BIJLAGE: EISEN BERICHTENVERKEER GEMEENTE HELMOND

1. Inleiding;

De gemeente streeft ernaar om het aantal schakels in het berichtenverkeer zo veel mogelijk te beperken. Daarbij is actieve beveiliging en monitoring van het berichtenverkeer noodzakelijk. De gemeente Helmond heeft voorzieningen in huis om dit goed te kunnen uitvoeren. We maken daarbij gebruik van de volgende producten van Enable-U;

a. 2Secure als API-gateway voor het beveiligen van inkomend en uitgaand extern verkeer
b. 2Orchestrate als ESB voor translatie en orchestratie
c. 2 Secure ebMS module als digikoppeling adapter voor ebMS verkeer met landelijke voorzieningen

2. Signalering & beveiligingsmaatregelen

Voor de monitoring van het berichtenverkeer en de signalering van verstoringen, maken we gebruik van Managed Services van Enable-U. Hierbij wordt het berichtenverkeer 24/7 gemonitord en in het geval van verstoringen worden de beheerders van de koppelingen direct geïnformeerd. In de praktijk loopt daarom in principe al het berichtenverkeer langs ons netwerk.
De interne API Gateway voorziet o.a. in de volgende beveiligingsmaatregelen;

a. Virtualisatie:
De API-gateway publiceert nieuwe “virtuele” end points/koppelvlakken.
b. TLS 1.3 of hoger (2-way SSL) wordt geborgd, door het meesturen van het PKIO certificaat van de gemeente Helmond en het trusten van het client certificaat van de aanroepende partij.
c. De virtuele koppelvlakken kunnen op bepaalde tijdstippen worden afgesloten voor de buitenwereld.
d. Op virtuele koppelvlakken kan worden ingesteld hoe vaak deze benaderd mogen worden per tijdseenheid (spam beveiliging).
e. Per koppelvlak dient IP-filtering te worden toegepast.

3. Uitgangspunten berichtenverkeer

Het berichtenverkeer tussen de gemeente Helmond en de Cloudapplicatie dient te allen tijde via de 2Secure API-gateway van de gemeente Helmond te verlopen. Cloud to Cloud berichtenverkeer dient in principe ook via de 2Secure API-gateway van de gemeente Helmond ontsloten te worden. Indien het niet mogelijk is om gebruik te kunnen maken van onze producten van Enable-U en er noodzaak is aan direct berichtenverkeer tussen de oplossing van een Cloud leverancier en de oplossing van een andere Cloud leverancier en/of berichtenverkeer tussen de oplossing van een Cloud leverancier en een landelijke of sectorale voorziening, dan gelden de volgende spelregels;

a. Dat er uitdrukkelijk toestemming is gegeven vanuit het architectuur board van de gemeente Helmond.
b. De leverancier (of onderaannemer) beschikt over een API Gateway die voorziet in de bij punt 2 genoemde interne API gateway beveiligingsmaatregelen. Hierover is bij de realisatie afstemming met de gemeente Helmond.
c. In de SLA worden afspraken gemaakt over de monitoring en incidentafhandeling van het berichtenverkeer en rapportages hierover.
d. Het berichtenverkeer en de onderliggende componenten die dit mogelijk maken, kunnen ge-audit worden.
e. De gemeente behoudt te allen tijde het recht om het berichtenverkeer alsnog via het eigen netwerk te laten lopen. De leverancier werkt in deze situatie kosteloos mee aan de herconfiguratie.

BIJLAGE: EISEN BERICHTENVERKEER GEMEENTE HELMOND

4. Opbouw berichtenverkeer

a. De benodigde koppelingen tussen de Cloudapplicaties en de Helmond on-premisse applicatie(s) of tussen de verschillende Cloud to Cloudapplicaties dienen gerealiseerd te worden op basis van TLS 1.3 of hoger (2-way SSL m.b.v. PKIO certificaten). Alternatieve protocollen t.b.v. authenticatie zoals, OAuth, OpenID en SAML, m.b.v. een autorisatie token kunnen in overleg ook toegepast worden. De berichtenuitwisseling dient plaats te vinden op basis van XML/SOAP of REST/JSON.

b. De berichten uitwisseling dient waar mogelijk, plaats te vinden op basis van StUF standaarden of gedocumenteerde API's zie ook OpenAPI Specifications.

c. Indien één van de te koppelen on-premisse applicaties van Helmond (nog) niet is toegerust om de koppeling op bovenstaande methodiek te faciliteren, is het mogelijk om in onderling overleg hiervan af te wijken.

d. Indien er naast de informatie-uitwisseling zoals beschreven onder punt 4a en 4b er ook nog aanvullende bestanden (pdf, csv etc) dienen te worden uitgewisseld dan kan dit op basis van onderstaande methodieken gefaciliteerd worden;

- Directe bestandsuitwisseling via API's (voorkeur)
- SFTP (SSH File Tranfer Protocol)
- FTPS (File Transfer Protocol SSL)