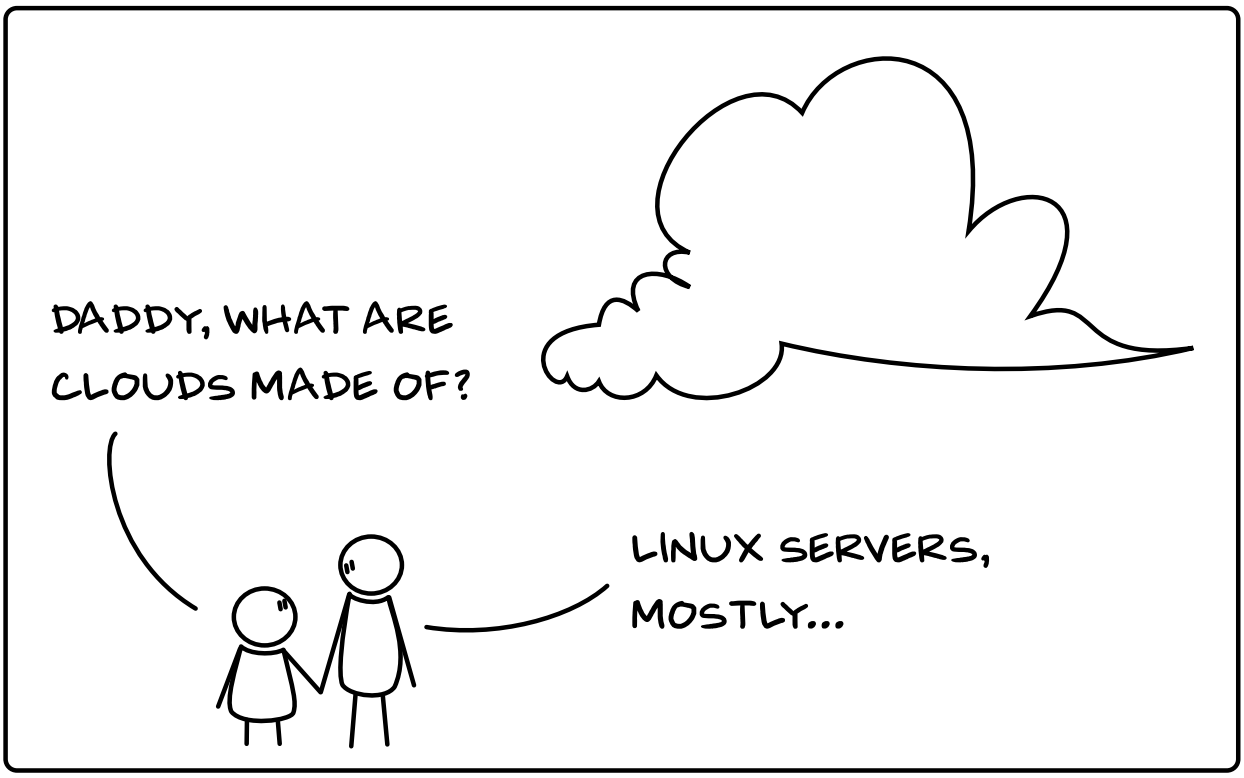
Gemeente Ede

Aansluitvoorwaarden Cloudgebaseerde Diensten



Versie: 2.13

Auteurs: Jeroen Visser/Tooraj Namdar
Review: Carel Aalbers/Jolien v.d. Vries

1 https://creativecommons.org/licenses/by-sa/4.0/deed.nl
2 https://creativecommons.org/licenses/by-sa/4.0/legalcode.nl

1 Revisies:

–	–	–	Voorgaande revisie-informatie verwijderd….
08-07-2019	JV	1.6	tekstuele aanpassingen en afronding
01-01-2020	JV	1.7	Aanpassing RTO/RPO
22-09-2020	JV	2.0	Aanpassing OTA(P)
23-09-2020	JV	2.1	Omvorming document naar aansluitvoorwaarden. Concept.
06-10-2020	JV	2.2	Aanpassingen hfdst. 4, 7, 8 en 9. Concept. Toegevoegd: ESB en Privacy shield. Concept.
08-10-2020	JV	2.3	Aantal spellingsfouten verwijderd
12-10-2020	JV	2.4	Zinsconstructies 6.10 aangepast Spelfouten…
04-12-2020	JV	2.5	Least Privilege toegevoegd Dienstgebonden Auditlogging toegevoegd
22-05-2021	JV	2.6	Remote Beheer Leverancier aangepast. E-mail met domein ede.nl afzender via on-prem oplossing en niet via SPF records includes meer, te foutgevoelig. Toevoeging rechten apps op mobiele platformen.
02-07-2021	JV	2.7	Aanpassingen ADFS finetuning en SSO definitie.
11-03-2022	JV	2.8	Certificering-eis verwijderd i.v.m. ambigue formulering. Aansluiting Back-up beleid volgt in 2.9... Toegevoegd, onveilig beschouwde IOT en Apparatuur. GEOpolitiek toegevoegd.
10-09-2022	JV	2.9	Aanpassing OTAP, procuratiehouder niet toegestaan, applicatie moet in staat zijn om zonder productiedata ketens te testen.
22-08-2023	JV	2.9.1	Wettelijke aanpassingen en kosten. Onderaannemers en voorwaarden.
02-11-2023	JV	2.10	AI en Zelflerende systemen toegevoegd aan document.
19-11-2024	JV	2.10	ADFS uitgebreid met Entra-ID, gezien migratie EDW.
30-01-2025	JV	2.11	Aanpassingen op gebied van AI. Aanpassingen op gebied van Exit Strategie Aanpassingen van de TLS-versleutelingsvereisten Toevoegen koppelingsautorisatiemethodiek. Aanpassingen op wachtwoordbeleid, MFA verplicht. Toegankelijkheidsopties aangepast.
16-05-2025	JV	2.12	Aanpassing GEO-restricties Aanpassing EER → EU
12-09-2025	JV	2.13	Pseudonimiseringsprotocol overgenomen uit gemeentebreed document en samengevat in korte eisen
06-10-2025	JV	2.13	Hernoeming van hoofdstuk Toegankelijkheid → Afscherming van de dienst en toevoeging alleen indien gegevens gevoelig van aard zijn, i.v.m. toekomstige ontwikkelingen
20-11-2025	JV	2.13	Aanpassing tracking verduidelijking app/applicaties/webapplicaties. Geen nieuwe betekenis, alleen tekstuele verduidelijking dus geen nieuw versienummer.

2 Inleiding

De gemeente gebruikt een groot aantal websites en webapplicaties om te communiceren met haar inwoners, daarnaast gebruikt het zelf diverse “as a Service-diensten”, zoals daar zijn: SaaS, IaaS, Paas, ter ondersteuning van bedrijfsprocessen. Op dit moment zijn deze diensten bij een groot aantal verschillende leveranciers ondergebracht en is het van groot belang om een veilige werking te garanderen.

De gemeente dient te voldoen aan de BIO[3] normen en heeft daarnaast te maken met de Meldplicht Datalekken[4] vanuit de AVG[5]. Beide eisen dat de gemeentelijke informatie afdoende en naar de laatste stand der techniek beveiligt.

Gemeenten liggen bij landelijke media regelmatig onder loep betreffende de aanwezige veiligheidsmaatregelen en waargenomen datalekken en spreken deze er op aan als systemen niet conform richtlijnen of common practices zijn beveiligd. Daaruit volgt dat de gemeente als overheidsinstantie een voorbeeldfunctie vervult als het gaat om beveiliging van systemen.

Een digitale inbraak of een datalek heeft zowel voor de gemeente als voor de leverancier grote gevolgen, zodat alles in het werk gesteld moet worden om dit te voorkomen. Mocht er ondanks alle maatregelen toch een inbraak plaatsvinden dan dienen beide partijen hier op voorbereid te zijn, zodat zo snel mogelijk achterhaald kan worden wat er exact gebeurd is en zij beiden verantwoording kunnen afleggen m.b.t. de geaccepteerde restrisico’s.

Uiteraard heeft de beveiliging van persoonsgegevens de hoogste prioriteit. Echter, ook verspreiding van nepnieuws en defacement, het verspreiden van malware en/of het aanvallen van andere systemen vanaf gemeentelijke websites hebben onze aandacht en worden met de juiste maatregelen onwaarschijnlijker.

Op basis van voornoemde wetgeving, de opgedane ervaringen en de ontwikkelingen in de markt zijn deze voorwaarden opgesteld. Het vakgebied van informatieveiligheid is, zeker op technisch vlak, dusdanig dynamiek, dat deze richtlijnen voortdurend aan verandering onderhevig zijn. Voor de laatste versie kunt u contact opnemen met de auteurs.

3 https://www.informatiebeveiligingsdienst.nl/project/baseline-informatiebeveiliging-overheid/
4 https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken
5 https://wetten.overheid.nl/BWBR0040940

Inhoudsopgave

3 Leeswijzer

We gaan in op de beveiligingsrichtlijnen die voor alle diensten gelden die extern toegankelijk zijn of toegankelijk worden gesteld door de gemeente.

Deze richtlijnen zijn per definitie binnen een Programma van Eisen of andere aanschafprocedure allen een eis. Indien afgeweken moet worden van deze richtlijnen kan dit alleen met een uitzondering die vastgesteld wordt door één van de security medewerkers (CISO/ISO/Security Architect). Voor verdere duiding m.b.t. tot de status van de richtlijnen (zijn ze een eis of een wens) kunt u zich richten tot de bijgevoegde spreadsheet. Daarin is vooraf door de (CISO/ISO/Security Architect) een schifting gemaakt tussen eisen en wensen m.b.t. een specifiek Programma van Eisen.

De nader in het document gespecificeerde maatregelen worden uitgesplitst in de hoofdstukken/categorieën *Algemeen, Koppelingen, Configuratie, Procedureel, Certificering* en *Uitsluitingen*.

Algemeen; hierin worden algemeen geldende eisen opgenomen die niet in de overige categorieën vallen.

Koppelingen; in deze categorie vallen alle eisen die direct met koppelen van systemen te maken hebben. Onder koppeling wordt in deze context verstaan: wanneer data tussen de systemen wordt uitgewisseld, geautomatiseerd dan wel manueel.

Configuratie; alle onderwerpen die met het configureren van systemen te maken hebben worden in deze categorie behandeld.

Procedureel; bij de aanschaf van diensten en software zijn procedurele eisen van belang. Deze worden in dit hoofdstuk behandeld.

Certificering; eisen met betrekking tot certificering van de aanbieder op diverse vlakken worden in dit hoofdstuk uiteengezet.

Uitsluitingen; er zijn een aantal situaties die tot directe uitsluiting van deelname aan een aanbesteding of anderzijds gebruikte aanschafprocedure leiden. Wanneer uw product aan één van deze uitsluitingen voldoet, heeft deelname geen zin. Het verdient aanbeveling deze lijst als eerste door te nemen.

4 Algemeen

4.1 Standaard oplossingen

Landelijk uitgangspunt[6] is dat de overheid, rijks- en lokaal, zoveel mogelijk gebruik maakt van open standaarden. Hiervan zijn enkelen zelfs verplicht. Oplossingen die de standaarden van Forum Standaardisatie gebruiken, verdienen dan ook de voorkeur.

Hiermee wil de gemeente "vendor lock-in" voorkomen, door gebruik te maken van software die geen mogelijkheid heeft tot export van gegevens in een open standaard of zelf ontwikkelde software met enkel de mogelijkheid tot opslag en export in eigen, gesloten formaten. (Zie ook Exit Strategie 7.3)

4.2 Wettelijke eisen

Gedurende de looptijd van de contractuele afspraken m.b.t. de afname van de dienst of het product gaat de opdrachtnemer/leverancier de verplichting aan om aan de in en voor Nederland vigerende wettelijke eisen te voldoen, alsmede de in dit document vastgestelde normen en afspraken.

De opdrachtnemer/leverancier heeft de plicht om de afgenomen dienst of product op technisch vlak aan deze kaders te laten voldoen zonder daarvoor extra kosten in rekening te brengen bij de opdrachtgever.

Indien, gedurende looptijd, functionele wijzigingen en werkzaamheden noodzakelijk zijn om aan de in en voor Nederland vigerende wettelijke eisen te kunnen voldoen, geschieden deze altijd in overleg met opdrachtgever. Eventuele uit werkzaamheden voortkomende kosten kunnen niet in rekening worden gebracht zonder overleg en akkoord vanuit opdrachtgever.

In het kader van de verplichtingen die voortvloeien uit de Europese NIS2 richtlijn, kan de gemeente in de context van deze afspraken een periodieke accountantscontrole op deze aansluitvoorwaarden uitvoeren. Opdrachtnemer verplicht zich aan deze controle mee te werken.

4.3 Onderaannemers en subverwerkers

Deze aansluitvoorwaarden (eisen en wensen) inclusief het ingevulde spreadsheet zijn onderdeel van het contract en zijn zodoende ook van kracht op de onderaannemers van de opdrachtnemer daar waar het werkzaamheden betreft die ten goede komen of onderdeel uitmaken van de te leveren oplossing. Verantwoordelijkheid met betrekking tot communicatie hierover ligt bij opdrachtnemer en wordt door opdrachtnemer richting onderaannemers verzorgt.

6 https://forumstandaardisatie.nl/

4.4 Zelflerende systemen en Artificiële Intelligentie

De gemeente Ede sluit het gebruik van dit type techniek niet uit, maar stelt wel een aantal voorwaarden aan het gebruik ervan. In afwachting van de invoering wetgeving betreffende zelflerende systemen en artificiële intelligentie houdt de gemeente de volgende verplichtingen aan.

Op het moment dat de leverancier zelflerende functionaliteit in de geleverde producten/diensten heeft of aanbrengt, dient onverwijld de gemeente op de hoogte gesteld te worden. In samenwerking met een medewerker van de gemeente dient een registratie opgenomen te worden in het algoritmeregister van de gemeente.

De opdrachtgever geeft ten behoeve van de AI-geletterdheid van de medewerkers van de gemeente aan welke kennis m.b.t. AI voor het gebruik van het systeem benodigd is en bied daarvoor documenten met instructies aan. Dit gaat verder dan alleen een handleiding en gaat daarbij ook in op risico's m.b.t. het gebruik van de oplossing, de mate van vertrouwen op de output van de oplossing en mogelijk herstel van foutieve output van de oplossing.

Geen van de door de leverancier gebruikte zelflerende functionaliteiten mogen verrijkt worden met de door de gemeente aangeleverde gegevens. Hiermee wordt gedoeld op het verrijken van het algemeen gebruikte statistische model, zoals een LLM et. al. Wel kan de output van een dergelijk model met de door de gemeente aangeleverde gegevens verrijkt worden om tot een voor de gemeente een passende output te krijgen. Dit moet echter van tijdelijke aard zijn en mag niet leiden tot verrijking van de modellen die door overige klanten van de leverancier gebruikt worden. Deze additieve gegevens moet ook op elk moment door de gemeente te verwijderen zijn.

Te allen tijde dient de uitkomst van een zelflerend systeem verklaarbaar te zijn door inzicht te geven in de statistisch afwegingen die binnen het gebruikte model tot de uitkomst hebben geleid.

4.5 Autorisaties cloud2cloudkoppelingen

Wanneer de aangeboden oplossing externe koppelingen ondersteund, denk hierbij aan een Application Programming Interface, mogelijkheden tot connecties met een Enterprise Service Bus of anderzijds het geautomatiseerd versturen of ontvangen van gegevens buiten de user interface om, mag de opdrachtnemer alleen koppelingen inrichten die door de gemeente zijn goedgekeurd.

De gemeente levert hiervoor een lijst met personen aan die gemachtigd zijn om het maken van deze koppelingen goed te keuren. Dit kan in sommige gevallen een enkel persoon zijn, maar ook een gremium waarin verschillende disciplines zijn vertegenwoordigd. Dit wordt apart aangegeven.

4.6 Pseudonimiseringseisen

Daar waar de gemeente vereist dat in de dataverwerking pseudonimisering wordt toegepast moet deze aan de volgende eisen voldoen:

1. De te pseudonimiseren gegevens worden vervangen door een willekeurige tekenreeks. Het heeft de voorkeur om hiervoor een willekeurig gegenereerde tekenreeks in de vorm van een UUID[7] te gebruiken. Dit is een erkende standaard en generatie is in veel software en database engines ingebouwd. Tijdens de generatie wordt, door gebruik te maken van de interne procedures, vrijwel altijd een willekeurig gegenereerde initialisatie vector gebruikt welke de entropie[8] ten goede komt.

   Wanneer een UUID niet gebruikt kan worden, dient door de leverancier expliciet aangegeven te worden waarom dit het geval is en dient de wijze van pseudonimiseren aan de gemeente voorgelegd te worden ter goedkeuring.

2. Pseudonimiseren aan de hand van hashing is expliciet niet[9] toegestaan. Ook niet als de broninformatie die gehashed wordt is voorzien van salting[10]. Ook de bekende wijzen van hashen die bestand zouden zijn tegen een brute force aanval zgn. key derivation algoritmen[11], lees: scrypt, bcrypt, PBKDF2, etc, zijn uitgesloten van gebruik.

3. Gepseudonimiseerde brongegevens en hun UUID worden niet opgeslagen in de infrastructuur van de leverancier welke ook de gepseudonimiseerde gegevens gaat verwerken. Wanneer dit wel het geval is, wordt het nut van de pseudonimisering bij een inbraak of dataverlies teniet gedaan.

4. Daar waar correlatie nodig is tussen verschillende tabellen met een overeenkomstige brongegevens (lees: primaire key of secondaire key in genormaliseerde[12] databases), dient deze correlatie tot stand te komen aan de hand van het pseudoniem. In geval van de noodzaak tot de-pseudonimisering kan de databron met de brongegevens en de UUID geraadpleegd worden. Hiermee wordt eenzelfde functionaliteit bereikt als men met hashing zou bereiken, zonder de introductie van ongewenste de-pseudonimisering bij een datalek, inbraak of menselijke fout.

7 https://nl.wikipedia.org/wiki/Universally_unique_identifier
8 https://en.wikipedia.org/wiki/Entropy_(computing)
9 https://www.autoriteitpersoonsgegevens.nl/themas/beveiliging/beveiliging-van-persoonsgegevens/gegevens-pseudonimiseren
10 https://en.wikipedia.org/wiki/Salt_%28cryptography%29
11 https://en.wikipedia.org/wiki/Key_derivation_function
12 https://nl.wikipedia.org/wiki/Databasenormalisatie

5 Koppelingen met de dienst

5.1 Uitwisseling van gegevens

De gemeente tracht het aantal koppelvlakken met externe diensten te minimaliseren. Door het aantal koppelvlakken beperkt te houden, worden beheerwerkzaamheden vereenvoudigd, risico's beperkt, oplossingen flexibeler gehouden en kunnen veiligheidsissues eenvoudiger worden opgelost. Om dit te bereiken wordt het volgende geëist.

1. Gegevensuitwisseling, met betrekking tot door de gemeente verwerkte gegevens, vindt plaats via de reeds ingerichte Enterprise Service Bus[13]. (Denk hierbij aan inwonersinformatie etc.).
2. Uitwisseling van deze gegevens via de ESB, wordt middels de daartoe verplichte standaarden[14] gedaan. (Denk aan StUF, GWSW en Geo Informatie).
3. Uitwisseling van gegevens die niet passen binnen de verplichte standaarden worden middels de set aan aanbevolen standaarden[15] gedaan.
4. Wanneer er gegevens uitgewisseld moeten worden die niet via de ESB verwerkt kunnen worden kan dit alleen in overleg met Security Personeel en na uitdrukkelijke goedkeuring.
5. Wanneer er gegevens uitgewisseld moeten worden die met verplichte of aanbevolen standaarden verzonden kunnen worden kan dit alleen in overleg met Security personeel en na uitdrukkelijke goedkeuring.
6. Elke vorm van informatie-uitwisseling, die na goedkeuring is toegestaan buiten de ESB en standaarden om, wordt geïnitieerd vanuit het netwerk van de gemeente zelf, om zodoende statefull firewalling[16] te kunnen toepassen en alleen met uitdrukkelijke toestemming van het Security personeel.
7. Verbindingen die vanuit de dienst richting het netwerk van de gemeente opgezet dienen te worden om gegevens uit te wisselen worden niet toegestaan. Hiervoor is de ESB ingericht.
8. Elke vorm van gegevensuitwisseling (geautomatiseerd dan wel manueel) wordt afdoende versleuteld. (zie onder andere 6.2).
9. Voor alle overige afwijkingen, niet genoemd in bovenstaande tekst, wordt contact gezocht met het Security personeel, zodat een risicoprofiel gemaakt kan worden.

5.2 Technische logging

Alle logs van alle gebruikte devices (webservers, databaseservers, firewalls, IDS, enzovoorts) worden op een separate geïsoleerde en afdoende beveiligde server voor een periode van minimaal 6 maanden bewaard. Als er persoonsgegevens worden verwerkt dienen de logs voor minimaal de vastgestelde wettelijke bewaartermijn van het type persoonsgegevens[17] + 6 maanden bewaard te worden.

Als er sprake is van een (mogelijk) security-incident, kunnen de logs als enige bron uitsluitsel geven over wat er is gebeurd. Als alles netjes gelogd is kan er sneller en effectiever onderzocht worden of er daadwerkelijk sprake is van een digitale inbraak / datalek.

Let wel dat bijzondere persoonsgegevens zoals BSN-nummers nooit ongemaskeerd in de logs mogen staan. De gemeente verwacht van de opdrachtnemer dat deze zelf op regelmatige basis (minimaal wekelijks, liefst geautomatiseerd) de logs controleert op mogelijk verdachte zaken. Als er verdachte situaties vastgesteld worden, dan dienen deze zo snel mogelijk gemeld te worden bij de in de verwerkersovereenkomst genoemde verantwoordelijken.

13 https://en.wikipedia.org/wiki/Enterprise_service_bus
14 https://forumstandaardisatie.nl/open-standaarden/verplicht
15 https://forumstandaardisatie.nl/open-standaarden/aanbevolen
16 https://en.wikipedia.org/wiki/Stateful_firewall
17 https://www.avgdashboard.nl/wettelijke-bewaartermijnen/

5.3 Gebruik van e-Mail

Voor gebruik van e-mail zijn een drietal scenario's beschikbaar. Afhankelijk van de inrichting, mate van beveiliging en ondersteuning van diverse protocollen door de af te nemen dienst, wordt de keuze bepaald. Wanneer meerdere scenario's toe te passen zijn, is de keuze m.b.t. het toe te passen scenario ter discretie van de gemeente.

Algemene verplichtingen

Conform de opgelegde richtlijnen vanuit forum standaardisatie, dient de gemeente en diens ketenpartner(s), maatregelen te nemen om het versturen van "valse e-mails" zoals spam en phishing tegen te gaan.

De verplichte standaarden hiervoor zijn: DNSSEC, SPF / DKIM, DMARC en TLSA DANE[18]. *Standaard worden deze zo ingesteld dat het onmogelijk is om e-mail, als derde partij, namens het betreffende domein te versturen naar ontvangers die deze instellingen controleren.*

Verder dienen de volgende richtlijnen gerespecteerd te worden bij het verzenden van e-mail:

1. Persoonsgegevens worden nimmer per e-mail verstuurd. (gebruikers worden hier actief op gewezen)
2. Uitgaande e-mail wordt middels TLS-encryptie verstuurd, (Wanneer vanaf een domein in eigendom van de gemeente wordt verstuurd, zal het benodigde certificaat door de gemeente worden verstrekt.)
3. De inkomende e-mailserver ondersteunt TLS-encryptie.
4. De volgende internetstandaarden worden minimaal ondersteund door die e-mailserver:
    - TLSA DANE
    - STARTTLS
    - DMARC
    - SPF
    - DKIM
    - DNSSEC
5. Er zijn afdoende anti-spammaatregelen genomen, minder dan 1% van de berichten kan als ongewenst worden geclassificeerd.
6. Er wordt een actief updatebeleid toegepast op de e-mailserver. Zie patchbeleid.
7. Alle relevante aan beveiliging gerelateerde logs voldoen aan 2.1
8. De betreffende machine wordt niet voor andere doeleinden gebruikt (bijvoorbeeld als webserver). Dit om het risico op een digitale inbraak te verkleinen.
9. Beheer van de e-mailserver vindt uitsluitend plaats via een beveiligde VPN-verbinding (géén direct vanaf internet benaderbare web-shell, ssh-shell, en dergelijke). Zie punt remote beheer voor meer details rondom beheer.

18 https://www.forumstandaardisatie.nl/open-standaarden/verplicht

Verzending onder eigen domeinnaam

Wanneer gekozen wordt om e-mailberichten vanuit de domeinnaam van de leverancier te versturen of vanaf een domeinnaam van een subverwerker van de leverancier of anderzijds een domeinnaam die niet in beheer is van de gemeente, is de houder van de domeinnaam is samenwerking met de leverancier verantwoordelijk om aan de algemene verplichtingen m.b.t. e-mail te (blijven) voldoen. Dit scenario is alleen toepasbaar als alleen naar de medewerkers van de gemeente gestuurd wordt.

Verzending onder subdomein van de gemeente

Wanneer de leverancier vanaf een domeinnaam van de gemeente e-mail gaat versturen, zonder daarbij gebruik te maken van de infrastructuur van de gemeente, wordt hier voor een subdomein door de gemeente ingericht.

In samenspraak met het technisch personeel van de gemeente worden de juiste verplichte maatregelen genomen. Met daarbij als extra voorwaarde dat alleen in deze situatie gebruik gemaakt mag worden van SPF includes om de mailservers van de leveranciers te authenticeren voor verzending van deze e-mail.

Er wordt, per afgenomen dienst, een subdomein toegekend, zodat fouten bij SPF includes geen invloed hebben op onderlinge dienstverlening van verschillende leveranciers.

Bij inrichting en onderhoud, wordt, door de gemeente en de leverancier, aan de algemene verplichtingen m.b.t. e-mail voldaan.

Verzending vanaf hoofddomein van de gemeente

Wanneer de situatie vereist dat de leverancier uit naam van het hoofddomein van de gemeente e-mail moet versturen, kan dat alleen als dit via de infrastructuur van de gemeente loopt. SPF includes worden, vanwege de regelmatig voorkomende storingen op dit gebied en de onbeheersbaarheid waartoe vele includes leiden, niet geaccepteerd.

Dit houdt in dat de leverancier de mail aflevert op de infrastructuur van de gemeente via SMTP submission/submit op de in het Technisch- of Low-Level design aangegeven host(s) en poort(en) en/of in samenspraak met het technisch personeel van de gemeente.

5.4 Aansluiting op ADFS en/of Entra ID

Als de betreffende SaaS applicatie door de medewerkers van de gemeente gebruikt wordt, moet worden gekoppeld aan de ADFS[19] of Entra ID[20] omgeving van de gemeente. Verder in het onderstaande stuk wordt met centrale authenticateservice verwezen naar of ADFS of Entra ID.

Als er middels deze centrale authenticatieservice gekoppeld is, zijn de gestelde eisen m.b.t. wachtwoorden (6.1) niet meer van toepassing, met uitzondering van de eisen m.b.t. het buiten de centrale authenticatieservice omgeving inloggen bij beheerhandelingen van de leverancier.

Het kan voorkomen dat een hybride oplossing geleverd wordt met een zowel centrale authenticatieservice toegang als een publiekelijke toegang. Daarvoor geldt, dat voor bij de gemeente aangesloten entiteiten (zoals samenwerkingsverbanden of onderaannemers) zich altijd authenticeren met de centrale authenticatieservice als zij zijn opgenomen in de AD van de gemeente. Daarnaast gelden de wachtwoordeisen alsnog voor die accounts die niet via de centrale authenticatieservice ontsloten worden.

De aansluiting van de leverancier via de centrale authenticatieservice ondersteunt SSO (Single Sign-On) op een wijze die het mogelijk maakt om geautomatiseerd in te loggen, zonder extra handelingen van de eindgebruiker. De doorverwijzing naar de centrale authenticatieservice van de gemeente is automatisch, zonder dat daarbij door de eindgebruiker een identifier ingevoerd hoeft te worden of anderzijds inlog-handelingen noodzakelijk zijn, indien de centrale authenticatieservice opnieuw inloggen niet noodzakelijk acht.

Uitgezonderd van de geautomatiseerde doorverwijzing naar de centrale authenticatieservice installatie van de gemeente, zijn die diensten die gebruikmaken van een hybride inlogmethodiek zoals hierboven beschreven. De mogelijkheid om via centrale authenticatieservice in te loggen wordt dan aangeboden middels het klikken op een knop. Ook bestaat de mogelijkheid om voor centrale authenticatieservice- en extern-inloggen een tweetal specifieke landingspagina's te maken op verschillender URL's, waarbij de centrale authenticatieservice landingspagina geautomatiseerd doorverwijst naar de centrale authenticatieservice installatie van de gemeente, alwaar het inlogproces plaatsvindt.

De opdrachtnemer sluit aan bij de laatste implementatie van ADFS en of Entra ID volgens de Microsoft methodieken. Bij updates van ADFS en of Entra ID zonder backwards compatibiliteit, beweegt opdrachtnemer met deze ontwikkelingen mee, zonder extra kosten in rekening te brengen.

Bij inloggen met de centrale authenticatieservice is de rechtenstructuur van de opdrachtnemer leidend. Vanuit de centrale authenticatieservice van de gemeente komt alleen een identifier en een go/no-go m.b.t. inloggen.

Onderlinge communicatie betreffende de ADFS[21] configuratie dient via een meta-datafile plaats te vinden welke online benaderbaar is. De minimale eisen waaraan deze meta-datafile dient te voldoen zijn:

- Alle de te gebruiken certificaten worden in de meta-datafile opgenomen.
- De meta-datafile dient bij wijzigingen in de configuratie automatisch geüpdatet te worden.
- De meta-datafile van de gemeente dient één keer per etmaal opgevraagd en verwerkt te worden aan de zijde van de opdrachtnemer.
- De leverancier dient Certificate-Rollover te ondersteunen.
- Bij wijzigingen aan de zijde van de opdrachtnemer wordt de meta-datafile geautomatiseerd aangepast en beschikbaar gesteld voor de gemeente. De gemeente zal periodiek, met een maximale doorlooptijd van 24 uur, deze meta-datafile opvragen en verwerken.

19 https://en.wikipedia.org/wiki/Active_Directory_Federation_Services
20 https://www.microsoft.com/nl-nl/security/business/identity-access/microsoft-entra-id
21 https://docs.microsoft.com/en-us/windows-server/identity/active-directory-federation-services

5.5 Monitoring

Opdrachtnemer beschikt over een monitoringsysteem om de beschikbaarheid en performance van de aangeboden diensten te monitoren, zodat de beheersorganisatie direct gealarmeerd wordt bij onder andere, maar niet uitputtend: uitval, performanceproblemen, (D)DOS-aanvallen, onverklaarbare toename in verkeer naar internet, verlopen van beveiligingscertificaten, ongeautoriseerde wijzigingen aan configuratiebestanden, ongeautoriseerde wijzigingen aan systeembestanden, enzovoorts.

Opdrachtnemer heeft statistieken van zijn internetverkeer en systeemperformance beschikbaar van ten minste 2 jaar terug.

Monitoring van de dienstverlening is aan te sluiten op de monitoring van de gemeente, zodat de gemeente in staat is de kwaliteit van de dienstverlening te meten.

5.6 Afscherming van de dienst

Als de dienst alleen bedoeld is voor intern gebruik bij de gemeente en indien de verwerking van de gegevens gevoelig ligt, wordt toegang tot de applicatie beperkt tot de door de gemeente gebruikte publieke ip adressen.

Als de dienst meerdere koppelpunten heeft, bijvoorbeeld een gedeelte waarop medewerkers van de gemeente inloggen en een gedeelte waar publiekelijk ingelogd/gekeken kan worden, dient de dienst de mogelijkheid te hebben om het gedeelte voor medewerkers op basis van IP filtering te scheiden van de publiekelijke toegang.

Let op: IP filtering is verplicht als er sprake is van een niet productie omgeving (bv test, acceptatie of ontwikkel omgeving). Deze kunnen niet ongefilterd op het internet ontsloten worden.

6 Configuratie en voorwaardelijke instellingen

6.1 Wachtwoorden

Wachtwoorden zijn tot op heden de meest gebruikte manier van authenticatie. De praktijk heeft uitgewezen dat dit vaak een zwakke schakel is. De gemeente stelt de volgende eisen aan wachtwoorden welke afgeleid zijn van de NIST 800-63[22] richtlijnen.

- Wachtwoorden dienen een minimale lengte van 8 posities te hebben, niet een default waarde van een leverancier te bevatten EN het wachtwoord dient minstens een Hoofdletter, cijfer en leesteken bevatten. Bij wachtzinnen van 20 posities, vervalt deze complexiteitseis. Wachtwoorden tot 64 karakters moeten ondersteund worden, deze waarde mag hoger zijn. Langere wachtzinnen[23] worden aangeraden.
- Wachtwoorden moeten tenminste half jaar gewijzigd worden.
- Er kan alleen ingelogd worden met multi-factor-authenticatie zoals TOTP[24], HOTP[25] of U2F[26]. SMS en E-mail is niet toegestaan.
- Er is een password reset-optie beschikbaar.
- Wachtwoorden worden altijd versleuteld opgeslagen, waarbij gebruik gemaakt wordt van salting en stretching algoritmes. Zoals daar zijn: CRPING voor salting en ARGON2, BCRYPT, SCRYPT of PBKDF2 voor stretching[27].
- Gebruikersnamen en wachtwoorden worden nimmer door de browser gecached.
- Wachtwoorden die door de opdrachtnemer worden gebruikt op systemen van de gemeente zijn uniek en worden niet bij andere klanten van de opdrachtnemer gebruikt.
- Wachtwoorden moeten gescreend worden tegen een lijst met veel gebruikte en gecompromitteerde wachtwoorden, repetitieve of sequentiële karakters, en context specifieke woorden zoals gebruikersnamen, organisatienaam, naam van de dienst etc. Dit kan gecheckt worden bij het aanmaken van het account en bij het resetten van het wachtwoord.

22 https://pages.nist.gov/800-63-3/sp800-63b.html
23 https://en.wikipedia.org/wiki/Passphrase
24 https://en.wikipedia.org/wiki/Time-based_One-time_Password_algorithm
25 https://en.wikipedia.org/wiki/HMAC-based_One-time_Password_algorithm
26 https://en.wikipedia.org/wiki/Universal_2nd_Factor
27 https://crackstation.net/hashing-security.htm

6.2 TLS/SSL-beveiliging - Certificaten

De gemeente heeft een voorbeeldfunctie als het gaat om de beveiliging van systemen. Toegang tot alle websites ongeacht de inhoud dienen te allen tijde voorzien te zijn van HTTPS / SSL / TLS.

Onversleuteld verkeer (HTTP) is, de facto, niet toegestaan. Redirects van http naar https zijn wel toegestaan, mits bij deze redirect geen gegevens worden verzonden.

Wanneer een dienst expliciet het gebruik van versleuteling niet toestaat, dient daarvoor een exception permit geschreven te worden door her architectenteam van de gemeente.

Verkeer naar alle websites van de gemeente en naar alle afgenomen SaaS-diensten dient beveiligd te zijn middels TLS. Voor de eisen van de TLS verbinding kijken we onder andere naar de ICT-beveiligingsrichtlijnen voor TLS van NCSC[28] en de Security/Server Side TLS wiki van Mozilla[29]. Hierbij wordt gekeken naar compatibiliteit en veiligheid. De richtlijnen komen grotendeels overeen met de Intermediate configuratie uit de richtlijnen van Mozilla, hierbij wordt minimaal deze software vanaf het getoonde versie nummer ondersteund.

Configuratie	Firefox	Android	Chrome	Edge	Java	OpenSSL	Opera	Safari
Modern	63	10.0	70	75	11	1.1.1	57	12.1
Intermediate	27	4.4.2	31	12	8u31	1.0.1	20	9
Old	1	2.3	1	12	6	0.9.8	5	1

De richtlijnen van de gemeente zijn als volgt:

- Certificaten voor domeinen van de gemeente worden alleen door de gemeente zelf aangevraagd, om misbruik te voorkomen.
- Als er via een officieel kanaal van de gemeente gecommuniceerd wordt met burgers (bijvoorbeeld e-loketten), dan wordt er gebruik gemaakt van een commerieel verkregen certificaat met domeinvalidatie.
- Wildcard-certificaten worden niet toegestaan.
- TLS 1.2 en TLS 1.3 zijn ingeschakeld, oudere TLS versies worden niet toegestaan.
- De volgende cipher suites zijn ingeschakeld voor TLS 1.2. Oudere en onveiligere Cipher suites zijn uitgeschakeld. ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:DHE-RSA-CHACHA20-POLY1305. Als TLS 1.3 ondersteund wordt zijn de volgende cipher suites ook ingeschakeld TLS_AES_128_GCM_SHA256:TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256.
- Het certificaat type is RSA 4096bits of ECDSA (P-256)
- (Perfect) Forward Secrecy[30] dient gebruikt te worden.
- Er dient gebruik gemaakt te worden van minimaal HMAC-SHA-256 voor het versleutelen van gegevens, bij voorkeur wordt er HMAC-SHA-512 gebruikt.
- SNI[31] mag gebruikt worden.
- In de CSR dient de volgende informatie opgenomen te worden:
- Subject: C=NL, ST=Gelderland, L=Ede, O=gemeente Ede, OU=ICT Beheer/emailAddress=beheer@ede.nl, CN=[hostname].<gewenste domein>.nl
- Uw CSR wordt altijd door de gemeente gecontroleerd op correctheid.

Op de website: https://www.ssllabs.com/ssltest/ kan getest worden of aan de genoemde eisen wordt voldaan. Elke score minder dan een “A” is onacceptabel.

28 https://www.ncsc.nl/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1
29 https://wiki.mozilla.org/Security/Server_Side_TLS
30 https://en.wikipedia.org/wiki/Forward_secrecy
31 https://en.wikipedia.org/wiki/Server_Name_Indication

6.3 Network Security Monitoring

Om mogelijke aanvallen te detecteren beschikt opdrachtnemer over tooling om verdachte zaken in het netwerkverkeer te detecteren. Dit kan middels een IDS, IPS, HIDS of HIPS. Deze dient ingesteld te worden voor de bescherming van de specifieke situatie. De logs van deze tooling worden uiteraard conform de beschrijving van punt 5.2 opgeslagen en bewaard.

6.4 (D)DOS Maatregelen

Afpersing middels DoS- of DDoS-aanvallen[32] is steeds succesvoller. De gemeente vereist van de opdrachtnemer dat deze afdoende maatregelen heeft genomen om (D)DoS-aanvallen in ieder geval binnen 12 uur succesvol af te slaan.

De opdrachtnemer overlegt vóór opdrachtverstrekking de procedure hoe zij gaat handelen in het geval van een (D)DoS-aanval en legt eventuele afwijkingen met betrekking tot de geldende 12 uur in een SLA vast.

6.5 Opslag van vertrouwelijke en privacygevoelige informatie

Als er op de betreffende systemen vertrouwelijke of privacygevoelige informatie opgeslagen wordt dient deze te allen tijde adequaat versleuteld te zijn.

Hierbij worden de richtlijnen van de autoriteit persoonsgegevens[33] gevolgd, hoofdstuk: Beveiliging van persoonsgegevens[34]

Mochten kwaadwillende personen toegang krijgen tot deze gegevens dan moeten deze voor hen onbruikbaar zijn.

6.6 Back-up

De gemeente verwacht van de opdrachtnemer dat die op regelmatige basis back-up's maakt van de betreffende systemen/data. De interval en bewaartermijn van de back-up is afhankelijk van de betreffende dienst en wordt beschreven in de SLA die Opdrachtgever met de gemeente afsluit.

In deze SLA wordt betreffende de backup op zijn minst gedefinieerd wat de RPO en RTO van de gegevens en de daarmee de dienst is (de B van BIV Classificatie).

RPO: Recovery Point Objective:
RPO staat voor het feit dat een voorval leidt tot een bepaalde mate van dataverlies. Met andere woorden: wat is de afgesproken hoeveelheid data die acceptabel wordt geacht verloren te zijn gegaan.

RTO: Recovery Time Objective
De toepassing of applicatie zal een bepaalde tijd niet beschikbaar zijn, ofwel: ongeplande downtime. Bij RTO gaat het dus om de tijd waarbinnen de applicatie weer beschikbaar dient te zijn.

Alle back-ups dienen versleuteld en adequaat beveiligd bewaard te worden. De gemeente eist dat de opdrachtnemer op regelmatige basis controleert of de in gebruik zijnde systemen en data hersteld kunnen worden van de gemaakte back-up.

32 https://en.wikipedia.org/wiki/Denial-of-service_attack
33 https://www.autoriteitpersoonsgegevens.nl/nl/zelf-doen/thematische-beleidsregels
34 https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_beveiliging_van_persoonsgegevens.pdf

6.7 Systeemisolatie

Om te voorkomen dat gecompromitteerde systemen laterale netwerkbewegingen faciliteren, worden de volgende eisen gesteld:

- Systemen worden nimmer gedeeld met andere klanten (shared hosting is niet toegestaan).
- Pentesten moeten uitgevoerd kunnen worden zonder invloed uit te oefenen op systemen van andere klanten
- Systemen van de gemeente zijn logisch gescheiden van systemen ten behoeve van andere klanten (firewalling en netwerksegmentering).
- Alle software die niet noodzakelijk is voor de correcte werking van de dienst is uitgeschakeld of verwijderd.
- Alle poorten die niet noodzakelijk zijn voor correcte werking van de dienst, maar niet uitgeschakeld of verwijderd kunnen worden, zijn middels een hostbased firewall gesloten

6.8 Beheer op afstand (door leverancier)

Aanvallers blijken regelmatig binnen te komen via beheeringangen van de betreffende systemen (bijvoorbeeld RDP, SSH of beheer-webinterface). RDP connectie naar de beheerinterface van de dienst die direct vanaf internet benaderbaar zijn, zijn expliciet uitgesloten.

De gemeente vereist van de opdrachtnemer dat beheertoegang alleen mogelijk is via een correct beveiligde VPN-verbinding en dat er logging van die VPN-verbindingen aanwezig is. Inloggen op deze VPN verbinding geschiedt op basis van Multi Factor Authenticatie.

Verder dienen alle beheerhandelingen herleid te kunnen worden naar de betreffende beheerder. Handelingen van beheerders wordt gelogd zoals beschreven bij 5.2.

6.9 Gebruik van trackers op websites en webdiensten

De gemeente is een overheidsinstelling, burgers moeten ervan uit kunnen gaan dat hun privacy is gewaarborgd op het moment dat websites van de gemeente bezocht worden. Het is dan ook niet toegestaan om trackers te gebruiken op de betreffende website wegens de grote schending van privacy en het niet in controle hebben over welke software (javascript) er wordt uitgevoerd op het apparaat van de gebruiker.

6.10 Gebruik van trackers en logging in apps/(web)applicaties

Daar waar gebruik gemaakt wordt van apps/(web)applicaties zijn deze ontdaan van debugging opties, externe logging en trackers.[35] [36]

Mocht gebruik van debugging, logging of tracking noodzakelijk zijn voor de, door de gemeente vereiste, functionaliteit van deze app/(web)applicatie, dient dit specifiek per debugging optie, logging optie of tracker aangegeven te worden en waarvoor. Ook dient aangegeven te worden welke gegevens worden verzameld en wanneer dit om persoonsgegevens gaat, wat hiervoor de grondslag is en moet dit in de verwerkersovereenkomst bijgevoegd zijn, inclusief subverwerkers.

Het is expliciet niet toegestaan om gebruikers bij installatie of gebruik te vragen naar het accepteren van voorwaarden die niet genoemd zijn in de overeenkomst die is afgesloten tussen aanbieder en de gemeente. De overeenkomst met de gemeente is daarin leidend. Dit geldt ook voor mogelijk noodzakelijke apps/applicaties van derde partijen.

Dientengevolge gebruikt de app/applicatie minimale rechten op de platforms waarvoor deze ontwikkeld is. De door de app gevraagde rechten, denk hierbij aan o.a. toegang tot locatie, contactgegevens of opslag, zijn strikt noodzakelijk voor de, door de gemeente geëiste, functionaliteit.

6.11 OTA(P) straat

Er wordt, zonder daarvoor extra kosten te berekenen, een vorm van OTA (Ontwikkel, Test, Acceptatie) omgeving beschikbaar gesteld. Er wordt op zijn minst voorzien in een Acceptatieomgeving.

Voor diensten die niet gekoppeld zijn met de gemeente, is dit niet noodzakelijk, echter voor systemen die wel koppelen met de gemeente ten behoeve van gegevensuitwisseling of bewerking zonder tussenkomst van de gebruiker (denk hierbij aan aansluiting op de ESB), is dit verplicht.

Wanneer tests uitgevoerd moeten worden op de OTA omgevingen is het expliciet verboden om daarvoor productiedata te gebruiken. De gemeente begrijpt dat in sommige gevallen een test zonder correcte gegevens zeer lastig uit te voeren is en stelt daarom de mogelijkheid open om gedocumenteerd een exceptie aan te vragen. Deze exceptie wordt samen met de CISO/ISO en de Privacyjurist van de gemeente opgesteld en periodiek, minimaal jaarlijks, herzien.

De ingerichte omgevingen (Ontwikkel, Test, Acceptatie en Productie) zijn thematisch goed van elkaar te onderscheiden. Denk hierbij een kleurstelling van de applicatie of een zeer duidelijke afwijking in de presentatie van de omgeving (banners etc.), om vergissingen aan de zijde van de gebruikers van de omgevingen zo veel mogelijk te voorkomen.

35 https://exodus-privacy.eu.org/en/page/what/ (uitleg daar waar het android apps betreft, begrippen zijn universeel toepasbaar)
36 https://en.wikipedia.org/wiki/Web_tracking

6.12 Dienstgebonden Auditlogging

Onder dienstgebonden auditlogging wordt verstaan dat benadering en wijziging van gegevens die verwerkt worden, bijgehouden wordt in een log, beschikbaar voor raadplegen door de gemeente Ede bij de dienst zelf of op een centrale locatie van de gemeente.

De gemeente hanteert met betrekking tot auditlogging een gradatieschaal op basis van de BIV classificatie[37] van de data die met de betreffende dienst verwerkt wordt en varieert in de daarmee in de vast te leggen informatie als wel de tijdsduur. Welke schaal gebruikt wordt, staat in bijgevoegde spreadsheet genoemd.

Basis:

Vastleggen van authenticatiepogingen, zowel correcte als foutieve, en tijdstip van deze pogingen in de log management oplossing van de dienst. Vastleggen van relevante input en output van een IT-systeem of service in deze oplossing. Deze gegevens worden bewaard voor een periode van 6 maanden.

Midden:

Vastleggen van authenticatiepogingen, zowel correcte als foutieve, en tijdstip van deze pogingen in de log management oplossing of een centraal gecontroleerde log management oplossing. Vastleggen van relevante input en output van een IT-systeem of service in deze oplossing. Deze gegevens worden bewaard voor een periode van 6 maanden. Op deze gegevens word geautomatiseerde controle uitgevoerd om in uitzonderingsgevallen gealarmeerd te worden.

Hoog:

Vastleggen van authenticatiepogingen, zowel correcte als foutieve, en tijdstip van deze pogingen in een centraal gecontroleerde log management omgeving. Vastleggen van relevante input en output van een IT-systeem of service. Deze gegevens worden bewaard voor een periode van 12 maanden. Op deze gegevens wordt geautomatiseerde controle uitgevoerd om in uitzonderingsgevallen gealarmeerd te worden. Alle mutaties op de gewijzigde brongegevens worden vastgelegd en kunnen ongedaan gemaakt worden. Oudere versies van brongegevens zijn in te zien en te herstellen.

BBN (Basis BeveiligingsNiveau):

De gemeente bevind zich in een overgangsfase van de BI naar de BIO. De BIO maakt gebruik van de BBN structuur. Wanneer verwezen wordt naar de BIO, vallen de verwerkte gegevens vrijwel zonder uitzondering in BBN 2[38]. Wanneer de gegevens in een ander BBN[39] vallen, zal hiervoor in bijgevoegde spreadsheet een uitzonderingsdefinitie gemaakt worden door de gemeente. De vertaling naar de bovengenoemde drie gradaties is daarin ook opgenomen.

37 Zie BIV classificatie document voor interne referentie voor beoordeling classificatie data. Voor Intern gebruik.
38 https://www.informatiebeveiligingsdienst.nl/project/baseline-informatiebeveiliging-overheid/
39 BBN = Basis Beveiligings Niveau

7 Procedures en afspraken

7.1 Controle op bekende kwetsbaarheden

De gemeente verwacht van de opdrachtnemer dat deze zelf op regelmatige basis controleert of de betreffende dienst kwetsbaar is voor tenminste de 10 meest voorkomende kwetsbaarheden zoals deze zijn gespecificeerd door het Open Web Application Security Project (OWASP)[40].

7.2 Patchbeleid

Installatie van beveiligingsupdates en patches is een van de belangrijkste beveiligingsmaatregelen die genomen kan worden. De gemeente eist van opdrachtnemer dat beveiligingsupdates tijdig worden geïnstalleerd aan de hand van onderstaande implementatienormen:

- Adviezen van softwareleveranciers worden opgevolgd.
- Kritische beveiligingsupdates worden binnen 24 uur na uitgifte geïnstalleerd.
- Alle software op alle gebruikte systemen dient geüpdatet te worden!
  Dus niet alleen software die vanaf het internet benaderbaar is.
- Niet kritische beveiligingsupdates en gewone updates worden periodiek geïnstalleerd met een maximale doorlooptijd van een maand.
- De opdrachtnemer houdt een logboek bij van geïnstalleerde updates. Hiermee moet het achteraf altijd mogelijk zijn om te toetsen, wanneer een bepaalde update geïnstalleerd is.

7.3 Exit-strategie

Websites en diensten van de gemeente moeten met een minimale inspanning en op kostenefficiënte wijze bij een andere leverancier ondergebracht kunnen worden. Het gebruik van maatwerkoplossingen moet tot een minimum worden beperkt en is alleen toegestaan na schriftelijke toestemming van de gemeente.

Vóórdat een overeenkomst met de gemeente wordt aangegaan moet inzichtelijk gemaakt worden wat de aanpak van een exit is (zijnde een migratieplan met grove schatting van de begroting; het vermelden van een uurtarief is expliciet onvoldoende, verdere uitwerking komt tot uitdrukking het PvE).

40 https://owasp.org/www-project-top-ten/

7.4 Locatie van apparatuur, data en onderaannemers

De gemeente eist dat alle gemeentelijke- en overheidsdata binnen de grenzen van de Europese Unie opgeslagen wordt, om discrepanties tussen verschillende privacywetgevingen te voorkomen en mogelijke onduidelijke constructies m.b.t. overlappende wetgeving en veiligheidseisen te vermijden.

De gemeente geeft er expliciet de voorkeur aan om alle apparatuur en data op Nederlands grondgebied onder te brengen onder auspiciën van een in Nederland gevestigde onderneming.

De gemeente wil graag weten waar haar data is opgeslagen en vereist dan ook dat in de overeenkomst beschreven wordt op welke fysieke locaties haar data is ondergebracht. Hiervoor wordt een volledige leverketenbeschrijving geëist op zowel contractueel als technisch vlak.
(Zie ook verwerkersovereenkomst indien van toepassing).

Daarnaast dient opdrachtnemer ervoor te waken dat deze opgeslagen data van de gemeente te allen tijde aan de gestelde eisen blijft voldoen. Dit geldt voor de gehele leverketen. Eventuele kosten die voortvloeien uit het feit dat de opslag niet meer voldoet, zijn voor rekening van opdrachtnemer.

Enkele voorbeelden van risicovolle situaties die niet zonder meer zijn toegestaan zonder daar expliciete afspraken over te maken:

- Gebruik maken van een back-up dienst (al dan niet van derden) waarbij niet 100% zeker is dat de data binnen de grenzen van de Europese Unie blijft.
- Gebruik maken van beheerdiensten van partijen gevestigd buiten de grenzen van de Europese Unie. (Follow the Sun, etc.)
- Gebruik maken van ontwikkeldiensten van partijen gevestigd buiten de grenzen van de Europese Unie.
- Hergebruik van gemeentelijke data voor test- en acceptatiedoelen, zonder expliciete schriftelijke toestemming van de gemeente.
- Opslag van gemeentelijke data buiten de beveiligde omgeving, bijvoorbeeld op laptops van medewerkers om ‘even’ wat te testen, fouten te zoeken, et cetera.
- Verhuizingen van programmatuur en apparatuur naar een leverancier buiten de grenzen van de Europese Unie.

7.5 Privacywetgeving

Opdrachtnemer is zich bewust van de ongeldigverklaring van het Privacy Shield[41] en houdt daarmee rekening in zoverre dit van toepassing is op de dienst die geleverd wordt. Toekomstige kosten met betrekking tot het voldoen aan de huidige en toekomstige vigerende wetgeving m.b.t. privacy, zijn voor opdrachtnemer.

De gemeente maakt geen gebruik van modelcontracten (ook wel standaardbepalingen, standard contractual clauses of SCC's) om zodoende uniformiteit van levering en regelgeving over het gehele spectrum van afgenomen diensten binnen de gemeente te waarborgen.

7.6 Verwerkersovereenkomst[42]

Een separate verwerkersovereenkomst, zoals deze is opgesteld door de VNG[43], maakt te allen tijde onderdeel uit van de overeenkomst indien persoonsgegevens worden verwerkt.

41 https://autoriteitpersoonsgegevens.nl/nl/nieuws/privacy-shield-voor-doorgifte-naar-vs-ongeldig-verklaard
42 Dit staat ook in de GIBIT, echter zonder de VNG vereiste.
43 https://www.informatiebeveiligingsdienst.nl/project/verwerkersovereenkomst-gemeenten/

7.7 Audits - The Right to Audit

Om te verifiëren of de opdrachtnemer voldoet aan de gestelde eisen, kan de gemeente op jaarlijkse basis audits uitvoeren. Van de opdrachtnemer wordt volledige medewerking en transparantie verwacht bij deze audits. Als blijkt dat de opdrachtnemer in gebreke blijft, krijgt deze een bepaalde termijn (die afhankelijk is van de ernst van de situatie) om de gebreken te herstellen.

7.8 Fysieke beveiliging

De opdrachtnemer dient een (fysiek) toegangsbeleid te hebben waar in staat hoe de fysieke beveiliging van de locaties en apparatuur wordt gewaarborgd. Hierin worden onder andere de fysieke beveiligingszones, toegangsbeveiliging en juiste plaatsing en bescherming van de apparatuur gedefinieerd. Zie voor voorbeelden onder andere de Handreiking Toegangsbeleid van de IBD[44] en Hoofdstuk 11 van de BIO[45].

7.9 Responsible Disclosure

De gemeente hecht veel belang aan de beveiliging van haar systemen en die van haar opdrachtnemers. Ondanks alle voorzorgsmaatregelen blijft het mogelijk dat een zwakke plek in de systemen te vinden is. Daarom maakt de gemeente gebruik van een Responsible Disclosure-beleid.

Aangezien een keten zo zwak is als de zwakste schakel, vereist de gemeente dat opdrachtnemer ook een dergelijk beleid voert.

De opdrachtnemer houdt hier dan ook rekening mee en werkt actief mee aan dergelijke beleidsvoering. Indien een kwetsbaarheid gemeld wordt, zal de opdrachtnemer, per direct, samen met de gemeente, een analyse maken van de kwetsbaarheid in haar dienst of software en alles in het werk stellen om de gevonden kwetsbaarheid zo snel mogelijk te verhelpen.

7.10 Incident Response en forensisch onderzoek

De gemeente vereist dat de opdrachtnemer tenminste 7*15 uur (van 07:00 - 22:00 uur CET) telefonisch bereikbaar is, voor het geval we te maken krijgen met een digitale inbraak of een (D)DoS-aanval.

In verband met de Meldplicht Datalekken heeft de gemeente 72 uur om een mogelijk datalek te melden bij de Autoriteit Persoonsgegevens. In deze 72 uur moet er inzicht komen in de aard en omvang van de digitale inbraak. Daarom is het noodzakelijk dat er ook buiten kantooruren met de opdrachtnemer geschakeld kan worden en dat deze ook ter zake deskundig personeel kan inzetten om de mogelijke inbraak te onderzoeken.

Daarnaast wordt vereist dat de opdrachtnemer een Incident Response-procedure heeft en dat men voorbereid is op een mogelijke digitale inbraak waarbij medewerkers weten wat zij wel en wat zij vooral niet moeten doen bij het onderzoek.

Ook is vereist dat de opdrachtnemer onvoorwaardelijk meewerkt aan een mogelijk forensisch onderzoek, waarbij op korte termijn kopieën van gebruikte machines en alle andere relevante informatie (logs, monitoringrapportages, en dergelijke) overhandigd kan worden aan een door de gemeente ingezet forensisch onderzoeksbureau.

44 https://www.informatiebeveiligingsdienst.nl/product/toegangsbeleid/
45 https://www.informatiebeveiligingsdienst.nl/product/baseline-informatiebeveiliging-overheid-bio/

7.11 Principe van Least Privilege

De aangeboden oplossing biedt de mogelijkheid tot het inrichten van een toegangsstructuur volgens het principe van Least Privilege[46].

Daarbij dient rekening gehouden te worden met het feit dat hier uitdrukkelijk gesproken wordt over een tweetal kanten daar waar het Least Privilege behelst.

De rechtenstructuur m.b.t. ingelogde entiteiten en hun toegang tot gegevens die zich op eenzelfde toegangsniveau bevinden.

Hiermee wordt bedoeld dat personen, systemen of andere entiteiten die zich authenticeren op de aangeboden oplossing alleen toegang hebben tot die data die strikt noodzakelijk is voor de vooraf gedefinieerde werking of het vooraf gedefinieerde werk van deze entiteit en dan specifiek op gegevens die zich op hetzelfde rechten niveau bevinden. De zogenaamde laterale/zijwaartse privilege escalatie.

Voorbeeld:

Gebruiker A en gebruiker B zijn beide medewerker van eenzelfde afdeling en maken dus gebruik van eenzelfde dataset. Uit deze dataset is dossier 1 specifiek toegewezen aan gebruiker A en dossier 2 specifiek toegewezen aan gebruiker B. Het is niet mogelijk voor gebruiker A om dossier 2 in te zien, zonder dat dit vooraf door het rechtensysteem is goedgekeurd. (Zie ook 6.11 Dienstgebonden Auditlogging)

De toegang tot het systeem resources van ingelogde entiteiten en hun mogelijkheden tot toegang op een ander toegangsniveau.

Hiermee wordt bedoeld dat personen, systemen of andere entiteiten die zicht authenticeren op de aangeboden oplossing zich niet zonder meer kunnen toevoegen als- of kunnen opereren onder een andere/hogere entiteit. De zogenaamde verticale privilege escalatie.

Voorbeeld:

Gebruiker A en beheerder B zijn beide in de oplossing gedefinieerd. Daarbij heeft beheerder B aanzienlijk meer rechten op diverse gegevens en gegevensbronnen dan gebruiker A. Het is voor gebruiker A niet mogelijk zich voor te doen als beheerder B zonder dat daarvoor in het rechtensysteem expliciet mogelijkheden worden aangegeven. Het kan zijn dat gebruiker A en beheerder B eenzelfde persoon is, maar hierbij geldt dan dat dagelijkse werkzaamheden onder het gebruiker A account uitgevoerd worden en beheerzaken alleen onder het beheerder B account. Het is niet mogelijk om als gebruiker A beheertaken uit te voeren. (Zie ook 6.11 Dienstgebonden Auditlogging)

46 https://en.wikipedia.org/wiki/Principle_of_least_privilege

8 Uitsluitingen en uitzonderingen

8.1 Geopolitieke uitzonderingen

Restricties herkomst software

Software afkomstig uit gebieden of staten die een offensief cyberprogramma hanteren, wordt door de gemeente met de grootst mogelijke voorzichtigheid gewogen en aangeschaft. Onder software wordt verstaan, alle programmacode die aansturing van hardware bewerkstelligd.

O.a. maar niet uitputtend: Operating Systems, Applicaties (apps), Firmware, Drivers, IoT logica, BIOS.

Software dient aantoonbaar niet uit staten met een offensief cyberprogramma betrokken te worden of door deze staten ontwikkeld te zijn, wanneer deze staten een dreiging vormen voor de Nederlandse Staat of de Nederlandse Staat onwelwillend zijn[47]. Hieronder vallen onder andere de landen genoemd in de publicatie van de AIVD "Offensief cyberprogramma - Een ideaal businessmodel voor staten[48]". Deze lijst is echter niet volledig en de gemeente behoudt zich het recht voor deze lijst bij start van de aanbestedingsprocedure, zonder opgaaf van reden, aan te vullen of aan te passen in de bijgevoegde spreadsheet.

Software betrokken uit landen die de Nederlandse Staat welgezind zijn (EU, NAVO-bondgenoten), en die een offensief cyberprogramma hanteren, dient aantoonbaar en verifieerbaar geïsoleerd te kunnen worden, als de software toegang biedt tot gegevens met een I[49] van 3 of wanneer de software of hardware toegang biedt tot gegevens met een V[49] van 3.

Restricties herkomst hardware

Hardware uit staten met een offensief cyberprogramma welke een dreiging vormen voor de Nederlandse Staat of de Nederlandse Staat onwelwillend zijn, is niet toegestaan. Vanuit praktische overwegingen is hardware vanuit China wel toegestaan. (Onder hardware wordt verstaan: alle fysieke componenten of onderdelen die in een computer een rol spelen)

Wel dient extra aandacht geschonken te worden aan embedded software op deze platformen. De gemeente behoudt zich nadrukkelijk het recht voor om bij aanschaf van hardware specifiek informatie hierover bij de leverancier in te winnen en aan de hand van deze informatie alsnog te besluiten van de aanschaf van de hardware af te zien indien embedded software niet aan de eisen voldoet.

47 https://www.aivd.nl/documenten/publicaties/2022/11/28/dreigingsbeeld-statelijke-actoren-dbsa-2
48 https://www.aivd.nl/actueel/nieuws/2019/06/27/offensief-cyberprogramma-een-ideaal-businessmodel-voor-staten
49 De I en de V verwijzen naar de BIV (CIA) classificatie. Deze worden door de gemeente bepaald en van tevoren aangereikt in de in de leeswijzer genoemde spreadsheet.

8.2 W3C compatibiliteit

Vereist is dat de aangeboden dienst W3C[50] Compliant is en dus correct werkt met de laatste versies van de meest gebruikte internetbrowsers. De dienst werkt in ieder geval op de standaard browser van de gemeente (Firefox Quantum 68.4.1esr (64-bits)) of hoger, alsmede op de meest gebruikte mobiele platformen, zoals iOS en Android.

Diensten die het gebruik van Internet Explorer of Edge afdwingen, worden per definitie niet goedgekeurd, hier wordt geen uitzondering op gemaakt.

Diensten die alleen onder enkele versie/soort van een browser en/of rendering engine[51] werken, worden per definitie niet goedgekeurd, hier wordt geen uitzondering voor gemaakt.

50 https://www.w3.org/standards/
51 https://en.wikipedia.org/wiki/Browser_engine

8.3 Uitsluiting gebruik van het RDP protocol

Voor diensten die niet ontwikkeld zijn voor webbrowsers maar via RDP geldt een zeer strikte restrictie. Het RDP protocol is in het verleden dusdanig geplaagd geweest met beveiligingsproblematieken, dat het gebruik er van een, voor de gemeente, onacceptabel risico vormt.

Diensten die gebruik van het RDP protocol afdwingen buiten de directe infrastructuur[52] van de gemeente om, worden per definitie niet goedgekeurd, hier worden geen uitzondering op gemaakt.

8.4 Opgave client side applicaties

Wanneer de dienst gebruik maakt van client side applicaties[53], anders dan die al geïnstalleerd zijn op de omgevingen van de gemeente, dienen hier vooraf zeer duidelijke afspraken over gemaakt te worden. Het gebruik van dergelijke applicaties maakt het netwerk van de gemeente kwetsbaarder, de businesscase ingewikkelder en het beheer omslachtiger. De voorkeur gaat uit naar diensten die volledig gebruik maken van de browser (8.2).

Wanneer blijkt dat vooraf niet goed is aangegeven dat de dienst client side applicaties nodig heeft om gebruikt te kunnen worden, behoudt de gemeente zich het recht voor om per direct, met enkel dit als opgaaf van reden, het traject te beëindigen. Mogelijke daaruit voortvloeiende kosten die de gemeente gemaakt heeft zullen op de opdrachtnemer verhaald worden.

Mobiele apps vormen hierop geen uitzondering en worden als client side applicatie geschouwd, ook dit dient vooraf aangegeven te worden. Ook noodzakelijke beheertooling die niet in de browser gebruikt wordt, valt hieronder.

8.5 Uitsluiting client side plugins

De gemeente wil in haar eigen infrastructuur geen (mogelijk kwetsbare) plugins. Daarom wordt geëist dat er geen plugins zijn om van de dienst gebruik te maken en dat de betreffende dienst werkt op alle standaard besturingssystemen zonder aanpassingen of installatie van additionele software.

Enkele voorbeelden van niet toegestane plugin’s zijn: Flash, Java, ActiveX en Silverlight.

8.6 DRM / EME afhankelijkheid

De gemeente is in de kern een open organisatie voor haar inwoners en ingezeten bedrijven. Zodoende is communicatie door middel van open standaarden een grote pré en vaak zelfs verplicht.

Als gekozen moet worden tussen applicaties die EME[54] en/of DRM[55] afdwingen en applicaties die dat niet doen, hebben applicaties zonder deze EME/DRM een absolute voorkeur. Mocht EME/DRM noodzakelijk zijn voor alle aangeboden applicaties, dan kan een uitzondering alleen tot stand komen in overleg met de medewerkers van Informatie Beveiliging en Security.

> https://www.forumstandaardisatie.nl/
> “Op eenduidige manieren samenwerken om informatie zo beter te kunnen beveiligen en makkelijker uit te wisselen en toegankelijker te maken voor iedereen. Dat is hoe open standaarden de samenwerking bevorderen tussen de overheid, burger en het bedrijfsleven.”

52 https://en.wikipedia.org/wiki/Local_area_network
53 https://en.wikipedia.org/wiki/Client-side
54 https://www.w3.org/TR/encrypted-media/
55 https://en.wikipedia.org/wiki/Digital_rights_management