Bijlage 11- Technische architectuur (TA) gemeente ‘s-Hertogenbosch
Vervangen afvalkalender-app, website en CMS Afvalstoffendienst
Gemeente ’s-Hertogenbosch
Europees openbare aanbesteding

Technische Architectuur (TA)

Gemeente ’s-Hertogenbosch

Beschrijving Technische Architectuur Gemeente ’s-Hertogenbosch

Versie : 2024.3
Status : Definitief
Datum : 12 september 2024

Inhoudsopgave

1. Inleiding

De Technische Architectuur (TA) 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 TA 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 TA 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 TA 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. Daarnaast heeft deze bijeenkomst tot doel, te inventariseren waar er zich eventuele knelpunten voordoen in relatie tot de TA.

De TA is geschreven onder verantwoordelijkheid van en vastgesteld door het Hoofd ICT. Periodiek 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 moeten voldoen. Hoofdstuk 6 ten slotte behandelt een aantal centraal beheerde infrastructuurcomponenten die binnen Gemeente ’s-Hertogenbosch worden gebruikt.

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 twee 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 andere locatie. Tussen deze twee hoofdlocaties is een bandbreedte van 40 GB/sec beschikbaar.

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

Vanuit de beide Datacenters (MER’s) zijn op basis van redundante 40 Gbps verbindingen de 4 hoofdlocatie sterpunten aangesloten. Vanuit deze 4 sterpunten worden de gebruikers switches (SER’s) voorzien van hun (bij voorkeur redundante) aansluiting op het netwerk.
De serveromgeving, op beide hoofdlocaties, 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, publieke omgevingen, acceptatie- en productieomgeving) logisch te scheiden. Binnen de productieomgeving zijn ook de serveromgeving en de werkstation omgeving 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 Diginet en Internet. In deze paragraaf worden beide soorten verbindingen nader toegelicht.

2.2.1 Verbindingen via publieke netwerken

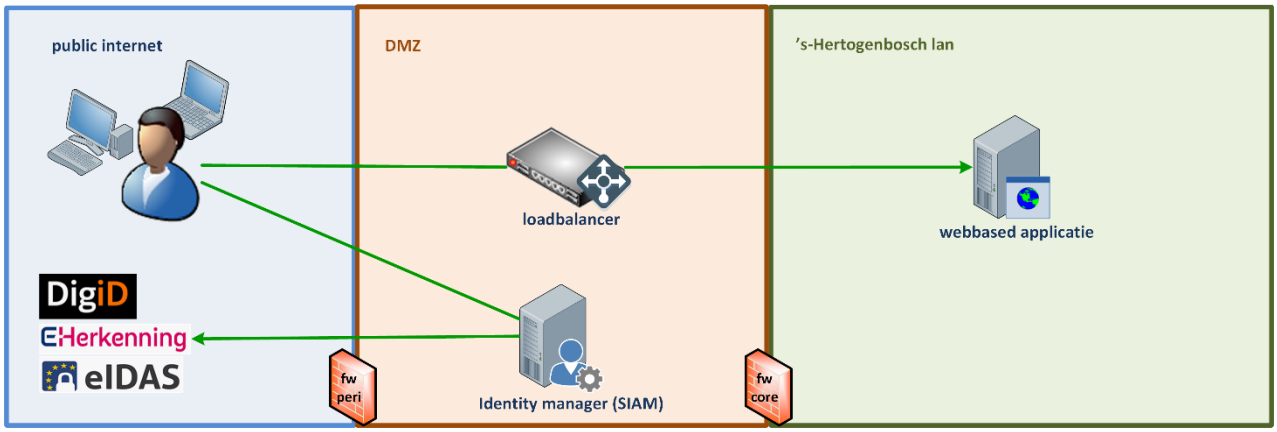
Binnen Gemeente ’s-Hertogenbosch worden alle netwerken waarop partijen kunnen aansluiten zonder een overeenkomst met gemeente ’s-Hertogenbosch beschouwd als publieke netwerken volgens het principe van Zero Trust. Het gaat hierbij dus niet alleen om het Internet maar ook om Diginet. De toegang vanaf de 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 de interne netwerken en externe netwerken zoals

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, waarbij voor diensten die de gemeente aanbiedt geldt dat hier zowel IPv4 als IPv6 wordt gebruikt. Het hierbij gebruikte DMZ faciliteert deze verbindingen via daarin geplaatste servers. Bij de communicatie van deze servers naar publieke netwerken en vice versa wordt in geval van IPv4 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 in uiterste gevallen 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 diensten die vanaf het gemeentelijke netwerk via de load balancers naar externe netwerken worden aangeboden, geldt dat deze diensten uit veiligheidsoverwegingen zijn ondergebracht op servers die zich op een afgeschermde plek binnen het gemeentelijke netwerk bevinden.

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, via DigiD voor burgers en 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 load balancer. (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 de Afdeling ICT. Als standaard wordt vanuit de Afdeling ICT 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 Gemeente 's-Hertogenbosch is gemaakt om te dienen als intermediair van berichtenverkeer tussen applicaties. Een koppeling waarbij minimaal een van de applicaties on-premises staat loopt altijd via de integratielaag van gemeente ’s-Hertogenbosch.” We onderscheiden twee soorten berichtenverkeer, synchroon en asynchroon. Synchroon verkeer is verkeer dat rechtstreeks antwoord nodig heeft. Bijvoorbeeld als een gebruiker wacht op antwoord. Voor synchroon verkeer is een API 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 ciphers e.d... Voor intern verkeer of ‘van binnen naar buiten’ is geen 2-zijdige TLS verbinding verplicht. Hierop is het document "Gebruik TLS en HTTP headers" van toepassing.

Voor asynchroon verkeer wordt de gemeentelijke ESB/Broker ingezet. Deze is de regisseur van een geautomatiseerd workflow proces, inclusief queueing en foutafhandeling en daarmee verantwoordelijk voor het initiëren en afhandelen van processen binnen de hele keten. Concreet houdt dit in dat de gemeentelijke broker altijd het initiatief heeft en neemt en dat te koppelen applicaties in overeenstemming met deze methodiek moeten kunnen werken.

2.4 Draadloos netwerk

Ten behoeve van externen en eigen medewerkers is op bijna alle gemeentelijke locaties een draadloos netwerk met internettoegang aangelegd. Dit netwerk is niet rechtstreeks verbonden met het gemeentelijke netwerk. Toegang tot het gemeentelijke netwerk verloopt net zoals bij andere externe verbindingen via de perimeter firewall. De beschikbare providers op het draadloos netwerk zijn govroam en publicroam.

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 virtualisatietechnieken.

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 en de acceptatieomgeving. Hierbij is de acceptatieomgeving zoveel mogelijk een kopie van de productieomgeving. 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 twee serverplatformen aangeboden: Windows en Linux. Het beleid van de gemeente is om alle servers zoveel mogelijk te virtualiseren volgens het principe van een service per server. Dit wordt voor het Windows en Linux platform gedaan middels door gebruik te maken van VMWare vSphere. De gevirtualiseerde systemen zijn verspreid over beide serverruimtes. De Oracle en SQL servers zijn fysieke redundant opgezette servers waarvan de databases worden opgeslagen op de lokale storage.

3.1 Servers

3.1.1 Serverplatformen

Binnen de technische architectuur worden de volgende server besturingssystemen aangeboden: Windows en Linux. De Windows servers worden ingezet als file- en printservers, applicatieservers en SQL databaseservers. De Linux servers dienen als platform voor applicatieservers en database servers (Oracle en MariaDB). De Windows en Linux servers zijn zoveel mogelijk gevirtualiseerd met behulp van VMware vSphere. De SQL- en Oracle servers zijn fysieke redundant opgezette servers 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 Applicatieservers

De applicatieservers 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), Weblogic Application Server (applicatie omgeving voor JAVA-applicaties), LAMP (Linux, Apache, MariaDB en PHP), NGINX (webserver en reverse-proxyserver), SQUID (caching proxy).

3.1.3 Databases

Als database omgeving worden de volgende databases ondersteund: Microsoft SQL, Oracle en MariaDB, waarbij het Microsoft SQL server 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, redundantie en recovery mogelijkheden 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 vier schijfsystemen op locaties Stadskantoor en Weener XL. De opslagcapaciteit op deze systemen wordt ontsloten via een virtualisatielaag.

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 op locatie Weener XL (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.

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 en Weener XL.

Alle back-up data zijn opgeslagen op twee locaties: Stadskantoor en Weener XL. Hierbij wordt de initiële back-up gemaakt op een schijfsysteem op Stadskantoor 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 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, specifieke toepassingen door middel van ZENWorks Configuration management (ZCM) gedistribueerd naar de werkplekken. Op het werkstation hebben gebruikers geen administrator rechten. 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 Apple iPhone. Daarnaast wordt er mobiel gewerkt op laptops en ultrabooks en wordt er in beperkte mate gebruikt gemaakt van Apple iPads. Het gebruik van Android tablets is beperkt tot situaties waar de tablets persoonsonafhankelijk gebruikt worden in een single app Kiosk-modus. Alle mobiele devices worden beheerd door middel van een MDM-oplossing en zijn niet rechtstreeks gekoppeld met het gemeentelijk netwerk.

4.1.3 Telefonie

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 gemeente breed 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. Inmiddels is het mogelijk om

gesprekken op te nemen en terug te luisteren. Bijvoorbeeld voor trainingsdoeleinden. Verder is er een voicemailsysteem, een Call Centeroplossing en een kostenregistratiesysteem aangesloten op de telefooncentrale.
De telefooncentrale en alle hierboven vermelde subsystemen zijn via het zero-trust principe gekoppeld aan de gemeentelijke LAN/WAN omgeving.

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 copiers 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 laten wij uitvoeren door een externe 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 Post wordt binnengekomen post gescand op een hoog volume scanner.

4.1.4.2 Memory Stick

Er wordt een standaard type memory stick 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 Gemeente ’s-Hertogenbosch worden aangeschaft dienen aan de volgende voorwaarden te voldoen:

a. De applicatie is een webapplicatie of webservice die werkt onder de in deze TA ondersteunde browsers en hoger met standaard beveiligingsinstellingen. De interface is zonder beperking van functionaliteit, benaderbaar zonder gebruik te maken van browser plug-ins of andere methodieken/software.
b. Interfaces voor inwoners en bedrijven van de ICT-oplossing voldoen aan de eisen vermeld op www.digitoegankelijk.nl.
c. 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.)
d. Het gebruik van TLS en HTTP-headers voldoet aan de laatste stand van de techniek. De vereiste maatregelen op dit punt zijn uitgewerkt in het document “Gebruik van TLS en HTTP response headers”, dit is een losse bijlage).
e. Webapplicaties maken bij voorkeur gebruik van een koppeling met Single Sign On (SSO) met Azure AD/Entra ID 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 en email. De SSO-koppeling is bedoeld voor authenticatie, autorisatie dient plaats te vinden binnen de gekoppelde applicatie. Voor de toegang tot applicaties wordt gebruik gemaakt van Conditional Access. Als SSO via Azure AD/Entra ID 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.
f. Als er sprake is van de verwerking van persoonsgegevens dient er met de leverancier van de applicatie een verwerkersovereenkomst te worden afgesloten.
g. Bij verwerking van bijzondere en/of gevoelige persoonsgegevens levert de SaaS-Leverancier jaarlijks een SOC II Type II verklaring en/of een TPM op basis van een andere erkende norm op het gebied van informatieveiligheid.
h. Wanneer de SaaS-applicatie een financieel proces verwerkt dat bijv. voor de jaarrekening van materieel belang kan zijn levert de SaaS-leverancier jaarlijks een ISAE 3402 Type II verklaring.
i. De SaaS-Leverancier en de hostende partij beschikken over een ISO27001-certificering. Waarbij de verklaring van toepasbaarheid dient te worden aangeleverd.
j. De data moet zijn opgeslagen binnen de Europese Economische Ruimte. Daarnaast is de vestigingsplaats van de inschrijver binnen de Europese Economische Ruimte.
k. De volgende aandachtspunten moeten in ieder geval worden opgenomen in de SLA met de leverancier:

[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

- een autorisatieproces voor toegang en rechten van gebruikers en beheerders van de applicatie;
- 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;

l. Uitzonderingen en andere gebeurtenissen die van belang zijn voor de beveiliging worden vastgelegd in zogenaamde “audit logs”, die tenminste het volgende bevatten:
   - 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.
   - De audit logs zijn beschermd zodat ze niet aangepast of gemanipuleerd kunnen worden.
   - De audit logs zijn 24/7 te raadplegen en exporteren in een gangbaar bestandsformat voor geautoriseerde medewerkers van gemeente ’s-Hertogenbosch.

m. SaaS applicaties en websites welke gebruikmaken van domeinen die eigendom zijn van de gemeente dienen te voldoen aan de volgende uitgangspunten.
   - Productie SaaS applicaties en websites tebedenkennaam.gemeentelijkdomein.tld
   - Acceptatie SaaS applicatie en websites tebedenkennaam.accp.gemeentelijkdomein.tld
   - De domeinennamen dienen vervolgens gekoppeld te worden op basis van het IP-adres aan een A- en AAAA-record.
   - Het gebruik van CNAME-records voor het verwijzen naar diensten is niet toegestaan.

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 tijde verantwoordelijk voor de goede en veilige werking inclusief compliancy van de complete oplossing.

5.2 Voorwaarden koppelingen SaaS-applicaties

Koppelingen tussen een SaaS-applicatie en een intern systeem van Gemeente ’s-Hertogenbosch kunnen zowel synchroon als asynchroon plaatsvinden. Gezien de complexiteit geldt dat nieuwe ontwerpen van koppelingen altijd via een intakeprocedure lopen. Voor transportbeveiliging en vaststelling van identiteit over niet vertrouwde 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 aanvullende maatregelen worden genomen. Deze afweging wordt mede gemaakt op basis van de resultaten van dataclassificatie en risicoanalyse.

5.2.1 Asynchrone koppelingen

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

- Vanuit de applicatie kunnen gegevens worden gepusht naar onze omgeving. Hierbij wordt bij voorkeur gebruik gemaakt van ebMS XML of webservice berichtenverkeer.
- Vanuit een applicatie in het interne netwerk van Gemeente ’s-Hertogenbosch wordt periodiek gecontroleerd 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 load balancer 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 checklist testen van Logius en het Beveiligingsassessment DigiD. Voor het Beveiligingsassessment DigiD dient jaarlijks een TPM worden afgegeven door de SaaS-leverancier.

5.2.4 Koppelingen met systemen met basisregistratiegegevens

Binnen Gemeente ’s-Hertogenbosch wordt er veelvuldig gebruik gemaakt van gegevens uit eigen of landelijke basisregistraties. Deze gegevens worden verzonden naar applicaties door middel van koppelvlakken. De praktijk heeft uitgewezen dat het absoluut noodzakelijk is om consistentiecontroles tussen systemen te doen, omdat er niet zomaar uitgegaan kan worden van het feit dat de gegevens in systeem A ook exact gelijk zijn aan de gegevens in systeem B. Er kan onderweg nog wel eens wat fout gaan in het berichtenverkeer tussen systemen; onder andere dat gewijzigde gegevens vanuit systeem A niet verzonden worden naar systeem B, de gewijzigde gegevens niet ontvangen worden door systeem B, het formaat waarin de gegevens vanuit systeem A naar systeem B worden gestuurd wordt niet begrepen door systeem B, et cetera.
Om dit goed te kunnen monitoren is hiervoor een consistentiecontrole-tool in gebruik, namelijk KwaliteitsMonitor GegevensBeheer (KMGB) van leverancier Synaxion. In deze tool worden periodiek consistentiecontroles tussen het datadistributiesysteem en afnemende systemen uitgevoerd en elke applicatie die gekoppeld is met het datadistributiesysteem moet meegenomen worden in de consistentiecontrole.
In bijlage 3 is er een beschrijving van alle velden die de consistentiecontrole-tool kán vergelijken. Alle velden die in de database van een afnemende applicatie aanwezig zijn en qua context overeenkomen met de lijst, moeten beschikbaar worden gesteld (op basis van de aangegeven technische kaders/methodieken) om daar de consistentiecontrole op uit te kunnen voeren.

Om de consistentiecontrole uit te kunnen voeren, is er een periodieke (frequentie en tijdstip nader te bepalen) dump nodig uit de database van de afnemende applicatie; zie voor de requirements van de dataontsluiting hoofdstuk 5.2.1 Asynchrone koppelingen. Als er door de leverancier afgeweken wordt van bovenstaande oplossing met betrekking tot het uitvoeren van een consistentiecontrole of dataontsluiting voor de betreffende consistentiecontrole, wordt er een wens ingediend zodat er binnen x tijd – maximaal 1 jaar – wel de data ontsloten kan worden. Mocht dit niet in die periode te realiseren zijn, dan zouden we graag één (of meerdere) alternatieve oplossing(en) willen ontvangen en bespreken, dat als tijdelijke oplossing implementeren en daarna verder kijken tot het uiteindelijk wel kan op onze gewenste manier.

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) 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 toegang tot een service/api gateway door een service, of services, te publiceren waar de leverancier gebruik van kan maken. Deze services zijn beveiligd met mutual TLS (MTLS) en IP-restricties.
De service om de mail te versturen ondersteunt een aantal Microsoft Graph operaties.
Daarbinnen zijn er de volgende mogelijkheden:

- In de afhandeling van het bericht zal de service/api gateway een token ophalen bij Microsoft 365. Dit token wordt aan het bericht van de aanroepende partij toegevoegd en verstuurt naar Microsoft Graph. Hierbij wordt dus gebruik gemaakt van één service, één endpoint
- Of er zijn twee endpoints beschikbaar
    - een service/endpoint voor de tokenaanvraag bij microsoftonline
    - een service/endpoint voor de Microsoft Graph operaties

  In dat laatste geval zal de service/api gateway geen token toevoegen maar verwacht het dat de aanroepende partij dit gedaan heeft.

NB het is dus niet toegestaan om rechtstreeks met de Microsoft Graph Api te verbinden namens de gemeente.

** = Met externe applicaties bedoelen we applicaties die niet in het gemeentelijke netwerk zijn ondergebracht, dus bijvoorbeeld SaaS applicaties en websites extern gehost.*

6. 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 de Afdeling ICT. 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.

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 (Nexus)

Omschrijving De broker wordt gebruikt om (asynchroon) 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.

ETL (FME)

Omschrijving FME wordt gebruikt om (asynchroon) datasets tussen systemen op een gestandaardiseerde wijze te kunnen uitwisselen.

Managed File Transfer (GoAnywhere)

Omschrijving GoAnywhere wordt gebruikt om (asynchroon) bestanden tussen systemen op een gestandaardiseerde wijze te kunnen uitwisselen.

Bijlage 1: Actuele versies hard- en software

In onderstaande tabellen zijn de actuele versies van de door de Afdeling ICT ondersteunde hard- en software opgenomen. Nieuwe aangeboden software dient te functioneren in samenhang met deze versies. Gemeente ’s-Hertogenbosch gaat uit van de meest actuele stabiele versies van deze hard- en software en aangeboden software zal ook in de toekomst hiermee compatibel moeten blijven.

Servers Software:		
Naam software	Versie	Functie
VMware vSphere	v7/v8	Besturingssysteem Virtualisatie servers
VMware Horizon	v7.13.3/v8.12.0	Thuiswerk applicatie VDI
Ubuntu server	22.04	Besturingssysteem server
Oracle Linux	8	Besturingssysteem server
MS Windows	2019 en 2022	Besturingssysteem server
Microsoft IIS	10	Internet Information Services, webserver voor .net toepassingen
Apache2	2.4.52	Http server
Weblogic Server	12.2.1.3.0	Applicatie omgeving voor JAVA-applicaties
Tomcat	9.0.13	Java Servlet container
nginx	1.18.0 (Ubuntu)	Webserver en reverse-proxyserver
Squid	4.10	Caching Proxy server

Databases:		
Naam software	Versie	Functie
Oracle	19	Database management systeem
SQL Server	2022	Database management systeem
MariaDB	10.6.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	Elite Mini 600 G9, 12th Gen Core i5-12500T with HT Technology 16 GB intern geheugen	CAD werkplek
VMware	2 CPU en 10GB intern geheugen	Administratieve VDI werkplek

Overige apparatuur:		
Leverancier	Type	Functie
Canon	MPC	Werkplekdomein printers kleur en z/w
Canon		Printer Burgerzaken en Parkeervergunningen
Zebra	ZT230	Labelprinter

Werkstation inrichting:		
Naam software	Versie	Functie
Microsoft Windows	Windows 10 64 21H2	Besturingssysteem werkstations
MS-Office	Microsoft 365 Versie 2404 build 17531.20152 64 bits	Tekstverwerking, Spreadsheet en Presentatie software, Cliënt E-mail en agenda functionaliteit
Oracle Cliënt	12.2.0	Cliënt Oracle database
PDF Exchange PRO	9.5.366.0	Het kunnen lezen / downloaden van bestanden in pdf-formaat
Virusscanner (Defender)	Windows Defender	Virusscanner
Dot Net	4.8 (4.804084)	Runtime omgeving voor Dot Net
Edge Chromium	124.0.2478.105	Browser (update is dagelijks/wekelijks)
ZCM Agent	23.3.0.333	Toekenning applicaties

Bijlage 2: Dataset consistentiecontrole-tool

Hieronder staat het volledige overzicht van de dataset die vergeleken kán worden in de consistentiecontrole-tool:

Personen
A-nummer
BSN
Voornamen
Voorletters
Voorvoegsel
Geslachtsnaam diacriet
Geboortedatum
Datum Overlijden
Geslacht
Indicatie geheim
Burgerlijke staat
Aanduiding naamgebruik
Geslachtsnaam partner
Datum inschrijving
Gemeentecode
Datum ingang adreshouding
Verblijfsadres
ID codes verblijfadres
VBL-categorie onderzoek
VBL-datum ingang onderzoek
VBL-datum einde onderzoek
Datum ingang correspondentieadres
Correspondentieadres
ID codes correspondentieadres
COR-categorie onderzoek
COR-datum ingang onderzoek
COR-datum einde onderzoek

Nummeraanduiding
Identificatie
Nummeraanduiding
Identificatie TGO
Straatnaam
Identificatie woonplaats
Naam woonplaats
Identificatie woonplaats afwijkend
Naam woonplaats afwijkend
Status Nummeraanduiding
Indicatie actief
Woonplaats nummer
Volgnummer adres
Indicatie hoofdadres

Verblijfsobject
ID Verblijfsobject
Type VBO
Oppervlakte
Gebruiksdoel 1
Gebruiksdoel 2
Gebruiksdoel 3
Gebruiksdoel 4
Gebruiksdoel 5
Indicatie geconstateerd
Indicatie onderzoek
Indicatie authentiek
Brondocumentnummer
Brondocumentdatum
Gebeurteniscode BAG
Datum ingang VBO
Datum einde VBO
Datum begin geldigheid cyclus
Datum eind geldigheid cyclus
ID hoofdadres
Status VBO
Adresnummer BAG
Indicatie actief

Ligplaatsen
ID ligplaats
Type object
Oppervlakte
Gebruiksdoel 1
Gebruiksdoel 2
Gebruiksdoel 3
Gebruiksdoel 4
Gebruiksdoel 5
Indicatie geconstateerd
Indicatie onderzoek
Indicatie authentiek
Brondocumentnummer
Brondocumentdatum
Gebeurteniscode BAG
Datum ingang VBO
Datum einde VBO
Datum begin geldigheid cyclus
Datum eind geldigheid cyclus
ID hoofdadres
Status ligplaats
Adresnummer BAG
Indicatie actief

Pand
ID pand
Bouwjaar pand
Indicatie geconstateerd
Indicatie onderzoek
Indicatie authentiek
Brondocumentnummer
Brondocumentdatum
Gebeurteniscode BAG
Datum ingang pand
Datum einde pand

Huisnummer
Huisletter
Toevoeging
Aanduiding
Postcode
Woonplaats
Gemeentecode
Wijkcode
Buurtcode
Indicatie onderzoek
Indicatie geconstateerd
Indicatie authentiek
Brondocumentnummer
Brondocumentdatum
Gebeurteniscode
Datum ingang
Datum einde
Datum begin geldigheid
Datum einde geldigheid
X-coördinaat
Y-coördinaat
Z-coördinaat
Straatcode
Identificatie OR
Naam OR
Hoofdvestiging
In surseance
Failliet
BIK code hoofdactiviteit
BIK code nevenactiviteit1
BIK code nevenactiviteit2
Aantal werknemers
Aantal werknemers fulltime
Aantal werknemers part- en fulltime
Telefoonnummer
Email
URL Website
Vestigingsdatum adres
Verblijfsadres

Standplaatsen
ID Standplaats
Type object
Oppervlakte
Gebruiksdoel 1
Gebruiksdoel 2
Gebruiksdoel 3
Gebruiksdoel 4
Gebruiksdoel 5
Indicatie geconstateerd
Indicatie onderzoek
Indicatie authentiek
Brondocumentnummer
Brondocumentdatum
Gebeurteniscode BAG
Datum ingang VBO
Datum einde VBO
Datum begin geldigheid cyclus
Datum eind geldigheid cyclus
ID hoofdadres
Status standplaats
Adresnummer BAG
Indicatie actief

Datum begin geldigheid cyclus
Datum einde geldigheid cyclus
Status pand
Indicatie actief

Niet-natuurlijke personen
Dossiernummer en subdossiernummer
Dossiernummer
Subnummer
RSIN
Vestigingsnummer
Vestigingsstatusindicator
Fiscaalnummer
Zaaknaam
Handelsnaam
Statutaire naam
Rechtsvorm
Rechtsvormomschrijving
Datum oprichting
Datum ontbinding
Datum inschrijving
Datum einde

Identificatiecodes verblijfadres
VBL-categorie onderzoek
VBL-datum ingang onderzoek
VBL-datum einde onderzoek
COR-datum ingang adres
Identificatiecodes correspondentieadres
COR-categorie onderzoek
COR-datum ingang onderzoek
COR-datum einde onderzoek

Gemeenten
Gemeentecode
Gemeentenaam
Gemeentenaam NEN
Gemeentegeometrie
Datum begin geldigheid gemeente
Datum einde geldigheid gemeente
Gemeentecode in overgegaan