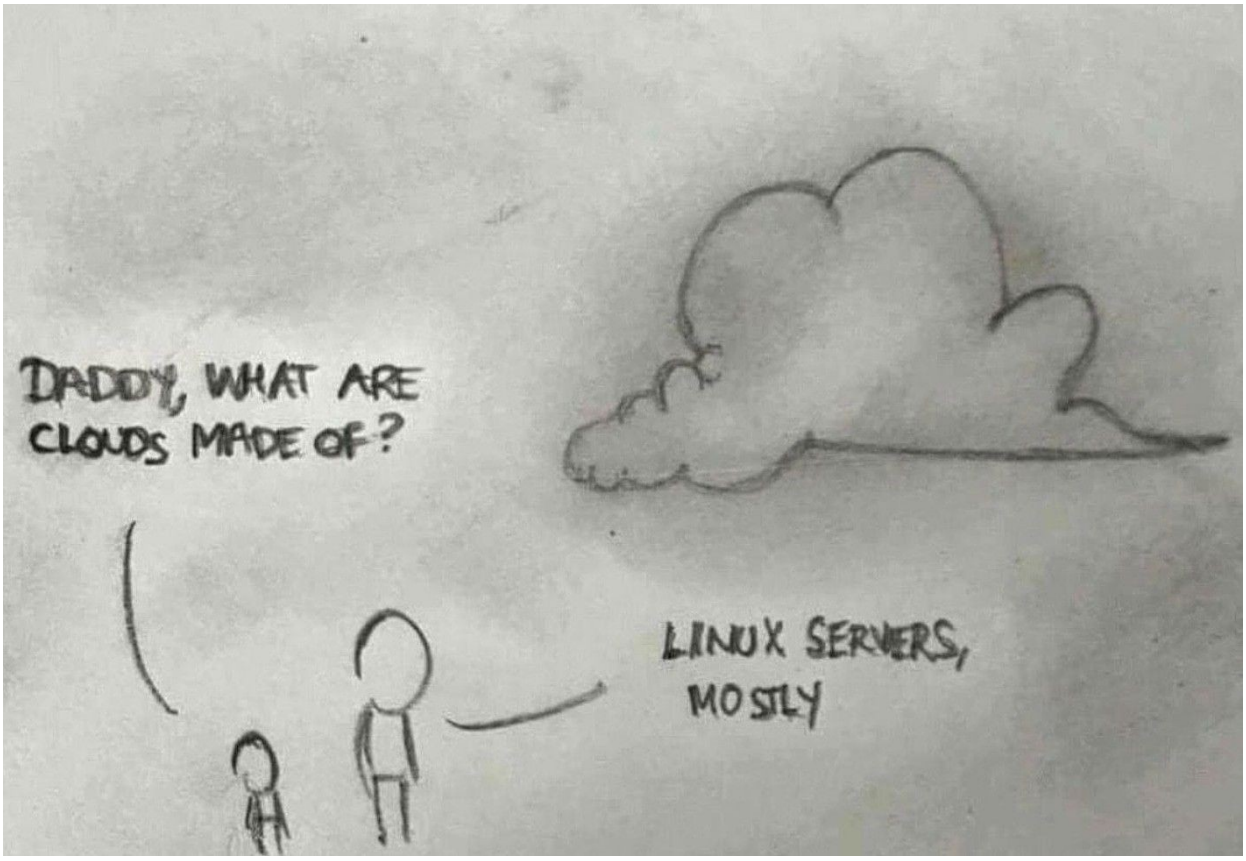
Gemeente Ede

Aansluitvoorwaarden Cloudgebaseerde diensten



Versie 2.4

Auteurs: Jeroen Visser
Tristan Jordens
Review: Peter Weersink
Martijn van Ginkel

1 Revisies:

–	–	–	Voorgaande revisie-informatie verwijderd….
11-04-2018	JV	1.4	4.3 aangepast, bewaren van pcaps verwijdert
04-70-2019	TJ	1.5	aangepast aan nieuwe eisen, technische controle
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 spellingfouten verwijderd
12-10-2020	JV	2.4	Zinsconstructies 6.10 aangepast Spelfouten...

2 Inleiding

De gemeente gebruikt een groot aantal websites en webapplicaties om te communiceren met haar inwoners, daarnaast gebruikt het zelf diverse Software as a Service-diensten (SaaS) ter ondersteuning van bedrijfsprocessen. Op dit moment zijn deze websites bij een groot aantal verschillende leveranciers ondergebracht en zijn er onvoldoende afspraken gemaakt om een veilige werking te garanderen.

De gemeente dient te voldoen aan de BIO[1] normen en heeft daarnaast te maken met de Meldplicht Datalekken[2] vanuit de AVG[3]. Beide eisen dat de gemeente 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 best 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 datalekken 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 richtlijnen 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.

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

Inhoudsopgave

3 Leeswijzer

We gaan in op de beveiligingsrichtlijnen die voor alle (web-based) 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). 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 invul sheet.

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 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[4] 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 https://forumstandaardisatie.nl/

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 veilheidsissues 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[5]. (Denk hierbij aan inwonersinformatie etc.).
2. Uitwisseling van deze gegevens via de ESB, wordt middels de daartoe verplichte standaarden[6] 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[7] 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[8] 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 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[9] + 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.

5 https://en.wikipedia.org/wiki/Enterprise_service_bus
6 https://forumstandaardisatie.nl/open-standaarden/verplicht
7 https://forumstandaardisatie.nl/open-standaarden/aanbevolen
8 https://en.wikipedia.org/wiki/Stateful_firewall
9 https://www.avgdashboard.nl/wettelijke-bewaartermijnen/

5.3 Gebruik van e-Mail

Deze richtlijnen gelden zowel voor het versturen vanaf het domein van de gemeente als vanaf een ander domein.
Conform de opgelegde richtlijnen dient de gemeente 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 vanaf 2020 TLSA DANE[10].
Standaard worden deze zo ingesteld dat het onmogelijk is om e-mail namens het betreffende domein te versturen. Als het wel noodzakelijk is dat er e-mail verstuurd gaat worden namens deze domeinen dient de leverancier de standaarden DMARC, SPF en DKIM in overleg met de gemeente te implementeren.
De gemeente stelt onderstaande in voor geparkeerde / niet e-mail-verzendende domeinen:

- DNS SPF Record = "v=spf1 -all"
- DNS DMARC Record = "v=DMARC1; p=reject”

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:
    - Dane
    - StartTLS
    - DKIM
    - SPF DKIM
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.

5.4 Aansluiting op ADFS

Als de betreffende SaaS applicatie intern door de gemeente gebruikt wordt, moet gekoppeld worden aan de ADFS[11] omgeving van de gemeente. Als er middels ADFS 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 ADFS omgeving loggen bij beheer handelingen van de leverancier.

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

10 https://www.forumstandaardisatie.nl/open-standaarden/verplicht
11 https://en.wikipedia.org/wiki/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 Toegankelijkheid

Als de dienst alleen bedoeld is voor intern gebruik bij de gemeente, dan wordt toegang tot de applicatie beperkt tot de door de gemeente gebruikte publieke ip adressen.

Let op: Dit is altijd het geval als er sprake is van een niet productie omgeving (bv test, acceptatie of ontwikkel omgeving).

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[12] richtlijnen.

- Wanneer er geen gebruik gemaakt kan worden van 2FA, moet wachtwoord een minimale lengte van 8 posities hebben, niet gelijk zijn aan de default waarde van een leverancier EN moet het wachtwoord 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[13] worden aangeraden.
- Wachtwoorden moeten tenminste elk jaar gewijzigd worden als gebruik gemaakt wordt van MFA/2FA[14]. Elke 90 dagen als er geen gebruik gemaakt wordt van MFS/2FA.
- Bij toegang tot privacygevoelige data of bij beheer handelingen kan alleen ingelogd worden met 2-factor-authenticatie zoals TOTP[15], HOTP[16] of U2F[17]. 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 straching algoritmes. Zoals daar zijn: CRPING voor salting en ARGON2, BCRYPT, SCRYPT of PBKDF2 voor stretching[18].
- 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.

12 https://pages.nist.gov/800-63-3/sp800-63b.html
13 https://en.wikipedia.org/wiki/Passphrase
14 https://en.wikipedia.org/wiki/Multi-factor_authentication
15 https://en.wikipedia.org/wiki/Time-based_One-time_Password_algorithm
16 https://en.wikipedia.org/wiki/HMAC-based_One-time_Password_algorithm
17 https://en.wikipedia.org/wiki/Universal_2nd_Factor
18 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 niet toegestaan. Redirects van http naar https zijn wel toegestaan, mits bij deze redirect geen gegevens worden verzonden.

Verkeer naar alle websites van de gemeente en naar alle afgenomen SaaS-diensten dient beveiligd te zijn middels TLS (ook al betreft het een statische website). Voor de eisen van de TLS verbinding kijken we onder andere naar de ICT-beveiligingsrichtlijnen voor TLS van NCSC[19] en de Security/Server Side TLS wiki van Mozilla[20]. 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.

Configuration	Firefox	Android	Chrome	Edge	Internet Explorer	Java	OpenSSL	Opera	Safari
Modern	63	10.0	70	75	--	11	1.1.1	57	12.1
Intermediate	27	4.4.2	31	12	11 (Win7)	8u31	1.0.1	20	9
Old	1	2.3	1	12	8 (WinXP)	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 organisation validated certificaat. In alle andere gevallen kan met domeinvalidatie gebruikt worden.
- Wildcard-certificaten worden niet toegestaan.
- TLS 1.2 en bij voorkeur 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. 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[21] 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[22] mag gebruikt worden.
- HSTS[23] wordt geïmplementeerd op de betreffende website of SaaS-dienst.
- 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=www.<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.

19 https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls
20 https://wiki.mozilla.org/Security/Server_Side_TLS
21 https://en.wikipedia.org/wiki/Forward_secrecy
22 https://en.wikipedia.org/wiki/Server_Name_Indication
23 https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security

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[24] 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[25] gevolgd, hoofdstuk: Beveiliging van persoonsgegevens[26]

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.

24 https://en.wikipedia.org/wiki/Denial-of-service_attack
25 https://www.autoriteitpersoonsgegevens.nl/nl/zelf-doen/thematische-beleidsregels
26 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

Aanvallers blijken regelmatig binnen te komen via beheeringangen van de betreffende systemen (bijvoorbeeld SSH-poorten of beheer-webinterface). De gemeente vereist dat uitsluitend de poorten benodigd voor een correcte werking van de dienst benaderbaar zijn vanaf het internet.

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

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 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.

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)[27].

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).

27 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 EER 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 EER blijft.
- Gebruik maken van beheerdiensten van partijen gevestigd buiten de EER.
- Gebruik maken van ontwikkeldiensten van partijen gevestigd buiten de EER.
- 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 EER.

7.5 Privacywetgeving

Opdrachtnemer is zich bewust van de ongeldigverklaring van het Privacy Shield[28] 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[29]

Een separate verwerkersovereenkomst, zoals deze is opgesteld door de VNG[30], maakt te allen tijde onderdeel uit van de overeenkomst indien persoonsgegevens worden verwerkt.

28 https://autoriteitpersoonsgegevens.nl/nl/nieuws/privacy-shield-voor-doorgifte-naar-vs-ongeldig-verklaard
29 Dit staat ook in de GIBIT, echter zonder de VNG vereiste.
30 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[31] en Hoofdstuk 11 van de BIO[32].

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.

31 https://www.informatiebeveiligingsdienst.nl/product/toegangsbeleid/
32 https://www.informatiebeveiligingsdienst.nl/product/baseline-informatiebeveiliging-overheid-bio/

8 Certificering, standaarden en beleid

De gemeente hecht veel waarde aan het op orde zijn van de beveiliging van opdrachtnemers. Een manier om hieraan handen en voeten te geven is het in bezit hebben van certificaten. Het aantonen van het in bezit zijn van een certificaat kan, afhankelijk van het type certificaat, een pluspunt zijn.

8.1 ISO27001

ISO 27001[33] is mogelijk het bekendste veiligheidscertificaat dat verkregen kan worden.

Wanneer een opdrachtnemer aangeeft dat de ISO27001 certificering is behaald, zegt dit alleen iets over het feit dat de opdrachtnemer risico's in kaart heeft gebracht en daar een beslissing over genomen heeft. Het zegt niets over het feit om een risico geaccepteerd is of niet en als dit niet geaccepteerd is, welke maatregelen er genomen zijn.

Dit laat de opdrachtnemer een grote bandbreedte ter beschikking met betrekking tot invulling geven aan dit certificaat. De beslissing om een risico te accepteren of niet en de kwaliteit van de evenuteel genomen maatregel, bepaalt echter de mate en de kwaliteit van beveiligingen, het certificaat zelf zegt niets. (Een autocoureur heeft ongetwijfeld een rijbewijs, dit zegt echter niets over zijn rijkunsten).

De gemeente stelt dat als opdrachtnemer in het bezit is van een ISO 27001 certificaat, hij tevens de aandachtspunten die uit het certificeringsproces zijn voortgevloeid en de maatregelen die ter mitigatie zijn getroffen, ter beoordeling deelt met de gemeente.

8.2 ISAE 3402

ISAE 3402[34] is een standaard die klanten van opdrachtnemer verzekert dat deze opdrachtnemer controle over diverse bedrijfsprocessen heeft. Dit door middel van een terugkerende audit van deze bedrijfsprocessen (Financieel en IT gerelateerd). De certificering vertelt echter niet ***welke*** bedrijfsprocessen gecontroleerd worden. Voor de gemeente is dan een voorwaarde dat naast de certificering ook de bedrijfsprocessen die in kaart zijn gebracht onderdeel uitmaken van een beoordeling.

8.3 NEN 7510

NEN 7510[35] lijkt veel op de ISO 27001. Wanneer een opdrachtnemer aangeeft dat de NEN 7510 certificering is behaald, zegt dit alleen iets over het feit dat de opdrachtnemer risico's in kaart heeft gebracht en daar een beslissing over genomen heeft. Het zegt niets over het feit om een risico geaccepteerd is of niet en als dit niet geaccepteerd is, welke maatregelen er genomen zijn.

Dit laat de opdrachtnemer een grote bandbreedte ter beschikking met betrekking tot invulling geven aan dit certificaat. De beslissing om een risico te accepteren of niet en de kwaliteit van de evenuteel genomen maatregel, bepaald echter de mate en de kwaliteit van beveiligingen, het certificaat zelf zegt niets. (Een autocoureur heeft ongetwijfeld een rijbewijs, dit zegt echter niets over zijn rijkunsten).

De gemeente stelt dat als opdrachtnemer in het bezit is van een NEN 7510 certificaat, hij tevens de aandachtspunten die uit het certificeringsproces zijn voortgevloeid en de maatregelen die ter mitigatie zijn getroffen, ter beoordeling deelt met de gemeente.

33 https://en.wikipedia.org/wiki/ISO/IEC_27001
34 https://www.isae3402.nl/wat-is-isae3402
35 https://nl.wikipedia.org/wiki/NEN_7510

9 Uitsluitingen en uitzonderingen

9.1 W3C compatibiliteit

Vereist is dat de aangeboden dienst W3C[36] 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[37] werken, worden per definitie niet goedgekeurd, hier wordt geen uitzondering voor gemaakt.

9.2 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[38] van de gemeente om, worden per definitie niet goedgekeurd, hier worden geen uitzondering op gemaakt.

9.3 Opgave client side applicaties

Wanneer de dienst gebruik maakt van client side applicaties[39], 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 (9.1).

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.

9.4 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.

36 https://www.w3.org/standards/
37 https://en.wikipedia.org/wiki/Browser_engine
38 https://en.wikipedia.org/wiki/Local_area_network
39 https://en.wikipedia.org/wiki/Client-side

9.5 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[40] en/of DRM[41] 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."

40 https://www.w3.org/TR/encrypted-media/
41 https://en.wikipedia.org/wiki/Digital_rights_management