Programma van eisen Security en Koppelvlakken

Versie: 0.9.1, 22 december 2021

Colofon

Naam auteurs	CERT-GM
Versie	0.91 Concept
Versiedatum	6 december 2021
Versiebeheer	Het beheer van dit document berust bij de Specialist Informatiebeveiliging van Gemeente Maastricht.

Inhoudsopgave

Inleiding

Aanbestedingen van Gemeente Maastricht met een ICT-component, dienen onderstaande security eisen mee uit te vragen. De eisen uit dit document moeten in zijn volledigheid mee uitgevraagd worden. Mocht in de looptijd van het traject meerwerk nodig zijn, dan zijn de relevante eisen bekend en afgedekt.

Eisen

Aan inschrijver wordt gevraagd om aan te geven of en aan welke eisen wordt voldaan. Om te toetsen of een inschrijver voldoet aan de gestelde eisen, zal de gemeente Maastricht gedurende een “Proof of Concept” (hierna te noemen POC) een aantal specifieke zaken testen. In de bijlage Testprotocol staat opgenomen waarop de applicatie wordt getoetst. Indien een opdrachtgever niet voldoet aan een van deze criteria, dan geldt dit als een knock-out.

	Algemeen	***Opmerking(en)***
1.	Conform Gibit 2020 artikel 25,1 en 6.1 voldoet de ICT-prestatie voor de functie en het verwerkingsgebied aan de Gemeentelijke ICT-kwaliteitsnormen. Hierin wordt onder norm C1 gesteld dat “de ICT Prestatie over de functionele en technische mogelijkheden beschikt waarmee de Opdrachtgever kan voldoen aan de Baseline Informatiebeveiliging Overheid (BIO)”.	
2.	Conform Gibit 2020 artikel 25.1 en 6.1 voldoet de ICT-prestatie voor de functie en het verwerkingsgebied aan de Gemeentelijke ICT-kwaliteitsnormen. Hierin wordt onder norm B2 gesteld dat “Het betreffende deel van de ICT Prestatie voldoet aan de wettelijke standaarden, de open standaarden van de Pas- toe-of-leg-uit-lijst en de landelijke gemeentelijke standaarden, voor zover het werkingsgebied van deze standaarden overeenkomt met het organisatorische of functionele werkingsgebied van het betreffende deel van de ICT Prestatie”. Voor een overzicht van deze standaarden zie: https://www.forumstandaardisatie.nl/open-standaarden/lijst/verplicht	
	Authenticatie	
3.	De aangeboden oplossing maakt geen gebruik van lokale gebruikers, maar sluit aan op de gemeentelijke authenticatiemogelijkheden, waaronder LDAP en Kerberos. Het is niet toegestaan andere authenticatiemethoden te gebruiken of een eigen systeem in het netwerk van de opdrachtgever te plaatsen.	***On-premise***
4.	De aangeboden oplossing maakt geen gebruik van lokale gebruikers, maar sluit aan op de gemeentelijke authenticatiemogelijkheden, waaronder Azure AD Connect. Het is niet toegestaan andere authenticatiemethoden te gebruiken of een eigen systeem in het netwerk van de opdrachtgever te plaatsen.	***SaaS***
5.	Ten behoeve van accountsynchronisatie wordt gebruik gemaakt van Azure AD Connect.	
6.	Authenticatie voor burgers vindt plaats met DigiD en/of eIDAS. Als de DigiD aansluiting via Gemeente Maastricht wordt aangevraagd, dient de opdrachtnemer jaarlijks een TPM-verklaring, opgesteld door een RE, aan te leveren ten behoeve van de ENSIA-verantwoording aan Logius. De jaarlijkse kosten van deze TPM worden meegenomen in de totale kosten van de aangeboden webapplicatie. Ook de kosten van de TPM t.b.v. de aansluit audit worden meegenomen.	***DigiD***
7.	Indien er een gemeentelijke DigiD aansluiting wordt gebruikt, dient de opdrachtnemer alle info aan te leveren inclusief het gebruikte publieke certificaat en metadata (XML), beide aangeleverd als bestand.	**DigiD**
8.	Authenticatie voor bedrijven vindt plaats middels eHerkenning betrouwbaarheidsniveau EH2/EH2+/EH3/EH4*	***eHerkenning*** **Parameter aanvullen door opdrachtgever*
	Web Services	
9.	Connecties via http worden automatisch doorverwezen naar https middels een http response status code 3xx.	

10.	De webapplicatie is conform de ict-beveiligingsrichtlijnen voor webapplicaties van het NCSC gebouwd. https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties	***SaaS***
11.	Een webbased userinterface is zonder beperking van functionaliteit benaderbaar door de laatste twee versies van de meest gangbare en ondersteunde browsers (Microsoft Edge, Google Chrome, Apple Safari en Mozilla Firefox) zonder gebruik te maken van NPAPI plug-ins (zoals Flash, Silverlight, ActiveX, etc.).	
12.	De omgeving waarop medewerkers van de opdrachtgever inloggen maakt het mogelijk om alleen benaderbaar te zijn vanaf de gemeentelijke infrastructuur.	*Parameter, invullen afhankelijk van de aanbesteding.*
	File Transfer Service	
13.	Indien een file transfer service noodzakelijk is, kan alleen gebruik gemaakt worden van SFTP (voorkeur) of Explicit FTPS (TLS enforcement).	
	DNS	
14.	Wordt door opdrachtnemer een 'eigen' domein gebruikt, dan moet DNSSEC (Domain Name System Security Extensions) worden toegepast.	
15.	Domeinen waarvoor certificaten zijn uitgegeven dienen CAA records (DNS Certification Authority Authorization) te publiceren.	
	Encryptie	
16.	Bij asymmetrische encryptie wordt het sleutelpaar op het betreffende systeem gegenereerd, de private sleutel verlaat het systeem niet.	
	TLS	
17.	Certificaten worden uitgegeven door opdrachtgever als een van de domeinnamen van Gemeente Maastricht wordt gebruikt. Opdrachtgever bezorgt opdrachtnemer een login voor de Certificaat portal. Hierin kan de opdrachtnemer de Certificate Signing Request (CSR) plaatsen en na validatie van de opdrachtgever wordt het certificaat verstrekt. Indien een domeinnaam wordt gebruikt die niet eigendom van Gemeente Maastricht is, dient de opdrachtnemer een officieel erkend certificaat te gebruiken.	
18.	De server is zo ingericht en onderhouden dat deze een A+ rating behaalt op SSL Labs: *https://www.ssllabs.com/ssltest/index.html (*1)*	
	Governance	
19.	De inschrijver en eventuele onderaannemers zijn ISO27001 (Informatiebeveiliging) gecertificeerd en/of is in het bezit van een geldige ISAE3402 SOC2 assurance rapportage en/of levert ten tijde van de inschrijving en jaarlijks een TPM-verklaring over de gehele dienstverlening inclusief onderaannemers, uitgegeven door een IT Auditor (RE en/of CISA), waarmee assurance wordt afgegeven over de kwaliteitsaspecten integriteit, beschikbaarheid en vertrouwelijkheid in opzet, bestaan en werking. De jaarlijkse kosten van de TPM worden meegenomen in de totale kosten van de aangeboden dienstverlening.	
20.	De opdrachtnemer werkt (kosteloos) mee aan audits uitgevoerd door of in opdracht van de aanbesteder. Deze audits worden uitgevoerd door of onder verantwoordelijkheid van een RE of CISA.	
	Cloud	
21.	De ICT-infrastructuur van de geboden oplossing is in zijn geheel ondergebracht in een datacenter binnen de EER.	
	Koppelingen	
22.	Koppelingen/verbindingen tussen systemen en/of services (ook als deze op hetzelfde systeem draaien) worden door opdrachtnemer bij inschrijving inzichtelijk gemaakt in een protocol matrix, waarin de verkeerstromen zijn opgenomen. Deze matrix bestaat minimaal uit de volgende velden: Source IPv(4/6) | Source Port | Destination IPv(4/6) | Destination Port | Layer 4 protocol (TCP/UDP/...) | Application protocol (http/https/smtp/dns/...)	

23.	Alle koppelingen tussen de aangeboden dienst en Gemeente Maastricht lopen via de integratie laag van de opdrachtgever, waarbij de uitwisseling van gegevens gelogd en/of gemonitord wordt. De integratie laag bestaat uit een API-Gateway en een Enterprise Service Bus. De Opdrachtgever stuurt daarbij aan op veilig, snel en robuust berichtenverkeer. De Opdrachtgever houdt zelf de regie bij het realiseren van de koppelingen.	
24.	Koppelingen vanuit de SaaS-omgeving van de opdrachtgever naar derden (bijvoorbeeld SaaS-omgevingen van andere leveranciers of landelijke voorzieningen) lopen òf - Via de integratielaag van de Opdrachtgever. Hierbij koppelt Opdrachtnemer via de Secure Gateway van de gemeente Maastricht naar genoemde voorzieningen van derden òf - Opdrachtnemer koppelt rechtstreeks met de genoemde voorzieningen en biedt Opdrachtgever gedurende de looptijd van de overeenkomst rechtstreeks toegang tot de logging waarmee inzichtelijk wordt wie, wat op welk moment met wie heeft uitgewisseld. Gebeurtenissen worden 6 maanden bewaard.	
25.	Koppelingen met onze integratie laag hebben minimaal het onderstaande beveiligingsniveau: REST architectuur: TLS & API Key SOAP / StUF architectuur: TLS Mutual Authentication	
26.	Het aanbieden van RDP-koppelingen (of vergelijkbaar) evenals het gebruik van Remote Desktop Gateway is niet toegestaan.	
27.	Koppelingen tussen de Opdrachtnemer en Opdrachtgever kunnen enkel tot stand gebracht worden via een beveiligde https-verbinding waarbij gebruik gemaakt wordt van een PKI-certificaat, uitgegeven door een vertrouwde certificate authority.	
28.	Verbindingen vanuit de Opdrachtnemer naar de Opdrachtgever worden geïnitieerd vanaf vooraf gedefinieerde publieke IP-adressen. Op basis van deze source adressen verschaft de Opdrachtnemer toegang tot interne diensten.	
	Versiebeheer	
29.	De webapplicatie en onderliggende software en besturingssystemen zijn altijd up-to-date. Opdrachtnemer mag maximaal 1 versie achterlopen, mits deze versie nog volledig wordt ondersteund.	
30.	NVT	
31.	NVT	
32.	NVT	
33.	NVT	
34.	NVT	
	Database(s)	
35.	Conform artikel 18.1 van de Gibit 2020 wil de Opdrachtgever toegang krijgen tot de met de ICT Prestatie ten behoeve van de Opdrachtgever verwerkte gegevens, ingestelde autorisaties en overige gemaakte instellingen (bedrijfsregels, macro's etc.). Opdrachtgever beschikt over een datawarehouse en wil derhalve in staat zijn om bij voorkeur te allen tijde maar tenminste eenmaal per etmaal zelfstandig gegevens/autorisaties middels een geautomatiseerde koppeling op te vragen (Gibit 18.2 lid ii). Opdrachtnemer verstrekt (conform Gibit 18.2 lid iii) aan Opdrachtnemer een juiste, volledige en gedetailleerde beschrijving van de aan de ICT-prestatie ten grondslag liggende datamodellen zodat Opdrachtgever in staat is gegevens zelfstandig te ontsluiten. Door de Opdrachtgever, bij upgrades en updates, verstrekte releasenotes bevatten ook wijzigingen in de onderliggende database.	
	Security incidenten	
36.	Security incidenten worden onverwijld (binnen 4 uur), na hiervan op de hoogte te zijn, gemeld bij de opdrachtgever (per E-Mail aan*: ...@maastricht.nl* en *...@maastricht.nl*).	

	De gevolgen worden zo snel mogelijk ongedaan gemaakt, dan wel beperkt, waardoor het incident onder controle wordt gebracht. De Opdrachtgever wordt geïnformeerd over de genomen maatregelen.	
	Logging	
37.	De oplossing beschikt voor alle mutaties over een niet-muteerbare audit-trail met daarin minimaal: ▪ de gebeurtenis; ▪ de benodigde informatie die nodig is om het incident te kunnen herleiden tot een gebruiker; ▪ het gebruikte apparaat; ▪ het resultaat van de handeling; ▪ een datum en tijdstip van de gebeurtenis.	
38.	Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.	
39.	Ten behoeve van de loganalyse is de bewaarperiode van de logging bepaald op 6 maanden. Binnen deze periode is de beschikbaarheid van de loginformatie gewaarborgd.	
40.	Het versturen van E-Mail vanuit een van de domeinen van opdrachtgever, kan alleen indien de opdrachtnemer gebruik maakt van de volgende standaarden: SPF, DKIM, STARTTLS, DANE. Het versturen van mails gaat via een subdomein van opdrachtgever via het platform van de opdrachtnemer. Het versturen van mails via de gemeentelijke mailvoorziening is niet toegestaan. Gebruikt de opdrachtnemer een eigen domein als afzender adres, dan dienen de standaarden SPF, DKIM, STARTTLS, DMARC en DANE geïmplementeerd te zijn.	