Technische Architectuur

2021-2025

Gemeente ’s-Hertogenbosch

Beschrijving Technische Architectuur Gemeente ’s-Hertogenbosch

Versie : 2021.1
Status : Definitief
Datum : 11 juni 2021

Versiebeheer

Versie	Datum	Aangepast door	Opmerking
2021.1	11-06-2021	Arjan Kieboom	

Inhoudsopgave

1. Inleiding 4
2. Netwerk en verbindingen 5
2.1 Technisch ontwerp 5
2.2 Verbindingen met externe netwerken 5
2.2.1 Verbindingen via publieke netwerken 5
2.2.2 Vaste directe verbindingen 7
2.3 Verbindingen via de integratielaag 7
2.4 Draadloos netwerk 7
3. Servers en dataopslag 8
3.1 Servers 8
3.1.1 Serverplatformen 8
3.1.2 Applicatie servers 8
3.1.3 Databases 8
3.2 Dataopslag en Back-up 9
3.2.1 Opslag 9
3.2.2 Back-up 9
4. Werkplekomgeving 10
4.1 Technische omschrijving werkplekomgeving 10
4.1.1 Werkstation 10
4.1.2 Mobiele devices 10
4.1.3 Telefoon/fax 10
4.1.4 Overige apparatuur 11
5. Voorwaarden SAAS applicaties en websites 12
5.1 Algemene voorwaarden SAAS applicaties en websites 12
5.2 Voorwaarden koppelingen externe applicaties 13
5.2.1 Asynchrone koppelingen 13
5.2.2 Synchrone koppelingen 13
5.2.3 DigiD koppelingen 13
5.3 Voorwaarden mailen vanuit externe applicaties 14
6. Standaarden 15
6.1 Generieke infrastructuur componenten 15
6.2 Protocollen 15
Bijlage 1: Actuele versies hard- en software 17
Bijlage 2: Gebruik van TLS en HTTP headers 19

1. Inleiding

De Technische Architectuur 2021-2025, afgekort ”TA2025”, beschrijft de ICT-infrastructuur van Gemeente ’s-Hertogenbosch. De ICT-infrastructuur is er om de gebruikers optimaal te ondersteunen in hun bedrijfsvoering en in het flexconcept dat wij als gemeente hanteren. De inhoud van de Technische Architectuur is daarom ook bepaald vanuit de ICT behoefte van de organisatie.

Doel van dit document
Om de complexiteit van de ICT-infrastructuur en het beheer ervan in de hand te kunnen houden, wordt voortdurend gestreefd naar standaardisatie, uniformiteit, centralisatie, schaalbaarheid en beheersbaarheid van zowel de hardware als de software. Vanwege deze redenen wordt alleen die software en hardware, die aan de in dit document beschreven technische eisen voldoet, in het gemeentelijke netwerk opgenomen. De TA2021 dient als onderdeel voor het programma van eisen van nieuwe software en stelt kaders waarbinnen toepassingen verplicht dienen te worden aangeboden en geïnstalleerd. Dit document geeft een momentopname weer, kleine aanpassingen in deze TA2021 worden autonoom of voortvloeiend uit intakeverzoeken doorgevoerd.

Reikwijdte
Dit document biedt een toetsingskader voor leveranciers om te bepalen of hun systeem binnen het netwerk van Gemeente ’s-Hertogenbosch geïnstalleerd kan worden. Vanwege de complexiteit van de ICT-infrastructuur en zijn uitgangspunten kan indien nodig een bijeenkomst belegd te worden met de afdeling ICT (M&D/ICT) en de technische specialisten van de kandidaat-leverancier om inzicht te krijgen in hoe een en ander ingericht dient te worden. Tevens heeft deze bijeenkomst tot doel, te inventariseren waar er zich eventuele knelpunten voordoen in relatie tot de TA2021.

De TA2021 is geschreven onder verantwoordelijkheid van en vastgesteld door het Hoofd ICT. Jaarlijks zal het document worden geëvalueerd, geactualiseerd en vastgesteld.

Referentiekader
De Technische Architectuur van Gemeente ’s-Hertogenbosch dient ter ondersteuning van de Informatiearchitectuur van de gemeente en valt binnen de kaders van het Beleid Informatieveiligheid.

Opbouw van dit document
Dit document geeft een beschrijving van de gemeentelijke ICT-infrastructuur waarop de nieuwe programmatuur (inclusief maatwerk) kan worden geïnstalleerd en/of waarmee nieuwe programmatuur in samenhang dient te functioneren. In hoofdstuk 2 tot en met 4 worden de belangrijkste componenten uit de technische architectuur beschreven. Hoofdstuk 2 is een beschrijving van het netwerk (LAN/WAN-Infrastructuur) van Gemeente ’s-Hertogenbosch. In hoofdstuk 3 is de dataopslag en de server omgeving beschreven en in hoofdstuk 4 de werkplekomgeving. Hoofdstuk 5 geeft de kaders weer waaraan SAAS oplossingen die door Gemeente ’s-Hertogenbosch worden ingezet moten voldoen. Hoofdstuk 6 ten slotte behandelt een aantal standaard componenten en protocollen die binnen Gemeente ’s-Hertogenbosch worden gehanteerd.

2. Netwerk en verbindingen

Het netwerk (LAN/WAN-infrastructuur) van Gemeente 's-Hertogenbosch is een modern netwerk dat is ingericht volgens de laatste stand der techniek. Het netwerk voldoet aan hoge eisen op het gebied van beschikbaarheid, schaalbaarheid, beheersbaarheid en beveiliging.

In paragraaf 2.1 is het fysieke netwerkontwerp van Gemeente 's-Hertogenbosch beschreven. In paragraaf 2.2 is weergegeven op welke wijze externen kunnen worden gekoppeld aan het netwerk van Gemeente 's-Hertogenbosch. In paragraaf 2.3 zijn de verbindingen via de gemeentelijke integratielaag beschreven en in 2.4 het draadloos netwerk.

2.1 Technisch ontwerp

Op de vijf hoofdlocaties binnen het netwerk zijn centrale switches geplaatst. Deze zijn langs verschillende fysieke routes met elkaar verbonden, waardoor een storing op één van de locaties niet leidt tot storingen op de overige locaties. Tussen deze vijf hoofdlocaties is een bandbreedte van 40 Gb/sec beschikbaar.

De computerruimte van Gemeente 's-Hertogenbosch is verspreid over twee fysiek gescheiden locaties. Twee centrale switches zorgen ervoor dat deze twee locaties samen één virtueel rekencentrum vormen.

Vanuit de centrale switches op de hoofdlocaties zijn, op basis van een redundante 10 Gb/sec koppeling, zowel de secundaire computerruimtes (SER's) als de nevenlocaties op access switches aangesloten. De serveromgeving is aangesloten via distributie switches.

De koppeling van het gemeentelijke netwerk met de buitenwereld is gerealiseerd door middel van redundant uitgevoerde (Perimeter) Firewalls, aangevuld met een Intrusion Prevention en Detection (IPS/IDS) module.

VLAN's (Virtueel Local Area Network) worden ingezet om verschillende omgevingen (zoals externe netwerken, opleidingsomgevingen, publieke omgevingen en productieomgeving) logisch te scheiden. Binnen de productieomgeving zijn ook de serveromgeving en de werkstationomgeving op deze manier van elkaar gescheiden.

2.2 Verbindingen met externe netwerken

Binnen de gemeente onderscheiden we twee verschillende soorten verbindingen met externe netwerken. Eigen vaste directe verbindingen en verbindingen via publieke netwerken zoals Gemnet en Internet. In deze paragraaf worden beide soorten verbindingen nader toegelicht.

2.2.1 Verbindingen via publieke netwerken

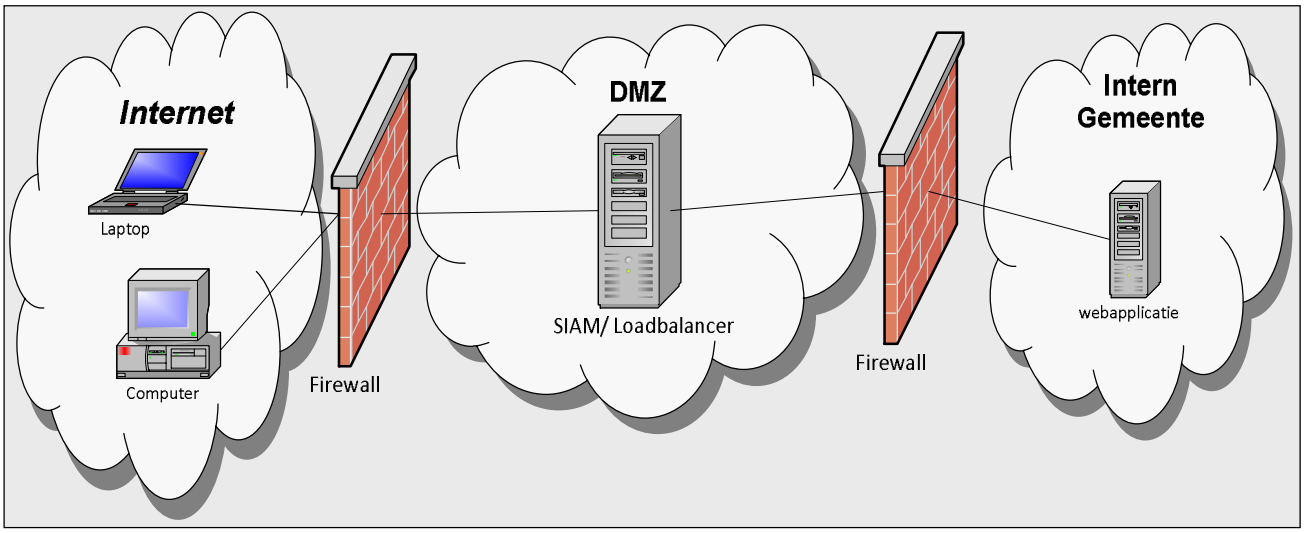
Binnen Gemeente 's-Hertogenbosch worden alle netwerken waarop partijen kunnen aansluiten zonder een overeenkomst met de gemeente 's-Hertogenbosch beschouwd als publieke netwerken. Het gaat hierbij dus niet alleen om het Internet maar ook om Gemnet. De toegang vanaf de werkplek naar het Internet, evenals verbindingen vanuit het Internet naar het interne netwerk, dienen op een veilige manier plaats te vinden. Het is daarom niet mogelijk rechtstreekse verbindingen op te bouwen tussen publieke netwerken en systemen in het gemeentelijke netwerk. Hiervoor wordt gebruik gemaakt van een DMZ (demilitarized zone).

Dit is een beveiligde zone tussen het interne netwerk en het Internet. Voor de verbindingen met de publieke netwerken zijn voorzieningen getroffen om deze op een beheersbare, schaalbare en veilige wijze mogelijk te maken.

Verbindingen van en naar publieke netwerken vinden altijd plaats op basis van de TCP/IP protocol suite. Het hierbij gebruikte DMZ faciliteert deze verbindingen via daarin geplaatste servers. Bij de communicatie van deze servers naar publieke netwerken en vice versa wordt gebruik gemaakt van network address translation (NAT) en al het verkeer wordt geïnspecteerd en gereguleerd door gebruik te maken van firewall- en IPS/IDS-technieken. De TCP-poorten die voor het opzetten van verbindingen naar publieke netwerken standaard kunnen worden gebruikt zijn 80/tcp (http), 443/tcp (https) en 4242/tcp en lopen altijd via in de DMZ geplaatste webproxy-servers of de "gemeentelijke integratielaag", servers t.b.v. synchroon en asynchroon berichtenverkeer. Andere verbindingen naar publieke netwerken zijn na overleg met specialisten van ICT mogelijk in de vorm van port-forwarding, een mechanisme waarbij een combinatie van een "Private Address Space" (rfc 1918) ip-adres en tcp-poort toegang geeft tot een op een publiek netwerk geplaatste dienst.

Verbindingen van publieke netwerken naar het gemeentelijke netwerk lopen eveneens via eerdergenoemd DMZ. Omdat het externe verkeer ook in het DMZ wordt getermineerd, moet er in het DMZ een dienst aanwezig zijn die, indien nodig, het verkeer op een veilige manier verder het gemeentelijke netwerk binnenleidt. Standaardfaciliteiten die daarbij kunnen worden gebruikt zijn in het DMZ geplaatste load balancers en de gemeentelijke integratielaag (zie paragraaf 2.3).

Voor een veilige gecentraliseerde internettoegang tot webbased applicaties binnen het gemeentelijke netwerk is een geïntegreerde oplossing ingericht. Dit framework biedt een veilige gecentraliseerde internettoegang tot webbased applicaties binnen het gemeentelijke netwerk. Ook draagt het framework zorg voor veilige authenticatie tot webbased applicaties, middels DigiD voor burgers en middels eHerkenning voor bedrijven. Hierbij is het mogelijk om gebruik te maken van verschillende beveiligingsniveaus. Ook is het mogelijk om interne webapplicaties beschikbaar te maken op het Internet via de reverse proxy functionaliteit van een loadbalancer. (zie figuur 1)



Figuur1 Verbindingen van extern naar intern

2.2.1.1 Remote beheer

Remote beheer moet plaatsvinden via een beveiligde verbinding die wordt ondersteund binnen de Technische Architectuur. Remote beheer vindt altijd plaats via een werkstation onder toezicht van een medewerker van Bureau Automatisering. Als standaard wordt vanuit Bureau Automatisering het pakket teamviewer gebruikt.

2.2.2 Vaste directe verbindingen

Voor het kunnen benaderen van toepassingen die bij derden (bijv. rekencentrum) draaien, kan gebruik worden gemaakt van vaste verbindingen tussen het gemeentelijke netwerk en derde partijen.

2.3 Verbindingen via de integratielaag

De integratielaag van de Gemeente s-Hertogenbosch is gemaakt om te dienen als intermediar van berichtenverkeer tussen applicaties. We onderscheiden twee soorten berichtenverkeer, synchroon en a-synchroon. Synchroon verkeer is verkeer dat rechtstreeks antwoord nodig heeft. Bijvoorbeeld als een gebruiker wacht op antwoord. Voor synchroon verkeer is een XML gateway ingericht, intern genoemd de Service Gateway. Al het synchrone serviceverkeer hoort via de Service Gateway te lopen.

Van buiten (SaaS) naar binnen geldt dat een 2-zijdige TLS verbinding noodzakelijk is op basis van de laatste beveiligingsstandaarden (TLS 1.2, TLS 1.3). Op basis van het meegeleverde client-certificaat wordt er geauthentiseerd en geautoriseerd. De certificaten moeten zijn uitgegeven door een vertrouwde instantie (dus niet self-signed), met organization validation en met moderne keysizes e.d.. Voor intern verkeer of 'van binnen naar buiten' is geen 2-zijdige TLS verbinding verplicht.

Voor a-synchroon verkeer wordt de ESB/Broker ingezet. De broker is de regisseur van een geautomatiseerd workflowproces. Queueing en foutafhandeling horen hier ook bij. De broker initieert en is regisseur van de hele keten. Indien gekoppeld wordt met een ESB-achtige oplossing, dan zal deze zozeer afgebakend worden, zodat de gemeentelijke broker in de lead blijft. Dit betekent dat applicaties met koppel/workflow mogelijkheden zich aan moeten passen, zodat de gemeentelijke ESB de regisseur blijft.

2.4 Draadloos netwerk

Ten behoeve van externen en eigen medewerkers is op bijna alle locaties in het gemeentelijke netwerk een draadloos netwerk met een Internetverbinding aangelegd. Dit netwerk is niet rechtstreeks verbonden met het gemeentelijke netwerk. Toegang tot het gemeentelijke netwerk verloopt dan ook net als bij andere externe verbindingen via de perimeter firewall.

3. Servers en dataopslag

Het serverpark van Gemeente ‘s-Hertogenbosch is een toekomstgericht serverpark dat zo effectief en efficiënt mogelijk is ingericht naar de huidige stand van de techniek. Voor dataopslag heeft de gemeente de beschikking over een centrale opslagomgeving die gebruik maakt van virtualisatie technieken.

Gemeente ’s-Hertogenbosch beschikt over twee fysieke serverruimtes die zich bevinden op verschillende locaties. De dataopslag van de gemeente is verspreid over deze twee locaties. Logisch gezien bestaat het serverpark uit vier strikt gescheiden omgevingen: de productieomgeving, de test/acceptatieomgeving, de ontwikkelomgeving en de opleidingsomgeving. Hierbij is de test/acceptatieomgeving zoveel mogelijk een kopie van de productieomgeving. De ontwikkelomgeving en de opleidingsomgeving zijn kleinschalig en worden ingezet voor specifieke projecten. Uitgangspunt is dat alle servers maken gebruik van een centrale dataopslag: een gevirtualiseerde centrale opslagomgeving welke redundant is uitgevoerd over twee locaties.

Op dit moment worden binnen Gemeente ’s-Hertogenbosch drie serverplatformen aangeboden: Windows, Linux en Solaris (Oracle SPARC(Oracle DB)). Het beleid van de gemeente is om alle servers zoveel mogelijk te virtualiseren. Dit wordt voor het Windows en Linux platform gedaan middels VMWare vSphere. De gevirtualiseerde systemen zijn verspreid over beide serverruimtes. De Oracle SPARC servers zijn fysieke redundant opgezette servers met lokale opslag, ook verspreid over beide serverruimtes.

3.1 Servers

3.1.1 Serverplatformen

Binnen de technische architectuur worden de volgende serverbesturingssytemen aangeboden: Windows, Linux, en Solaris (Oracle SPARC). De Windows servers worden ingezet als file- en printservers, applicatieservers en database servers. De Linux servers dienen als platform voor applicatieservers en database servers. De Solaris (Oralce SPARC) servers dienen alleen als database servers. De Windows en Linux servers zijn zoveel mogelijk gevirtualiseerd met behulp van vSphere. De Solaris (Oralce SPARC) servers zijn fysieke redundant opgezette servers met lokale opslag verspreid over de twee serverruimtes.

Het is efficiënter en meer beheersbaar om zoveel mogelijk standaard hardware in te zetten. In bijlage 1 zijn de specificaties van de huidige serverplatformen (hard- en software) weergegeven.

3.1.2 Applicatie servers

De applicatie servers worden aangeboden op de besturingssystemen Windows en Linux. De volgende applicatieservers worden ondersteund: Microsoft IIS (Internet Information Services, webserver voor .net toepassingen), Apache (http server), Tomcat (Java Servlet container) en Weblogic Application Server (applicatie omgeving voor JAVA-applicaties).

3.1.3 Databases

Als database omgeving worden de volgende databases ondersteund: Oracle en Microsoft SQL Server, waarbij het Oracle ons hoofdplatform is en normaliter de voorkeur geniet. Voor eenvoudige webapplicaties waar de data en applicatie niet (eenvoudig) gescheiden kunnen worden en zaken als schaalbaarheid, performance en redundancy minder van belang zijn, is ook het gebruik van MariaDB toegestaan.

3.2 Dataopslag en Back-up

3.2.1 Opslag

De opslagomgeving bestaat uit twee schijfsystemen op locaties Stadskantoor en Stadhuis. De opslagcapaciteit op deze systemen wordt ontsloten via een virtualisatielaag. In de schijfsystemen zitten SSD, SAS en NL-SAS schijven. In de schijfsystemen wordt "intelligente" functionaliteit geregeld zoals mirroring, thin provisioning, automatic tiering en het maken van snapshots. Er wordt gebruik gemaakt van automatic tiering, waarbij getiered wordt met SSD, SAS en NL-SAS schijven.

Synchronisatie van de data tussen de schijfsystemen op beide locaties vindt plaats door HyperMetro. HyperMetro plaatst van elke LUN een exemplaar op het schijfsysteem in het Stadskantoor en een kopie in het Stadhuis (of andersom) en houdt deze beide exemplaren synchroon.
Het grote voordeel van deze oplossing is dat bij het uitvallen van één van de computerruimtes (of een storing van een opslagcomponent) geen verstoring van de opslag services plaatsvindt, want de servers zien nog steeds dezelfde LUN's en hebben geen weet van de kopieën die HyperMetro maakt tussen beide locaties. De data integriteit is ook bij een verstoring gegarandeerd en rebooten van servers is niet nodig. Alle LUN's worden gespiegeld over de beide locaties en dus kan één ervan desgewenst verplaatst, gewijzigd of onderhouden worden zonder verstoring van de storage services.

Er zijn drie opslagcategorieën gedefinieerd: GOLD, SILVER en BRONZE.
GOLD: deze categorie bestaat uit SSD (78%) en SAS (22%) schijven. Deze categorie wordt gebruikt voor toepassingen die snelle opslag nodig hebben, zoals bv. SQL databases en opslag van gebruikersprofielen.
SILVER: deze categorie bestaat uit SSD (10%), SAS (77%) en NL-SAS (13%) schijven. De schijfruimte in deze categorie wordt gebruikt voor het VMWare ESX cluster.
BRONZE: deze categorie bestaat alleen uit NL-SAS schijven. De schijfruimte in deze categorie wordt gebruikt voor filesystemen op Windows servers.

Een ander voordeel van de virtualisatielaag is dat er verschillende merken en typen storage aan gekoppeld kunnen worden met behoud van functionaliteit.

3.2.2 Back-up

De back-up van alle omgevingen wordt gedaan door middel van een geïntegreerde oplossing en wordt weggeschreven naar schijfsystemen. Deze schijfsystemen staan op Stadskantoor, Stadhuis en Weener XL

Alle back-up data wordt opgeslagen op twee locaties, Stadskantoor en Weener XL òf Stadhuis en Weener XL. Hierbij wordt de initiële back-up gemaakt op een schijfsysteem op Stadskantoor of Stadhuis en vervolgens wordt deze data gekopieerd naar een schijfsysteem op Weener XL.

Van de Oracle databases wordt dagelijks een volledige back-up gemaakt. Van de overige platformen wordt in het weekend een volledige back-up gemaakt en de rest van de week een differential back-up. Elke maand wordt er een periode back-up gemaakt die één jaar wordt bewaard en jaarlijks wordt er een jaar back-up gemaakt die volgens de wettelijke gestelde bewaartermijnen worden bewaard. Voor de acceptatieomgeving is een bewaartijd van 2 maanden van toepassing. De periode- en jaarbackup vinden plaats op de eerste zaterdag van respectievelijk de maand en het jaar.

4. Werkplekomgeving

4.1 Technische omschrijving werkplekomgeving

In deze paragraaf is de werkplekomgeving van de Gemeente 's-Hertogenbosch verder uitgewerkt. Achtereenvolgens komen het werkstation, de mobiele devices, de VDI omgeving, telefoon, fax en randapparatuur aan de orde.

4.1.1 Werkstation

De werkstations binnen Gemeente 's-Hertogenbosch zijn zoveel mogelijk gestandaardiseerd. De standaard werkplek is gevirtualiseerd voor middel van Virtual Desktop Infrastructure (VDI) en is voorzien van een werkstation-image waarin de software is opgenomen die standaard aan alle gebruikers in het gemeentelijke netwerk wordt aangeboden. De VDI werkplekken zijn zowel binnen als buiten het gemeentelijke netwerk bereikbaar.

In Bijlage 1 is een lijst opgenomen met de standaard werkplek inrichting. Naast deze standaardsoftware worden, per gebruiker, gebruikersspecifieke toepassingen door middel van ZCM gedistribueerd naar de werkplekken. Op het werkstation hebben gebruikers geen administrator rechten. De Gemeente 's-Hertogenbosch werkt in een flex-concept, waarbij medewerkers geen vaste werkplek hebben. Tijdelijke bestanden met vertrouwelijke gegevens dienen daarom in het profiel van de medewerker in de map %APPDATA% te worden opgeslagen. Werkstations (clients) kunnen onderling niet rechtstreeks communiceren en servers kunnen niet rechtstreeks contact maken met een client. Het initiatief tot communicatie ligt altijd bij de client.

Het werkstation image wordt maximaal 2 keer per jaar vernieuwd. Tussentijdse updates in de standaardsoftware kunnen, indien nodig, door middel van ZCM/WSUS eerder worden geïnstalleerd op de werkplekken.

4.1.2 Mobiele devices

Ten behoeve van mobiel e-mail verkeer, agenda en telefoon wordt gebruik gemaakt van de iPhone. Daarnaast wordt er mobiel gewerkt op laptops en ultrabooks en wordt er in beperkte mate gebruikt gemaakt van iPads. Alle mobiele devices worden beheerd door middel van een MDM oplossing en zijn niet rechtstreeks gekoppeld met het gemeentelijk netwerk.

4.1.3 Telefoon/fax

Gemeente 's-Hertogenbosch anticipeert op veranderende communicatiebehoeften en mogelijkheden. Geïntegreerde applicaties, apparatuur, infrastructuur en VoIP zullen op termijn de standaard vormen voor communiceren. Daarom is geïnvesteerd in een infrastructuur die dit mogelijk maakt.

De telefooncentrale (een Openscape UC platform) is gemeentebreed ingezet. Eén gemeentelijk nummerplan is gerealiseerd. Aan de centrale is naast enkele analoge en digitale toestellen een VoIP omgeving gekoppeld ten behoeve van de overige gemeentelijke locaties. Verder is een voicemailsysteem, een Call Centeroplossing en een kostenregistratiesysteem aangesloten op de telefooncentrale.
De telefooncentrale en alle hierboven vermelde subsystemen zijn middels het zero-trust principe gekoppeld aan de gemeentelijke LAN/WAN omgeving. Alle faxen zijn analoog en worden aangesloten via een analoge

lijn of via een VoIP converter. Alle faxen zijn standalone opgesteld er wordt geen gebruik gemaakt van de fax-mogelijkheden op de multifunctionals.

4.1.4 Overige apparatuur

Naast de eerder beschreven componenten maken nog een aantal apparaten deel uit van de Technische Architectuur van Gemeente 's-Hertogenbosch. Deze worden in deze paragraaf beschreven. De specificaties van deze componenten zijn te vinden in Bijlage 1.

4.1.4.1 Printen/kopiëren/scannen

Ook de gebruikte printers en kopiers zijn binnen de gemeente zoveel mogelijk gestandaardiseerd. Er wordt zo veel mogelijk gebruik gemaakt van zwart/wit en kleuren multifunctionals die geschikt zijn voor printen en kopiëren (50 pagina's per minuut). Grote printopdrachten moeten gebruikers laten uitvoeren door de Repro. Op kleine locaties kan een kleinere zwart/wit multifunctional worden geplaatst.

Naast de standaard multifunctionals zijn er ook nog speciale printers voor Burgerzaken en Parkeervergunningen. Dit vanwege de wettelijke eisen die op dit gebied aan de printers worden gesteld. Verder wordt er binnen de technische architectuur ook nog een labelprinter ondersteund.

Door de afdeling Documentaire Zaken wordt binnengekomen post gescand op een hoog volume scanner. Op sommige decentrale locaties zijn kleinschalige USB Scanners geplaatst.

4.1.4.2 Memory Stick

Er wordt een standaard type memory stick (Kingston DataTraveler) geleverd, waarbij encryptie van opgeslagen data wordt afgedwongen.

5. Voorwaarden SAAS applicaties en websites

5.1 Algemene voorwaarden SAAS applicaties en websites

SAAS applicaties en extern gehoste websites die door de Gemeente 's-Hertogenbosch worden aangeschaft dienen aan de volgende voorwaarden te voldoen:

- De applicatie is een webapplicatie of webservice die werkt onder de in deze TA ondersteunde browsers en hoger met standaard beveiligingsinstellingen.
- De applicatie voldoet aan de beveiligingsrichtlijnen voor webapplicaties van het NCSC[1], is versleuteld met protocollen en algoritmen volgens de laatste stand van de techniek[2] en moet voldoen aan de pas-toe-of-leg-uit lijst (PTOLU) van het Forum Standaardisatie[3] (o.a. https://, DNSSEC, IPv6 etc.)
- Het gebruik van TLS en HTTP headers voldoet aan de laatste stand van de techniek. De vereiste maatregelen op dit punt zijn uitgewerkt in Bijlage 2, Gebruik van TLS en HTTP response headers.
- Webapplicaties maken bij voorkeur gebruik van een koppeling met Single Sign On (SSO) met Azure AD als de Identity Provider. De SAAS-leverancier mag hierbij gebruik maken van SAML 2.0 of Open-id connect (OAuth 2.0). We gaan uit van minimale set aan gegevens en attributen: voor- en achternaam, email en afdeling. Voor de toegang tot applicaties wordt gebruik gemaakt van Conditional Access. Indien SSO via Azure AD niet mogelijk is, is het mogelijk om de toegang tot de applicatie te beperken tot het IP-adres van het vaste netwerk van de gemeente (dit is niet mogelijk voor mobiele apps), of gebruik te maken van 2-factor authenticatie.
- Het datacentra van de hostende partij beschikt over een ISAE3402 - en/of ISO 27001-certificering.
- Indien er sprake is van de verwerking van persoonsgegevens dient er met de leverancier van de applicatie een verwerkersovereenkomst te worden afgesloten.
- De volgende aandachtspunten moeten in ieder geval worden opgenomen in de SLA met de leverancier:
    - methoden om toegang te verkrijgen (gebruikersnaam en wachtwoord, welke eisen worden hieraan gesteld)
    - een autorisatieproces voor toegang en rechten van gebruikers;
    - de verplichting tot het bijhouden van een lijst van geautoriseerde personen tot het gebruik van een dienst en hun rechten en privileges ten aanzien van een dergelijk gebruik;
    - beperkingen ten aanzien van het kopiëren en openbaar maken van informatie;
    - verantwoordelijkheden ten aanzien van installatie en onderhoud van hardware en software;
    - het beoogde niveau van de service (responsetijden, beschikbaarheid), evenals onaanvaardbare serviceniveaus;
    - het recht om contractueel vastgelegde verantwoordelijkheden te controleren of deze controle door een derde te laten uitvoeren;
    - het vaststellen van een escalatieproces voor het oplossen van problemen;
    - uitzonderingen en andere gebeurtenissen die van belang zijn voor de beveiliging worden vastgelegd in zogenaamde "audit logs", die tenminste het volgende bevatten:

[1] Zie https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html

[2] Zie https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet

[3] Zie: https://www.forumstandaardisatie.nl/lijst-open-standaarden/in_lijst/verplicht-pas-toe-leg-uit

- gebruikers-ID's;
- data en tijdstippen van aanloggen en afmelden;
- overzichten van geslaagde en geweigerde pogingen om toegang te krijgen tot het systeem;
- overzichten van geslaagde en geweigerde en andere pogingen om toegang te krijgen tot individuele onderdelen van het systeem en bestanden;
- overzichten van raadplegingen en mutaties inclusief gebruikers-ID's, data en tijdstippen in geval van verwerking van persoonsgegevens en of vertrouwelijke gegevens.

Toetsing van een volledige en correcte implementatie van deze voorwaarden vindt vóór in gebruik name in overleg met de gemeentelijke security-officer plaats. Deze toets zal jaarlijks worden herhaald. In geval van SAAS applicaties blijft de leverancier te allen tijden verantwoordelijk voor de goede en veilige werking inclusief compliancy van de complete oplossing.

5.2 Voorwaarden koppelingen externe applicaties

Koppelingen met een externe applicatie met een intern systeem van Gemeente 's-Hertogenbosch kunnen zowel synchroon als asynchroon plaatsvinden. Gezien de complexiteit geldt dat nieuwe ontwerpen van koppelingen altijd van een intakeprocedure lopen. Voor transportbeveiliging en vaststelling van identiteit over onvertrouwde netwerken wordt altijd, ongeacht het vertrouwelijkheidsniveau van de informatie, gebruik gemaakt van PKI. Bij informatieverwerkingen van persoonsgegevens en of gegevens met een vertrouwelijkheidsniveau van 'vertrouwelijk' of hoger, moeten mogelijk aanvullende maatregelen worden genomen. Deze afweging wordt gemaakt op de basis van de resultaten van dataclassificatie en risicoanalyse.

5.2.1 Asynchrone koppelingen

Asynchrone koppelingen tussen een intern systeem en een externe applicatie worden ondersteund op onderstaande wijzen:

- Vanuit de applicatie kunnen gegevens worden gepusht naar onze omgeving. Hierbij wordt gebruik gemaakt van ebMS XML of webservice berichtenverkeer wat in een interne queue wordt gezet voor onze broker.
- Vanuit een applicatie in het interne netwerk van Gemeente 's-Hertogenbosch wordt gepold op de gegevens in de applicatie. Dit gaat altijd via een veilige verbinding. Voor https koppelingen gebruiken we de Service Gateway. Voor sftp, ftps etc. gebruiken we GoAnywhere.
- Gegevens worden aangeboden aan een interne applicatie door middel van een webformulier en de broker.

Systeemtechnische koppelingen, zoals bijvoorbeeld automatische updates, kunnen via de webproxy of de loadbalancer lopen.

5.2.2 Synchrone koppelingen

Bij synchrone koppelingen wordt gebruik gemaakt van webservices om informatie tussen systemen uit te wisselen. Via een webservice aanroep wordt de benodigde informatie opgevraagd en direct teruggeleverd. De koppelingen met applicaties via webservices lopen via een Service Gateway.

5.2.3 DigiD koppelingen

Voor applicaties kan indien nodig een DigiD koppeling worden aangevraagd. De applicatie dient hiervoor te voldoen aan de eisen uit de DigiD cheklist testen van Logius en het Beveiligingsassessment DigiD. Voor het Beveiligingsassessment DigiD dient jaarlijks een TPM worden afgegeven door de SAAS-leverancier.

5.3 Voorwaarden mailen vanuit externe applicaties

Het beleid van de gemeente staat niet toe dat e-mail voor domeinen die gebruikt worden door de organisatie zelf wordt verstuurd via e-mail servers van derden. Mail kan worden verzonden via de volgende mogelijkheden:

1. E-mail versturen via externe, niet in beheer van de gemeente zijnde mailservers, met zelf aan te vragen domeinen (al bij de gemeente horende domeinen zoals @s-hertogenbosch.nl kunnen dus niet worden gebruikt). De oplossing moet voldoen aan het gemeentelijke beveiligingsbeleid en moet gebruik maken van de relevante technieken zoals op de pas-toe-of-leg-uit lijst (PTOLU) [4] staan vermeld (SPF, DKIM, DMARC, STARTTLS+DANE).

2. E-mail versturen via de gemeentelijke mailservers met al door de gemeente in gebruik zijnde domeinen. De gemeente biedt de mogelijkheid om via mutual TLS (MTLS) verbindingen met IP-restricties door derden te versturen e-mail in de vorm van xml-berichten te ontvangen, te converteren en via de eigen e-mail infrastructuur te versturen. Alle te versturen mail wordt verzonden namens een no-reply-adres. De voorwaarden voor het opzetten en gebruiken van een MTLS-verbinding inclusief xml-berichten worden door de gemeente in overleg met de externe partij bepaald.

[4] Zie: https://www.forumstandaardisatie.nl/open-standaarden/verplicht

6. Standaarden

6.1 Generieke infrastructuur componenten

Generieke componenten zijn beheerdiensten die zorgen voor het afhandelen van de belangrijkste centrale functies binnen het gemeentelijke netwerk, die om redenen van beheer centraal zijn ingericht. Deze generieke componenten zijn zowel functioneel als technisch in beheer bij ICT/Automatisering. Elk nieuw informatiesysteem dat in het gemeentelijke netwerk wordt opgenomen dient voor deze diensten te kunnen koppelen met deze generieke componenten.

Directory Services (Active Directory)	
Omschrijving	Centrale beheerdatabase met authenticatiegegevens van medewerkers voor toegang tot het netwerk.
Mail Server (Exchange)	
Omschrijving	Dienst voor e-mail en agenda.
Identity en Access Management (SIAM)	
Omschrijving	Authenticatie-proxy, filtert o.a. netwerkverkeer vanaf het Internet en verzorgt de communicatie met DigiD
Load Balancer (F5)	
Omschrijving	Zorgt voor het beschikbaar maken richting het Internet (via reverse proxy) en het load balancen van webapplicaties.
DNS Server (Microsoft)	
Omschrijving	Dienst die zorgt voor het vertalen van IP-adressen in domeinnamen en omgekeerd.
DHCP Server (Microsoft)	
Omschrijving	Voorziening voor het toekennen van IP-adressen binnen het netwerk.
Wifi	
Omschrijving	Draadloos netwerk met Internet toegang. Deze dienst is beschikbaar op de meeste gemeentelijke locaties. Het Wifi netwerk is niet gekoppeld met het netwerk van Gemeente 's-Hertogenbosch.
Broker (Adeptia)	
Omschrijving	De broker wordt gebruikt om (a-synchroon) berichten tussen systemen op een gestandaardiseerde wijze te kunnen uitwisselen.
Service Gateway (Broadcom API gateway)	
Omschrijving	De Service Gateway wordt gebruikt om (synchroon) berichten tussen systemen op een gestandaardiseerde wijze te kunnen uitwisselen.

6.2 Protocollen

Protocollen beschrijven hoe de communicatie tussen verschillende ICT-componenten binnen het gemeentelijke netwerk dienen te verlopen. Versies van deze protocollen volgen elkaar snel op. De meest recente versie moet worden gebruikt:

Naam Protocol	Functie
HTTPS	Berichtentransport. Voor eisen hieraan zie Bijlage 2.
LDAP	Opvragen gegevens in directory (Secure LDAP is hierbij het uitgangspunt)
SOAP	Berichtenuitwisseling tussen applicaties
XML	Beschrijving berichtenstructuur
REST	Berichtenuitwisseling tussen applicaties
JSON	Beschrijving berichtenstructuur
WDSL	Beschrijving van WEB services
TCP/IP	Transport en netwerkprotocol (IPv4 en IPv6)
Ethernet	Datalink protocol
802.1x	Beveiligingsprotocol voor poortgebaseerde authenticatie

Bijlage 1: Actuele versies hard- en software

Servers Software:		
Naam software	Versie	Functie
VMware vSphere	6.7	Besturingssysteem Virtualisatie servers
Solaris	11.4	Besturingssysteem Oralce SPARC tbv Oralce Databases
VMWare VIEW	7.1	Thuiswerk applicatie VDI
Ubuntu Server	20.04	Besturingssysteem server
MS Windows	2016 en 2019	Besturingssysteem server
Microsoft IIS	10	Internet Information Services, webserver voor .net toepassingen
Apache	2.4.39	http server
Weblogic Server	12.2.1.3.0	Applicatie omgeving voor JAVA-applicaties
Tomcat	9.0.13	Java Servlet container

Databases:		
Naam software	Versie	Functie
Oracle	12.2	Database management systeem
SQL Server	2016	Database management systeem
MariaDB	10.5.x	Database voor webapplicaties die niet gescheiden kunnen worden de database

Telefoontoestellen:		
Leverancier	Type	Functie
iPhone		IOS Smartphone (E-mail, agenda en Telefoon)

Werkplekken Hardware:		
Leverancier	Type	Functie
HP	Elitedesk 800 G1, Intel Core i5, 8 Gb intern geheugen	CAD werkplek
VmWare	2 CPU en 8Gb intern geheugen	Administratieve VDI werkplek

Overige apparatuur:		
Leverancier	Type	Functie
Ricoh	MPC 4503 en MPC 305	Werkplekdomein printers kleur en z/w
Ricoh	SP 4310n en SP 4510n	Printer Burgerzaken en Parkeervergunningen
Zebra	ZT230	Labelprinter

Werkstation inrichting:		
Naam software	Versie	Functie
Microsoft Windows	Windows 10 64 1909	Besturingssysteem werkstations
MS-Office	Office 2019 Versie 1808 build 10372.20060	Tekstverwerking, Spreadsheet en Presentatie software
Outlook	Office 2019	Cliënt E-mail en agenda functionaliteit
Java JRE	1.8 Update 152	Uitvoeren van JRE
Oracle Cliënt	12.2.0	Cliënt Oracle database
PDF Exchange PRO	8.0.336.0	Het kunnen lezen / downloaden van bestanden in pdf-formaat
Virusscanner (Defender)	Windows Defender	Virusscanner
Dot Net	4.8	Runtime omgeving voor Dot Net
Edge Chromium	90.0.818.56	Browser
ZCM Agent	20.1.0.343	Toekenning applicaties

Bijlage 2: Gebruik van TLS en HTTP headers

Bij gemeente 's-Hertogenbosch wordt veel gebruik gemaakt van op webtechnologie gebaseerde diensten. Denk hierbij aan websites, web-portals en mechanismes voor berichtenverkeer. Deze memo geldt voor alle diensten waarbij gemeente 's-Hertogenbosch verantwoordelijk is voor de exploitatie ervan, ongeacht waar deze is ondergebracht of hoe deze benaderbaar is. Het maakt dus niet uit of desbetreffende dienst is ondergebracht op het gemeentelijke netwerk of als SaaS-oplossing bij derden is ondergebracht. Relevante technieken die bij het veilig maken van de netwerkcommunicatie worden gebruikt staan bekend onder de naam Transport Link Security (TLS) en HTTP headers. Onderstaande maatregelen op dit gebied zijn hierbij vereist:

Maatregelen

1. Er wordt verplicht gebruik gemaakt van TLS. Als al gebruik wordt gemaakt van een niet-beveiligde verbinding, is deze alleen bedoeld om te verwijzen naar de met TLS beveiligde variant;
2. In geval van doorverwijzing moet de domeinnaam eerst zelf te verwijzen naar zijn HTTPS-variant, voordat deze eventueel doorverwijst naar een andere domeinnaam. Dit zorgt er ook voor dat een webbrowser de HSTS-policy kan accepteren. Een voorbeeld van een correcte verwijzing is: http://[www.]domein-a.nl -> https://[www.]domein-a.nl -> https://[www.]domein-b.nl;
3. Er wordt verplicht gebruik gemaakt van vertrouwde PKI-certificaten. Elke website geeft naast het certificaat waarmee de website wordt geïdentificeerd ook de nodige tussenliggende certificaten door. Gebruikers mogen niet worden geconfronteerd met foutmeldingen veroorzaakt door het niet juist inzetten van servercertificaten;
4. Voor verbindingen die vanaf het gemeentelijke netwerk naar websites worden gelegd en alleen voor medewerkers van gemeente toegankelijk zijn, geldt dat hier ook gebruik mag worden gemaakt van PKI-certificaten die door onze interne Certificate Authority (CA) zijn uitgeven;
5. Er wordt minimaal gebruik gemaakt van TLS versie 1.2;
6. Bij alle verbindingen (HTTP en HTTPS) met uitzondering van berichtenverkeer, worden de volgende HTTP response headers verplicht meegestuurd:
    - *X-Content-Type-Options*;
    - *X-Frame-Options* (niet verplicht als *frame-ancestors* in de *Content-Security-Policy* wordt gebruikt);
    - *X-Xss-Protection*;
    - *Content-Security-Policy*;
    - *Referrer-Policy*;
    - *Permissions-Policy*.;
7. De lijst van geldende aanbevolen instellingen voor de *Content-Security-Policy* is terug te vinden bij de testuitleg op de site https://internet.nl. Als aanscherping van deze maatregel geldt dat applicaties waarvoor een DigiD assessment van toepassing is geen van de waarden van *unsafe-eval* of *unsafe-inline* zijn toegestaan voor scripts en/of stylesheets (https://www.norea.nl/download/?id=8904);
8. Bij beveiligde verbindingen (HTTPS) met uitzondering van berichtenverkeer, wordt verplicht ook de HTTP response header *Strict-Transport-Security* meegestuurd;
9. Het meesturen van HTTP response headers waaruit kan worden opgemaakt op welk platform de aangeboden dienst draait, zoals *Server* en *X-Powered-By*, is niet toegestaan, tenzij de werking van de dienst daardoor negatief wordt beïnvloed;
10. Voor alle meegestuurde HTTP response headers geldt dat de waarde ervan zodanig moet worden ingesteld dat een optimale beveiliging wordt bereikt zonder afbreuk te doen aan de functionaliteit van de geboden dienst;
11. Alle meegestuurde cookies zijn van het type secure, httponly en samesite en bevatten geen gevoelige informatie. Zie https://scotthelme.co.uk/tough-cookies/ voor de "best practices". Voor samesite (https://web.dev/samesite-cookies-explained/) is gebruik van de optie "none" alleen toegestaan na expliciete toestemming van het intaketeam van ICT/A;

12. Waar de gebruikte oplossing het toestaat, wordt gebruik gemaakt van OCSP-stapling, zodat het voor de afnemer van de dienst gemakkelijker is om de validiteit van het geboden TLS-certificaat te controleren;
13. Maak gebruik van ciphers die forward secrecy ondersteunen. Dit zorgt voor extra afluisterbescherming van versleuteld verkeer. Gebruik daarbij geen standaard Diffie-Hellman (DH) ciphersuites om onder andere CVE-2020-1968 (Raccoon Attack) te voorkomen. Let op: Het gaat hier alleen om DH-ciphersuites en niet om ECDH-ciphersuites;
14. Waar de gebruikte oplossing het toestaat, wordt geen gebruik gemaakt van op Cipher Block Chaining (CBC) gebaseerde ciphers;
15. Diensten die niet in productie zijn, mogen niet door derden en niet via openbare netwerken zoals het internet benaderbaar zijn, tenzij met het intaketeam van ICT/A anders is overeengekomen;
16. Voor diensten die niet in productie zijn, geldt dat DNS-records hiervan niet mogen worden opgenomen in publiek benaderbare DNS-services, tenzij door het intaketeam van ICT/A anders bepaald;
17. Alle diensten worden voordat ze in productie worden genomen en daarna periodiek door een externe partij getest op kwetsbaarheden. Deze tests beperken zich niet tot TLS en HTTP response headers, maar zijn zeker ook bedoeld om de veiligheid van de aangeboden applicatie te testen;
18. Om te testen of de configuratie van TLS voldoet, kan gebruik worden gemaakt van een dienst van SSLLABS: https://www.ssllabs.com/ssltest/, waarbij als resultaat een minimale score "A" moet worden gehaald;
19. Om te testen of de configuratie van HTTP response headers voldoet, kan gebruik worden gemaakt van een dienst van Scott Helme: https://securityheaders.com/, waarbij als resultaat een minimale score "A" moet worden gehaald;
20. Op de site https://internet.nl/ kan de juiste implementatie van TLS en HTTP response headers worden gecontroleerd op "best practices" zoals aanbevolen door partijen uit de internetgemeenschap en de Nederlandse overheid. Als hier 100% wordt gescoord, dan wordt aan alle voorwaarden voldaan en zijn zaken met betrekking tot IPv6 en DNSSEC die buiten de scope van dit document vallen ook in orde. De voorwaarden voor het gebruik van IPv6 en DNSSEC staan vermeld in de gemeentelijke technische architectuur (TA), paragraaf 5.1. Voor TLS en HTTP response headers is het uitgangspunt dat de verbinding voldoende is beveiligd en dat alle applicatie-beveiligingsopties zijn ingesteld (zie afbeelding);
21. Indien het testen van de configuratie van TLS en HTTP response headers niet mogelijk is via het

internet, kan gebruik worden gemaakt van hulpprogramma's zoals curl (https://curl.haxx.se/) en testssl.sh (https://testssl.sh/). Hoewel deze programma's geen score opleveren, kunnen ze wel een goede indicatie geven over de kwaliteit van desbetreffende configuratie;
22. Relevante documentatie die kan worden gebruikt om de configuratie van TLS en HTTP response headers in orde te maken:
    - https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices;
    - https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers;
    - https://wiki.mozilla.org/Security/Server_Side_TLS (gebruik minimaal "Intermediate compatibility").