

De ICT-Omgeving van gemeente Huizen



Versie 1.1
31-01-2025



- 1. Inleiding**
- 2. Huidige situatie**
 - 2.1 On-Premise Software en Hardware
 - 2.2 Netwerkinfrastructuur
 - 2.3 Telefontie en Communicatie
 - 2.4. Printvoorzieningen
 - 2.5 Applicatielandschap
 - 2.6 Microsoft Azure omgeving Gemeente Huizen
 - 2.7 Client management
- 3. Toekomstige situatie**
 - 3.1 On-Premise hardware en software
 - 3.2 Netwerkinfrastructuur
 - 3.3 Telefontie
 - 3.4 Applicatielandschap
 - 3.4 Microsoft Azure
 - 3.5 Client management

1. Inleiding

Dit document beschrijft de huidige en gewenste situatie (IST-SOLL) van de gehele ICT-omgeving van de gemeente Huizen. Het biedt een overzicht van de bestaande infrastructuur, software, hardware, telefonie, printers, speciale toepassingen en de Azure-omgeving, en schetst de gewenste toekomstige situatie.

Het doel van dit document is om potentiële ICT-dienstverleners een volledig beeld te geven van de huidige ICT-landschap en de transitie die wij voor ogen hebben. Het dient als leidraad om te begrijpen welke systemen en technologieën momenteel in gebruik zijn, welke verbeteringen en veranderingen gewenst zijn, en hoe een nieuwe ICT-dienstverlener hierin een rol kan spelen.

De volgende aspecten komen aan bod:

- **On-premise software en hardware:** Beschrijving van de bestaande oplossingen, inclusief servers, opslag en netwerken.
- **Telefonie en communicatie:** Overzicht van de huidige telefonie-infrastructuur en -diensten.
- **Printvoorzieningen:** Inventarisatie van printers en multifunctionele apparaten.
- **Applicatielandschap:** Overzicht van het applicatielandschap.
- **Azure-omgeving:** Uiteenzetting van de huidige cloud-omgeving en onze toekomstige ambities hierin.
- De (digitale) werkplek en mobiele devices

Met dit document streeft de gemeente Huizen naar een heldere en gestructureerde samenwerking met een nieuwe ICT-dienstverlener, gericht op een toekomstbestendige en efficiënte ICT-omgeving.

2. Huidige situatie

In dit hoofdstuk wordt de huidige ICT-omgeving van de gemeente Huizen in kaart gebracht. Het omvat een overzicht van de bestaande infrastructuur, waaronder on-premise software en hardware, netwerken, telefonie, printers, speciale toepassingen en de Azure-omgeving. Deze beschrijving biedt inzicht in de huidige stand van zaken en vormt de basis voor de overgang naar de gewenste toekomstige situatie.

2.1 On-Premise Software en Hardware

De gemeente beschikt over een hybride ICT-infrastructuur, waarin een deel van de software en hardware nog on-premise is ingericht. De on-premise infrastructuur omvat zowel hardwarecomponenten, zoals servers, opslag en netwerkkapparatuur, als software voor de dienstverlening. Dit onderdeel beschrijft de huidige inrichting van de on-premise omgeving, de gebruikte technologieën en de rol ervan binnen het bredere ICT-landschap van de gemeente.

De on-premise infrastructuur van de gemeente omvat de volgende componenten:

1. Servers en hardware

Hypervisors:

- 1x Dell PowerEdge R430 Server: Draait op Windows Server 2016.
- 2x Dell PowerEdge R440 Servers: Draait op Windows Server 2019 Standard.

Opslag:

- Dell Powervault ME412 SAN: Centraal opslagplatform voor data en virtuele machines.

2. Besturingssysteem

- Alle fysieke en virtuele servers draaien op het Windows-besturingssysteem.

3. Applicaties

- De servers worden gebruikt voor het beheer en de uitvoering van essentiële gemeentelijke diensten en applicaties, waaronder:
- Domaincontrollers
- Netwerkbeheerssoftware
- Distributiepunt SCCM
- Telefoniesoftware

4. Virtualisatie

- Hypervisor-software: Hyper-V wordt gebruikt voor virtualisatie.
- Virtuele machines (VM):
- De servers hosten verschillende virtuele machines. Een gedetailleerd overzicht van welke software op welke VM draait, is opgenomen in [bijlage 9i GemHZ_VMs.xlsx](#) (Deze bijlage is op verzoek toe te sturen en op deze stukken is een geheimhoudingsverklaring van toepassing. Meer informatie over de geheimhoudingsverklaring en het toezenden van de betreffende stukken is terug te vinden in de aanbestedingsomgeving van TenderNed).

5. Onderhoudsstatus

- Afschrijvingstermijn: De hardware bevindt zich in de laatste fase van de afschrijvingstermijn.
- Einde ondersteuning: Een overzicht van de specifieke data over het einde van de support is opgenomen in [bijlage 7c](#).

2.2 Netwerkinfrastructuur

In de huidige situatie is de gemeente Huizen eigenaar van alle netwerkkapparatuur. De netwerkinfrastructuur is gedocumenteerd en uitgewerkt in een Layer 1-, Layer 2- en Layer 3-netwerktekening, op deze stukken is een geheimhoudingsverklaring van toepassing. Meer informatie

over de geheimhoudingsverklaring en het toezenden van de betreffende stukken is terug te vinden in de aanbestedingsomgeving van TenderNed". Alle netwerkapparatuur is opgenomen in bijlage 7c Lijst met hardware.

2.2.1 Palo Alto Global Protect VPN

Gemeente Huizen maakt gebruik van GlobalProtect VPN van Palo Alto Networks om veilige toegang te bieden tot bepaalde applicaties en de netwerkschijven. Deze oplossing zorgt ervoor dat medewerkers overal en altijd op een veilige manier verbinding kunnen maken met de interne netwerkomgeving, ongeacht hun locatie.

2.3 Telefonie en Communicatie

In de huidige situatie maakt de organisatie voor vaste telefonie gebruik van VNG GT Vast (geleverd door VodafoneZiggo) in combinatie met de telefonieoplossing van Mitel. Deze zorgt ervoor dat oproepen naar het vaste doorkiesnummer worden doorgezet naar het mobiele nummer van de desbetreffende medewerker. Elke medewerker beschikt over de Mitel MiCollab-software op de werkplek. Deze software biedt een centrale plek voor communicatie, maar kent beperkingen in flexibiliteit en integratie met andere moderne digitale werkplekoplossingen.

Daarnaast maken de mobiele telefoons van medewerkers gebruik van simkaarten van Odido, wat de mobiele bereikbaarheid van het personeel garandeert.

2.4. Printvoorzieningen

De gemeente gebruikt Xerox multifunctional printers, 2 x Xerox AltaLink C8070 en 10 x Xerox AltaLink C8030/C8035. Deze worden geleverd en onderhouden door een externe leverancier. Deze leverancier levert ook de bijbehorende software, SafeQ6 (van Ysoft), voor follow-me printen en scannen naar email.

2.5 Applicatielandschap

Het applicatielandschap van Gemeente Huizen is volop in beweging. De organisatie maakt gebruik van vele verschillende applicaties (zie bijlage 7b Lijst met Applicaties). Het huidige applicatielandschap van de organisatie is een mix van on-premise applicaties, gehoste applicaties in Azure, maatwerkoplossingen en SaaS-diensten. Sommige applicaties draaien nog op fysieke servers binnen de eigen infrastructuur, zoals de Aruba en Mitel software, terwijl andere al zijn gemigreerd naar de Huizen Azure cloud. Hierdoor is het beheer van het applicatielandschap complex en vereist het veel inspanning om een consistente werking, beveiliging en integratie tussen systemen te waarborgen.

De applicaties in de fysieke serverruimte en in Azure worden door de huidige ICT-dienstverlener technisch beheerd. De applicaties die aangeboden worden als SaaS worden door de SaaS leveranciers zelf beheerd. Het functioneel beheer wordt gedaan door de functioneel beheerders van de gemeente Huizen.

De Microsoft 365 applicaties zijn een essentieel onderdeel van het applicatielandschap. Deze suite van applicaties, zoals Word, Excel, PowerPoint, Outlook en Teams, vormt de kern van de digitale werkplek en wordt breed ingezet door medewerkers voor dagelijkse werkzaamheden, communicatie en samenwerking. De organisatie maakt gebruik van E5-licenties. Gemeente Huizen is eigenaar van de E5 licenties.

2.5.1 Type applicaties

In de onderstaande tabel worden de verschillende typen applicaties weergegeven die door de gemeente Huizen worden gebruikt. Elk type applicatie brengt een specifieke beheerlast met zich mee, variërend van zeer minimale inspanningen tot het volledige beheer, inclusief hosting en het beschikbaar stellen van een client-serverapplicatie.

Type applicatie	Beschrijving
Type 0	Applicatie die op hardware van een individuele gebruiker wordt geïnstalleerd. De rol van de inschrijver is beperkt tot het beoordelen of installatie van de applicatie past binnen de securitykaders. De gebruiker krijgt geen ondersteuning bij het gebruik van de applicatie. Deze applicaties worden niet centraal door de gemeente gecoördineerd en staan daarom niet op de applicatielijst.
Type 1	Snelkoppeling naar website, bijvoorbeeld voor SaaS-applicaties.
Type 2	Client-only applicatie.
Type 3	Client-server applicaties.

Tabel 2.5.1 – Types applicaties

2.6 Microsoft Azure omgeving Gemeente Huizen

De Microsoft Azure-omgeving van de gemeente is ingericht als een schaalbare en veilige infrastructuur voor het hosten van bedrijfsapplicaties, opslagoplossingen en ondersteunende IT-diensten. Deze omgeving bestaat uit vijf subscriptions, waarvan één fungeert als de hoofdscription. Alle resources zijn gehost in de regio West-Europa, en de infrastructuur is opgedeeld in 25 resource groups voor een gestructureerd beheer. Een overzicht van de opzet en inrichting van de Azure omgeving van Opdrachtgever is toe te sturen, op deze stukken is een geheimhoudingsverklaring van toepassing. Meer informatie over de geheimhoudingsverklaring en het toezenden van de betreffende stukken is terug te vinden in de aanbestedingsomgeving van TenderNed".

2.6.1 Virtuele machines en hun functionaliteiten

De virtuele machines (VM's) in de Azure-omgeving ondersteunen een breed scala aan bedrijfsprocessen en infrastructuurbehoeften. De belangrijkste toepassingen zijn:

- **Bedrijfsapplicaties:** Diverse kritieke applicaties van de gemeente draaien op Windows-servers
- Ondersteunende applicaties:
 - Scan- en OCR-oplossingen: Automatiseren en digitaliseren van documenten.
 - Follow-me printstelsysteem: Voor veilige en efficiënte printoplossingen.
- **Opslag:** Twee Windows-fileservers bieden gedeelde netwerkopslag aan gebruikers en systemen.
- **Remote Desktop Services (RDS):** Een RDS-omgeving is ingericht voor het hosten van de bedrijfsapplicatie Civision Samenlevingszaken.
- **UiPath automatiseringsomgeving:** Twee servers en clients ondersteunen de UiPath-automatiseringsoplossingen.
- **Databaseservers:** De omgeving ondersteunt meerdere database-oplossingen, waaronder Oracle, SQL, en PostgreSQL.
- Infrastructuurservers:
 - Domeincontrollers (DC)
 - Azure AD Connect: Voor synchronisatie tussen de on-premise Active Directory en Azure AD.
 - Certificate Services: Voor beveiligde certificaatuitgifte.
 - Logging en monitoring: Servers voor logging en monitoring, waaronder Paessler PRTG, die toezicht houden op de beschikbaarheid en prestaties.
 - Applicatiedeployment en clientmanagement: Beheerd via SCCM (System Center Configuration Manager).
- **Server voor beheerswerkzaamheden:** Ondersteunt IT-beheerders bij dagelijkse operationele taken.

De lijst met VM's en waar deze gehost zijn, is op verzoek toe te sturen, op deze stukken is een geheimhoudingsverklaring van toepassing. Meer informatie over de geheimhoudingsverklaring en het

toezenden van de betreffende stukken is terug te vinden in de aanbestedingsomgeving van TenderNed".

2.6.2 Toegang en beveiliging

De beveiliging van de Azure-omgeving is ingericht om zowel interne als externe toegang te beheren:

- **Toegang voor externe leveranciers:** Externe leveranciers krijgen toegang tot de virtuele machines via Azure Bastion. Hierbij zijn gebruikersgroepen ingericht per leverancier en maken leveranciers gebruik van naam gebonden accounts, wat de traceerbaarheid verhoogt.
- **Geen gebruik van Connection Strings:** Er worden geen Connection Strings gebruikt, wat het risico op ongeautoriseerde toegang minimaliseert.
- **Application Gateways:** Er zijn twee application gateways ingericht. Een voor het ontsluiten van de zelf ontwikkelde webapplicaties van de gemeente en de andere biedt toegang tot een DMZ-server.

2.6.3 Virtual Network (VNet)

De Azure-omgeving van de gemeente is ingericht met een Virtual Network (VNet)-architectuur die de basis vormt voor de netwerkconnectiviteit en -segmentatie tussen verschillende systemen en applicaties. Hieronder worden de belangrijkste onderdelen van de VNet-configuratie beschreven.

Hoofd Virtual Network

De omgeving bevat één hoofd-VNet waarin meerdere subnets zijn ingericht. Deze subnets zijn gesegmenteerd op basis van specifieke functies en workloads. Dit ontwerp zorgt voor overzichtelijke netwerkbeheer en minimaliseert het risico op ongeautoriseerde toegang.

Er is een VNet-peering geconfigureerd naar een extern netwerk:

- **Peer-to-peer verbinding:** Het VNet is verbonden met een netwerk in een aparte Azure-subscriptie.
- **Toepassing:** Deze peering biedt veilige toegang voor een software ontwikkelteam van de gemeente, dat in deze subscriptie applicaties ontwikkelt. De applicaties in dit netwerk hebben gecontroleerde toegang tot resources in de omgeving van de gemeente.

ExpressRoute VPN:

- **Connectiviteit:** De gemeente maakt gebruik van een ExpressRoute-verbinding om de on-premise infrastructuur te verbinden met de Azure-omgeving.
- **Fysieke Verbinding:** Deze verbinding loopt via een fysieke KPN-router, die is geplaatst in het gemeentehuis.
- **Verkeer:** Binnen Azure wordt verkeer over de ExpressRoute-tunnel geleid naar de on-premise omgeving. Daar wordt het verder ontsloten via de firewall en routing van het lokale netwerk.
- **Firewallbeheer:** De VPN-inrichting op de on-premise firewall valt buiten de Azure-configuratie en wordt lokaal beheerd.

2.6.4 Data-gedreven werken

De gemeente Huizen richt zich actief op data-gedreven werken om beleidsvorming en besluitvorming te ondersteunen. Dit gebeurt door gebruik te maken van Microsoft Fabric en SAS. Deze activiteiten worden uitgevoerd binnen twee aparte Microsoft Azure-subscription.

Op dit moment maakt Microsoft Fabric verbinding met verschillende databronnen, namelijk:

- Digitaal LeefPlein (DLP)
- LDF
- iCollect

- Civision Samenlevingszaken
- Adminportal database

Het Digitale Leefplein (DLP) maakt verbinding via een API, terwijl de overige databronnen worden benaderd via een directe databaseverbinding.

2.6.5 Webapplicatieontwikkeling

De gemeente ontwikkelt eigen webapplicaties binnen specifieke subscriptions die uitsluitend voor dit doel zijn ingericht. Deze App Services worden ontsloten via een Azure Application Gateway. Dit geeft de gemeente controle over de ontwikkeling en het beheer van deze applicaties.

Momenteel bevinden zowel de productie- als testomgeving van de ontwikkelde softwareproducten zich binnen dezelfde subscription. Hoewel dit functioneel werkt, kan het leiden tot complexiteit in governance en verhoogde risico's door mogelijke overlapping tussen de omgevingen.

2.6.6 Active directory

De gemeente Huizen beschikt over een hybride Active Directory (AD)-omgeving. Tot 2018 maakte de gemeente gebruik van een volledig on-premise Active Directory, die lokaal werd beheerd. Sindsdien is deze on-premise omgeving gemigreerd naar de Microsoft Azure-cloudomgeving. Deze overstap heeft bijgedragen aan een meer flexibele en schaalbare infrastructuur voor identiteits- en toegangsbeheer.

Binnen deze hybride setup worden diverse applicaties gekoppeld aan de Azure AD-omgeving om toegang te verlenen aan medewerkers. Voorbeelden hiervan zijn het HR-systeem Motion en iConnect van Pinkroccade, die essentieel zijn voor processen zoals personeelsbeheer en interne communicatie. In bijlage 7b Lijst met Applicaties staat een overzicht van de applicaties die zijn gekoppeld aan de Active Directory.

Daarnaast maakt de gemeente gebruik van Microsoft Entra ID (voorheen bekend als Azure AD), een uitgebreide oplossing voor identiteitsbeheer die onder andere Single Sign-On (SSO), Multi-Factor Authentication (MFA) en beveiligde toegang tot cloudapplicaties mogelijk maakt. Entra ID en Microsoft Active Directory synchroniseren elke dag met elkaar.

2.6.7 Regionale inrichting en resourcebeheer

Alle resources binnen de Azure-omgeving zijn gecentraliseerd in de regio West-Europa. Deze regionale focus zorgt voor optimale prestaties, lage latentie en naleving van de Europese regelgeving voor gegevensbescherming. De resources zijn verdeeld over verschillende resource groups, wat bijdraagt aan een overzichtelijke en efficiënte organisatie van de infrastructuur.

2.7 Client management

In dit onderdeel wordt beschreven hoe de gemeente het client management heeft ingericht voor het beheer van laptops, smartphones en tablets. Hiervoor wordt gebruikgemaakt van SCCM en Microsoft Intune, twee krachtige tools die het mogelijk maken om apparaten efficiënt en veilig te beheren, zowel binnen als buiten het bedrijfsnetwerk.

2.7.1 Laptops

De laptops binnen de gemeente worden beheerd door een combinatie van SCCM en Microsoft Intune, die samen zorgen voor een efficiënt en veilig client management. De Windows clients zijn co-managed, wat betekent dat zowel SCCM als Intune een rol spelen in het beheer en de configuratie van de apparaten.

SCCM is verantwoordelijk voor de initiële installatie van het besturingssysteem, de configuratie van de laptops en de deployment van applicaties. Via een Task Sequence in SCCM worden nieuwe laptops

geconfigureerd. Daarnaast verzorgt SCCM de uitrol van de bedrijfsapplicaties. Deze applicaties worden toegewezen aan gebruikersgroepen, die worden beheerd in Active Directory. De toewijzing van de gebruikers aan de groepen wordt bepaald door de gemeente zelf. Voor verdere configuratie maakt de gemeente gebruik van Group Policies via SCCM. Dit zorgt ervoor dat alle configuraties in lijn zijn met de bedrijfsstandaarden en beveiligingsrichtlijnen. Updates van de bedrijfsapplicaties worden beheerd door SCCM Applications, die door de gemeente worden aangevraagd en door OGD worden gebouwd. De uitrol van deze applicaties gebeurt volgens de gedefinieerde gebruikersgroepen.

Intune speelt een cruciale rol in het beheer van device configuration policies, update policies en het monitoren van de apparaten. De OS-updates worden vanuit Intune beheerd via Update Rings. Er zijn al verschillende updategroepen gedefinieerd.

Op deze manier zorgen SCCM en Intune samen voor een gestroomlijnd en effectief beheer van de laptops binnen de gemeente, waarbij zowel de configuratie, updates, als applicaties efficiënt worden uitgerold en gemonitord.

2.7.2 Smartphone en Tablet management

Voor het beheer van smartphones en tablets maakt de gemeente gebruik van Microsoft Intune, waarmee een breed scala aan beheertaken wordt uitgevoerd. Zie bijlage 7c Lijst met hardware voor de complete lijst van alle devices.

De volgende diensten van Intune worden ingezet:

- Compliance Policies voor het definiëren van beveiligings- en conformiteitsvereisten.
- Configuration Policies voor het instellen van apparaatspecifieke configuraties.
- Endpoint Security voor compliance, beveiligingsmonitoring en rapportage.
- Applicatie Deployment voor het distribueren van mobiele apps.
- Reports voor monitoring en troubleshooting van apparaten en applicaties.
- Windows Update deployment voor het beheren van updates op apparaten.
- Koppelingen met Apple Store, Apple Business Management, Apple Enrollment Program Token en MDM voor het beheren van Apple-apparaten.

Met Intune wordt alleen het beheer van mobiele applicaties voor iOS-apparaten, zoals iPhones en iPads, uitgevoerd. Dit gebeurt via een koppeling met de Apple Business beheersomgeving.

Vanuit Intune worden de applicaties aangeboden aan specifieke gebruikersgroepen. Gebruikers kunnen via de Bedrijfsportaal-app op hun iPhone of iPad toegang krijgen tot de beheerde applicaties. Via de beheerde Apple Store kunnen zij vervolgens de benodigde applicaties installeren. Dit proces zorgt ervoor dat de applicaties centraal beheerd worden en voldoet aan de beveiligings- en configuratienormen van de gemeente.

Op deze manier biedt Intune volledige ondersteuning voor het beheer van iOS-apparaten en zorgt het ervoor dat de smartphones en tablets van de gemeente effectief en veilig worden beheerd.

3. Toekomstige situatie

De toekomstige ICT-architectuur van de organisatie is gericht op het creëren van een schaalbare, flexibele en toekomstbestendige infrastructuur. Hierbij is er een duidelijke visie op een aantal essentiële aspecten die snel moeten worden doorgevoerd. Tegelijkertijd wordt erkend dat bepaalde onderdelen van de architectuur nog in ontwikkeling zijn. Voor deze elementen wordt een partner gezocht die dankzij uitgebreide ervaring en expertise bij andere klanten proactief meedenkt, adviseert en ondersteunt bij het realiseren van innovatieve oplossingen. Met deze aanpak wordt een ICT-

landschap gerealiseerd dat niet alleen voldoet aan de eisen van vandaag, maar ook toekomstbestendig is.

3.1 On-Premise hardware en software

In de gewenste toekomstige situatie wordt volledig afscheid genomen van de on-premise servers en wordt de serverruimte afgeschaald. Alle IT-infrastructuur en applicaties worden ondergebracht in Azure of afgenomen als SaaS-diensten bij gespecialiseerde leveranciers. Deze verschuiving biedt aanzienlijke voordelen voor de organisatie, zowel op korte als lange termijn, en sluit aan bij de wens om een moderne, flexibele en schaalbare IT-omgeving te creëren.

Het beheer van de IT-infrastructuur wordt hierdoor sterk vereenvoudigd. Omdat er geen fysieke servers meer onderhouden hoeven te worden, vervalt de noodzaak van tijdrovende taken zoals het vervangen van hardware en het installeren van updates. In plaats daarvan biedt Azure een centraal platform waarmee het beheer en de monitoring van de IT-omgeving volledig digitaal en geautomatiseerd kunnen plaatsvinden.

Daarnaast verlaagt deze aanpak de kosten aanzienlijk. Grote investeringen in hardware en serverruimte zijn niet langer nodig, wat een directe financiële verlichting betekent. Het kostenmodel verschuift naar een flexibel “pay-as-you-go”-principe, waardoor alleen betaald wordt voor daadwerkelijk gebruik. Dit maakt het mogelijk om IT-kosten beter te beheren en aan te passen aan de behoeften van de organisatie.

De overstap naar Azure en SaaS-diensten biedt schaalbaarheid en flexibiliteit. Wanneer de vraag naar IT-resources groeit, kan de omgeving eenvoudig en vrijwel direct worden opgeschaald. Dit maakt het bijvoorbeeld mogelijk om snel in te spelen op piekbelastingen of nieuwe projecten.

De continuïteit van de dienstverlening wordt gewaarborgd door de hoge beschikbaarheid en herstelmechanismen van Azure. Dankzij ingebouwde back-up- en disaster recovery-oplossingen blijft de organisatie operationeel, zelfs bij onverwachte storingen of calamiteiten.

Een uitzondering binnen deze nieuwe situatie betreft de RAAS-server. Deze blijft nog wel bestaan, maar het beheer ervan wordt volledig verzorgd door de Rijksdienst voor Identiteitsgegevens (RvIG). Hierdoor wordt de organisatie ontzorgd van het technische beheer van deze specifieke server en blijft deze cruciale functionaliteit gewaarborgd.

3.2 Netwerkinfrastructuur

VPN naar Zero Trust Architectuur (ZTA)

In de toekomstige situatie zetten we een fundamentele stap in het moderniseren en versterken van onze IT-werkplek door de traditionele VPN-oplossing uit te faseren en over te stappen naar een Zero Trust Architectuur. Deze transitie is essentieel in een tijd waarin de grenzen tussen interne netwerken en de buitenwereld steeds meer vervagen door cloudadoptie, hybride werken en de toename van SaaS-oplossingen.

Het traditionele VPN-model biedt een veilige verbinding naar interne bronnen, maar kent beperkingen in een moderne, gedistribueerde IT-omgeving. Een VPN vertrouwt impliciet op de identiteit van de gebruiker en biedt na verbinding vaak brede toegang tot het netwerk. Zero Trust daarentegen elimineert dit impliciete vertrouwen en hanteert het principe “Never Trust, Always Verify”.

Zero Trust gaat uit van:

- **Identiteitsgestuurde toegang:** Toegang wordt alleen verleend op basis van de identiteit van de gebruiker en de context (locatie, apparaat status, tijdstip).
- **Microsegmentatie:** Gebruikers krijgen alleen toegang tot specifieke applicaties of data die zij nodig hebben, zonder toegang tot het bredere netwerk.

- **Continue verificatie:** Toestemmingen worden voortdurend geëvalueerd en herzien, waarbij gedragsanalyses en risicosignalen centraal staan.

Met de overgang naar Zero Trust zullen gebruikers profiteren van snellere en eenvoudigere toegang tot applicaties en data, zonder de noodzaak voor VPN-verbindingen. Toegang wordt gepersonaliseerd, zodat gebruikers alleen de gegevens en applicaties kunnen benaderen die voor hen relevant zijn, wat de efficiëntie verhoogt. Deze naadloze, veilige toegang verbetert de productiviteit, vooral voor hybride en remote werkmodellen, zonder concessies te doen aan de gebruikerservaring.

3.3 Telefonie

In de toekomstige situatie beschikt de organisatie over een moderne telefonieoplossing die naadloos integreert met de digitale werkplek en de IT-architectuur. Deze oplossing biedt medewerkers de flexibiliteit om communicatie en samenwerking vanuit één centrale omgeving te beheren, ongeacht locatie of apparaat.

Telefonie wordt volledig geïntegreerd met cloudgebaseerde tools zoals Microsoft Teams, waardoor medewerkers direct kunnen bellen vanuit hun werkplek of eenvoudig kunnen schakelen tussen spraak, video en chat. De oplossing sluit aan op de IT-architectuurprincipes, met nadruk op schaalbaarheid, beveiliging en hoge beschikbaarheid, ondersteund door authenticatie via Entra ID.

Deze aanpak vermindert complexiteit, verlaagt beheerkosten en maakt de organisatie klaar voor toekomstige ontwikkelingen in communicatie en samenwerking.

3.4 Applicatielandschap

Groei van SaaS applicaties

De huidige trend is dat leveranciers steeds meer overstappen naar Software-as-a-Service (SaaS)-oplossingen. Deze verschuiving betekent dat minder applicaties in onze Azure-omgeving gehost zullen worden, omdat deze functionaliteiten direct via SaaS aangeboden worden. In de toekomstige situatie zien wij veel applicaties verdwijnen uit de Huizen Azure omgeving, omdat de softwareleverancier het product “VerSaaS” heeft.

Dit biedt kansen voor:

- **Kostenbesparing en eenvoudiger beheer:** Minder operationele overhead en onderhoud van applicaties in onze eigen cloudomgeving.
- **Focus op integratie:** De uitdaging verschuift van hosting naar het koppelen van SaaS-oplossingen met onze gemeentelijke processen en systemen.

Onze rol verandert van primair beheerder naar regisseur van een landschap waarin SaaS-oplossingen een centrale plaats innemen. Dit vraagt om een strategische samenwerking met een dienstverlener die expertise heeft in het orkestreren van hybride IT-omgevingen.

Groei van interne ontwikkelingen

Naast het werken met SaaS en standaardoplossingen blijven we investeren in maatwerkontwikkeling. Onze softwareontwikkeling en het uitbreiden van ons datawarehouse zijn essentiële pijlers in onze infrastructuur:

- **Softwareontwikkeling:** Het bouwen van applicaties die specifieke gemeentelijke processen ondersteunen, met gebruik van moderne frameworks en DevOps-principes in Azure.
- **Datawarehouse:** Het centraliseren van data voor analyse, rapportage en beleidsondersteuning. Deze omgeving blijft groeien en wordt verder verrijkt met data uit nieuwe bronnen.

Microsoft 365 applicaties

In de toekomstige situatie blijft Microsoft 365 Apps een centrale rol spelen binnen het applicatielandschap van de organisatie, maar wordt er meer focus gelegd op het optimaal benutten van de mogelijkheden die de suite en de E5-licenties bieden. Teams, SharePoint en andere applicaties zullen intensiever en doelgerichter worden ingezet om samenwerking en productiviteit te verbeteren.

Functioneel beheer van de Microsoft 365-applicaties wordt intern belegd, wat zorgt voor snellere ondersteuning, betere aansluiting op de organisatorische behoeften en meer grip op het gebruik van de suite en onze data.

Kunstmatige intelligentie

In de komende jaren zal het applicatielandschap ingrijpend transformeren door de integratie van AI-technologieën. AI zal niet alleen processen automatiseren, maar ook de dienstverlening naar een hoger niveau tillen. Denk hierbij aan AI-gestuurde chatbots die inwoners proactief ondersteunen, en geavanceerde AI-modellen die voorspellingen doen en diepgaandere analyses van data mogelijk maken. Deze ontwikkelingen zullen leiden tot efficiëntere processen, betere besluitvorming en een verbeterde interactie met inwoners.

Om deze transitie succesvol te maken, zoeken we een dienstverlener die niet alleen een cloud beheer beheerst, maar ook proactief kennis ontwikkelt en implementeert op het gebied van AI.

3.4 Microsoft Azure

In de komende jaren zal de Microsoft Azure-omgeving van de gemeente zich verder ontwikkelen naar een schaalbare infrastructuur, waarbij de focus ligt op optimalisatie, flexibiliteit en veiligheid. Door de overstap van veel “on-premise” software naar SaaS-oplossingen worden een groot aantal virtuele machines (VM's) afgeschaald, wat resulteert in een kostenbesparing en een vereenvoudigd beheer.

3.4.1 Azure Landing Zone

De gemeente streeft naar een moderne, schaalbare en veilige ICT-infrastructuur die flexibel inspeelt op de behoeften van een steeds digitaler wordende samenleving. Om dit te realiseren, worden Azure Landing Zones ingezet als fundament voor de toekomstige cloudomgeving. Deze zones bieden een gestandaardiseerde architectuur waarmee de gemeente consistent, veilig en efficiënt workloads in de cloud kan beheren. Azure Landing Zones ondersteunen de transitie naar een volledig cloudgebaseerde omgeving, waarbij de focus ligt op:

- **Flexibiliteit:** Een schaalbare omgeving die snel kan worden aangepast aan veranderende behoeften van de organisatie en burgers.
- **Centralisatie:** Eén platform voor het beheer van alle applicaties, gegevens en infrastructuur.
- **Veiligheid en Compliance:** Een omgeving die voldoet aan wet- en regelgeving, zoals de AVG, en die bescherming biedt tegen dreigingen.

Met deze aanpak legt de gemeente een solide basis voor innovatie en digitalisering, terwijl continuïteit en betrouwbaarheid van de dienstverlening worden gegarandeerd.

Software ontwikkeling & Data analyse

Het software team en data team behouden in de toekomstige situatie een eigen subscription. In de toekomstige situatie richten we onze Azure-omgeving zo in dat test- en productieomgevingen strikt gescheiden blijven, ook wanneer ze binnen dezelfde subscription bestaan.

Role-Based Access Control & Active directory

In de toekomstige situatie zal de nadruk liggen op Microsoft Entra ID. De nieuwe applicaties die als SaaS aangeboden worden zullen gekoppeld worden met Entra ID. De gemeente streeft naar een

efficiëntere en veiligere manier om toegang tot de IT-omgeving te beheren. In de toekomstige situatie willen we Role-Based Access Control (RBAC) implementeren, zodat gebruikers alleen toegang krijgen die passend is bij hun rol en verantwoordelijkheden. Dit is een kernonderdeel van onze visie op modern en veilig beheer, waarmee we de juiste balans willen bereiken tussen toegang en beveiliging.

3.5 Client management

In de toekomstige situatie wordt SCCM uitgefaseerd en wordt er volledig gebruik gemaakt van Microsoft Intune. Hiermee kan de toekomstige dienstverlener op afstand vanuit de cloud al het client management voor de gemeente regelen. Met de overgang naar een volledig cloud-gebaseerd beheer, zal de gemeente voortaan Microsoft Intune inzetten voor het beheer van alle apparaten.

Door het volledige beheer van laptops, smartphones en tablets te centraliseren in Intune, kunnen we alle apparaten eenvoudig configureren, beveiligen en monitoren via één enkele interface. Intune maakt het mogelijk om niet alleen Windows-apparaten, maar ook iOS- en Android-apparaten te beheren, wat zorgt voor een uniforme en gestroomlijnde aanpak voor het beheer van alle devices binnen de gemeente.