5.

Brainstormsessie

Door een brainstormsessie met de betrokkenen over verschillende onderwerpen te houden, kunnen de betrokkenen dit vertalen naar de praktijkervaring en kennis. Deze methode wordt gebruikt om de betrokkenen mee te laten denken in het project en om nieuwe inzichten te krijgen. De kennis die is opgedaan uit vorige hoofdstukken wordt als input gebruikt voor deze gesprekken.

Interview

Om een beter inzicht te krijgen in de mogelijkheden van HelloID is er contact geweest met een medewerker van Tools4ever, de softwareleverancier van HelloID. Deze worden in deze paragraaf verwerkt.

Ontwerpprincipes

In deze paragraaf wordt er gekeken met wat voor functionaliteiten, die als MSP aangeboden kunnen worden, rekening gehouden dient te worden in het ontwerp. Ontwerpprincipes zijn principes uit de literatuur. De ontwerpprincipes worden als basis gebruikt voor het ontwerp, op deze manier kunnen keuzes op een duidelijke wijze verantwoord worden.

11.2 Resultaten

In deze paragraaf worden de resultaten van de aanpak uitgewerkt.

Brainstormsessie

Tijdens de brainstormsessie met Bart Brevink en David Krabbenborg is er verder ingegaan op de wensen om de dienst als MSP in te zetten. Bart Brevink gaf aan dat Microsoft redelijk ver is met applicaties als IAM/PAM, maar dan voornamelijk op Microsoftgebied en niet voor 3th party applicaties zoals HRM-softwarepakketten.
Het is van belang dat de softwareapplicatie rapporten uit kan draaien over de bestaande accounts. Uit deze rapporten is uit te lezen welke accounts zich binnen de organisatie bevinden. Dit resulteert in meer grip op de bestaande gebruikersaccounts. Een bijkomende wens is dat de rechten van deze accounts ook zichtbaar zijn in het rapport en er een impactanalyse gemaakt kan worden op basis van het rapport.
Een andere wens die is besproken is dat de implementatie van het softwarepakket uitgevoerd kan worden voor meerdere klanten. Als het softwarepakket eenmalig geïnstalleerd en ingericht kan worden scheelt dit veel tijd en kosten. PCI IT heeft een eigen on-premise omgeving waar de applicatie aangeboden kan worden. Maar als het softwarepakket op basis van een SaaS-dienst aangeboden wordt is dat ook geen probleem.
Een eis die is besproken is dat er geen vaste verbinding naar de eindklant benodigd dient te zijn. Dit zou weer tot beveiligingsproblemen kunnen leiden.

Interview

Tijdens het interview met Tools4ever heb ik diverse vragen gesteld met betrekking tot de mogelijkheden die de tool biedt om het in te zetten als MSP. De belangrijkste punten zijn hieronder samengevat:

- HelloID is te koppelen aan meerdere applicaties en AD-tenants. Om HelloID als MSP uit te rollen is het mogelijk om een beheerdersportaal te creëren, waar verschillende tegels aangemaakt kunnen worden voor alle klanten.
- Het is niet wenselijk om alle klanten in één keer uit te rollen, aangezien alle klanten verschillende applicaties gebruiken waardoor andere koppeling benodigd zijn. Daarnaast verschillen de functieprofielen en de daarbij behorende rechten ook per organisatie.
- De koppeling maken met verschillende applicaties is gemakkelijk te maken, aangezien HelloID al 150 applicaties out-of-the-box ondersteund.
- HelloID maakt het mogelijk om klanten veel diensten zelf te regelen.

Het volledige interview is terug te vinden in Bijlage 5: Interview met Tools4ever (softwarepakket HelloID).

Conclusie

Om HelloID in te zetten als MSP-dienst kunnen verschillende eindklanten worden gekoppeld aan tegels, op basis van deze tegels krijgen de eindklanten een eigen tenant. In deze eigen tenant zijn klant specifieke eisen en wensen in te richten. Door middel van een agent worden de gegevens van de klant verzameld en verwerkt binnen HelloID. Om meer grip te creëren op de bestaande accounts en de toegewezen rechten, is er binnen HelloID een functionaliteit beschikbaar om auditing reports af te drukken. Op basis van dit auditing report kan er een impact analyse worden gedaan.
In paragraaf 12.2 Resultaten wordt verder ingegaan op de werking van de agent. In paragraaf Self-service diensten is te zien welke diensten ingezet kunnen worden als MSP.

12. Deelvraag 6: Hoe zou de implementatie van een dergelijk product in het dienstportfolio en dienstmanagement (dagelijks beheer) bij PCI IT eruitzien?

In dit hoofdstuk wordt er antwoord gegeven op deelvraag 6.

12.1 Gebruikte methodieken

In deze paragraaf wordt er gekeken naar de aanpak voor het beantwoorden van de deelvraag.

Interview

Er is een interview gehouden met een medewerker van Tools4ever, de informatie die op is gedaan tijdens het interview wordt hier verwerkt.

Literatuurstudie

In publieke bronnen wordt er gekeken wat de verschillende mogelijkheden zijn voor het afnemen van HelloID. Daarnaast wordt er gekeken wat de mogelijkheden zijn voor PCI IT om dit als dienst aan te bieden op basis van haar huidige dienstportfolio.

Implementatie

In dit onderdeel wordt door middel van een stappenplan beschreven hoe de implementatie van HelloID eruitziet.

Dagelijks beheer

In deze paragraaf wordt uitgelegd hoe het dagelijks beheer van HelloID eruitziet.

12.2 Resultaten

In deze paragraaf worden de resultaten van bovenstaande aanpak verwerkt.

Interview

Tijdens het interview met Tools4ever zijn er diverse vragen gesteld met betrekking tot de implementatie van het pakket die zij aanbieden, namelijk HelloID. De belangrijkste punten zijn hieronder samengevat:

- De implementatie van het softwarepakket kan door een technische medewerker van Tools4ever worden gedaan;
- Er zijn gratis cursussen beschikbaar voor het implementeren van het softwarepakket;
- Er zijn gratis cursussen beschikbaar voor het maken van API-koppelingen;
- Er zijn gratis cursussen beschikbaar voor het dagelijkse beheer.

Het volledige interview is terug te vinden in Bijlage 5: Interview met Tools4ever (softwarepakket HelloID).

Literatuurstudie

Om een juist advies te kunnen geven over welke diensten PCI IT aan kan bieden, is er gekeken naar de verschillende modules die beschikbaar zijn binnen HelloID. Het dienstenportfolio van PCI IT is terug te vinden in de paragraaf Diensten/ producten.

Modules binnen HelloID

Er zijn 3 verschillende modules die worden aangeboden door HelloID:

1. Provisioning:
    - Source system management.
        - Koppelingen die standaard beschikbaar zijn zoals HR, SIS en planningsystemen
        - Cloud en on-premises system provisioning
        - Op maat gemaakte koppelingen door middel van PowerShell
    - Identity information.
        - Kluis met persoonlijke identiteit gegevens
        - Persoon en contract informatie
        - Toegewezen rechten, accounts en groepen
        - Audit logging
    - Target system management.
        - Standaard koppeling van doeleinden als AD, AAD, O365, Exchange en NTFS.
        - Op maat gemaakte koppelingen door middel van PowerShell
        - Gebruikersaccount mapping en transformatie
        - Email notificatie
        - Audit logging
    - Customization.
        - Eigen organisatie URL
        - Zelf aan te passen naar huisstijl en lay-out
    - Business rules management (RBAC)
        - Uitgebreide configuraties voor de persoonlijke identiteit gegevens (niet downloadbaar e.d.)
        - Rechten en bedrijfsregels
        - Beheer van de accountlevenscyclus/ life cycle management
        - Impact analyse van de aangepaste wijzigingen
        - Bedrijfsregels kunnen worden toegepast als concept (testdoeleinden)

2. Service Automation:
    - Universal Directory
        - Cloud directory
        - Zelf aan te passen attributen en velden
        - Zelf aan te passing overzichten en transformaties
        - Meerdere AD-tenant koppelingen
        - AD account authentication en gebruiker and groep synchronisatie
    - Workflows
        - Automatische goedkeuringen
        - Zelf aan te passen goedkeuringen
        - Personen aanwijzen voor goedkeuringen
    - Data Management
        - Share en resource eigenaar management
        - Automatische ACL-constructor
    - Automation
        - Werkprocessen automatiseren
        - Geïntegreerde taken catalogus

    - Gebruiker, groep en folder gebeurtenis triggers
- Auditing & reporting
    - Standaard, zelf aan te passen en periodieke auditing reports
- Self-Service
    - Gebruiker & Manager self service
    - Product vervaldatum en automatische teruggave/inname rechten
    - Scheiding van verantwoordelijkheden
    - Productrisicofactoren
    - Verzoek namens
    - Gedelegeerd beheer van AD
- Dynamic Forms
    - Zelf aan te passen formulieren
    - Data uit formulieren zijn te gebruiken voor het automatiseren van taken

3. Access Management:
- Multi Factor Authentication (MFA)
    - SMS, E-mail, softtokens (inclusief Microsoft Authenticator en Google Authenticator) en RADIUS integratie
- Single Sign-on (SSO)
    - Identiteit Provider routing (IDP)
    - Geïntegreerde applicatie catalog
    - Desktop, Mobile en On-premises SSO
- Access rules and policies
    - Beveiliging en login policies
    - Groep en applicatie toegang policies
- Auditing & reporting

De lijst met volledige functionaliteiten is terug te vinden op de website van Tools4ever (Tools4ever, 2021).

Implementatie

Naar aanleiding van contact met Tools4ever ben ik doorverwezen naar het forum van Tools4ever (Tools4ever, 2021). Op het forum van Tools4ever zijn consultants actief die alle technische vragen in behandelingen nemen. Na diverse berichten met Arnout van der Vorst ben ik doorverwezen naar zijn YouTube kanaal, hier zijn meerdere korte filmpjes te vinden over wat HelloID is en wat kan (Tools4ever, 2021).

De implementatie is te verdelen in 16 stappen (Tools4ever, 2021). Deze stappen zijn hieronder te vinden met een korte instructie wat er in deze stap uitgevoerd wordt. De schatting voor een implementatie voor het Provisioning gedeelte is 4,5 werkdag.

1. Agents

HelloID is een cloud platform en om de on-premise omgeving te kunnen verbinden dient er een agent geïnstalleerd te worden. Deze agent communiceert met het cloud platform van HelloID. Dit is alleen uitgaand verkeer door middel van HTTPS (Tools4ever, 2021).

2. Import van HR

In stap 2 worden de bron connectoren ingericht. Hier wordt, indien beschikbaar, een API-koppeling gemaakt met de HR-applicatie. Verstandig is om hier eerst een snapshot te maken vanuit de HR-applicatie om de data veilig te stellen. Vervolgens dient de data opgehaald te worden door een import te draaien en dienen de personen gevalideerd te worden. Eventuele extra data of custom

velden zijn hier ook toe te voegen. Als deze import compleet is en de personen zijn gevalideerd is staat de data in HelloID.

3. Correlatie

Bij deze stap wordt aangegeven hoe de accounts aan elkaar gekoppeld dienen te worden, hoe het correleert. Aangezien HelloID vaak ingezet wordt bij een omgeving die al bestaat dient deze stap uitgevoerd te worden.
Bij het aanmaken van een target system, een connectie met de AD, wordt er een 'Correlation report' gemaakt waar de accounts naar voren komen die gekoppeld zijn, de accounts die niet juist gekoppeld zijn en accounts die niet gekoppeld kunnen worden aan personen (denk aan serviceaccounts). De accounts die niet gekoppeld kunnen worden aan een persoon dienen opgelost te worden, anders wordt er bij livegang van de implementatie een account aangemaakt voor deze personen (Tools4ever, 2021).

4. Configuratie AD/ Azure

In stap 1 is de agent geïnstalleerd in de omgeving waar HelloID geïmplementeerd wordt. Hier is een agent-pool aangemaakt waar meerdere koppelingen in gemaakt kunnen worden, denk aan on-premise AD en Azure AD. De agent kan op een willekeurige VM of machine worden geïnstalleerd in het netwerk van de AD. De agent zoek zelf om zich heen voor de AD. In het volgende stadium wordt de synchronisatie aangemaakt. Hier kan worden gekozen om alle gebruikers en groepen binnen te halen of een selectief gedeelte hiervan. Daarnaast kan er aangegeven worden wat er gedaan moet worden met de gebruikers die verwijderd zijn in de AD, maar nog wel in HelloID zitten (Tools4ever, 2021).
Stappen die tijdens de implementatie aangegeven dienen te worden in stap vier zijn zaken als, in welke OU de gebruikers gesynchroniseerd moeten worden en hoe er met naamgeving omgegaan dient te worden. Dit wordt gedaan door een deel JAVA-scripting en PowerShell scripting.
De schatting voor deze eerste vier stappen is dat hier al snel 1 á 1,5 dag werk in zit.

5. Notificaties inrichten

Basis notificaties inrichten om de testen juist uit te kunnen voeren. Dit kan later verder uitgebreid worden.

6. Testen met 1 persoon richting AD/ Azure

In stap 6 worden testen uitgevoerd, met deze testen kan worden gekeken of voorgaande instellingen juist ingesteld staan. Dit kan je het beste doen met iemand die uit dienst is, of nog in dienst moet komen. Pas de scope aan naar deze ene persoon en voer de implementatie zo vaak uit als nodig tot alles scherp is afgesteld.

7. Business rules

Als stap 6 netjes is afgerond is de volgende stap de Business rules. Hier is veel input benodigd van de klant. Er kan een keuze gemaakt worden om nieuwe accounts in te richten op basis van een basisstructuur met applicaties en rechten, echter is dit niet aan te raden. De andere mogelijkheid is om functieprofielen op te nemen en rechten op basis van functie uit te delen. Dit is een aan te raden optie aangezien hier de rechten per afdeling meteen volledigere ingericht worden en als prettiger worden ervaren door de eindgebruikers. Een nadeel hieraan is wel dat het een langduriger proces kan zijn als niet alle functies en bijbehorende rechten al in kaart zijn gebracht.

8. Additionele connectors (terug naar HR?)

In deze stap is het belangrijk om te bepalen of de HR-applicatie nog informatie terug dient te ontvangen. Als we bijvoorbeeld kijken naar AFAS als voorbeeld, dan zijn de API-connectoren al

aanwezig om data terug te schrijven. Als de API-koppeling nog niet beschikbaar is staan er ook veel custom koppelingen op basis van PowerShell in de Github van HelloID (Tools4ever, 2021).

9. Preview test met 1 persoon per connector per lifecycle

In stap 9 worden de voorgaande stappen nogmaals getest. Belangrijk is om hier te controleren of een eventuele ingestelde connector bij stap 8 de data juist wegschrijft. Er kan gebruik gemaakt worden van dezelfde test persoon als in stap 6. Na deze stap wordt er gewerkt richting de livegang.

10. Scope tests uitbreiden, bijvoorbeeld 1 afdeling

De configuratie is nu zo ver om een grotere test uit te voeren. Namelijk 1 afdeling importeren.

11. Activeren thresholds en rules naar volledige scope

Een threshold is een drempel die ingesteld kan worden zodra de accounts tussen de gekoppelde systemen niet meer overeenkomen. Deze accounts worden in eerste instantie geblokkeerd bij de livegang en zijn terug te vinden in een rapport onder 'Entitlements'. Vervolgens kunnen de accounts alsnog geapproved worden of de informatie aangepast worden naar wens (Tools4ever, 2021).

12. Enforcement van volledige scope

De volledige thresholds zijn geactiveerd. De volgende stap is om de enforcement van de volledige scope uit te voeren. De volledige scope wordt hier nagelopen en enforced.

13. Doorvoeren van alle blocked entitlements

Aangezien de volledige scope nu is doorgelopen zijn er ongetwijfeld een aantal fouten, blocked entitlements. Dit zijn vaak fouten als rechten die nog niet helemaal goed staan, paden die nog niet bestaan of koppelingen die niet juist lopen.

14. Nazorg op restpunten bij uitvoeren van alle entitlements

Bij stap 14 worden bovenstaande punten als nazorg opgelost.

15. Import op scheduled zetten, livegang

Bij deze stap wordt de import schedule live gezet, dit betekent dat na deze schedule de omgeving live is.

16. Monitoring van de notificaties

De laatste stap is het monitoren van de notificaties die na de schedule naar voren komen.

Na de implementatie van de Provisioning kunnen de gewenste service automatiseringen ingericht worden. Hoe dit het beste gedaan kan worden wordt opgenomen in het hoofdstuk 14 Ontwerp.

Dagelijks beheer

Als bovenstaande implementatie stappen uit zijn gevoerd is de module Provisioning van HelloID geïmplementeerd. Er is een koppeling tussen het HR-systeem, de user accounts in het netwerk en eventuele andere applicaties of identiteit providers zoals AD. Door deze koppeling kunnen gebruikersaccounts automatisch aan worden gemaakt in de gekoppelde applicaties met de juiste rechten. Hierdoor is er op dit gebied geen dagelijks werk meer voor de IT-beheerders van PCI IT. Echter kunnen de koppeling een foutmelding geven of een proces niet juist doorlopen. Dit is dan ook waar het beheer uit bestaat. Het controleren van de logs en eventuele foutmeldingen.
Daarnaast kan er verder gekeken worden naar nieuwe ontwikkelingen of automatiseringen binnen HelloID (Tools4ever, 2022).

Kosten

De kosten om de implementatie uit te laten voeren door techneuten van HelloID dient nader onderzocht te worden.
De kosten voor cursussen om de implementatie zelf uit te voeren, API-koppelingen te maken en het dagelijks beheer zijn gratis te volgen.

De HelloID-modules kunnen afzonderlijk worden aangeschaft (Tools4ever, 2021) en de prijs wordt berekend per gebruiker per maand. Staffelkortingen zijn beschikbaar, hoe meer gebruikers hoe goedkoper de inkoopprijs wordt. De tool om de berekening te maken voor de kosten is terug te vinden op de website van Tools4ever.

De kosten voor de modules is per gebruiker vanaf 200 gebruikers:

Module	Prijs gebruiker p/m
Provisioning	€2,00
Service Automation	€1,14
Acces Management	€1,24
Totaal	€4,38

Tabel 11 Prijzen modules 200 gebruikers

De kosten voor de modules is per gebruiker vanaf 200 gebruikers:

Module	Prijs gebruiker p/m
Provisioning	€1,75
Service Automation	€1,00
Acces Management	€1,08
Totaal	€3,83

Tabel 12 Prijzen modules 400 gebruikers

De kosten voor de modules is per gebruiker vanaf 1000 gebruikers:

Module	Prijs gebruiker p/m
Provisioning	€1,31
Service Automation	€0,75
Acces Management	€0,81
Totaal	€2,87

Tabel 13 Prijzen modules 1000 gebruikers

12.3 Conclusie

Bij implementatie van HelloID moet worden bepaald van welke functionaliteiten gebruik gemaakt dient te worden. Dit bepaalt de impact en de duur van de implementatie. De doorlooptijd voor de implementatie van de module Provisioning kan rekening worden gehouden met 4,5 werkdag.
De impact voor de implementatie van deze module is afhankelijk van het aantal applicaties wat gekoppeld dient te worden en of deze applicatie vooraf te koppelen valt.
Als deze applicatie niet vooraf te koppelen is, wordt het maatwerk om de koppeling werkend te krijgen. In paragraaf 13.3 Voorbeeldklant wordt verder ingegaan op de vooraf gekoppelde applicaties.
Voor de overige modules is geen richtlijn te geven aangezien dit maatwerk is per omgeving of eindklant en haar wensen.

Het dagelijks beheer van HelloID is afhankelijk van de modules die worden geïmplementeerd. Veel werkprocessen kunnen worden geautomatiseerd, deze automatiseringen dienen beheerd te worden. Welke automatiseringen dit zijn is klant afhankelijk. Dit dient nader onderzocht te worden.

De verschillende modules en functionaliteiten van de modules zijn nu overzichtelijk. In Tabel 14 Module per must have system requirements worden de must have system requirements gekoppeld aan de beschikbare modules van HelloID.

S-ID	Requirement	Prioriteit	(Niet) Functioneel	HelloID module
S-01	Het product dient een koppeling te kunnen maken met meerdere applicaties door middel van een API-koppeling.	Must	Functioneel	Provisioning
S-02	Er dienen meerdere klanten gekoppeld te kunnen worden aan het product.	Must	Functioneel	Provisioning
S-03	Het product dient een koppeling te hebben met Azure Active Directory	Must	Functioneel	Provisioning
S-04	Het product moet een koppeling kunnen maken met Active Directory	Must	Functioneel	Provisioning
S-05	Het product moet, als er data opgeslagen wordt, data opslaan binnen de Europese Economische Ruimte (EER)	Must	Functioneel	*
S-06	Het product dient MFA te ondersteunen.	Must	Functioneel	Acces Management

Tabel 14 Module per must have system requirements

Uit bovenstaande tabel is te zien dat er gebruik gemaakt dient te worden van 2 modules om aan alle must have requirements te voldoen. Bij S-05 staat er een sterretje in de tabel, dit is aangezien hier geen module voor benodigd is. HelloID wordt gehost in Microsoft Azure en voldoet daarmee aan de eis om data op te slaan binnen de EER.
In Bijlage 9: Module per system requirements is een overzicht te zien van alle system requirements en welke module er benodigd is om te voldoen aan de system requirement. Hierin is te zien dat aan alle gestelde system requirements kan worden voldaan, als alle drie de modules ingezet worden.
De prijs om de implementatie van HelloID uit te laten voeren is dient nader onderzocht te worden. Om de implementatie zelf uit te voeren kunnen cursussen gratis worden gevolgd.

13. Deelvraag 7: Op welke manier kan PCI IT de life cycle managementoplossing het beste inzetten als self-service oplossing voor de klanten van PCI IT?

In dit hoofdstuk wordt er antwoord gegeven op deelvraag 7.

13.1 Gebruikte methodieken

In deze paragraaf wordt het proces om de deelvraag te beantwoorden beschreven.

Brainstormsessie

In een brainstormsessie met David Krabbenborg hebben we diverse onderwerpen besproken met de mogelijkheden om bepaalde diensten als self-service dienst aan te bieden.

Literatuurstudie

In publieke bronnen wordt er gekeken wat de mogelijkheden zijn om diensten als self-service aan te bieden.

13.2 Resultaten

In deze paragraaf worden de resultaten van bovenstaand proces om de deelvraag te beantwoorden uitgewerkt.

Brainstormsessie

In een brainstormsessie met David Krabbenborg is naar voren gekomen dat het wenselijk is om processen te automatiseren, maar dat hier niet de focus op ligt. Door alle ontwikkelingen rondom het Corona-virus is het grootste probleem momenteel dat er allerlei accounts rondzwerven over het internet en de IT-beheerders, maar ook de organisatie hier geen overzicht meer over heeft. Aangezien er geen overzicht is van de accounts, kan er ook niet gekeken worden naar de eventuele impact van een account dat blijft bestaan.

Wanneer al deze problemen opgelost zouden zijn, zou een volgende stap zijn om processen te automatiseren. Diensten die geautomatiseerd kunnen worden:

- aanvragen van gebruikersaccounts
- opheffen van gebruikersaccounts
- rechten toewijzen aan gebruikersaccounts
- applicaties toewijzen aan gebruikersaccounts

Literatuurstudie

In paragraaf 12.2 zijn de verschillende modules en de functionaliteiten benoemd van HelloID. De module ‘Service Automation’ beschikt over verschillende functionaliteiten die beschikbaar kunnen worden gesteld als self-service dienst.

Self-service diensten

Naast de gewenste automatiseringen, die in de brainstormsessie naar voren zijn gekomen, zijn in deze paragraaf een aantal adviezen gegeven over andere mogelijkheden die ook als self-service dienst ingezet kunnen worden. De volgende 7 functionaliteiten van HelloID zijn in te zetten als self-service dienst:

1. Aanvragen van gebruikersaccounts:
    - accounts aan laten vragen door eindgebruikers of klanten
    - accounts aan laten vragen door bevoegde gebruikers

Door de aanvragen van gebruikersaccounts, voor zowel eindklanten als interne medewerkers van PCI IT, via het producten portaal van HelloID te laten lopen is het mogelijk om deze aanvraag geautomatiseerd uit te voeren. Door dit te automatiseren verkort de doorlooptijd van de aanvraag en is er geen tussenkomst van een medewerker van PCI IT benodigd. Door middel van workflows wordt bepaald hoe de aanvraag verloopt, dit wordt verder uitgelegd in de paragraaf Workflows.

2. Wijzigen rechten van een gebruikersaccount (extra rechten toevoegen of rechten verminderen):
    - rechten voor een map
    - rechten voor een applicatie
    - toegang tot een account
    - toegang tot bepaalde postvakken
    - toegang tot Teams binnen Teams

Als de gebruikersaccounts aan zijn gemaakt kan het ook voorkomen dat gebruikers meer of minder rechten nodig hebben. Extra aanvragen voor mappen of applicaties kunnen worden gedaan door de gebruiker zelf. Vervolgens kan er toegang worden gegeven of tijdelijke toegang worden gegeven. Ook is het mogelijk om toegang te vragen tot een account of een postvak, ook hier is het mogelijk om toegang te geven of tijdelijke toegang.

3. Opheffen van gebruikersaccounts:
    - accounts opheffen zodra het contract van een medewerker verloopt

Bovenstaande benoemde aanvragen kunnen ook andersom werken, om het gebruikersaccount op te heffen. Dit kan bijvoorbeeld gekoppeld worden aan het contract van de medewerker. Als deze verloopt op een bepaalde datum is het mogelijk om door middel van HelloID het gebruikersaccount ook na deze datum te laten verlopen. Hiervoor is wel een koppeling met het HR-systeem nodig en dient de informatie in het HR-systeem verwerkt te zijn.

4. Aanpassen van gebruikersaccounts:
    - als een medewerker trouwt en de achternaam van zijn/haar man/vrouw neemt

Uiteraard zijn er ook wijzigingen te maken op de al aangemaakte accounts bijvoorbeeld door de naam aan te passen.

5. Beperken dat bepaalde informatie op de lokale apparaten van gebruikers komt:
    - verbieden dat persoonlijke documenten van een externe locatie wordt gedownload naar een device

Nu de cruciale informatie gekoppeld is, zoals contracten door middel van een gekoppeld HR-systeem, is het van belang dat de beveiliging ook aangescherpt wordt. Hiervoor kan er worden bepaald dat bepaalde gebruikers, devices of er vanaf bepaalde locaties geen bestanden kunnen gedownload.

6. Auditing & reporting:

Nu er overzicht is gecreëerd over welke accounts er allemaal bestaan en over welke rechten de accounts beschikken kunnen er rapporten worden afgedrukt. Door middel van deze rapporten is het mogelijk om een impact analyse te doen als een account wordt gehackt.
Door de functionaliteit Auditing & reporting wordt de system requirement S-16 behaald.

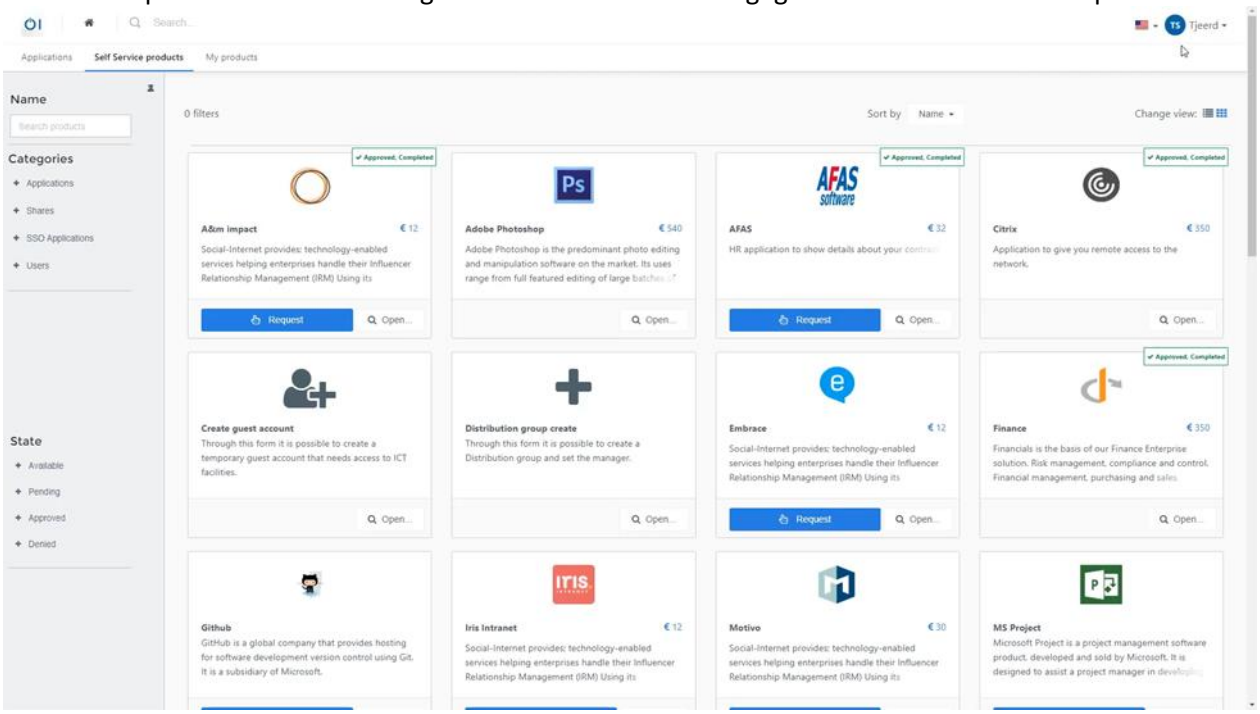
7. Workflows:
    - automatische goedkeuringen
    - zelf aan te passen goedkeuringen
    - personen aanwijzen voor goedkeuringen

Daarnaast zijn ook workflows te automatiseren. Hier kunnen zaken geregeld worden als automatische goedkeuringen, denk bijvoorbeeld aan een applicatie als Adobe. In paragraaf Workflows wordt hier verder op ingegaan.

Producten of diensten beschikbaar maken voor self-service

In paragraaf 12.2 Literatuurstudie is beschreven dat het met de module Service Automation mogelijk is om verschillende werkprocessen te automatiseren.

De eindgebruiker ziet na implementatie van het Self Service product een overzicht met de diensten en producten die beschikbaar zijn gesteld door de administrators. Dit kunnen applicaties zijn die worden gebruikt binnen de organisatie of diensten zoals een gebruiker aanmaken in de AD, een groep verwijderen van een gebruiker, wachtwoord resetten, toegang vragen tot een share en nog veel meer opties. In onderstaand figuur is een voorbeeld weergegeven van een self-service portaal:



Figuur 8 Self Service Products

In de portal van HelloID zijn deze producten of diensten aan te maken onder de tab ‘Self Service’ en vervolgens onder ‘Products’. Gegevens die meegegeven kunnen worden aan een product zijn zaken als: naam van het product, eigenaar of eigenaren van het product (Resource owner), hoe de route/workflow van de aanvraag gaat (zie hiervoor de volgende paragraaf Workflows), een formulier, omschrijving, prijs (optioneel), voor wie is de applicatie beschikbaar, maximale beschikbaarheid (denk aan licenties), risicofactor, afbeelding of icoon, categorie en welke agent pool de taak af dient te handelen.

Vervolgens zijn er nog acties die uitgevoerd kunnen worden als de aanvraag goed is gekeurd of als de gebruiker aangeeft de applicatie terug te willen geven. Een voorbeeld hiervan is een aanpassing doen aan de gebruiker in de AD zijn groepslidmaatschap. Als de AD gekoppeld is aan HelloID en toegang geregeld is via een AD-groep dan kan de aanvrager via een AD-groep lid worden gemaakt van de AD-groep. Daarnaast kan eraan worden gegeven wat er gedaan moet worden zodra de gebruiker

aangeeft de applicatie niet meer nodig te hebben. In dit geval zou dat dan zijn dat de gebruiker geen lid meer hoeft te zijn van de AD-groep. Het sturen van mails staat hier los van, dit is al in de workflow opgenomen.

De volgende stap is het toewijzen van de groepen die toegang hebben om de applicatie of dienst aan te vragen. Dit kunnen groepen zijn vanuit HelloID, vanuit de AD of andere systemen die gekoppeld zijn en waarvan de groepen zijn gesynchroniseerd.

Bij de vierde stap kunnen tijdlimieten worden gegeven aan de applicatie of dienst. Als de instelling voor 'limit type' op 'fixed duration' wordt gezet kan er een tijd worden aangegeven waarop de applicatie maximaal beschikbaar is. De eindgebruiker kan vervolgens aangeven voor hoeveel dagen hij of zij de applicatie wil gebruiken. Vervolgens ziet de manager, die goedkeuring dient te geven voor de aanvraag, de volledige aanvraag inclusief het aangevraagde aantal dagen. De manager kan dit goedkeuren of toegang geven voor een ander aantal dagen dan aangevraagd. Er kan ook gekozen om de tijdlimiet van de applicatie uit te zetten, dan is de applicatie voor altijd toegankelijk voor de aanvrager.

Tot slot is er de optie 'Segregation' die kan worden ingezet als applicaties met elkaar conflicteren (Tools4ever, 2021).

Workflows

Workflows worden in HelloID gezien als routes die afgelegd dienen te worden voordat iets goedgekeurd kan worden.
Een standaard route die beschikbaar is, is goedkeuring door de 'Resource owner'. In de vorige paragraaf is de eigenaar van het product beschreven tussen de opties voor het aanmaken van een product. Als iemand uit de groep 'Resource owner' goedkeuring geeft, is de aanvraag goedgekeurd. Een andere mogelijkheid is een workflow te maken waar meerdere groepen goedkeuring dienen te geven. Daarnaast is er nog de optie om aan te geven dat beide groepen goedkeuring dienen te geven, of één van beide partijen.
Naast het gebruiken van deze groepen kan er ook een 'custom filter' aangemaakt worden, waar vele opties mogelijk zijn.
Als je een 'instant approval' workflow wil maken, een workflow die geen goedkeuring nodig heeft maar direct wordt goedgekeurd, kun je de optie 'Specify approvers' uit vinken. Op deze manier hoeft er geen goedkeuring gegeven te worden (Tools4ever, 2021).

13.3 Voorbeeldklant

Na kort telefonisch contact te hebben gehad met Sander Vosman is er een lijst met applicaties naar voren gekomen die veel gebruikt worden bij verschillende klanten en applicaties die wel eens voorkomen.

De applicaties die hoofdzakelijk gebruikt worden bij verschillende klanten:
Office365, Dynamics365, AFAS online, Exact online

Applicaties die soms voorkomen bij verschillende klanten:
ADP, Ecaris, Nedap, Topdesk, Cobra, Scansys, Swift-Syntess, NotisOne, SAP, King, Unit4, Cura, Youforce

Bovenstaande lijst is te vergelijken met de lijst met applicaties die al ondersteund worden door Tools4ever en daardoor direct te koppelen zijn, deze lijst is terug te vinden op de website van Tools4ever (Tools4ever, 2021).

Applicaties met beschikbare koppeling

De volgende veel voorkomende applicaties zijn al gekoppeld door Tools4ever (Tools4ever, 2021): Office365, AFAS (zowel Profit als online) en Exact.

De volgende applicaties die soms voorkomen bij verschillende klanten zijn al gekoppeld door Tools4ever: ADP (Perman, Workforce en PION), Ecaris, Nedap, Topdesk (inclusief integratie met ticketsysteem automatisch tickets aanmaken e.d., zie DEMO), Cobra, SAP, Unit4 (Personeel, Cura ECD & Cura Rooster) en Youforce.

Voor een aantal applicaties is het mogelijk om een uitgebreidere koppeling te maken dan alleen provisioning van gebruikersaccounts. Een voorbeeld hiervan is TopDesk. Binnen TopDesk kunnen automatisch tickets aan worden gemaakt en gesloten op basis van aanvragen die worden gedaan in de Self Service Portal binnen HelloID. Voor een lijst met alle mogelijkheden voor TopDesk zie de website van Tools4ever (Tools4ever, 2021).

De overige applicaties waar een uitgebreidere koppelingen voor mogelijk is, zijn de applicaties die een onderliggende link bevatten op de pagina van Tools4ever (Tools4ever, 2021).

Applicaties zonder beschikbare koppeling

De volgende veel voorkomende applicatie is nog niet gekoppeld door Tools4ever: Dynamics365.
De volgende applicaties die soms voorkomen bij verschillende klanten zijn nog niet gekoppeld door Tools4ever: Scansys, Swift-Syntess, NotisOne en King.
Applicaties die nog niet gekoppeld zijn kunnen niet direct gekoppeld worden aan HelloID door een bestaande koppeling. Dit betekent echter niet dat de applicatie niet te koppelen is. Applicaties die niet beschikken over een standaard koppeling kunnen worden gekoppeld door een generieke koppeling op basis van CSV, ODBC, tekstbestanden, SOAP/XML en webservices.
Daarnaast is er custom scripting beschikbaar op basis van PowerShell of andere scripting diensten en zijn al bestaande scripts beschikbaar op de github van Tools4ever (Tools4ever, 2021).

13.4 Conclusie

Zoals in Deelvraag 5: Hoe valt een dergelijke dienst als MSP in te zetten? vermeld dient elke klant een eigen tenant te krijgen binnen HelloID. Hierdoor kan PCI IT klant specifieke processen automatiseren door de functionaliteiten van HelloID als product aan te bieden in het Self Service portaal.
Producten of diensten die beschikbaar kunnen worden gesteld in de Self Service portal van HelloID zijn:

- Aanvragen voor gebruikersaccounts
- Wijzigingen voor gebruikersaccounts
- Toegang tot groepen (afhankelijk van de gekoppelde systemen)
- Toegang tot applicaties
- Verzoek voor toegang tot andere gebruikersaccounts
- Opheffen van gebruikersaccounts
- Auditing reports

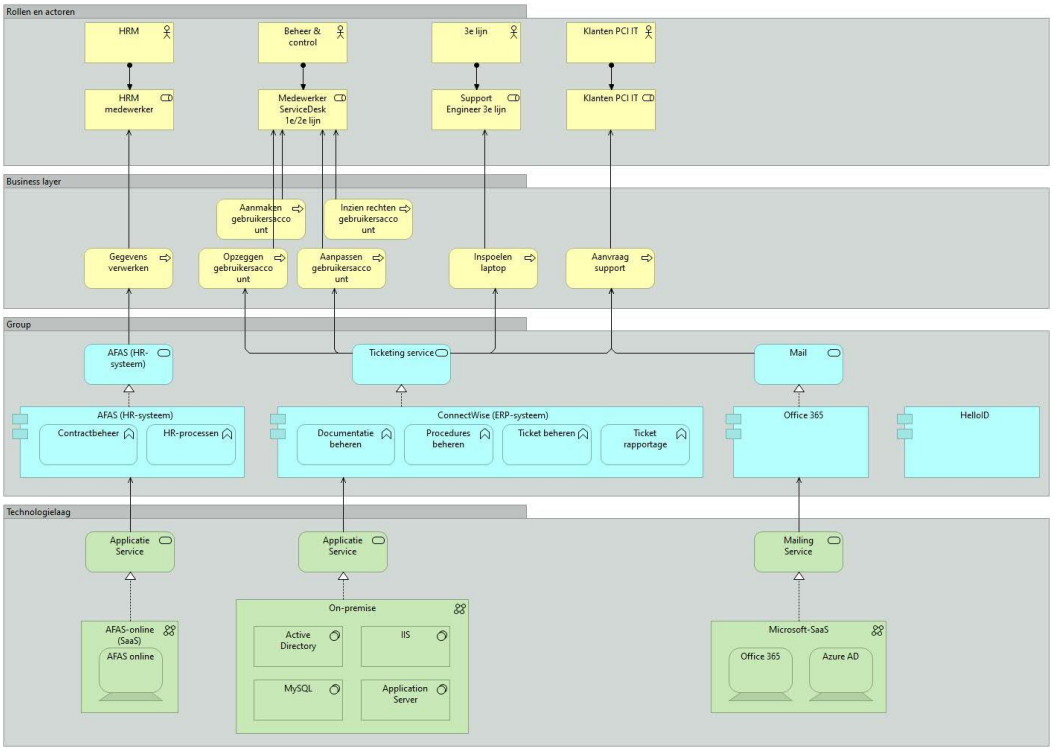
Op deze manier kunnen eindgebruikers diensten of producten zelf aanvragen zonder tussenkomst van een medewerker van de Servicedesk van PCI IT.

Het integratie traject om deze diensten als product aan te bieden vergt maatwerk per eindklant. De exacte duur voor de implementatie van de module Service Automation dient verder onderzocht te worden.

14. Ontwerp

14.1 Huidige situatie

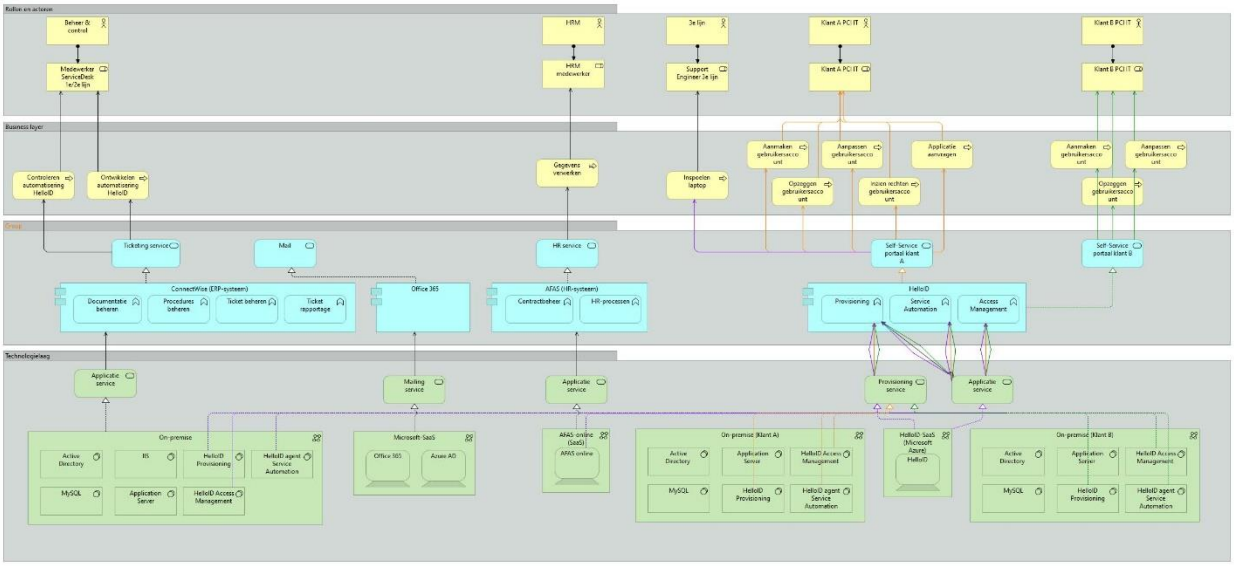
In onderstaande afbeelding is een Archimate tekening te zien die een overzicht biedt van de werkzaamheden van de engineers, ook biedt het de bijbehorende applicaties en infrastructuur delen die PCI IT nodig heeft voor het uitvoeren van de processen. Een uitvergrote versie van de Archimate tekening is terug te vinden in bijlage Bijlage 6: Archimate tekening huidige omgeving.



Figuur 9 Huidige infrastructuur PCI IT

14.2 Toekomstige situatie

In onderstaande afbeelding is een Archimate tekening te zien die een overzicht biedt wat voor werkzaamheden, applicaties en processen er veranderen bij een implementatie van HelloID binnen de huidige omgeving.
Om de veranderingen en verschillen tussen de omgevingen aan te geven is gebruik gemaakt van verschillende kleuren pijlen. De zwarte pijlen zijn niet gewijzigde connecties.
De paarse pijlen tonen de verbindingen tussen de processen, applicaties en infrastructuur van PCI IT.
De groene pijlen tonen de verbindingen van een voorbeeldklant (B) met andere processen dan de andere voorbeeldklant (A). De oranje pijlen tonen de verbindingen voor voorbeeldklant A.
Waar in Figuur 9 Huidige infrastructuur PCI IT de aanvragen en wijzigingen van gebruikersaccounts allemaal via de ServiceDesk diende te lopen, kunnen de aanvragen nu direct via HelloID lopen. Een uitvergrote versie van de Archimate tekening is terug te vinden in bijlage Bijlage 7: Archimate tekening omgeving met HelloID.



Figuur 10 Infrastructuur na implementatie HelloID

14.3 Authenticatie

In deze paragraaf wordt uitgelegd hoe een eindgebruiker, zowel intern bij PCI IT als gebruiker of een eindklant, zich kan authenticeren bij HelloID.

Access management

Door gebruik te maken van de module Access Management kunnen applicaties worden toegevoegd aan de portal van HelloID (Tools4ever, 2021). Alle applicaties kunnen in één overzicht worden weergegeven.
HelloID zorgt met deze module voor een schil om de huidige applicatie heen waardoor het mogelijk is om eigen authenticatie te gebruiken voor deze applicaties. Daarnaast zijn instellingen om gebruik te maken van MFA op verschillende manieren (hard- en software tokens) en SSO mogelijk. De werking van SSO wordt verder toegelicht in de paragraaf SSO.

Identity Provider (IdP)

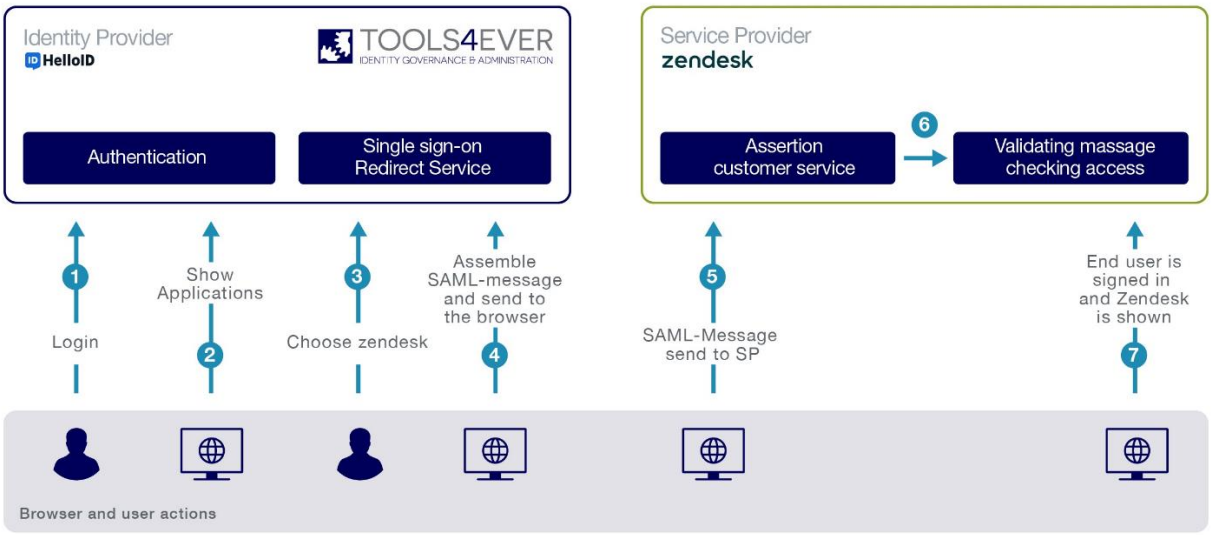
Een Identiteit Provider zorgt voor authenticatie in HelloID vanaf een extern systeem, zoals Microsoft Active Directory (Tools4ever, 2021). Door gebruik te maken van Microsoft Active Directory IdP kunnen ook synchronisatietaken worden geactiveerd voor het synchroniseren van groepen en gebruikers.

HelloID is te koppelen met verschillende Identity Providers zoals on-premises Active Directory, Azure AD, Active Directory Federation Services, Google G Suite, Salesforce en VMWare Workspace ONE (Tools4ever, 2021).
De authenticatie methode kan op verschillende manieren, bijvoorbeeld door gebruik te maken van SAML (Tools4ever, 2021) of OIDC (Tools4ever, 2021). De werking van SAML is uitgelegd in paragraaf SAML.

SAML

Security Assertion Markup Language (SAML) is één van de meest gebruikte standaarden voor het uitwisselen van authenticatiegegevens. SAML maakt veilige Single Sign-on mogelijk. SAML is de standaard voor veel Federated Identity Mangement oplossingen (FIM). FIM is een concept waarbij authenticatieoplossingen organisatie overschrijdend kan worden gebruikt. Andere voorbeelden zijn OpenID en OAuth.

SAML maakt gebruik van SAML-providers. Een SAML-provider is elke server die betrokken is bij de verificatie en autorisatie van een gebruiker tijdens een SAML-aanvraag. Er zijn twee typen SAML-providers: serviceproviders (SP) en identiteitsproviders (IdP). In onderstaande afbeelding is de werking visueel weergegeven, onder de afbeelding worden de stappen verder toegelicht.

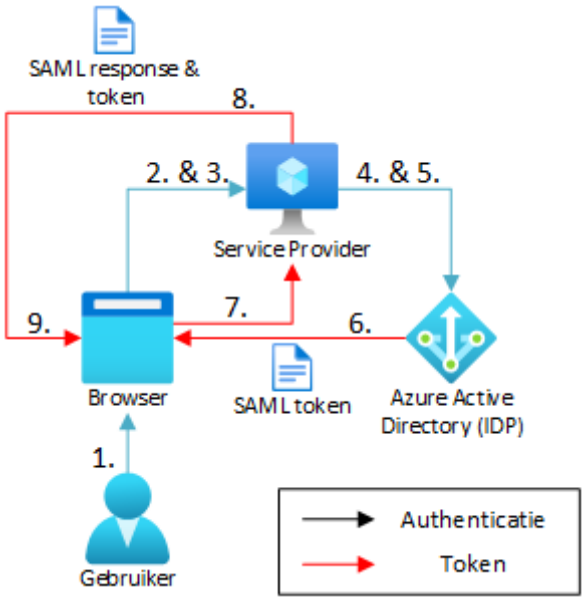


Figuur 11 Authenticatie door middel van SAML bij een 3-th party app

1. gebruiker logt in op de website van HelloID (IdP) met een gebruikersnaam en wachtwoord of andere authenticatie methode
2. vervolgens is de gebruiker ingelogd in de HelloID en worden de gekoppelde applicaties getoond
3. de gebruiker klikt op een van de beschikbare applicaties, in het voorbeeld wordt er gekozen voor Zendesk
4. de IdP maakt een SAML-bericht aan om authenticatie uit te voeren bij Zendesk. De IdP ondertekent en versleutelt het bericht door middel van een certificaat
5. het SAML-bericht wordt verstuurd naar Zendesk
6. Zendesk verifieert het SAML-bericht aan de hand van een certificaat en controleert de toegang
7. gebruiker is zonder tussenkomst van een inlogpagina ingelogd bij Zendesk.

SSO

In onderstaande afbeelding wordt getoond hoe een SSO-authenticatie verloopt, onder de afbeelding worden de stappen verder toegelicht.



Figuur 12 Authenticatie via SSO

1. gebruiker opent browser
2. gebruiker zoekt naar de gewenste applicatie (bijvoorbeeld AFAS Online)
3. gebruiker doet een verzoek voor toegang bij de Service Provider (SP) bijvoorbeeld AFAS Online
4. er wordt een SAML-authenticatie verzoek gemaakt en naar de Active Directory (Identity Provider, IDP) gestuurd
5. de gebruiker authenticeert zich bij de Active Directory met zijn SAML-token (XML-file)
6. de SAML-aanvraag wordt weer teruggestuurd naar de browser
7. SAML-token wordt verstuurd naar de SP
8. de SP valideert de SAML-token en krijgt een en krijgt een response mee dat het geaccepteerd is
9. de gebruiker is nu geauthenticeerd en krijgt de beveiligde pagina te zien (Peyrott, 2022).

15. Conclusie & aanbevelingen

In dit onderzoek is gezocht naar een antwoord op de vraag: **In hoeverre kan PCI IT de life cycle van gebruikersaccounts in omgevingen die bestaan uit een mix van Saas, Paas, IaaS, private cloud en on-premise op een eenvoudigere en minder foutgevoelige wijze beheren en aanbieden aan haar klanten?** Om een antwoord op deze vraag te realiseren is een onderzoek op basis van 7 deelvragen uitgevoerd.

Om tot een passende oplossing te komen voor PCI IT is er gekeken naar de huidige situatie van de life cycle van gebruikersaccounts. Hierin is naar voren gekomen dat de processen handmatig uitgevoerd worden en hierdoor een lange doorlooptijd hebben. Naast het probleem van de lange doorlooptijd zijn de processen foutgevoelig door de handmatige uitvoering, blijven de accounts in verschillende omgevingen langdurig bestaan en is er geen overzicht van de rechtenstructuur over de verschillende accounts.
Uit bovenstaande knelpunten zijn 16 system requirements en zeven business requirements opgesteld. Met deze eisen en wensen is er gekeken naar een passende softwareapplicatie voor PCI IT. Door middel van een multicriteria-analyse is het softwarepakket HelloID gekozen als beste oplossing.
HelloID beschikt over drie verschillende modules die tezamen aan alle eisen en wensen van PCI IT voldoen. Provisioning is de module waarmee verbinding gemaakt kan worden met source systemen en target systemen. Naast de mogelijkheid om applicaties te koppelen, kunnen er business rules worden toepast. Met deze module kunnen personen gekoppeld worden aan accounts en is er meer grip op de gebruikersaccounts in verschillende omgevingen.
Om de life cycle van gebruikersaccounts minder foutgevoelig en efficiënter in te richten, is gekeken naar de mogelijkheid om processen te automatiseren. Hiervoor is de module Service Automation beschikbaar. Door de module Service Automation in te zetten is het mogelijk om producten en diensten te koppelen aan een Self-service portaal, waar eindgebruikers zelf producten en diensten aan kunnen vragen. Op deze wijze kunnen de aanvragen direct worden aangemaakt en automatische doorgang vinden. Hierdoor is het proces minder foutgevoelig en efficiënter.
Naast deze twee modules is de module Access Management beschikbaar. Deze module maakt het mogelijk om MFA op verschillende manieren als authenticatie methode toe te voegen aan de loginprocedure. Daarnaast biedt Access Management de mogelijkheid om SSO te activeren voor de gekoppelde applicaties binnen HelloID.
Voor implementatie van het softwarepakket HelloID, zijn gratis cursussen beschikbaar bij Tools4ever, de softwareleverancier van HelloID. Daarnaast zijn gratis cursussen beschikbaar voor het dagelijks beheer en de werking van API-koppelingen van HelloID.
De uitvoering van de implementatie kan worden gedaan door een medewerker van Tools4ever of door PCI IT zelf, na het volgen van de cursus. Implementatie van de module Provisioning is naar verwachting te realiseren binnen vier en een halve werkdag. De implementatie duur van de overige modules dient nader onderzocht te worden.
De prijs voor alle drie de modules op basis van 500 gebruikers, is €3,56 per gebruiker per maand.
Voordat de implementatie van HelloID plaats kan vinden, is de aan te raden om met Tools4ever een demo te plannen en het ontwerp door te spreken. Er dient kritisch gekeken te worden naar hoe meerdere klanten te koppelen zijn aan HelloID en welke applicaties beschikbaar zijn voor een koppeling. Daarnaast dient er gekeken te worden of automatiseringen en workflows te gebruiken of te kopiëren zijn voor meerdere klanten waardoor de implementatie efficiënter kan worden uitgevoerd voor verschillende klanten.

Bibliografie

American Psychological Association. (2021). *APA*. Opgehaald van APA: https://www.apa.org/

Auth0. (2021, November 15). *Access Management*. Opgehaald van auth0.com: https://auth0.com/access-management

BeyondTrust. (2021, November 25). *The Forrester Wave™: Privileged Identity Management, Q4 2020*. Opgehaald van beyondtrust.com: https://www.beyondtrust.com/forrester-wave-privileged-identity-management

Bureau Tromp. (2021). *Een proces verbeteren dankzij een SIPOC*. Opgehaald van bureautromp: https://bureautromp.nl/wat-is-sipoc/

Bureautromp. (2021). *Stakeholdersanalyse*. Opgehaald van https://bureautromp.nl/stakeholderanalyse/: https://bureautromp.nl/stakeholderanalyse/

Centrify. (2021, November 11). *Authentication Service*. Opgehaald van Centrify.com: https://www.centrify.com/pam/server-suite/authentication-service/

Citrix. (2021). *What is a desktop as a service (DaaS)?* Opgehaald van citrix.com: https://www.citrix.com/nl-nl/solutions/vdi-and-daas/what-is-desktop-as-a-service-daas.html

Citrix. (2021, Oktober). *What is single sign-on (SSO)?* Opgehaald van citrix.com: https://www.citrix.com/nl-nl/solutions/secure-access/what-is-single-sign-on-sso.html

cloudaware. (2021, November). *CloudTrial+*. Opgehaald van cloudaware: https://www.cloudaware.com/

Computable. (2021). *Requirementsanalyse: het einde van de informatieanalyse?* Opgehaald van Computable: https://www.computable.nl/artikel/opinie/business-analytics/2564400/1509029/requirementsanalyse-het-einde-van-de-informatieanalyse.html

Cyberark. (2021, December). *access management*. Opgehaald van cyberark.com: https://www.cyberark.com/products/access-management/

Dynamicsonline. (2021, September). *Wat is on-premise en wat is de cloud?* Opgehaald van dynamicsonline.nl: https://www.dynamicsonline.nl/erp-software/wat-is-on-premise-en-wat-is-de-cloud/

Fahad, F. (2021, September 14). *De probleemanalyse van je scriptie*. Opgehaald van 24editor: https://24editor.com/de-probleemanalyse-van-je-scriptie

Foeke van der Zee. (2021). *Deskresearch*. Opgehaald van Hulbijonderzoek: https://hulpbijonderzoek.nl/online-woordenboek/begrippen/deskresearch/

ForgeRock. (2021, November). *ForgeRock Acces Management*. Opgehaald van forgerock.com: https://www.forgerock.com/platform/access-management

G2. (2021, November 20). *Best User Provisioning and Governance Tools*. Opgehaald van g2.com: https://www.g2.com/categories/user-provisioning-and-governance-tools

Gartner. (2021, November 1). *Magic Quadrant for Access Management*. Opgehaald van Gartner: https://www.gartner.com/doc/reprints?id=1-27UNLMJO&ct=211103&st=sb

IAM Accelerators. (2021, November). Opgehaald van ilantus.com: https://www.ilantus.com/iam-accelerators/

IBM. (2021, November). *Workforce identity access management*. Opgehaald van ibm.com: https://www.ibm.com/nl-en/products/verify-saas/workforce-iam

jumpcloud. (2021, November). *User Management*. Opgehaald van jumpcloud.com: https://jumpcloud.com/platform/user-management

KPN. (2021). *Wat is public cloud?* Opgehaald van https://www.kpn.com/zakelijk/blog/private-cloud-vs-public-cloud-dit-moet-je-weten.htm#:~:text=De%20publieke%20cloud%20is%20de,resources%20beschikbaar%20aan%20het%20publiek.&text=In%20principe%20kan%20elk%20bedrijf,in%20al%20zijn%20computerbehoeften%20voor

ManageEngine. (2021, November). *M365 Manager Plus*. Opgehaald van manageengine.com: https://www.manageengine.com/nl/microsoft-365-management-reporting/

Marketingscriptie. (2021). *Vijkrachten model van porter*. Opgehaald van www.marketingscriptie.nl: https://www.marketingscriptie.nl/vijfkrachtenmodel-van-porter/

Microfocus. (2021, December). *NetIQ Identity and Access Management*. Opgehaald van microfocus.com: https://www.microfocus.com/en-us/cyberres/identity-access-management

Microsoft. (2021, December). *Identiteits- en toegangsbeheer (IAM)*. Opgehaald van azure.microsoft.com: https://azure.microsoft.com/nl-nl/product-categories/identity/

Microsoft. (2021). *Microsoft identity platform en OpenID-Verbinding maken protocol*. Opgehaald van docs.microsoft.com: https://docs.microsoft.com/nl-nl/azure/active-directory/develop/v2-protocols-oidc

Microsoft. (2021). *On-premises AD-domeinen integreren met Azure AD*. Opgehaald van https://docs.microsoft.com: https://docs.microsoft.com/nl-nl/azure/architecture/reference-architectures/identity/azure-ad

Microsoft. (2021). *Wat is IaaS?* Opgehaald van azure.microsoft.com: https://azure.microsoft.com/nl-nl/overview/what-is-iaas/#overview

Microsoft. (2021). *Wat is PaaS?* Opgehaald van azure.microsoft.com: https://azure.microsoft.com/nl-nl/overview/what-is-paas/

Microsoft. (2021). *Wat zijn hybride, openbare en privéclouds?* Opgehaald van azure.microsoft.com: https://azure.microsoft.com/nl-nl/overview/what-are-private-public-hybrid-clouds/#overview

Microsoft. (2021, 9 20). *What is Azure Active Directory?* Opgehaald van docs.microsoft.com: https://docs.microsoft.com/nl-nl/azure/active-directory/fundamentals/active-directory-whatis

Movements. (2021). *API koppeling ontwikkelen voor meer efficiëntie*. Opgehaald van Movements: https://www.movements.nl/blogs/api?gclid=Cj0KCQiAnaeNBhCUARIsABEee8V7t4rET40wsLz5rUVTxLmreWmDBSSsr2sOKwrVb8g_rt8CqoeStD4aAkVHEALw_wcB

NEN. (2021). *Informatiebeveiliging ISO 27001*. Opgehaald van NEN: https://www.nen.nl/ict/digitale-ehtiek-en-veiligheid/cyber-privacy/informatiebeveiliging

NEN. (2021). *Kwaliteitsmanagement ISO 9001*. Opgehaald van NEN: https://www.nen.nl/managementsystemen/kwaliteitsmanagement-iso-9001

Okta. (2021, November 22). *Customer Identity*. Opgehaald van Okta.com: https://www.okta.com/nl/customer-identity/

Okta. (2021). *Whats the difference between oauth openid connect and saml*. Opgehaald van okta: https://www.okta.com/nl/identity-101/whats-the-difference-between-oauth-openid-connect-and-saml/

Omada. (2021, November 9). *Omada Identity Cloud*. Opgehaald van omadaidentity.com: https://omadaidentity.com/products/omada-identity-cloud/

Oneidentity. (2021, November 2). *Identity Governance and Administration*. Opgehaald van oneidentity.com: https://www.oneidentity.com/identity-governance-and-administration/

optimadata. (2021). *DBaaS*. Opgehaald van optimadata.nl: https://www.optimadata.nl/DBaaS-advies-beheer-performance-database-health-check-quick-scan-consultant

Oracle. (2021, December 1). *Identity and Access Management (IAM)*. Opgehaald van oracle.com: https://www.oracle.com/nl/security/identity-management/

Panthera. (2021). *Wat is active directory en hoe werkt het?* Opgehaald van https://www.panthera.nl/nieuws/active-directory

Peyrott, S. (2022, Januari 6). *What is and how does single sign on work*. Opgehaald van auth0: https://auth0.com/blog/what-is-and-how-does-single-sign-on-work/

SailPoint. (2021, November 5). *Lifecycle Management*. Opgehaald van sailpoint.com: https://www.sailpoint.com/platform/lifecycle-management/

Salesforce. (2021). *Wat is SaaS?* Opgehaald van Salesforce.com: https://www.salesforce.com/nl/learning-centre/tech/saas/

Secureauth. (2021, December). *User lifecycle management*. Opgehaald van secureauth.com: https://www.secureauth.com/identity-access-management/user-lifecycle-management/

Sigma solutions. (2021). *Hoe werkt oath 2.0*. Opgehaald van Sigmasolutions: https://sigmasolutions.nl/blog/hoe-werkt-oauth-2.0/

Tools4ever. (2021, December). *Applicatie koppelingen*. Opgehaald van tools4ever.nl: https://www.tools4ever.nl/software/iam-identity-and-access-management-software/koppelingen/

Tools4ever. (2021). *Configure Azure AD as a SAML IdP*. Opgehaald van docs.helloid.com: https://docs.helloid.com/hc/en-us/articles/115002873353-Configure-Azure-AD-as-a-SAML-IdP

Tools4ever. (2021, Januari). *Configure Azure AD as an OIDC IdP*. Opgehaald van docs.helloid.com: https://docs.helloid.com/hc/en-us/articles/360013152200-Configure-Azure-AD-as-an-OIDC-IdP

Tools4ever. (2021, December). *Forum HelloID*. Opgehaald van forum.helloid.com: https://forum.helloid.com/

Tools4ever. (2021, December). *Github Tools4ever*. Opgehaald van github.com: https://github.com/Tools4everBV

Tools4ever. (2021). *HelloID IDaaS Cloud Single Sign On*. Opgehaald van tools4ever.nl: https://www.tools4ever.nl/software/helloid-idaas-cloud-single-sign-on/

Tools4ever. (2021). *HelloID Modules en Prijzen*. Opgehaald van tools4ever.nl: https://www.tools4ever.nl/helloid-modules-prijzen/

Tools4ever. (2021). *HelloID Provisioning: Correlatie*. Opgehaald van Youtube: https://www.youtube.com/watch?v=VFiYT2IGHrc

Tools4ever. (2021, December). *HelloID Provisioning: Implementatie Stappenplan*. Opgehaald van Youtube.com: https://www.youtube.com/watch?v=r7W3Xwd91vc&t=1s

Tools4ever. (2021). *HelloID Provisioning: Thresholds*. Opgehaald van Youtube: https://www.youtube.com/watch?v=cWYk7v6LETI

Tools4ever. (2021). *HelloID Security White Paper*. Opgehaald van tools4ever.com: https://az781118.vo.msecnd.net/cdn/9453a4ab78994f8e8692b2610361bd6d/d3fae5ec0426459c9298daea82df6ee4.pdf

Tools4ever. (2021). *HelloID Service Automation: Product Tegels*. Opgehaald van youtube: https://www.youtube.com/watch?v=goM5mTr4GCQ&list=PL-WJuj4MR3wyo4w1I3p9J6CSw252bBsSl&index=3

Tools4ever. (2021). *HelloID Service Automation: Workflows*. Opgehaald van https://www.youtube.com/watch?v=pvxY6K_Kl9s&list=PL-WJuj4MR3wyo4w1I3p9J6CSw252bBsSl&index=4

Tools4ever. (2021). *HelloID: Agent Setup*. Opgehaald van youtube: https://www.youtube.com/watch?v=-ZH7IJAHbx8

Tools4ever. (2021). *HelloID: Integreer je Active Directory*. Opgehaald van youtube: https://www.youtube.com/watch?v=ZwFQmAQLdWw

Tools4ever. (2021). *Identiteitsproviders - Overzicht*. Opgehaald van docs.helloid.com: https://docs.helloid.com/hc/en-us/articles/360014962633-Identity-Providers-Overview

Tools4ever. (2021, December). *Identity Governance*. Opgehaald van tools4ever.nl: https://www.tools4ever.nl/

Tools4ever. (2021). *Identity Provider Guiders*. Opgehaald van docs.helloid.com: https://docs.helloid.com/hc/en-us/sections/360003225313-Identity-Provider-Guides

Tools4ever. (2021, December). *Koppeling met Topdesk Enterprise*. Opgehaald van tools4ever.nl: https://www.tools4ever.nl/software/iam-identity-and-access-management-software/koppelingen/topdesk-enterprise/

Tools4ever. (2021). *Wat is mfa*. Opgehaald van Tools4ever: https://www.tools4ever.nl/wat-is-mfa/

Tools4ever. (2021, December). *youtube*. Opgehaald van Youtube.com: https://www.youtube.com/channel/UCikuulAZUvAdvmfDIm1It-Q/videos

Tools4ever. (2022, januari). *HelloID IDaaS Cloud Single Sign On*. Opgehaald van tools4ever.nl: https://www.tools4ever.nl/software/helloid-idaas-cloud-single-sign-on/#serviceautomation

Tools4ever. (sd). *Wat is saml en hoe werkt het*. Opgehaald van tools4ever: https://www.tools4ever.nl/wat-is-saml-en-hoe-werkt-het/

Toolshero. (2021, September). *Multicriteria analyse (MCA)*. Opgehaald van Toolshero: https://www.toolshero.nl/besluitvorming/multicriteria-analyse-mca/

TUV Nederland. (2021). *ISO 20000 certificering*. Opgehaald van TUV Nederland: https://www.tuv.nl/nl/diensten/certificering/iso-certificering/iso-20000-certificering/

TUV Nederland. (2021). *Wat is ISO 9001 certificering*. Opgehaald van TUV Nederland: https://www.tuv.nl/nl/iso-9001/wat-is-iso-9001-certificering/

TUV Nederland. (2021). *Wat is NEN 7510*. Opgehaald van TUV Nederland: https://www.tuv.nl/nen-7510/wat-is-nen-7510/

TUV Nederland. (sd). *Wat is ISO 270001*. Opgehaald van TUV Nederland: https://www.tuv.nl/nl/iso-27001/wat-is-iso-27001/

Vliet, H. v. (2021, September). *MoSCoW-methode*. Opgehaald van Wikipedia: https://nl.wikipedia.org/wiki/MoSCoW-methode

Wat is Design Thinking? (2021). Opgehaald van Leansixsigmagroep: https://leansixsigmagroep.nl/lean-agile-en-six-sigma/design-thinking/

Bijlage 1: Samenvatting interviews

Interview met Annemiek Meulenkamp - HRM

Het interview met Annemiek was mijn eerste interview. Annemiek is medewerker van de afdeling Human Resource Management. Hetgeen wat ik met Annemiek heb besproken ging veelal over de processen en wat voor stappen HRM in het proces van aanvragen/opzeggen van gebruikersaccount uitvoert.

Naast dat de processen me erg duidelijk zijn uitgelegd zijn een aantal dingen me erg bijgebleven uit het interview. Namelijk dat er redelijk wat frustratie zit bij HRM richting de medewerkers en managers over de aanvragen van gebruikersaccounts. De aanvragen worden vaak last minute gedaan waardoor er veel geregeld moet worden in korte periode. Dit zorgt bij iedereen tot frustratie. Daarnaast worden de checklists voor in-uitdienst treding vaak niet correct of volledig ingevuld.

Interview met Bart Brevink - Technical Field Service Manager

Het interview met Bart Brevink was de 2de interview. Ik had iets meer inzicht in de processen binnen de organisatie en had een beter beeld bij de loop van het proces. Met Bart heb ik vooral gesproken over de verschillende type klanten en de mogelijkheden binnen PCI ITmet een dergelijk pakket.

Bart gaf vrij snel aan inhoudelijk niet betrokken te zijn bij het proces voor het aanmaken en opzeggen van gebruikersaccounts of dingen die hierbij komen kijken. Hij is wel verantwoordelijk voor het portfolio van PCI IT, hier zijn we dan ook voornamelijk op ingegaan. We hebben gekeken naar de visie qua producten van PCI IT en de klanten die PCI IT heeft. Bij de klanten heb ik een beter beeld gekregen naar de exacte diensten die PCI IT levert bij haar verschillende klanten en op wat voor manier dit geleverd wordt.

Er zijn namelijk 3 type klanten;

1. Klanten die hun volledige IT afnemen bij PCI IT. Dit houdt in dat PCI IT de klant volledig ontzorgt op IT-gebied. Het inrichten tot en met beheren is de verantwoordelijkheid van PCI IT. Ook gebruikersvragen komen bij de Servicedesk van PCI IT binnen. Dit houdt in dat PCI IT ook haar producten in kan zetten waar nodig.
2. Klanten die gebruik maken van een soort hybride ondersteuning. Met een hybride ondersteuning wordt er af en toe gebruik gemaakt van de expertise van PCI IT, denk hierbij aan één keer per week een 3e lijn engineer op locatie voor diverse vraagstukken. Of de gehele infrastructuur is ingericht voor de klant verschilt per klant.
3. Ondersteuning op projectbasis. Daarnaast is er de 3de mogelijkheid en dat is om de expertise van PCI IT in te huren voor een project. Denk bijvoorbeeld aan een upgrade van VMWare van versie 5 naar 6, aangezien dit bijna wekelijks werk is voor PCI IT gaat een dergelijke upgrade veel sneller en is de kennis niet bij elke klant in huis.

Interview met Olaf Kornegoor - Servicedesk Teamleider

Het interview met Olaf Kornegoor was de 3de interview. Olaf is teamleider van de Servicedesk. In het interview ging het al vrij snel over de knelpunten die HRM ook benoemde, hier zijn al gesprekken over gevoerd (met Servicedesk en HRM) hoe dit te optimaliseren valt. Knelpunten die zoal naar voren kwamen;

1. Aanvragen voor gebruikersaccounts komen erg laat binnen
2. Onduidelijk is waar de nieuwe medewerker gaat beginnen (Haaksbergen of Lijnden)
3. Er zijn verschillende onboarding en offboarding documenten in omloop
4. Onboarding en offboarding documenten worden niet altijd volledig of juist ingevuld

Olaf zou erg blij zijn met een implementatie van een dergelijk product en verwacht dat dit wel 25 tot 30% van hun werk over zou kunnen nemen. Aangezien de medewerkers erg vaak druk zijn met navragen voor de onboarding en offboarding documenten en het resetten van gebruikersaccounts en dergelijke.

Interview met Mitchell Kel - Servicedesk Medewerker

Het interview met Mitchell Kel was de 5e interview. Mitchell is medewerker van de Servicedesk en maakt veel gebruikersaccounts aan. Mitchell gaf al snel de, al benoemde, knelpunten aan namelijk dat gebruikersaccount vaak laat aan worden gevraagd. Daarnaast merkt hij dat er erg vaak navraag gedaan dient te worden voor de rechten of waar de medewerker begint. Daarnaast is er nog wel eens onduidelijkheid over wie de laptop gereed maakt en waar de laptop vervolgens opgehaald wordt.

Mitchell gaf aan dat hij de manier van handmatig accounts aanmaken tegenwoordig toch wel wat veroudert vindt. Hij zou graag een applicatie hebben die dit voor hem doet. Dit geld ook voor het resetten van wachtwoorden, hier wordt erg veel tijd aan besteed en die tijd is erg kostbaar.

Interview met Tobias ten Brinke – 3e

Tobias ten Brinke is engineer van de 3e lijn en komt veel bij klanten over de vloer. Met Tobias ten Brinke heb ik mijn 6de interview uitgevoerd. Tobias ten Brinke heeft ondersteuning geboden bij een implementatie van ‘HelloID’ bij een klant. ‘HelloID’ is een applicatie die de een mogelijke oplossing zou zijn in dit project.

Het gesprek met Tobias ten Brinke begon over de functionaliteiten van ‘HelloID’ en hoe het in is gericht. Wat me hierin opviel is dat er na een beetje navragen, meteen een grote maar achter zat. Namelijk dat een wijziging in het pakket ‘HelloID’ door de techneut/ consultant van Tools4ever gedaan dient te worden. Er is geen duidelijke GUI waar de ITers iets aan kunnen passen. De functieprofielen worden eenmalig ingesteld en dit is de basis waar verder vanuit geborduurd kan worden. Vervolg stappen of extra rechten vanuit hier zijn alsnog handmatige instellingen.

Daarnaast was een andere opvallende opmerking dat het volgens Tobias ten Brinke wel minimaal een koppeling moet hebben met Citrix aangezien erg veel klanten hier gebruik van maken. Vervolgens heb ik eens doorgevraagd aan Tobias ten Brinke wat hij vindt wat de toekomst is, waarop vrij snel naar boven kwam dat hij steeds meer klanten gebruik ziet maken van Teams en andere Microsoft-producten. Eenmaal hier verder op ingegaan kwamen we tot de conclusie dat steeds meer klanten van Citrix afstappen en gebruik gaan maken van Intune. Echter is dit een grote transitie voor bepaalde klanten maar ook voor PCI IT aangezien er erg veel medewerkers altijd Citrix ingericht hebben en erg hardware gericht zijn.

Interview met Sander Pot - Servicedesk Teamleider

Sander Pot is teamleider en medewerker van de 2de lijn engineers. Het interview met Sander heeft me geen nieuwe inzichten gegeven over de werkwijze of processen. Sander gaf wel aan dat er veel baat is bij een dergelijk product voor automatisch accounts aanmaken en nog een aantal voordelen benoemt. Bijvoorbeeld AVG technisch gezien dat gebruikersnamen en wachtwoorden niet langer d.m.v. een email verstuurd hoeven te worden maar eventueel direct via een portal beschikbaar gesteld kunnen worden. Daarnaast benoemde hij dat er vaak kopieën worden gemaakt van gebruikers zodat de Servicedesk medewerkers niet handmatig alle rechten groepen bij elkaar hoeven te klikken. Dit is echter wel een risico aangezien deze medewerker tijdelijk toegang kan hebben tot een mailbox of al extra rechten hebben gekregen door een wisseling van zijn functie. De nieuwe medewerker krijgt dan ook direct deze rechten. Dit is zeker niet de bedoeling en daarom zou Sander erg graag zien dat er met functieprofielen wordt gewerkt.

Interview met David Krabbenborg – Projectleider/ Teamcoördinator Network & Security

Het interview met David Krabbenborg ben ik op een andere manier aangegaan om wat meer informatie te vergaren naar de wensen rondom het softwarepakket. Hierin is naar voren gekomen dat de wens er ligt om meerdere klanten aan het softwarepakket te kunnen koppelen zodat de HR-medewerker/ manager van afdelingen zelf de aanvraag voor een gebruikersaccount kunnen doen. Het is niet de bedoeling dat het pakket meerdere keren wordt ingericht bij de klant zelf. Er moet dus gekeken worden of er een mogelijkheid is in het softwarepakket om meerdere klanten aan te kunnen maken.

Interview met Stephan van Hulst – Functionaris gegevensbescherming, risicomanager en kwaliteitscoördinator

Het interview met Stephan ben ik aangegaan om meer te weten te komen over de Algemene verordening Gegevensbescherming.

Bijlage 2: ISO-normen

In dit hoofdstuk heb ik gekeken naar de verschillende ISO-normen en de exacte betekenis ervan.

ISO 9001

ISO 9001 is dé norm voor kwaliteitsmanagement. Bij een kwaliteitsmanagementsysteem wordt er gekeken naar de eisen en verwachtingen van de klant. Vervolgens wordt gewaarborgd dat de producten en diensten die het bedrijf levert aan de doelstellingen van deze klant voldoen. Het kwaliteitsmanagementsysteem bestaat uit de structuur van het bedrijf of de organisatie, in combinatie met de planning, processen, middelen en informatie die gebruikt wordt om de kwaliteitsdoelen te behalen.

In Nederland wordt de norm van de kwaliteit gepubliceerd door NEN, de volledige titel van ISO 9001 is dan ook: 'NEN-EN-ISO 9001'. ISO 9001 is een wereldwijd erkende norm met eisen op het gebied van kwaliteitsmanagement. Hierdoor is het een maatstaf voor transparantie en betrouwbaarheid in de markt.

De kracht van ISO 9001 is zichtbaar op meerdere vlakken. De kwaliteit staat uiteraard voorop. Door te werken met de PDCA-cyclus (Plan-Do-Check-Act-cyclus) wordt er continu gekeken naar verbetering binnen de organisatie. Ook als er meer klanten worden geworven, maar ook om de huidige klanten tevreden te houden.

Door de inzet van ISO 9001 blijven klanten tevreden, hierdoor blijft de omzet hoog, worden er kosten bespaard en wordt het aanpassingsvermogen hoger. Door processen juist in te richten wordt de kwaliteit die wordt geleverd ook beter. Hierdoor is de klant tevreden aangezien hij de juiste ondersteuning krijgt. Zodra deze processen juist ingericht zijn, kunnen de klant laten zien dat dit een hoge kwaliteit oplevert en voldoet aan de wet- en regelgeving. Bewezen is dat 60% van de bedrijven die ISO 9001 op een succesvolle manier hebben geïmplementeerd een hogere omzet behalen. Echter is dit niet de enige manier om geld te verdienen. Nu de processen gestroomlijnd zijn werkt de organisatie efficiënter en wordt er meer bereikt in minder tijd en met minder middelen. Hierdoor worden er ook kosten bespaard. Als laatste voordeel is er ook het aanpassingsvermogen wat ontstaat door het gebruik van ISO 9001. Door gebruik van de ISO-norm dient de organisatie continu bezig te zijn met procesbenadering en dus scherp op risico's en verbeter kansen (NEN, 2021; TUV Nederland, 2021).

ISO 27001

ISO 27001 is gericht op informatiebeveiliging. Met de ingang van de Algemene verordening persoonsgegevens (GPDR) in Europa zijn de regels rondom gegevensbescherming aangescherpt. Doordat hackers actiever zijn en er vaker datalekken zijn, zijn steeds meer bedrijven bezig met het behalen van ISO 27001. Deze ISO-norm beschrijft hoe er procesmatig met het beveiligen van informatie om dient te gaan. Het doel van deze ISO-norm is om de vertrouwelijkheid, beschikbaarheid en integriteit van informatie binnen de organisatie zeker te stellen. Dus bijvoorbeeld persoons- en/of bedrijfsgegevens beschermen tegen hackers en of inbraak.

Ook bij deze ISO-norm wordt er weer gebruik gemaakt van de PDCA-cyclus.

Steeds meer eindklanten eisen ook dat hun partners voldoen aan de strenge normeisen rondom informatiebeveiliging. Door te voldoen aan certificeringen d.m.v. ISO 27001 weten de eindklanten ook dat de informatiebeveiliging goed op orde is. Ook biedt het commerciële kansen voor de organisatie.

Doordat de informatiebeveiliging op orde is, is de kans op risico's en incidenten enorm teruggedrongen. Mits het toch voorkomt kan er snel opgetreden worden en kan reputatieschade veelal worden voorkomen. Hierdoor wordt de betrouwbaarheid ook verhoogd. Met ISO 27001 wordt er aangeduid dat de organisatie naar GPDR heeft gekeken, en dat er bewust met de informatie wordt gehandeld. Hiermee kan het bedrijf zich onderscheiden ten opzichte van anderen.

Opvolgend op de 27000-serie is de ISO 27002 hierin zijn de richtlijnen voor implementatie opgenomen en het uitvoeren van een audit is ISO 27007 (NEN, 2021; TUV Nederland, sd).

ISO 20000-1

ISO 20000-1 ook wel bekend als NEN-ISO/IEC 20000-1:2018 staat in connectie met ISO 27001 waar informatiebeveiliging aan voldoet. Bij ISO 20000-1 wordt er gekeken naar de IT-service management. Het stelt een aantal minimumeisen waaraan alle IT-Services dienen te voldoen.

ISO 20000-1 gaat uit van procesbenadering om zo uw IT-servicemanagementsysteem op te zetten, te implementeren, monitoren, onderhouden en verbeteren. Hierbij kan er ook gedacht worden aan asset management. Maar ook zaken als hoe ervoor gezorgd kan worden dat alle systemen zoals tooling overal hetzelfde werken.

Net als de andere ISO-normen is de structuur gebaseerd op de PDCA-cyclus. Het gaat er echter in de ISO 20000 over hoe de IT-Services geïmplementeerd kunnen worden op de bedrijfsdoelstellingen en deze doelstelling ook ondersteund wordt.

Voor het behalen van deze ISO-norm wordt er een audit uitgevoerd waar er op 13 verschillende onderdelen uit de norm wordt beoordeeld. Op deze manier kijkt de auditor of het proces op de juiste manier is ingeregeld.

1. Servicelevel Management
2. Servicerapportage
3. Management van servicebeschikbaarheid en continuïteit
4. Budgettering en accounting van IT-diensten
5. Capaciteitsbeheer
6. Management van informatiebeveiliging
7. SRM/CRM relatiemanagement
8. Leveranciersmanagement
9. Incidentenmanagement
10. Probleemmanagement
11. Configuratiemanagement
12. Verandermanagement
13. Releasemanagement

Er bestaat ook een tweede deel van de ISO 20000 standaard, namelijk de ISO 20000-2. Het tweede deel is de Code of Practice. Daarin staan handvatten en suggesties voor het voldoen aan de specificaties uit deel 1. Daarnaast kan er gebruik gemaakt worden van ITIL, mede doordat de hele basis van ITIL, zeker met het voldoen aan punt 1 tot en met 13, al is gelegd (TUV Nederland, 2021).

NEN 7510

NEN 7510 is voor de Informatiebeveiliging in de zorg.

Het NEN 7501 certificaat geeft aan dat de organisatie veilig omgaat met de informatie die er vergaard wordt. Dit is een vervolg op ISO 27001. Dit is een teken dat er wordt voldaan aan de eisen

voor het verwerken van informatie in de zorg. Een ander voordeel aan het NEN 7510 certificaat is dat de inspectie, ofwel de inspectie gezondheidszorg en jeugd (IGJ), minder controles uit zou voeren. De IGJ hecht ook erg veel waarde aan het certificaat, aangezien dit kenmerkt dat er gegarandeerd goed met de informatie om wordt gegaan.

Daarnaast is het ook voor de interne organisatie van belang. Het brengt namelijk ook inzicht in de datastromen. Het zorgt er namelijk voor dat alle gegevens binnen de zorginstellingen wordt geborgd. Aangezien alle datastromen in kaart gebracht dienen te worden en hier beheersmaatregel op uitvoert. In de norm staan tal van deze beheersmaatregelen opgesomd waarmee u aan de eisen in de norm kunt voldoen (TUV Nederland, 2021).

Verschillen NEN 7510 en ISO 27001

De NEN 7510 en ISO 27001 zijn beide voor het beveiligen, veilig opslaan van data. Echter is er wel degelijk een verschil. Namelijk de ISO 27001 is een norm voor informatiebeveiliging welke ten doel stelt om bedrijfsinformatie te beschermen. Dit is natuurlijk erg breed opgezet echter heeft elk bedrijf andere informatie. Dat is dan ook waar NEN 7510 voor is bedacht, een certificering speciaal voor in de zorg. Aangezien er in de zorg veel met essentiële persoonlijke en medische gegevens die invloed hebben op mensenlevens om wordt gegaan.

In feite is het dan een uitbreiding op de ISO 27001 norm. De NEN 7510 bevat dezelfde inhoud echter heeft het zorg specifieke eisen.

Bijlage 3: Contextanalyse

Met de contextanalyse is vast te stellen welke factoren eventueel invloed hebben op dit project. Dit kunnen bronnen zijn vanuit de interne organisatie en van buiten de organisatie, zoals concurrerende bedrijven of openbare informatie. Om dit te beschrijven is er gebruik gemaakt van de Micro-, Meso-, Macro-methode.

Macro

In de Macroanalyse wordt rekening gehouden met krachten rondom de markt en omgeving. Aangezien PCI IT een leverancier van IT is en hierdoor erg afhankelijk is van de markt en de producten is het belangrijk om hier rekening mee te houden.

Mede met de komst door het Corona-virus is zoals eerder benoemd de transitie naar de cloud en met name de transitie van de applicaties naar de cloud snel gegaan. Aangezien alle medewerkers vanuit huis gingen werken, zijn applicaties als SaaS-applicatie versneld beschikbaar gesteld.

Een andere ontwikkeling rondom het Corona-virus en het thuiswerken is dat er zowel op kantoor als thuis een werkplek beschikbaar dient te zijn. Hierdoor kiezen werkgevers vaak voor een laptop die de werknemer mee kan nemen en aan kan sluiten op een scherm. Hierdoor wordt er vaker gebruik gemaakt van Intune om ook deze apparaten te kunnen beheren maar ook te beveiligen.

Meso

Bij de meso-analyse wordt gekeken naar de directe omgeving van PCI IT. Of en waar er eventuele gevaren zijn wordt hierin betrokken. Om deze analyse te realiseren, kan gebruik gemaakt worden van het vijfkrachtenmodel van Porter (Marketingscriptie, 2021). Het vijf krachten model van Porter bestaat uit de volgende krachten:

- De macht van leveranciers
- De macht van afnemers
- Substituten & complementaire goederen
- Nieuwe concurrentie
- Interne concurrentie

Macht van leveranciers

Leveranciers kunnen prijzen verhogen of de kwaliteit van de producten verlagen. Op deze manier heeft PCI IT meer kosten of producten van mindere kwaliteit. Hierdoor is het van belang om de macht van leveranciers op te nemen.

Er zijn voldoende leveranciers in de ICT-branche om over te kunnen stappen naar een ander of om geen keuze te maken voor een vaste leverancier. Dit is een voordeel voor PCI IT. Er is dus geen monopolie positie voor 1 leverancier. Echter zijn er wel diverse keuzes die vanuit het management gemaakt kunnen worden waardoor er een beperkter scala aan leveranciers is. Bijvoorbeeld een keuze om alleen producten van HP te kopen en verkopen.

Daarnaast geldt dit ook voor de producten die aangeboden worden als dienst. Als een bedrijf alleen kennis heeft van Microsoft-producten is het logisch dat het bedrijf alleen deze producten aanbiedt. Hierdoor kan de keuze in leveranciers ook afnemen, gezien niet elke leverancier Microsoft-producten verkoopt.

In relatie tot het onderzoek wordt er een keuze gemaakt voor een applicatie. Deze applicatie zou waarschijnlijk alleen door de uitgever zelf worden aangeboden, dus de macht van de leverancier is hoog.

Macht van afnemers

De macht van de afnemers, of terwijl de klanten van PCI IT, is redelijk hoog. Klanten kunnen zelf bepalen wanneer ze geen diensten meer af willen nemen bij PCI IT, contract afhankelijk uiteraard. Echter zijn er inmiddels steeds meer ICT-bedrijven die soortgelijke diensten uit kunnen voeren. Dit maakt dat de concurrentie hoog is.

Als de ICT-omgeving goed draait is de verwachting dat een klant niet snel overstapt naar een andere ICT-partij, omdat dit veel impact heeft op de organisatie.

Nieuwe concurrentie

Tegenwoordig is de nieuwe concurrentie relatief hoog, door onder andere de komst van ZZP'ers. De komst van ZZP'ers is niet direct een probleem voor grotere partijen als PCI IT. Er is veel schaalgrote benodigd om volledige omgevingen van bedrijven te beheren, dat is niet te realiseren als ZZP'er.

Externe concurrentie

De concurrentie in de sector is zoals hierboven benoemd hoog. Er zijn diverse grote ICT-partijen in de omgeving die soortgelijke diensten verlenen als PCI IT. PCI IT ervaart veel tevreden klanten die naar verwachting geen andere ICT-leverancier kiezen. Hierboven is al eerder aangegeven dat de overstap naar een andere leverancier impact heeft. De momenten dat een klant voor een andere partij zou kunnen kiezen is bijvoorbeeld bij een aanbesteding waar PCI IT niet de goedkoopste leverancier is en er gestuurd wordt op kosten.

Micro

In het laatste gedeelte van de contextanalyse wordt met de microanalyse gekeken naar de interne krachten die invloed hebben op PCI IT.

Eén van de grootste interne krachten die heeft plaatsgevonden afgelopen jaren voor PCI IT is de overname van PCI Nederland. PCI IT was namelijk ongeveer twee jaar geleden nog ICT Spirit. ICT Spirit was een onafhankelijke IT-leverancier ontstaan uit Leferink IT. De oud-eigenaar, Mark Leferink, heeft aangegeven niet langer over de kennis te beschikken om het bedrijf verder te laten groeien. Hierdoor heeft hij doen besluiten om ICT Spirit en Office Works te verkopen.

PCI Nederland heeft de afgelopen jaren al meerdere IT-partijen overgenomen en had veel interesse om ICT Spirit over te nemen. Een voorwaarde van Mark Leferink voor de overname was dat ICT Spirit een eigen organisatie zou worden binnen PCI Nederland. Daar is de naam PCI IT uit voortgekomen. Door deze overname is zowel het klantenbestand als het personeelbestand van PCI Nederland enorm gegroeid. Hoewel er meer personeel en kennis beschikbaar is na de overname groeit het klantenbestand in dezelfde stijgende lijn. Hierdoor is er nog steeds veel vraag naar nieuwe medewerkers binnen PCI IT.

Conclusie

De conclusie uit de contextanalyse is dat PCI IT een uitstekende kans heeft om dergelijke producten te verkopen aan haar klanten. Een hoge slagingskans is mogelijk vanwege de sterke groei afgelopen jaar met SaaS-applicaties, maar ook rondom beveiliging. Sinds de beveiligingsproblemen steeds vaker in het nieuws zijn is dit een populairder onderwerp geworden. Met de oplossing die PCI IT zoekt, wordt er zowel grip op de accounts als grip op de beveiliging van de accounts gecreëerd. Aangezien dit de vraag is in de markt en van de klanten van PCI IT heeft dit product een grote slagingskans.

Een punt van aandacht is echter wel de snel bewegende markt, het is nu een trend om veel applicaties naar de cloud te brengen, echter moeten komende trends wel in de gaten gehouden worden. Dit geldt ook voor de leveranciers van PCI IT. Wanneer de leverancier de prijzen verhoogd, moet PCI IT bepalen of deze leverancier nog de juiste partij is.

Bijlage 4: Onderzoek d.m.v. Gartner Magic Quadrant

CyberArk

CyberArk haar klanten zijn veelal kleine tot middelgrote organisaties die opzoek zijn naar AM-personeel. Recente innovaties zijn onder meer wachtwoord loze mogelijkheden met behulp van QR-codes en FIDO2, AM-extensie voor adaptieve MFA voor desktops en servers, en identiteitsbevestigingsservice via een partnerschap met Ekata. CyberArk is van plan haar omzet van 23% te herinvesteren in een nieuw SaaS-platform voor geconvergeerde identiteits- en toegangsbeheer (IAM)-diensten en continue authenticatie toe te voegen.

Voordelen:

- Hoogste score voor operaties.
- Goede visie en speelt in op trends.
- Bovengemiddelde analysemogelijkheden met meer dan 70 kant-en-klare rapporten. Daarnaast kan het ook externe gebruikersanalyses en risicosignalen gebruiken voor adaptieve toegangsstromen.
- Goede keuze voor AM-product die ondersteuning biedt op het PAM-portfolio.

Waarschuwingen:

- Het vernieuwingspercentage van CyberArk haar SaaS-producten is gedaald ten opzichte van vorig jaar en scoort het laagst geëvalueerd voor dit onderzoek.
- CyberArk kreeg een onder gemiddelde score voor het gemak van implementatie.
- Prijs ligt ruim boven het gemiddelde.
- Geen SLA-optie voor 99,99% (deze stopt bij 99,9%.
- CyberArk biedt minder functies voor gebruiksscenario's van CIAM en ontwikkelaars.
- Scoort slecht voor API-toegangscontrole en ontwikkelaarstools.

ForgeRock

ForgeRock is leider volgens het Gartner kwadrant. ForgeRock verkoopt zijn Acces Management-product stand-alone of in een bundel, gelevers als SaaS of software. Haar activiteiten zijn divers en meestal gericht op grotere organisaties, meestal in de bank-, communicatie, media- en dienstsector, die op zoek zijn naar SaaS-gebaseerde, on-premises of hybride implementaties voor interne en externe AM-gebruikersscenario's.

Voordelen:

- ForgeRock biedt sterke productmogelijkheden voor interne en externe AM-gebruikersscenario's, gecombineerd met goede functies voor API-toegangscontrole en ontwikkelaarstools. Het bied een goede balans in adoptie voor voor interne en externe AM en gebruik door ontwikkelaars.
- ForgeRock scoorde hoog voor marktinzicht, met speciale aandacht voor klantervaring, ontwikkelaars en verticale afstemming met de zorg- en financiële sector.
- ForgeRock biedt een beschikbaarheids-SLA van 99,95%, met gratis niet-productieomgevingen in elk SaaS-abonnement en gratis toegang tot de softwareversies van de SaaS-producten (te installeren op hybride implementaties).
- Met het AM-product scoort hoog met de identiteit beveiligingsmogelijkheden met sterke directory services.
- Ook verkoopt ForgeRock IGA-softwareproducten die samenwerking aan kunnen bieden aan klanten die naar één oplossing opzoek zijn.

Waarschuwingen:

- De prijsstelling in vergelijking met zijn concurrenten is bovengemiddeld.

- De analysemogelijkheden zijn onder het gemiddelde. Er is geen UEBA-mogelijkheid en het verkrijgen van analytische inzichten over runtimegegevens is complex.
- De omzet van ForgeRock groeide maar het aantal klanten steeg niet zo hard als overige leiders in dit onderzoek.
- ForgeRock scoorde onder het gemiddelde in innovatieve en leverde niet op wat vorig jaar op de roadmap stond.

IBM

Het AM-product wordt aangeboden als software (IBM Security Verify Access) en SaaS-geleverde (IBM Security Verify) gericht op geconvergeerde aanpak voor AM en andere IBM Security-producten. De beschikbare activiteiten zijn geografisch en de klanten zijn voornamelijk in de banksector en de publieke sector, die op zoek zijn naar on-primises en hybride implementaties.

Recente productinnovaties omvatten nieuwe functies voor gegevens privacy en toestemmingsbeheer, een softwareontwikkelingskit (SDK) voor adaptieve toegangsstromen en een gecontaineriseerde versie van de proxy.

Voordelen:
- IBM biedt een goede prijs-kwaliteitverhouding.
- Prijs ligt lager dan die van zijn concurrenten.
- IBM heeft een dedicated instance van zijn SaaS-service uitgebracht die op andere clouds kan worden uitgevoerd.
- IBM is van plan meer samen te gaan werken met Cloud Pak en Red Hat OpenShift voor zijn AM-product.
- IBM scoort hoog in de identiteit administratie met veel mogelijkheden voor identiteit synchronisatie. Ook biedt het mogelijkheden voor fraudedetectie ingebed SaaS AM-product, evenals integratie met andere IBM Security-producten, waaronder IGA.

Waarschuwingen:
- Innovatie van afgelopen jaar was summier
- IBM scoorde onder het gemiddelde voor klantervaring
- SLA-optie voor beschikbaarheid stopt bij 99,9%
- Producten zijn complex in gebruik
- Moeilijk te implementeren en te beheren
- IBM scoorde onder het gemiddelde voor zijn marketing- en productstrategie
- Omzet was minimaal
- Interesse in het product is sterk afgenomen

Ilantus

Ilantus zijn Compact Identity-product is voornamelijk gericht op het leveren van AM als onderdeel van een geconvergeerd SaaS-geleverd IAM-platform voor kleine tot middelgrote organisaties. Haar activiteiten zijn voornamelijk gericht op de regio Azië/Pacific (APAC), met een kleiner deel van de klanten in het Midden-Oosten, Europa en Noord-Amerika.

Recente innovaties omvatten functionaliteiten als risico-engine, adaptieve toegang, een toegangsbeheerpunt op maat van middelgrote ondernemingen en bijbehorende professionele servicepakketten voor implementatie.

Voordelen:
- De prijs ligt onder het marktgemiddelde.
- Standaard SLA van 99,95% maar optioneel van 99,99%.

- Ilantus scoorde bovengemiddeld voor de mogelijkheden voor identiteitsbeheer en ondersteunt inkomende en uitgaande SCIM, accountkoppeling, dynamisch ophalen van gegevens en webhook-integratiepatronen.
- Voor kleine tot middelgrote ondernemingen die op zoek zijn naar een goedkoper, alles-in-één geconvergeerd IAM-platform voor AM, IGA en PAM.

Waarschuwingen:
- Scoort onder gemiddeld voor zijn AM-productmogelijkheden.
- Geen native app voor mobiele push MFA en sterke ontwikkelaarstools zoals visual flow designer of orchestration.
- Scoort erg laag qua strategie en innovatie.
- Ilantus heeft verreweg de minste documentatie van alle softwareleveranciers.
- Merkbekendheid is erg laag

Microfocus

De Micro Focus NetIQ Acces Manager-software en NetIQ AM Saas-modules zijn voornamelijk gericht op hybride implementaties met on-premises applicaties en uitbreidbaarheid in de cloud. Klanten zijn meestal grote organisaties in de productie, het bankleven en publieke sector.

Recente productinnovaties zijn diensten als AM SaaS-modules, aanvullende DevOps-mogeljkheden voor zijn API-beheertool en uitbreiding van MFA-mogelijkheden naar niet-web doeleinden. Micro Focus is van plan om 22% te herinvesteren in diensten als SaaS- en containerversies van zijn producten en meer privacy en analyse mogelijkheden toe te voegen.

Voordelen:
- Prijs ligt onder het gemiddelde.
- SLA van 99,95%.
- Micro Focus scoorde bovengemiddeld voor de productmogelijkheden in BYOI-integratie, maar ook voor autorisatie en adaptieve toegang dankzij de integraties met aangrenzende tools, Fortify en ArcSight Intelligence (voorheen Interset) voor beveiliging van applicatieontwikkeling en gedragsanalyses.
- De nieuwe Cloud Bridge-service van Micro Focus vereenvoudigt identiteitssynchronisatie met on-premises directory’s. Micro Focus blijft geschikt voor grotere organisaties en voor complexere hybride omgevingen (met name bestaande Micro Focus-klanten) die de voorkeur geven aan de flexibiliteit van het beheer van on-premises implementaties.
- Veel uitgebreide en fijne functionaliteiten

Waarschuwingen:
- Beperkte catalogus met vooraf geïntegreerde applicaties vergeleken met andere leveranciers.
- Implementatiegemak van NetIQ Access Manager is onder gemiddeld.
- Micro Focus scoort volgens Gartner het slechtste ten opzichte van zijn concurrenten op het gebied van ontwikkelingen en de roadmap.
- Functionaliteiten die bij concurrenten al bestaan dienen bij Microfocus nog ontwikkeld te worden.
- Geen volledige reeks van AM-mogelijkheden die als SaaS kunnen worden gebruikt.

Microsoft

Microsoft biedt het product Azure AD aan voor AM en wordt verkocht in bundels. Het richt zich op interne en externe AM-gebruikersscenario's. Haar diensten zijn goed verspreid en haar klanten variëren in grootte en sector.

Een recente ontwikkelingen in Azure AD is de toevoeging van FIDO2-ondersteuning, FIDO2 maakt het mogelijk om wachtwoord loos te authentiseren. Daarnaast hebben ze nog een agent voor deelname aan een AD-forest en adaptieve toegang voor CIAM (IAM voor klanten, die toegang benodigd hebben tot de organisatie haar informatie) geïmplementeerd. Microsoft is van plan 10% van de inkomsten vanuit beveiligingsinkomsten te herinvesteren in onderzoek en ontwikkeling voor risicobescherming in multicloud-infrastructuren, het verbeteren van aangrenzende IAM-mogelijkheden en het verbeteren van gedecentraliseerde identiteit en verifieerbare referentiefuncties.

Voordelen:

- De visie van Microsoft is het sterkste van allemaal uit dit onderzoek. Vanwege de identiteit gerichte, op veiligheid afgestemde AM-roadmapplannen. De roadmap bevat functionaliteiten rondom gecentraliseerde identiteitsnormen, multicloud-beveiliging ingebed in AM en geplande PAM- en IGA-mogelijkheden
- Prijs ligt onder het gemiddelde
- SLA 99,99% beschikbaarheid
- Hoogste score voor levensvatbaarheid en verkoopstrategie. Dit komt mede door de beslissing om Azure AD te bundelen met Microsoft 365- en EMS-licenties. Dit zorgde ervoor dat Microsoft het totaal aantal klanten wist te verdubbelen.

Waarschuwingen:

- Azure AD kreeg de laagste score voor productmogelijkheden. Externe AM-gebruiksscenario's en mogelijkheden voor sessiebeheer zijn onprofessioneel in vergelijking met de concurrenten. De meeste klanten gebruiken het alleen voor personeelsscenario's.
- Azure AD had eind 2020 en begin 2021 twee grote storingen van meer dan 16 uur. Dit toont aan dat de betrouwbaarheid nog niet is wat wordt beloofd.
- Nog geen hybride failover-opties beschikbaar voor deze diensten
- Microsoft loopt ondanks de investeringen achter op het gebied van AM-productmogelijkheden vooral in CIAM.
- De productinnovaties van vorig jaar waren vooral inhaalslag op de concurrenten.

Okta

Okta staat hoog in het kwadrant van Gartner en biedt een door SaaS geleverde geconvergeerd AM-platform, gericht op zwel interne als externe AM-gebruiksscenario's. Haar activiteiten zijn diverse en haar klanten zijn meestal kleine tot middelgrote organisaties.

Recente productinnovaties omvatten nieuwe ontwikkelen rondom CIAM, deze komen voornamelijk door de fusie met Auth0. Daarnaast is Okta Workflows voor klantidentiteit gelanceerd, nieuwe FedRAMP-certificeringen en verbeteringen aan de Okta Acces Gateway. Okta wil 27% van de omzet investeren voor een nieuw consumenteninitiatief genaamd Personal Okta, device beheer voor Windows en MacOS (Okta Devices), identiteitsorkestratie-uitbreidingen en on-premises extensies voor het beheer van Active Directory.

Voordelen:

- Okta scoort het hoogst op productmogelijkheden. Identiteit orkestratie (workflows) voor alle AM-gebruikersscenario's, daarnaast verbeterde Okta haar user interface.

- Scoort het hoogst op gebied van self-service voor gebruikers en het inschakelen van standaardapplicaties
- Gemakkelijke implementatie
- Okta kreeg de hoogste score voor klantervaring, maar scoorde ook hoog voor gebruik gemak, flexibiliteit bij de integratie met een groot aantal apps en de hoge kwaliteit van beschikbare documentatie.
- Okta scoort het hoogst voor beveiliging, veerkracht en dekking. Bij Okta kan er nu gebruik worden gemaakt van een automatische failover van cloud tot on-premises.
- Door deze automatische failover is de SLA-beschikbaarheid 99,99%
- Okta scoort ook zeer hoog op innovatie met voltooide acquisitie van Auth0 en de plannen om boven het marktgemiddelde te investeren in onderzoek en ontwikkeling.
- De visie van Okta is om haar AM-producten te laten groeien tot een geconvergeerd IAM-platform met IGA- en PAM-mogelijkheden, inclusief overname van atSpoke, een platform voor werkplekoperaties, in augustus 2021.

Waarschuwingen:
- Prijzen zijn ver boven het gemiddelde, terug te zien in klanten reviews.
- De AD-integratie en identiteitslevenscyclus blijven beperkt, vooral in vergelijking met haar concurrenten.
- Hoewel Okta een in verschillende geografische plekken een omgeving heeft is het grotendeels geconcentreerd in Noord-Amerika.
- Het managementteam is recentelijk volledig vernieuwd, waaronder een andere CTO, CFO en CMO. De vraag is wat hier de impact van is.

Okta (Auth0)

De benaming is wat verwarrend maar Okta heeft Auth0 overgenomen in mei 2021 en Auth0 is een onafhankelijke productunit binnen Okta. De AM-producten zijn voornamelijk gericht op door SaaS geleverde ontwikkelaars en CIAM-gebruiksscenario's. Haar klanten zijn meestal kleine tot grote organisaties die AM-besturingselementen willen toevoegen op maat ontwikkelde, API-gestuurde applicaties.

Recente innovaties omvatten meer mogelijkheden voor B2B0oartner- en klantbeheer, platformuitbreidingen en detectie en herstel van aanvallen met ingebouwde credential-stuffing. Auth0 is van plan te investeren in het uitbreiden van zijn mogelijkheden in B2B2E/B2B2C-gebruiksscenario's en nieuwe gebieden zoals fijnmazige autorisatie, en om de integratie met Okta Workflows te verdiepen.

Voordelen:
- Auth0 scoorde het hoogste voor innovatie, met verschillende AM-productverbeteringen en plannen voor hoge investering voor onderzoek en ontwikkeling.
- Ook de niet-technische ontwikkelingen waren opmerkelijk: Auth0 sluit deal met Salesforce en creëerde een OEM-product voor CIAM dat door Salesforce zou worden verkocht in zijn cloudplatform voor klanten.
- De prijzen van Auth0 zijn concurrerend. De prijzen liggen onder en soms rond het gemiddelde van de concurrenten.
- Auth0 biedt een SLA van 99,99% uptime.
- Auth0 biedt een speciale en gehoste service in Amazon Web Services (AWS).
- Auth0 biedt een goede lijst van CRM-integraties en de meest uitgebreide BYOI-integratielijst van zijn concurrenten.

- Goede UX-flows en UI-aanpassingsmogelijkheden kunnen volledig aangepaste pagina's hosten die verder gaan dan eenvoudige white labeling. Daarnaast heeft Auth0 behoorlijk wat developer tools en volledige API-ondersteuningen.

Waarschuwingen:

- De overname van Auth0 kan door Okta overlapping en verwarring veroorzaken. Ook kan het zorgen voor een andere visie door de gecombineerde bedrijven niet soepel lopen.
- Auth0 scoorde onder het gemiddelde op identiteitsbeheer aangezien het volledig afhankelijk is van externe tools (en API-integraties) voor basisfuncties, zoals levenscyclusbeheer en workflows.
- Het biedt geen kant-en-klare SCIM-gebaseerde connectoren, alleen generieke SCIM-connectoren die moeten worden aangepast telkens als er een toepassing geïntegreerd wordt.
- Auth0 heeft een beperkte catalogus van vooraf geconfigureerde SaaS-toepassingsintegraties.
- Het personeelsbestand dashboard met SSO wordt niet standaard geïnstalleerd, het vereist een aangepaste implementatie.
- Auth0 is sterk afhankelijk van externe identiteitsbewuste proxy; of serviceproviders, zoals NGINX, AWS Application Load Balancer (ALB), Okta Acces Gateway en bibliotheken van derden; of Apache SDK's

Bijlage 5: Interview met Tools4ever (softwarepakket HelloID)

In dit hoofdstuk is het volledige interview en de antwoorden van Tools4ever medewerker Jester van Steijn te vinden.

Het interview is telefonisch afgenomen op 30 november 2021.

- **Is de software multi-tenancy in te zetten? Dus als MSP in te zetten om meerdere klanten te koppelen zodat het niet elke keer opnieuw uitgerold hoeft te worden? Zo ja hoe gaat dit in zijn werk?**

Ja we kunnen de software aan meerdere applicaties en AD's koppelen. Er kan een hoofdportaal worden gecreëerd waar verschillende tegeltjes aan te maken zijn per klant, vervolgens kan er doorgeklikt worden naar de klant en de omgeving beheren.

- **Is er scripting beschikbaar zoals powershell om 3th party apps te koppelen?**

Ja. Standaard zijn er al 150 verschillende Apps gekoppeld in ons systeem en aangezien wij al 20 jaar de focus hebben op IAM en PAM. Door middel van Powershell, kunnen er koppelingen naar eigen wens aangemaakt worden, daarnaast zijn er al openbare scripts via GitHub te benaderen. De vuistregel voor ons is als er een API, SQL of andere koppeling mogelijk is, is het te koppelen. Als er nog geen koppeling is met een softwarepakket dan ontwikkelen we dat graag voor jullie. Op deze manier breiden wij onze apps uit en ondersteunen we jullie als klant.

- **Zijn er meerdere apps te koppelen d.m.v. API-koppelingen?**

Ja zie bovenstaand. Er zijn dus 150 apps te koppelen die bestaan uit HR-systemen, lokale AD, Azure AD, O365, filesystems, ticket-, ERP-, CRM-systemen en dergelijke.

- **Zit er iets van een auditing report ingebakken? Wie heeft welke rechten en mag waar exact bij, wat is de impact als zijn account is gehackt e.d.?**

Ja zeker, zeker nu AVG steeds meer een ding is en er erg veel actieve hackers zijn, zijn we hier heel actief in. Er zijn volledige rapporten uit te draaien direct vanuit HelloID, denk hierbij aan; rapporten waarin te zien is wie rechten heeft op een app, rapporten waarop te zien is hoelang iemand waarop nog rechten heeft, maar ook wie de rechten uit heeft gedeeld en wat de reden van aanvraag is.

- **Is er multi factor authenticatie? Zo ja, op welke manier(en)?**

Er zijn 3 modules bij Tools4ever, namelijk; HelloID, Provisioning en Service automation.
Bij Provisioning zit acces management in en dit kan zorgen voor multi factor authenticatie op basis van telefoon, email, app en dergelijke. De authenticatie kan er ook voor zorgen dat, mits er bepaalde apps zijn waar vaker ingelogd dient te worden, Tools4ever hier een schil overheen maakt waardoor er niet vaker in gelogd hoeft te worden.

- **Kunnen werkprocessen geautomatiseerd worden?**

Door middel van de module Service automation – kunnen medewerkers zelf IT-diensten aanvragen, er is hierbij geen self-service portaal, daar is een andere module voor. De medewerkers kunnen aanvragen voor rechten of applicaties doen en de manager of HR-medewerker kan de aanvraag goed of afkeuren, bepaalde aanvragen kunnen ook automatisch goedgekeurd worden.

- **Hoe gaat het in zijn werking zodra een medewerker een aanvraag doet?**

Er zit een werkproces achter de aanvraag die volledig gefinetuned kan worden. Hier zou gekozen kunnen worden dat het account automatisch aangemaakt wordt zonder tussenkomst van een medewerker, maar kan ook kiezen dat 1 of zelfs 2 mensen hier akkoord voor moeten geven in het kader van beveiliging.

Daarnaast is er een module om de servicedeks te ontzien van wachtwoord wijzigingen. De tool SSRPM (Self Service Reset Password Management) is bedoeld voor eindgebruikers die zelf hun wachtwoord kunnen resetten. Dit kan op basis van E-mail, sms, authenticator of een aantal persoonlijke vragen beantwoorden, dit is zelf in te stellen.

- **Zijn jullie bereid om HelloID te laten zien door middel van een demo?**

Uiteraard! Wij laten niet alleen zien wat mogelijk is en hoe geweldig hun pakket is maar ook wat het pakket niet kan. Dit vinden we belangrijk zodat daar geen verschillende meningen over kunnen komen in een later stadium.

- **Hoe ziet een eventuele implementatie eruit van HelloID?**

Als jullie na de demo nog enthousiast zijn en voor ons kiezen wordt er een intake gedaan voor de technische haalbaarheid voor een implementatie, daar komt een PvA uit, en vervolgens kunnen we een advies geven over hoe wat en wanneer het uitgevoerd dient te worden.

Standaard houdt Tools4ever rekening met 5 dagen implementatie, echter zijn deze 5 dagen wel verdeelt over 2 tot 3 maand. Hierin is het mogelijk om het technische gedeelte volledig in te laten richten net als het business gedeelte of om advies te krijgen over de inrichting qua rollen en rechten.

Daarnaast is het ook mogelijk om zelf gratis cursussen te volgen bij Tools4ever, over hoe HelloID in te richten is, maar ook hoe HelloID het beste met beheert en ingericht kan worden.

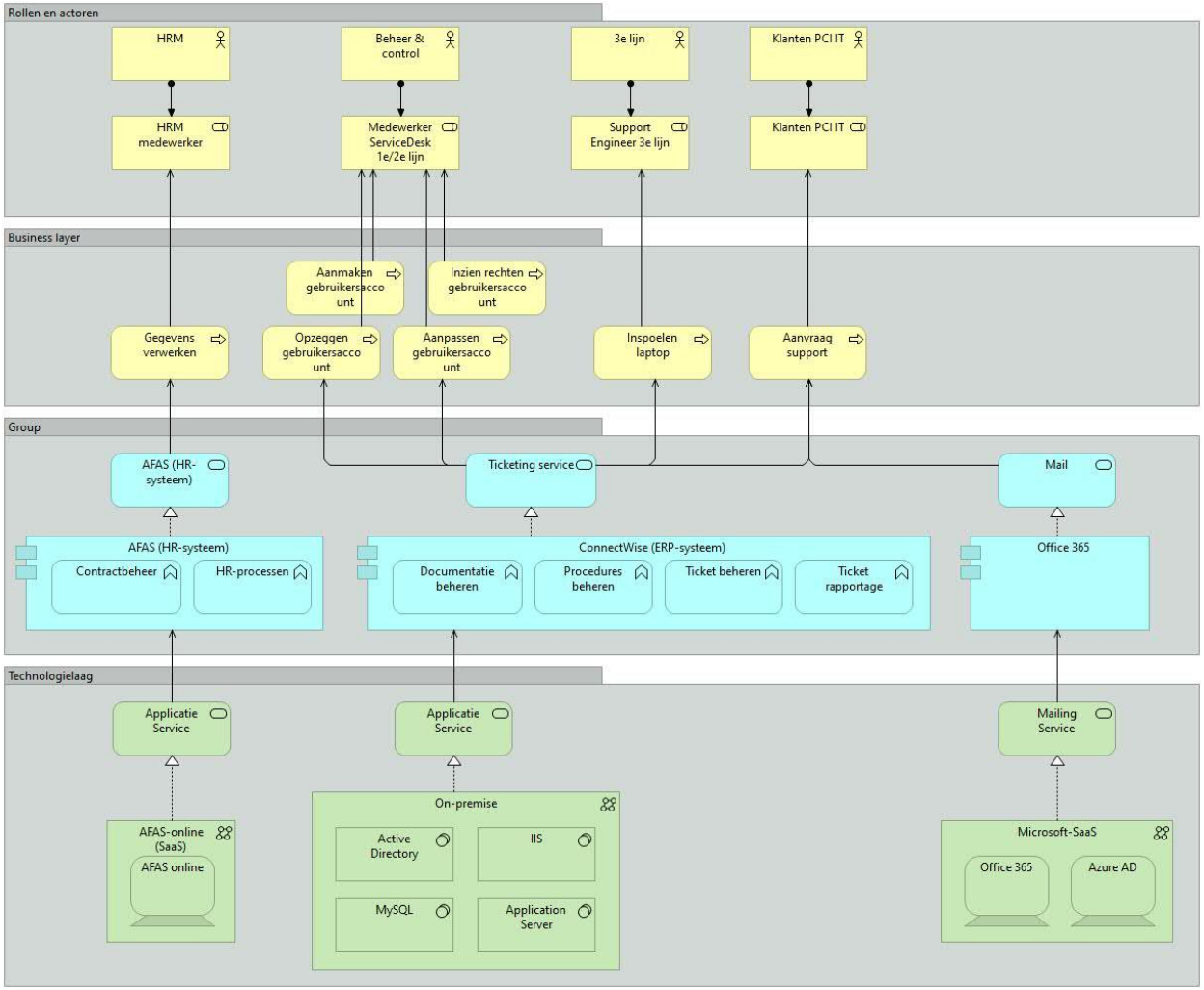
Qua beheer kunnen toevoegingen en wijzigingen later gemakkelijk toegevoegd worden, ook hier zijn gratis cursussen voor beschikbaar.

Het pakket wordt op SaaS-basis aangeboden en de hosting van Tools4ever wordt gehost in Europa.

- **Dient er een vaste koppeling te zijn met de infrastructuur van de klant?**

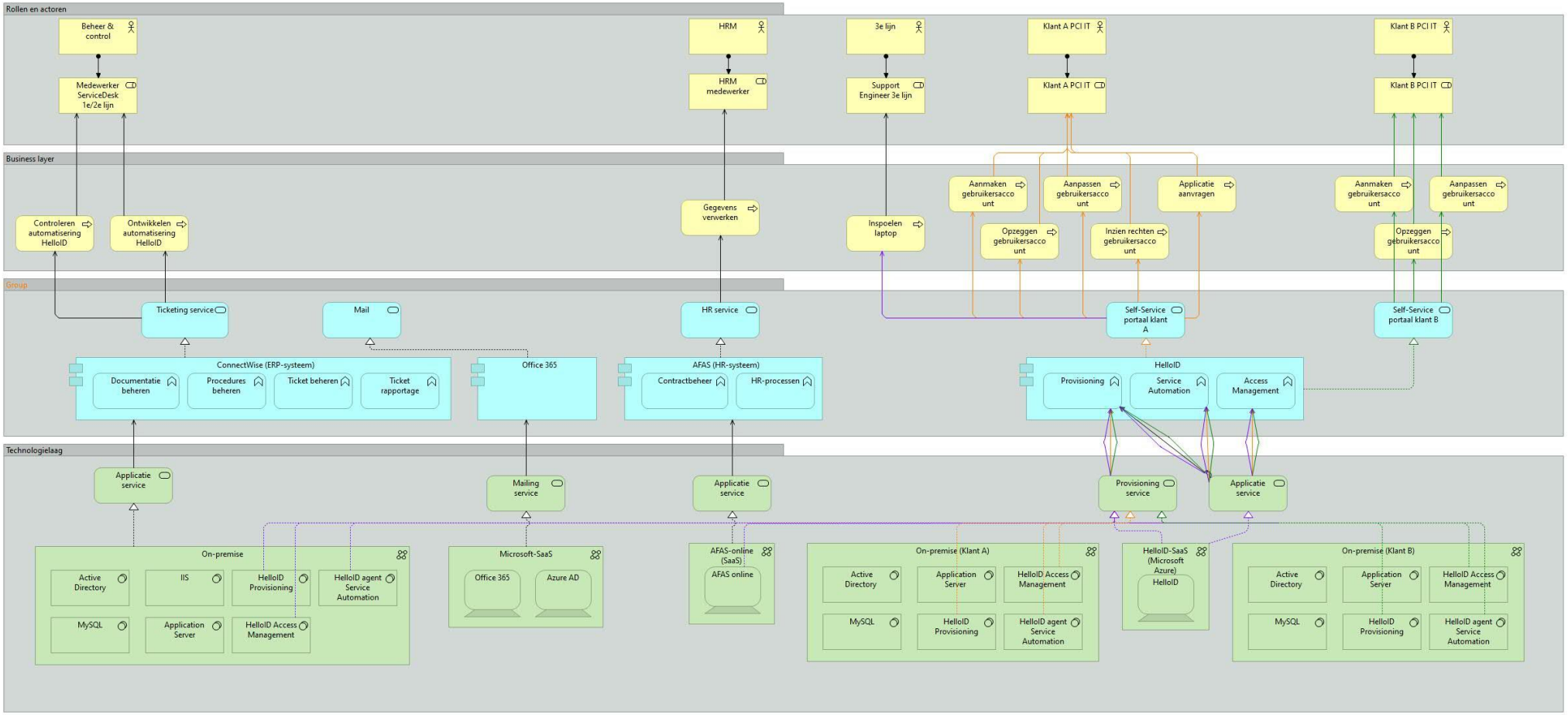
Er hoeft geen actieve koppeling te zijn tussen de verschillende klanten d.m.v. een VPN-verbinding o.i.d. dit wordt gedaan door middel van een API-koppeling.

Bijlage 6: Archimate tekening huidige omgeving



Figuur 13 Archimate huidige omgeving

Bijlage 7: Archimate tekening omgeving met HelloID



Figuur 14 Archimate tekening omgeving met HelloID

Bijlage 8: Requirements

User requirements

In onderstaande tabel zijn de user requirements vermeld en is in het veld ‘Gekoppeld aan’ te zien aan welke user story de user requirement is gekoppeld.

U-ID	Requirement	Prioriteit	Gekoppeld aan	Gekoppeld aan
U-01	Een bevoegde HR-medewerker dient binnen 10 minuten een overzicht te kunnen creëren van welke gebruikersaccounts welke rechten hebben.	Must	US11	K-06, K-07
U-02	Een gebruikersaanvraag die door een bevoegde eindgebruiker is ingediend dient ten alle tijden goedgekeurd te worden door een andere bevoegde medewerker (4-ogen principe).	Must	US02	
U-03	Er dient ten alle tijden een 4-ogen controle te zijn bij een aanvraag van een nieuwe gebruiker van zowel een bevoegde eindgebruiker als een HR-medewerker.	Must	US02	
U-04	Een bevoegde eindgebruiker (klant) dient zelf ten alle tijden een gebruikersaanvraag te kunnen doen zonder tussenkomst van PCI IT.	Should	US01	
U-05	Er dient een mogelijkheid te zijn om direct een melding te ontvangen zodra er een nieuw gebruikersaccount aan is gemaakt door een eindgebruiker.	Should	US02	
U-06	Er dient ten alle tijden een nieuw gebruikersaccount aangevraagd te kunnen worden op basis van functieprofielen.	Should	US04, US05	K-06
U-07	Een bevoegde HR-medewerker dient ten alle tijden een nieuw gebruikersaccount aan te kunnen vragen.	Should	US06	K-01
U-08	Een bevoegde manager dient ten alle tijden een nieuw gebruikersaccount voor zijn eigen afdeling aan te kunnen vragen.	Should	US07	K-03
U-09	Een bevoegde HR-medewerker dient een gebruikersaccount van een uit dienst getreden collega ten alle tijden op te kunnen heffen na goedkeuring van een bevoegde medewerker.	Should	US08	K-07
U-10	Een bevoegde manager dient ten alle tijden een gebruikersaccount van een uit dienst getreden medewerker uit zijn afdeling op te kunnen heffen.	Should	US09	K-07
U-11	Een bevoegde aanvrager van een nieuw gebruikersaccount dient een, indien bekend, einddatum van een gebruikersaccount op te kunnen geven (op basis van contract).	Should	US10	K-05, K-07
U-12	Een manager van een afdeling dient een overzicht te kunnen creëren van welke gebruikersaccounts welke rechten hebben binnen zijn afdeling.	Should	US12	K-06, K-07
U-13	Alle velden die benodigd zijn voor het aanmaken van een gebruikersaccount dienen verplichte velden te worden tijdens de aanvraag.	Should	US15	K-05

U-14	De bevoegde aanvrager van een nieuw gebruikersaccount dient aan te kunnen geven op welke locatie de nieuwe medewerker gaat beginnen.	Could	US14	K-05
U-15	De bevoegde aanvrager van het gebruikersaccount dient na het aanmaken van het gebruikersaccount de rechten nog aan te kunnen passen.	Could	US16, US17	K-06, K-07
U-16	Bevoegde HR-medewerkers dienen functieprofielen aan te kunnen passen.	Could	US17	K-06
U-17	De bevoegde aanvrager van het gebruikersaccount dient de status van zijn aanvraag in te kunnen zien.	Could	US18	

Tabel 15 User requirements

System requirements

In onderstaande tabel zijn de system requirements vermeld.

S-ID	Requirement	Prioriteit	(Niet) Functioneel
S-01	Het product dient een koppeling te kunnen maken met meerdere applicaties door middel van een API-koppeling.	Must	Functioneel
S-02	Er dienen meerdere klanten gekoppeld te kunnen worden aan het product.	Must	Functioneel
S-03	Het product dient een koppeling te hebben met Azure Active Directory	Must	Functioneel
S-04	Het product moet een koppeling kunnen maken met Active Directory	Must	Functioneel
S-05	Het product moet, als er data opgeslagen wordt, data opslaan binnen de Europese Economische Ruimte (EER)	Must	Functioneel
S-06	Het product dient MFA te ondersteunen.	Must	Functioneel
S-07	Het product dient powershell-scripting te ondersteunen.	Should	Functioneel
S-08	Het product moet een koppeling kunnen maken met Teams om gebruikers op basis van een functieprofiel automatisch lid te kunnen maken van bepaalde Teams.	Should	Functioneel
S-09	Het product moet een koppeling kunnen maken met Outlook om gebruikers rechten uit te kunnen delen op mailboxen.	Should	Functioneel
S-10	Het product moet een koppeling kunnen maken met lokale AD om verbinding te kunnen maken met de AD-accounts.	Should	Functioneel
S-11	Het product moet een koppeling kunnen maken met Azure-AD om gebruik te kunnen maken van groepen binnen Azure-AD.	Should	Functioneel
S-12	Het product moet gebruikers zelf hun wachtwoord kunnen laten resetten zonder tussenkomst van een medewerker van PCI IT.	Could	Functioneel
S-13	Het product dient geen vaste verbinding met de servers van de eindklant benodigd te hebben.	Could	Functioneel
S-14	Het product dient een mogelijkheid te hebben om serviceaccounts te beheren.	Could	Functioneel
S-15	Het product dient een mogelijkheid te hebben om ‘just in time acces’ te ondersteunen.	Could	Functioneel
S-16	Het product dient een rapportage aan te kunnen tonen wie, welke rechten heeft.	Could	Functioneel

Tabel 16 System requirements

Bijlage 9: Module per system requirements

S-ID	Requirement	Prioriteit	(Niet) Functioneel	Requirement mogelijk	Module benodigd
S-01	Het product dient een koppeling te kunnen maken met meerdere applicaties door middel van een API-koppeling.	Must	Functioneel	Mogelijk	Provisioning
S-02	Er dienen meerdere klanten gekoppeld te kunnen worden aan het product.	Must	Functioneel	Mogelijk	Provisioning
S-03	Het product dient een koppeling te hebben met Azure Active Directory	Must	Functioneel	Mogelijk	Provisioning
S-04	Het product moet een koppeling kunnen maken met Active Directory	Must	Functioneel	Mogelijk	Provisioning
S-05	Het product moet, als er data opgeslagen wordt, data opslaan binnen de Europese Economische Ruimte (EER)	Must	Functioneel	Mogelijk	
S-06	Het product dient MFA te ondersteunen.	Must	Functioneel	Mogelijk	Access Management
S-07	Het product dient powershell-scripting te ondersteunen.	Should	Functioneel	Mogelijk	Provisioning of Service Automation
S-08	Het product moet een koppeling kunnen maken met Teams om gebruikers op basis van een functieprofiel automatisch lid te kunnen maken van bepaalde Teams.	Should	Functioneel	Mogelijk	Provisioning
S-09	Het product moet een koppeling kunnen maken met Outlook om gebruikers rechten uit te kunnen delen op mailboxen.	Should	Functioneel	Mogelijk	Provisioning
S-10	Het product moet een koppeling kunnen maken met lokale AD om verbinding te kunnen maken met de AD-accounts.	Should	Functioneel	Mogelijk	Provisioning
S-11	Het product moet een koppeling kunnen maken met Azure-AD om gebruik te kunnen maken van groepen binnen Azure-AD.	Should	Functioneel	Mogelijk	Provisioning
S-12	Het product moet gebruikers zelf hun wachtwoord kunnen laten resetten zonder tussenkomst van een medewerker van PCI IT.	Could	Functioneel	Mogelijk	Service Automation
S-13	Het product dient geen vaste verbinding met de servers van de eindklant benodigd te hebben.	Could	Functioneel	Mogelijk	Provisioning
S-14	Het product dient een mogelijkheid te hebben om serviceaccounts te beheren.	Could	Functioneel	Mogelijk	Provisioning
S-15	Het product dient een mogelijkheid te hebben om ‘just in time acces’ te ondersteunen.	Could	Functioneel	Mogelijk	Provisioning
S-16	Het product dient een rapportage aan te kunnen tonen wie, welke rechten heeft.	Could	Functioneel	Mogelijk	Provisioning

Tabel 17 System requirements