

Beveiligingsrichtlijnen (externe) websites en SaaS-diensten

Versie Extern: 1.4 dd 11-04-2018

Revisie:

12-10-2016 RD 1.0 Initiële versie

14-12-2016 RD 1.1 5.4 toegevoegd met een voorkeur voor ADFS

5.23 toegevoegd restrictie op IP adres

08-11-2017 RD 1.2 Kleine tekstuele wijzigingen.

19-01-2018 RD 1.3 Eisen rondom CSR toegevoegd

11-04-2018 RD 1.4 4.3 aangepast, bewaren van pcaps verwijderd

1. Inleiding

De Gemeente Ede gebruikt een groot aantal websites en -applicaties om te communiceren met haar burgers, 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 BIG richtlijnen en heeft daarnaast te maken met de Meldplicht Datalekken. Beide eisen dat de gemeente informatie afdoende en naar de laatste stand der techniek beveiligd, om ongeautoriseerde toegang tot informatie te voorkomen. Daarnaast hebben recente security-incidenten tot nieuwe inzichten geleid.

De landelijke media nemen gemeenten regelmatig op de korrel 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 heeft zowel voor de gemeente als voor de leverancier grote negatieve gevolgen, er moet alles in het werk gesteld worden om een digitale inbraak te voorkomen. Mocht er ondanks alle maatregelen toch een inbraak plaats vinden dan dienen beide partijen hier op voorbereid te zijn, zodat zo snel mogelijk achterhaald kan worden wat er exact gebeurd is.

Op basis van voornoemde wetgeving, de opgedane ervaringen en de ontwikkelingen in de markt zijn deze nieuwe richtlijnen opgesteld.

2. Domeinnamen

Dit hoofdstuk is alleen voor intern gebruik.

3. e-Mail

Conform de opgelegde richtlijnen dient de gemeente maatregelen te nemen om het versturen van “valse e-mails” zoals spam en phishing tegen te gaan. Zie: https://www.ibdgemeenten.nl/wp-content/uploads/2016/06/20160602_Factsheet_emailauthenticatie_v1.01.pdf

Dit kan middels DNS-instellingen. De verplichte standaarden hiervoor zijn: DNSSEC¹, SPF² / DKIM³ en DMARC⁴.

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

¹ DNSSEC voegt een digitale handtekening toe aan de DNS-informatie. Daardoor weet je zeker dat, als mensen naar jouw site zoeken, ze ook bij jouw site uitkomen. En dat niemand jouw e-mails leest.

² Sender Policy Framework (SPF) is een protocol dat tot doel heeft te helpen spam te verminderen door vast te stellen of de verzender van een e-mailbericht gerechtigd is om een bericht te verzenden namens de afzender van het bericht.

³ DomainKeys Identified Mail (DKIM) is een techniek waarbij een organisatie verantwoordelijkheid kan nemen voor een bericht dat per e-mail wordt verzonden. DKIM zelf is geen technologie tegen spam, maar biedt een basis voor authenticatie, waarmee bijvoorbeeld reputatieservices opgezet kunnen worden. Deze reputatieservices op hun beurt kunnen dan gebruikt worden door anti-spamfilters.

⁴ Met een DMARC-record, kan in de DNS een beleidsregel gemaakt worden. Bijvoorbeeld (in versimpelde vorm): “als de DKIM-handtekening niet klopt, of als SPF faalt, stop deze mail dan in de spamfolder”.

Beveiligingsrichtlijnen (externe) websites en SaaS-diensten

Versie Extern: 1.4 dd 11-04-2018

leverancier de standaarden SPF en DKIM in overleg met de gemeente te implementeren. Als het een belangrijk communicatiekanaal van de gemeente wordt, is ook DMARC verplicht.

BIAS 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 bij middels TLS-encryptie verstuurd, het benodigde certificaat wordt door de gemeente verstrekt.
- 3 De inkomende e-mailserver ondersteund TLS-encryptie.
- 4 De volgende internetstandaarden worden minimaal ondersteund door die e-mailserver:
https://www.forumstandaardisatie.nl/lijst-open-standaarden/in_lijst/verplicht-pas-toe-leg-uit (oa Dane / StartTLS / DKIM / SPF / DKIM)
- 5 Er zijn afdoende anti-spammaatregelen genomen, minder al 1% van de berichten kan als ongewenst worden geclassificeerd.
- 6 Er wordt een actief updatebeleid toegepast op de e-mailserver. Zie punt 4.8 voor meer details.
- 7 Alle relevante aan beveiliging gerelateerde logs en e-maillogs worden 6 maanden bewaard op een separate en adequaat beveiligde machine. Zie punt 4.1 voor meer details over de loggingvereisten.
- 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 4.9 voor meer details rondom beheer.

4. Websites

De Gemeente Ede beschikt over een groot aantal websites, waarbij vele slechts statisch zijn en dienst doen als een informatievoorziening aan burgers en andere sites gebruikt worden voor het aanbieden van digitale diensten aan burgers. In alle gevallen moet voorkomen worden dat ongeautoriseerde personen toegang krijgen tot informatie op deze systemen of controle krijgen over deze sites en systemen. Uiteraard heeft de beveiliging van persoonsgegevens de hoogste prioriteit. Echter ook defacement⁵, het verspreiden van malware en/of het aanvallen van andere systemen vanaf gemeentelijke websites dient te allen tijden voorkomen te worden.

Bij het hosten van een website voor de Gemeente Ede dient aan de volgende richtlijnen voldaan te worden:

1 Logging

Alle logs van alle gebruikte devices (webserver, 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 een periode van 2 jaar 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 ongemaskerd in de logs mogen staan. De gemeente verwacht van de opdrachtnemer dat deze zelf op regelmatige basis (minimaal wekelijks) de logs controleert op mogelijk verdachte zaken. Als er verdachte situaties vastgesteld worden, dan dienen deze zo snel mogelijk gemeld te worden bij het Serviceplein van de Gemeente Ede (zie Bewerkingsovereenkomst voor de details).

⁵ Het ongewild van buitenaf aanpassen of vervangen van webpagina's door hackers.

Beveiligingsrichtlijnen (externe) websites en SaaS-diensten

Versie Extern: 1.4 dd 11-04-2018

2 Monitoring van aangeboden diensten

De Gemeente Ede verwacht van de opdrachtnemer dat deze zelf over een monitoringsysteem beschikt om de beschikbaarheid en performance van de aangeboden diensten te monitoren. Zodat de beheersorganisatie direct gealarmeerd wordt bij uitval, performanceproblemen, (D)DOS-aanvallen, onverklaarbare toename in verkeer naar internet, verlopen van beveiligingscertificaten, ongeautoriseerde wijzigingen aan configuratiebestanden, ongeautoriseerde wijzigingen aan systeembestanden, enzovoorts. De gemeente verwacht van de opdrachtnemer dat er statistieken zijn van internetverkeer en systeempowerformance, welke minstens 2 jaar bewaard worden.

3 Network Security Monitoring

Om mogelijke aanvallen te detecteren beschikt de opdrachtnemer over tooling om verdachte zaken in het netwerkverkeer te detecteren. Dit kan middels een IDS of IPS. Deze dient ingesteld te worden voor de bescherming van de specifieke situatie. De logs van deze tooling worden uiteraard conform de beschrijving van punt 4.1 opgeslagen en bewaard.

4 Wachtwoordeisen

Wachtwoorden zijn tot op heden de meest gebruikte manier van authenticatie. De praktijk heeft uitgewezen dat dit vaak een zwakke schakel is. Daarom stelt de gemeente de volgende eisen aan de gebruikte wachtwoorden:

- Een wachtwoord heeft een minimale lengte van 8 karakters, moeten 'sterk' zijn en niet gelijk zijn aan de defaultwaarde die een leverancier er vaak aan geeft. Wachtwoorden tot 30 karakters moeten ondersteund worden.
- Wachtwoorden moeten tenminste elke 90 dagen gewijzigd worden.
- Bij toegang tot privacygevoelige data of bij beheershandelingen kan alleen ingelogd worden met 2-factor-authenticatie.
- Er is een password reset-optie beschikbaar.
- Wachtwoorden worden altijd versleuteld opgeslagen, waarbij gebruikt gemaakt wordt van one-way hashing⁶ en salting⁷.
- Gebruikersnamen en wachtwoorden worden nimmer door de browser gecachet.
- Wachtwoorden die door de opdrachtnemer worden gebruikt op systemen van de gemeente zijn uniek en worden niet bij andere klanten van de opdrachtnemer gebruikt.

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 gevolgd

https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf) Mochten kwaadwillende personen toegang krijgen tot deze gegevens dan moet deze onbruikbaar zijn.

6 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 OWASP. Details vindt u hier: https://www.owasp.org/index.php/Top_10_2013-Top_10.

7 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.

Voor een "statische" website kan een week back-up en bewaartermijn van 3 maanden voldoende zijn.

⁶ Versleutelen.

⁷ Salting ('zouten') bestaat uit willekeurige bits die worden toegevoegd aan een wachtwoord. Het resultaat van de versleuteling van deze combinatie wordt opgeslagen.

Beveiligingsrichtlijnen (externe) websites en SaaS-diensten

Versie Extern: 1.4 dd 11-04-2018

Voor sites waar transacties plaatsvinden (e-diensten) worden tenminste dagelijkse back-ups gemaakt en worden die dagelijkse back-ups tenminste 2 weken bewaard.

De wekelijkse (full) back-up wordt tenminste 3 maanden bewaard. De maandelijkse (full) back-up wordt tenminste 12 maanden bewaard.

Alle back-ups dienen versleuteld en adequaat beveiligd bewaard te worden.

Een back-up is compleet waardeloos als niet gecontroleerd wordt of systemen hersteld kunnen worden met de back-up(s). 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.

8 Patchbeleid

Installatie van beveiligingsupdates is een van de belangrijkste beveiligingsmaatregelen. Systemen die direct benaderbaar zijn via internet worden aan de lopende band door criminelen gescand op kwetsbaarheden. De gemeente verwacht dan ook van de opdrachtnemer dat beveiligingsupdates tijdig worden geïnstalleerd. De gemeente vereist dan ook de volgende implementatietijden:

- Adviezen van softwareleveranciers worden gevolgd.
- Kritische beveiligingsupdates van technologie die direct vanaf internet te misbruiken is worden binnen 24 klokuren na uitgifte geïnstalleerd.
- Alle software op alle gebruikte systemen dient geüpdate te worden! Dus niet alleen software die vanaf het internet benaderbaar is.
- Niet kritische beveiligingsupdates worden binnen een week na uitgifte geïnstalleerd.
- De opdrachtnemer houdt een logboek bij wanneer bepaalde updates geïnstalleerd zijn, zodat achteraf altijd getoetst kan worden, wanneer een bepaalde update geïnstalleerd is.

9 Remote beheer van systemen

Aanvallers blijken regelmatig binnen te komen via beheeringsgangen 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 geopend zijn (in 99% van de gevallen is dat uitsluitend https://, ofwel TCP:443). Expliciet **niet** toegestaan zijn SSH, RDP, Webadmin, phpMyAdmin, enzovoorts.

De gemeente vereist van de opdrachtnemer dat beheertoegang alleen mogelijk is via een correct beveiligde VPN-verbinding (Ipsec) en dat er logging van die VPN-verbindingen aanwezig is.

Verder dienen alle beheerhandelingen herleid te kunnen worden naar de betreffende beheerder.

Handelingen van beheerders wordt gelogd zoals beschreven bij punt 4.1.

10 Systeemisolatie

Hackers komen binnen via een kwetsbaarheid op 1 machine en hoppen van de ene machine naar de andere. Om te voorkomen dat hackers via andere systemen van de opdrachtnemer toegang krijgen tot de systemen die voor de gemeente gebruikt worden, worden de volgende eisen gesteld:

- Systemen worden nimmer gedeeld met andere klanten (shared hosting is niet toegestaan).
- Systemen van de gemeente zijn logisch gescheiden van systemen ten behoeve van andere klanten (firewalling).
- Alle poorten die niet noodzakelijk zijn voor correcte werking van de dienst zijn middels een hostbased firewall gesloten.

11 Beveiligde verbinding SSL / TLS

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

Onversleuteld verkeer (http) is niet toegestaan. Redirects van http naar https zijn wel toegestaan, mits correct geïmplementeerd.

Zie ook hoofdstuk 6 voor de eisen die aan een beveiligde verbinding worden gesteld.

12 Gebruik client side plugins

De gemeente wil in haar eigen infrastructuur zo snel mogelijk afscheid nemen van kwetsbare browser plugins. Daarom wordt geëist dat er geen plugins of aanvullende software nodig is om van de dienst gebruik te maken en dat de betreffende dienst werkt op alle standaard besturingssystemen zonder

Beveiligingsrichtlijnen (externe) websites en SaaS-diensten

Versie Extern: 1.4 dd 11-04-2018

aanpassingen of installatie van additionele software. Enkele voorbeelden van niet toegestane plugin's zijn: Flash, Java, ActiveX en Silverlight.

Verder wordt verwacht dat de aangeboden dienst correct werkt met de laatste versies van de meest gebruikte internetbrowsers: Microsoft Internet Explorer / Edge, Mozilla Firefox, Google Chrome en Apple Safari, alsmede op de meest gebruikte mobiele platformen, zoals iOS en Android.

13 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, tenzij schriftelijk met de gemeente anders overeengekomen (bijvoorbeeld: Google Analytics wordt soms ingezet om statistieken te verzamelen).

Als zo'n tracker geplaatst mag worden, dan dient dit duidelijk in het privacy-statement op de betreffende website kenbaar gemaakt te worden.

14 Gebruik gestandaardiseerd CMS en Exit-strategie

De landelijke richtlijnen schrijven voor dat de gemeente zoveel mogelijk gebruik maakt van open standaarden. Ook wil de gemeente geen "vendor lock-in", bijvoorbeeld door het gebruik van een weinig gebruikt of zelf ontwikkeld CMS.

Websites 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 en kosten van een exit zijn (zijnde een migratieplan met een realistische begroting; het vermelden van een uurtarief is expliciet onvoldoende).

15 Locatie van apparatuur, data en onderaannemers

Conform de Nederlandse wetgeving dient alle overheidsdata binnen de EU opgeslagen te worden.

De gemeente geeft er expliciet de voorkeur aan om alle apparatuur en data op Nederlands grondgebied onder te brengen. En omdat de UK voornemens is de EU te verlaten worden er geen nieuwe overeenkomsten aangegaan waarbij data opgeslagen kan worden in de UK.

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.

Daarnaast dient de opdrachtnemer ervoor te waken dat alle data van de gemeente te allen tijden aan de gestelde eisen blijft voldoen. Enkele voorbeelden van risicovolle situaties die niet zijn toegestaan:

- Gebruik maken van een back-up dienst (al dan niet van derden) waarbij niet 100% zeker is dat de data binnen de EU blijft.
- Gebruik maken van beheer- en ontwikkeldiensten van partijen gevestigd buiten de EU.
- 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.

16 D(D)oS maatregelen

Afpersing middels DoS- of DDoS-aanvallen is steeds succesvoller. De gemeente vereist van de opdrachtnemer dat deze afdoende maatregelen heeft genomen om (D)DoS-aanvallen 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.

17 Incident Response en medewerking aan 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

Beveiligingsrichtlijnen (externe) websites en SaaS-diensten

Versie Extern: 1.4 dd 11-04-2018

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.

18 Responsible Disclosure

De Gemeente Ede heeft een Responsible Disclosure-beleid, wat geldt voor alle gemeentelijke websites. Op iedere website van de gemeente dient duidelijk kenbaar gemaakt te worden (middels een link / verwijzing naar de Responsible Disclosure-procedure op www.ede.nl) dat deze van toepassing is. De opdrachtnemer dient hier dan ook rekening mee te houden en actief mee te werken aan dit beleid. Zodat als er een kwetsbaarheid gemeld wordt, de opdrachtnemer per direct samen met de gemeente een analyse gaat maken van de kwetsbaarheid en alles in het werk zal stellen om de gevonden kwetsbaarheid zo snel mogelijk te verhelpen.

19 Bewerkingsovereenkomst

Een separate Bewerkingsovereenkomst maakt te allen tijden onderdeel uit van de overeenkomst.

20 Maandelijks kwetsbaarhedenonderzoek

Websites zijn meestal niet statisch en veranderen regelmatig, daarnaast worden er dagelijks nieuwe kwetsbaarheden gepubliceerd. Daarom wil de gemeente op maandelijkse basis al haar websites onderzoeken met een kwetsbaarheden-scanner. Dit om nieuwe mogelijke kwetsbaarheden tijdig te signaleren. Van de opdrachtnemer wordt verwacht dat deze volledige medewerking verleent en gevonden kwetsbaarheden zo snel mogelijk oplost.

21 Jaarlijkse Penetration Test (Pen Test)

Eens per jaar zal namens de Gemeente Ede door een gerenommeerd securitybedrijf een penetratietest worden uitgevoerd, die hierover direct aan de gemeente zal rapporteren. De gemeente vereist dat de leverancier hier onvoorwaardelijk aan meewerkt en eventueel gevonden kwetsbaarheden zo snel mogelijk verhelpt.

22 Audits - The Right to Audit

Om te verifiëren of de opdrachtnemer voldoet aan de gestelde eisen, gaat 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.

Mocht dit niet tot tevredenheid van de gemeente verlopen, ook niet na tussenkomst van Contract- en Leveranciersmanagement en Inkoop, dan zullen juridische stappen ondernomen worden. En wordt mogelijk ook de overeenkomst beëindigd.

5. SaaS-diensten (Software as a Service)

Daar een SaaS-dienst meestal ook als een website wordt aangeboden zijn alle vereisten uit hoofdstuk 4 van toepassing. Alleen op de hierna genoemde punten gelden afwijkende eisen.

4 Wachtwoorden.

Als de betreffende SaaS applicatie alleen intern door de gemeente gebruikt wordt, wordt bij voorkeur gekoppeld middels ADFS⁸. Als er middels ADFS gekoppeld kan worden zijn de onder 4.4 gestelde eisen niet van toepassing, met uitzondering van de eisen rondom 2 factor authenticatie bij beheer handelingen.

⁸ Active Directory Federation Services: https://en.wikipedia.org/wiki/Active_Directory_Federation_Services

Beveiligingsrichtlijnen (externe) websites en SaaS-diensten

Versie Extern: 1.4 dd 11-04-2018

10 Systeemisolatie

Is niet van toepassing.

14 Gebruik gestandaardiseerd CMS en Exit-strategie

De eisen rondom het gestandaardiseerde CMS en maatwerk zijn niet van toepassing. Echter, de eisen rondom de Exit-strategie zijn wel van toepassing. De gemeente wil vóór opdrachtverstrekking duidelijk hebben hoe (en in welk formaat) bij een exit de data aangeleverd wordt en wat de kosten van een exit zijn.

17 Incident Response en medewerking aan forensisch onderzoek

De gemeente kan zich voorstellen dat een SaaS-leverancier niet al haar data en systemen wil overhandigen aan een derde partij, daar er ook data van andere klanten bij zit. Daarom verwacht de gemeente dat de SaaS-leverancier bij het vermoeden van een digitale inbraak, zelf forensisch onderzoek laat uitvoeren door een gerenommeerd Nederlands onderzoeksbureau en de resultaten daarvan met de gemeente deelt. Bij het eerste vermoeden van een digitale inbraak of een datalek wordt de Gemeente Ede zo snel mogelijk op de hoogte gebracht van deze situatie zodat zij zelf een impactbepaling kan doen en maatregelen kan nemen.

Voor meer details wordt verwezen naar de Bewerkingsovereenkomst.

18 Responsible Disclosure

De gemeente verwacht van de opdrachtnemer dat zij zelf een Responsible Disclosure-procedure heeft ingericht.

21 Jaarlijkse Penetration Test (Pen Test)

De gemeente vereist dat de opdrachtnemer op jaarlijkse basis voor eigen rekening een penetratietest laat uitvoeren - en uiteraard daarin geconstateerde kwetsbaarheden verhelpt - om naar haar klanten te kunnen aantonen dat de gebruikte omgeving veilig is.

De gemeente vereist inzage in de samenvatting van het onderzoek.

Als de gemeente om wat voor reden dan ook twijfels heeft over de beveiliging van de aangeboden dienst behouden we ons het recht voor om alsnog een separate penetratietest te laten uitvoeren. Van de opdrachtnemer wordt dan volledige medewerking aan dit onderzoek verwacht.

23 Toegankelijkheid

Als de SaaS toepassing alleen bedoeld is voor intern gebruik bij de gemeente, dan wordt toegang tot de SaaS applicatie beperkt tot de door de gemeente gebruikte publieke ip adressen. Dit is altijd het geval als er sprake is van een niet productie omgeving (bv test, acceptatie of ontwikkel omgeving).

6. TLS/SSL-beveiliging - Certificaten

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). De TLS-encryptie en de gebruikte certificaten dienen aan de volgende vereisten te voldoen:

- 1 Certificaten voor domeinen van de gemeente worden alleen door de gemeente zelf aangevraagd, om misbruik te voorkomen. Dit is niet van toepassing op SaaS diensten.
- 2 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.
- 3 Wildcard-certificaten worden niet toegestaan.
- 4 Bij voorkeur wordt een key-lengte van 4.096 bits gebruikt, tot eind 2017 is 2.048 bits nog mogelijk.
- 5 Alleen TLS 1.2 mag gebruikt worden. Alle oudere protocollen (SSLV3, TLS1.0, TLS1.1) zijn kwetsbaar en **niet** meer toegestaan.

Beveiligingsrichtlijnen (externe) websites en SaaS-diensten

Versie Extern: 1.4 dd 11-04-2018

- 6 (Perfect) Forward Secrecy⁹ dient gebruikt te worden.
- 7 Er dient gebruik gemaakt te worden van SHA 256 Hashing voor het versleutelen van gegevens.
- 8 SNI¹⁰ mag gebruikt worden, indien noodzakelijk.
- 9 HSTS¹¹ wordt geïmplementeerd op de betreffende website of SaaS-dienst.
- 10 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.

⁹ PFS zorgt ervoor dat in het geval een bepaalde sleutel uit een communicatiekanaal gecompromitteerd wordt, de voorgaande sleutels niet afgeleid kunnen worden. Hierdoor zijn de voorgaande berichten ook niet af te leiden.

¹⁰ Server Name Indication, waardoor één server meerdere certificates op hetzelfde IP-adres en TCP-portnummer kan hebben.

¹¹ HTTP Strict Transport Security. Een beveiligingsmechanisme websites te beschermen doordat de webserver vereist dat webbrowsers alleen beveiligde HTTPS-verbindingen kunnen gebruiken, en nooit het onveilige HTTP-protocol.