Beleid
Websites, webapplicaties en e-mailbeveiliging
(webbeleid)
2024-2026

Informatiebeveiliging & Privacy
SWO

Auteurs : Wilbert Hepping

Versie : 2.0
Status : Definitief
Datum : 10 november 2023

INHOUDSOPGAVE

1. Inleiding 4
2. Websites en webapplicaties 6
2.1 Algemene uitgangspunten 6
2.2 Accountbeheer 6
2.3 Privacy-AVG 7
2.4 Webhosting en webserver 7
2.5 Beveiliging en certificaten 8
2.6 Domeinnamen 9
3. Toegankelijkheid 10
4. E-mailbeveiliging / e-mailauthenticatie 12
4.1 E-mailbeveiliging / e-mailauthenticatie 12
4.1.1 Beschrijf mailfunctionaliteit van de applicatie 12
4.1.2 SPF (Sender Policy Framework) 12
4.1.3 DKIM (DomainKeys Identified Mail) 12
4.1.4 DMARC (Domain-based Message Authentication, Reporting and Conformance) 12
4.1.5 STARTTLS en DANE 13
4.1.6 Forwarden e-mail 13
5. DigiD aansluitingen 14
Bijlage 1: TLS/SSL certificaat 15

Documenthistorie

Versie	Datum	Auteur(s)	Status / omschrijving wijziging
0.1	14-03-2018	W.B. Hepping	Initiële versie voor review
0.2	13-04-2018	W.B. Hepping	Tekstuele wijzigingen
0.3	02-05-2018	W.B. Hepping	Aanpassingen conform AVG
0.4/9	09-05-2018	W.B. Hepping	Wijzigingen doorgevoerd i.v.m. streefbeeldafspraak door Forum Standaardisatie
1.1	11-07-2022	W.B. Hepping	Beleid geactualiseerd
1.2	25-11-2022	W.B. Hepping	DigiD toegevoegd t.b.v. ENSIA
2.0	10-11-2023	J. Lemstra	Definitieve versie

Classificatie

Classificatie	Niveau
X	**Openbaar**
	Intern
	Vertrouwelijk
	Geheim

1. Inleiding

"Governance is essentieel voor het beheren van webomgevingen. Het biedt een structuur die het mogelijk maakt om webomgevingen van een hoge kwaliteit op te leveren. Webgovernance bestaat uit drie onderdelen: een governance-raamwerk (strategie), beleid en standaarden."

De Strategie voor digitale dienstverlening levert het kader om de dagelijkse, maar ook de meer strategische beslissingen te kunnen nemen. Het wordt verder uitgewerkt in governance en geeft dan aan wie de leiding heeft over de webomgevingen, wie de uiteindelijke beslissingen neemt over budgetten, bemensing en de uit te voeren activiteiten.

Het is een geaccordeerde strategie, die samenhangt met de overige doelen en ambities van de organisatie en het bestuur. Een belangrijke pijler is de al eerder vastgestelde visie Dienstverlening 2021-2025. In deze visie is het organisatiedoel vastgelegd en waarom de organisatie dat belangrijk vindt.

Webbeleid is belangrijk omdat dit een reeks van organisatorische richtlijnen biedt die moeten worden opgevolgd bij het creëren van webomgevingen. Beleidsrichtlijnen vormen ook een brug tussen aan de ene kant de strategische doelstellingen van een organisatie en aan de andere kant het dagelijkse werk aan en de ontwikkeling van webomgevingen in die organisatie. Webrichtlijnen voorkomen dat organisaties in de problemen komen door zeker te stellen dat al hun webomgevingen voldoen aan alle relevante (externe) wetten en richtlijnen die de organisatie van buitenaf worden opgelegd.
Dit laatste is meer en meer aan de orde.

Webstandaarden zijn uiterst belangrijk omdat zij tactische richtlijnen bieden voor het ontwikkelen van webcontent en webapplicaties. Standaarden manifesteren zich in documenten als het redactiehandboek, applicatieontwikkelinsprocessen en -procedures, etc.

In dit documenten wordt webbeleid en webstandaarden benoemd welke gelden voor alle websites, webapplicaties en e-mail van de Samenwerkingsorganisatie De Wolden Hoogeveen (hierna: SWO), gemeente Hoogeveen en gemeente De Wolden.
Afhankelijk van het type aanschaf/eigenaarschap kunnen bepaalde eisen wel/niet gelden.

De beleidsuitgangspunten die de SWO hanteert, zijn ontleend aan de Baseline Informatiebeveiliging Overheid v1.04 (BIO), de wereldwijd gehanteerde CIS Security baselines (Center of Internet Security), de AVG en standaarden van het Forum Standaardisatie.

Vanuit de BIO gaat dit over onderstaande controls en daaraan gekoppelde maatregelen.

H13. Communicatiebeveiliging
13.2.3: Elektronische berichten

H14. Acquisitie, ontwikkeling en onderhoud van informatiesystemen
14.1.2: Toepassingen op openbare netwerken beveiligen
14.1.3: Transacties van toepassingen beschermen

H15. Leveranciersrelatie
15.1.1: Informatiebeveiligingsbeleid voor leveranciersrelaties
15.1.2: Opnemen van beveiligingsaspecten in leveranciersovereenkomsten
15.1.3: Toeleveringsketen van informatie- en communicatietechnologie
15.2.1: Monitoring en beoordeling van dienstverlening van leveranciers
15.2.2: Beheer van veranderingen in dienstverlening van leveranciers

Mochten de uitgangspunten tegenstrijdig zijn tussen de verschillende richtlijnen dan prevaleren de BIO en AVG controls en maatregelen.

2. Websites en webapplicaties

Dit beleid gaat over websites en webapplicaties. Een website heeft als voornaamste doel het overbrengen van informatie en wordt vaak beheerd in een content management systeem (CMS) en draait in de cloud. Een webapplicatie is een applicatie die men via een webbrowser kunt bereiken en waarbij het doel interactie is. Een webapplicatie kan zowel on-premise als in de cloud draaien. Bij cloud-toepassingen spreken we dan over Software as a Service (SaaS). Een webapplicatie maakt doorgaans geen gebruik van een CMS maar wordt specifiek gebouwd voor een bepaalde functionaliteit of probleem.

De SWO heeft meerdere websites zoals de gemeentelijke websites (www.hoogeveen.nl en www.dewolden.nl) en een aantal subsites/projectsites. Vanuit beheeroogpunt willen we het aantal websites en CMS-en zo minimaal mogelijk houden. Dit is opgenomen in de strategie op Digitale Dienstverlening.

Daarnaast zetten veel leveranciers hun applicaties om in webapplicaties. En worden er door andere partijen steeds meer webapplicaties aangeboden of ingezet (zoals enquêtes, beheersystemen, etc.). Dit zijn ook vaak gratis, handige internettools, zoals bijvoorbeeld Trello, Miro, Basecamp of Google Apps. Ook dit soort tools kunnen niet zomaar gebruikt worden maar zullen ook getoetst moeten worden.

Bij elke website en webapplicatie moet er aandacht worden besteed aan (informatie)beveiliging & privacy, onderhoud, updates, etc.

2.1 Algemene uitgangspunten

1. Er wordt gebruik gemaakt van het basis-CMS van de SWO voor het beheren van websites, subsites en projectsites. Alleen in uitzonderlijke gevallen kan hier gemotiveerd van worden afgeweken. Webapplicaties worden door leveranciers zelf gebouwd voor een bepaalde (aanvullende) functionaliteit en niet als website. Dit is toegestaan, mits deze niet ingezet worden als (deel)vervanger van de website.
2. De website/webapplicatie is op de juiste manier gescript (conform W3C) met moderne technieken (HTML5 en CSS3) en valideert zonder fouten op https://validator.w3.org. Het niet valideren zal echter alleen leiden tot een opmerking in de test en niet tot afkeur.
3. De website/webapplicatie is responsive, werkt goed op alle soorten devices en in de meeste recente, moderne webbrowsers van maximaal één jaar oud.

2.2 Accountbeheer[1]

1. De website/webapplicatie moet voorzien in inlogaccounts die voldoen aan een sterk wachtwoordbeleid[2].
2. De website/webapplicatie maakt gebruikt gemaakt van persoonsgebonden accounts.
3. Er is vastgelegd welke personen toegang hebben tot de website/webapplicatie. De autorisaties worden periodiek gecontroleerd.
4. De website/webapplicatie dwingt het gebruik van 2FA/MFA af op het moment dat er ingelogd moet worden in de website of webapplicatie.

[1] Het uitgangspunt is dat er gekoppeld wordt aan de Azure AD van de SWO. Hierdoor worden de eisen aan de kant van de SWO afgevangen.
[2] Wachtwoorden bestaan uit minimaal 8 vrij te kiezen karakters, waarvan tenminste 1 kleine letter, 1 hoofdletter, 1 cijfer en 1 vreemd teken. Daarnaast zijn wachtwoorden maximaal 365 dagen geldig bij toepassing 2FA/MFA of 180 dagen geldig bij alleen ID/wachtwoord en mogen niet binnen zes keer herhaald worden.

2.3 Privacy-AVG

1. Indien via de website/webapplicatie persoonsgegevens worden verwerkt, dan is privacy wet- en regelgeving van toepassing (o.a. de AVG). Dit wordt vooraf getoetst. Indien nodig, dan dienen aanvullende maatregelen te worden genomen om de informatieveiligheid & privacy te waarborgen;
2. Er worden alleen functionele cookies gebruikt. Op het moment dat er analytische of tracking cookies aanwezig zijn, dan is er een cookie-melding beschikbaar waarmee de bezoeker deze niet-functionele cookies kan uitschakelen;
3. Er staat een privacy statement en cookieverklaring op de website/webapplicatie. Voor webapplicaties waarvan de SWO of één van de gemeenten eigenaar is wordt altijd gebruik gemaakt van de standaard privacyverklaring van de SWO of de betreffende gemeente;
4. Als er externe diensten worden gebruikt zoals bijvoorbeeld een Content Delivery Network (CDN), load balancing, caching, DDoS-protectie, web application firewall (WAF) bij bedrijven zoals Cloudflare, Microsoft, Google, etc. dan is het van belang dat deze diensten zodanig zijn ingericht dat ze voldoen aan de AVG-wet- en regelgeving.

2.4 Webhosting en webserver

Webhosting is een dienst die ruimte aanbiedt voor het opslaan van informatie, afbeeldingen, of andere inhoud die toegankelijk is via een website. De SWO en gemeenten hebben verschillende websites en webapplicaties. Deze worden gehost bij verschillende leveranciers en op verschillende onderhouden en beheerd.

1. De website/webapplicatie wordt gehost binnen de Europese Economische Ruimte (EER), bij voorkeur in Nederland bij een Nederlandse hostingpartij (vanwege voordelen met performance, contract- en leveranciersmanagement en wetgeving).
2. Bij de hosting van de website/webapplicatie moeten er afspraken gemaakt zijn voor het reguliere onderhoud, back-ups, beveiliging en DDoS protectie geregeld is. Bijvoorbeeld door het afsluiten van een SLA. De aandachtspunten hierbij zijn:
   - Maandelijks onderhoud: security checks, log checks, updates, monitoring controle.
   - 24/7 monitoring: acties bij storingen en bij situaties dat de server down is.
   - Backups: dagelijks een full backup naar een externe server met een minimale retentie van 7 dagen.
   - Security: zorgen dat de server altijd veilig is (door tijdig toepassen van updates/hotfixes en gebruik ‘moderne’ internetstandaarden).
   - DDoS protectie: welke acties worden er uitgevoerd als de server of hostingpartij onder vuur ligt.
3. De webserver worden periodiek up-to-date gehouden. Denk hierbij bijvoorbeeld aan Apache, Nginx, PHP, ASP.net, java-componenten, etc. De webserver bevat geen kwetsbaarheden of de kwetsbaarheden zijn gemitigeerd. Uitgangspunt is dat er uiterlijk binnen zes maanden naar de laatste (veilige) versie wordt gegaan.
4. De webserver(s) waarop een website/webapplicatie wordt gehost, scoort minimaal een A op SSL Labs (https://www.ssllabs.com).
5. De webserver(s) waarop een website/webapplicatie wordt gehost, ondersteunt naast IPv4 ook IPv6[3].

[3] *Standaard IPv6 en IPv4*
Internet Protocol versie 6 (IPv6) maakt communicatie van data tussen ICT-systemen binnen een netwerk, zoals internet, mogelijk. De standaard bepaalt dat ieder ICT-systeem binnen het netwerk een uniek nummer (IP-adres) heeft. De belangrijkste motivatie voor de ontwikkeling van IPv6 was het vergroten van de hoeveelheid beschikbare adressen ten opzichte van de tegenwoordig gangbare voorganger IPv4. Om interoperabiliteit maximaal te waarborgen heeft College Standaardisatie 'pas toe of leg uit' van toepassing verklaard op de combinatie van IPv4 en IPv6. Een organisatie moet dus beide versies vragen bij de aanschaf van een ICT-product/-dienst.

2.5 Beveiliging en certificaten

1. De website/webapplicatie wordt periodiek up-to-date gehouden (denk hierbij bijvoorbeeld aan WordPress-core, Drupal-core, frameworks, plugins, javascript, Jquery-library, thema's, etc). De website/webapplicatie bevat geen kwetsbaarheden of de kwetsbaarheden zijn gemitigeerd naar een niveau dat voor de SWO acceptabel is. Uitgangspunt is dat er uiterlijk binnen 6 maanden naar de laatste (veilige) versie wordt gegaan.
2. De website/webapplicatie scoort 100% op de test van internet.nl (in deze test zitten overlappende eisen vanuit deze paragraaf).
3. De website/webapplicatie wordt door de leverancier minimaal 1x per jaar getest d.m.v. een pentest.
4. De website/webapplicatie wordt door de leverancier minimaal 1x per kwartaal gescand op kwetsbaarheden d.m.v. een vulnerability scan.
5. De website/webapplicatie wordt beveiligd door een veilig TLS/SSL-certificaat[4] (https). De TLS-versie is minimaal TLS v1.2.
6. Het soort / type TLS/SSL-certificaat past bij de vorm van beveiliging die nodig is voor de website/webapplicatie. Zie de volgende punten voor een toelichting:
   a. Op het moment dat er persoonsgegevens verwerkt worden of bij bepaalde (overheids)diensten (zoals DigiD, Digikoppeling en e-Factureren) dient een certificaat te worden gebruikt met **Extended Validation (EV)**.
   b. Voor server verbindingen zoals een mailserver of server-server verbindingen dient een certificaat te worden gebruikt met **Domain Validation (DV).**
   c. Het gebruik van een gratis **Let's Encrypt** certificaat voor gemeentelijke/overheids websites/webapplicaties raden wij af vanwege het feit dat er geen validatie op de aanvrager wordt uitgevoerd.
7. Het TLS/SSL-certificaat is op de juiste manier geïnstalleerd (afdwingen https).
8. Er is geen mixed-content op de website (http over https).
9. Op de website is een security.txt geplaatst[5]. In dit tekstbestand staat contactinformatie, zodat ethische hackers of cyberonderzoekers kunnen lezen met welke afdeling of persoon zij contact op kunnen nemen als zij een kwetsbaarheid vinden.
10. RPKI moet worden toegepast door netwerkaanbieders en houders van blokken IP-adressen bij het aanbieden van netwerkconnectiviteit, ter beveiliging van het BGP (Border Gateway Protocol). Dit geldt zowel voor het publiceren van ROA's (Route Origin Authorisations) als voor het valideren en het 'droppen' van invalide routes.

Toevoeging van IPv6 in combinatie met IPv4 aan de lijst met open standaarden voor 'pas toe of leg uit' betekent dat nieuw aan te schaffen informatiesystemen met beide versies overweg moet kunnen. IPv4 is op dit moment alom gebruikt. IPv6 is niet backwards compatible met IPv4. De komende periode zullen IPv4 en IPv6 gelijktijdig gebruikt worden. Om interoperabiliteit met zowel de nieuwe IPv6-praktijk als de bestaande IPv4-praktijk te borgen, zijn beide versies van de standaard opgenomen.
In 2017 besloot het Forum Standaardisatie een standaardsyntaxis toe te passen op de beschrijving van de functioneel toepassingsgebieden van standaarden op de 'pas toe of leg uit'-lijst. Aan de hand van deze syntaxis hebben we het functioneel toepassingsgebied van deze standaard IPv6 en IPv4 aangepast. Dit is bekrachtigd door het Overheidsbrede Beleidsoverleg Digitale Overheid (OBDO) op 25 mei 2018.

[4] Zie bijlage 1
[5] Zie https://forumstandaardisatie.nl/open-standaarden/securitytxt

11. Security headers worden vaak vergeten bij de beveiliging van webapps of websites. Maar door aandacht te besteden aan de security headers en door deze goed in te stellen, zorg je voor een extra laag van beveiliging voor je website. Deze headers kunnen bijvoorbeeld getest worden op https://securityheaders.com.
    Op de website worden minimaal de volgende headers gezet:
    a. Er wordt een juiste **HSTS-policy** aangeboden van minimaal "max-age=31536000" env=HTTPS (afdwingen HTTPS voor terugkerende bezoekers voor een bepaalde periode).
    b. De **X-Frame-Options** is gezet op NONE of SAMEORIGIN (framen van de website).
    c. De **X-Content-Type-Options** wordt gezet "nosniff". Hierdoor mag de browser de content/type (type van content, bijvoorbeeld css of xml) niet meer raden, maar moet deze verwerken zoals deze is aangeboden.
    d. De **Referrer-Policy** "no-referrer-when-downgrade" wordt minimal toegepast. Hiermee voorkom je dat informatie over je website via een hyperlink wordt verzonden naar een andere onbeveiligde website.
12. Daarnaast is het de aanbevelingen om de volgende security headers ook toe te passen en bij eventuele afwijkingen dit toe te lichten:
    a. Toepassen van de **Content-Security-Polic**y als maatregel tegen Cross Site Scripting (XSS) aanvallen;
    b. De **Permissions-Policy** (voorheen Feature-Policy) is een header waarmee de features van een browser beperkt kunnen worden (bijvoorbeeld geocoding, camera, microfoon, api's).

2.6 Domeinnamen

Een domeinnaam is een unieke naam op internet. Een domeinnaam is bijvoorbeeld dewolden.nl. Meestal worden domeinnamen gebruikt voor websites.
Maar men kan ook een domeinnaam aanvragen voor een persoonlijk mailadres.

1. De SWO of gemeente is altijd eigenaar van een eigen domeinnaam en deze staat op naam van de SWO of één van de gemeenten en worden gehost bij één eigen leverancier[6]. Dit is vooral van belang bij herkenbaarheid van de gemeentelijke organisatie voor inwoners, ondernemers of ketenpartners.
2. Alleen bij SaaS-applicaties waarbij geen specifieke eigen domeinnaam van de gemeentelijke organisatie wordt gebruikt, vervalt deze eis bij 1.

DNSSEC is een uitbreiding op het Domain Name System (DNS). Het verhelpt een aantal kwetsbaarheden in DNS waardoor de 'bewegwijzering' van het internet veiliger en vertrouwder wordt. DNSSEC voorziet de DNS records van een digitale handtekening, zodat de aanvrager kan controleren of de record die terug komt, authentiek is.
Het "spoofen" van DNS, of zogeheten cache-poisoning, is hierdoor niet langer meer mogelijk. De DigiD-audit eist sinds 2017 dat domeinnamen beveiligd zijn door DNSSEC. Ook het Nationaal Beraad digitale overheid heeft als doelstelling dat alle overheidsorganisaties 100% voldoen aan DNSSEC.

3. Alle domeinnamen worden beveiligd door middel van DNSSEC.
   Dit betekent dat de DNS-server DNSSEC moet ondersteunen.
4. De nameserver (DNS) ondersteunt naast IPv4 ook IPv6.
5. Bij eigen domeinnamen houdt de SWO zelf controle over het DNS. Hiervoor worden de nameservers niet doorverwezen naar het DNS van een leverancier.

[6] Momenteel is dat iXL hosting.

3. Toegankelijkheid

Webtoegankelijkheid betekent: een internet-toepassing toegankelijk maken voor iedereen, inclusief ouderen en mensen met een functiebeperking. Toegang tot het internet is namelijk niet voor iedereen vanzelfsprekend. Het gaat (zeker in Nederland) niet om toegang tot het internet, maar om bruikbaarheid van de aangeboden diensten en informatie door mensen met een beperking. Denk aan personen met een verminderd gezichtsvermogen, blinden, slechtzienden maar ook bijvoorbeeld doven en slechthorenden en mensen met beperkte handfunctie of bijvoorbeeld beperkte leesvaardigheid. Omdat internet grotendeels visueel van aard is, hebben met name blinden en slechtzienden relatief vaak problemen met de toegankelijkheid van internet. En door de toename van multimedia (denk aan YouTube-filmpjes) wordt ook (het ontbreken van) geluid steeds belangrijker, met name voor doven en slechthorenden. Alle websites en mobiele apps van alle overheden en semioverheden moeten ook toegankelijk en bruikbaar zijn voor mensen met een handicap. Alle overheidsinstanties moeten de Europese (open) standaard voor digitale toegankelijkheid toepassen. Deze wettelijk verplichte toegankelijkheid geldt niet alleen voor externe websites geldt, maar ook voor interne intranetten en mobiele apps.

1. De website/webapplicatie voldoet aan de eisen die gesteld worden conform Richtlijnen voor Toegankelijkheid van Webcontent (WCAG)[7]. Zie hiervoor https://www.digitoegankelijk.nl. De toegankelijkheidseisen kunnen ingedeeld worden in de volgende onderdelen:
   a. Lever tekstalternatieven voor alle niet-tekstuele content, zodat die veranderd kan worden in andere vormen die mensen nodig hebben, zoals grote letters, braille, spraak, symbolen of eenvoudiger taal.
   b. Lever alternatieven voor op-tijd-gebaseerde media.
   c. Creëer content die op verschillende manieren gepresenteerd kan worden (bijvoorbeeld eenvoudiger lay-out) zonder verlies van informatie of structuur.
   d. Maak het voor gebruikers gemakkelijker om content te horen en te zien, waaronder scheiding van voorgrond en achtergrond.
   e. Maak alle functionaliteit beschikbaar vanaf een toetsenbord.
   f. Ontwerp content zodanig dat het geen toevallen veroorzaakt.
   g. Lever manieren om gebruikers te helpen navigeren, content te vinden en te bepalen waar ze zijn.
   h. Maak tekstcontent leesbaar en begrijpelijk.
   i. Maak het uiterlijk en de bediening van webpagina's voorspelbaar.
   j. Help gebruikers om fouten te vermijden en ze te verbeteren.
   k. Maximaliseer compatibiliteit met huidige en toekomstige user agents, met inbegrip van hulptechnologieën.

Het testen van een website op toegankelijkheid kun je op verschillende manier doen. Voor overheidsinstanties is het verplicht om een toegankelijkheidsonderzoek uit te laten voeren door een organisatie die hiervoor bevoegd is. Lang niet alle eisen zijn namelijk automatisch te toetsen. Toetsen blijft daarom ook mensenwerk en veel in de code kijken.

[7] https://zoek.officielebekendmakingen.nl/stb-2018-141.html

HOOFDSTUK 4. SLOTBEPALINGEN
Artikel 6. Gefaseerde toepassing
Aan de artikelen 3 en 4 wordt:
a. wat betreft websites die zijn gepubliceerd vanaf 23 september 2018 uiterlijk met ingang van 23 september 2019 voldaan;
b. wat betreft websites die zijn gepubliceerd voor 23 september 2018 uiterlijk met ingang van 23 september 2020 voldaan;
c. wat betreft mobiele applicaties uiterlijk 23 juni 2021 voldaan.

Tools zijn echter vaak een eerste indicatie voor de digitale toegankelijkheid van een website of webapplicatie. Voor het verder testen is specifieke kennis vereist over de norm en digitale toegankelijkheid.

Om de toegankelijkheid te testen wordt gebruik gemaakt van de volgende tools:

- Website scan via https://ismijnsitetoegankelijk.nl
- Firefox Developer
- Contrast van tekst t.o.v. de achtergrond m.b.v. Colour Contrast Analyser

4. E-mailbeveiliging / e-mailauthenticatie

Met e-mailauthenticatie kan een organisatie haar domeinnaam beschermen tegen betrouwbaar lijkende phishing e-mailberichten waarin bijvoorbeeld bijlagen of links naar malware of valse inlogpagina's zitten. Het zorgt ervoor dat derden niet zomaar de gemeentelijke domeinnaam als afzenderadres kunnen misbruiken. Dit wordt 'afzenderadres-vervalsing' of 'e-mail spoofing' genoemd en is uit te voeren zonder diepgaande technische kennis. E-mailauthenticatie voorkomt dit en zorgt er bovendien voor dat spam nauwkeuriger wordt herkend. Het werkt op basis van de open standaarden SPF, DKIM en DMARC.

4.1 E-mailbeveiliging / e-mailauthenticatie

4.1.1 Beschrijf mailfunctionaliteit van de applicatie

Maakt de applicatie gebruik van een mailfunctionaliteit voor het (geautomatiseerd) verzenden van e-mail vanuit de applicatie. Leg dan vast waarvoor de mailfunctionaliteit dient en op welke manier er mail verstuurd wordt. Pas daarnaast de volgende aanbevelingen toe om te voorkomen dat de e-mail misbruikt wordt.

4.1.2 SPF (Sender Policy Framework)

SPF is een protocol dat tot doel heeft te helpen spam te verminderen door te controleren of het e-mailadres van de verzender bestaat en dat de server die de mail verstuurt dat ook echt mag versturen. Met deze maatregel voorkomen we dat hackers de e-mailadressen van uw organisatie misbruiken en dat uw mail door anderen geblokkeerd wordt ('blacklist').

1. Voor alle e-maildomeinen wordt een SPF record in het DNS opgenomen dat (onder meer) aangeeft welke systemen mail voor het betreffende domein mogen versturen.

4.1.3 DKIM (DomainKeys Identified Mail)

DKIM is een techniek waarbij een organisatie verantwoordelijkheid kan nemen voor een bericht dat per e-mail wordt verzonden. Bij DKIM maakt de verzendende mailserver met behulp van een 'private key' een cryptografische handtekening en voegt die toe aan de mail in de vorm van een zogenaamde DKIM-header. Een soort echtheidskenmerk dus. De ontvangende partij ziet deze handtekening, zoekt in het DNS de bijbehorende publieke sleutel op en valideert de handtekening (en dus de mail) daarmee.

1. Voor alle e-maildomeinen wordt een DKIM record in het DNS opgenomen.

4.1.4 DMARC (Domain-based Message Authentication, Reporting and Conformance)

DMARC is een protocol dat helpt e-mail spoofing tegen te gaan door te controleren of de afzender legitiem is en dat de inhoud van de mail onderweg niet gewijzigd is. Met DMARC laat men aan partnerorganisaties weten dat e-mail door middel van SPF te controleren is, maar ook wat er moet gebeuren als blijkt dat de mail toch illegaal verstuurd is.

1. Voor alle e-maildomeinen wordt door middel van een DMARC-record in het DNS een beleid kenbaar worden gemaakt voor de ontvangende mailserver. Bijvoorbeeld (in versimpelde vorm): "als de DKIM-handtekening niet klopt, of als SPF faalt, stop deze mail dan in de spamfolder".

4.1.5 STARTTLS en DANE

De toepassing van STARTTLS in combinatie met DANE maakt het mogelijk verbindingen die in principe niet als beveiligd beschouwd mogen worden (hetzij omdat er geen enkele beveiliging op zit, hetzij omdat alleen zogenaamde 'opportunistische' encryptie mogelijk is) om te zetten naar een gecontroleerde, beveiligde verbinding voor e-mailverkeer. Hierdoor is het voor aanvallers niet meer mogelijk om berichtenverkeer 'af te luisteren' of te manipuleren. Door het gebruik van STARTTLS en DANE weet de verzendende mailserver dat de e-mail daadwerkelijk via een versleutelde verbinding is verstuurd naar een e-mailserver van de ontvangende partij. De toepassing van STARTTLS in combinatie met DANE kan worden gezien als een 'HTTPS' voor e-mail.

1. Voor alle e-maildomeinen wordt STARTTLS en DANE geïmplementeerd.

4.1.6 Forwarden e-mail

Bij zowel SPF als DKIM gooit het 'forwarden' van e-mail roet in het eten, omdat een 'forward' de mail kan wijzigen. Er worden namelijk extra headers toegevoegd en de e-mail wordt verzonden door een niet bekende mailserver. De oorspronkelijke DKIM-handtekening wordt hier ongeldig maakt en het SPF record voldoet niet meer. Hierdoor wordt e-mail niet meer (juist) afgeleverd.

1. Voor alle e-maildomeinen wordt geen gebruik gemaakt van automatische e-mail forwarders.

5. DigiD aansluitingen

Voor alle DigiD aansluitingen van de SWO en de gemeente Hoogeveen en De Wolden zijn er aanvullende maatregelen en verantwoordelijkheden van toepassing.

5.1 Normen

1. De SWO conformeert zich aan de laatste door Logius gepubliceerde Norm ICT-beveiligingsassessments DigiD.
2. Jaarlijks wordt dit normenstelsel in het kader van ENSIA door een externe auditor in samenwerking met de beveiligingsbeheerder Web getoetst.
3. Over deze toetsing vindt horizontaal (van college aan de raad) en verticaal (naar Logius) verantwoording plaats.

5.2 Eigenaarschap

1. Geheel in lijn met de BIO is het eigenaarschap van de DigiD webapplicaties (de webapplicaties die de DigiD functionaliteit aanroepen) belegd in de lijnorganisatie en is het betreffende systeemeigenaar[8] eindverantwoordelijk voor het goed functioneren van de applicatie en de te treffen maatregelen.

5.3 Functioneel applicatiebeheer

1. Per DigiD aansluiting is door de genoemde systeemeigenaar een functioneel applicatiebeheerder[9] aangewezen die de verantwoordelijkheid heeft de door Logius opgestelde beveiligingsnormen te implementeren, te controleren (middels een jaarlijks TPM verklaring) en de bewijslast ervan op te bouwen in een auditdossier.
2. Het auditdossier wordt jaarlijks aan een externe auditor beschikbaar gesteld en bevat tenminste:
    - de contracten en servicerapportages van onze SaaS-leverancier (B.05);
    - de incidentprocedure en een overzicht van de incidenten (U/WA.02);
    - de dataclassificatie (U/WA.05);
    - bewijs dat de webapplicatie gehardend is (U/NW.06, m.b.t. DNSSEC);
    - de beoordeelde releases (C.08).
3. Minimaal één keer per half jaar wordt er door de functioneel applicatiebeheerder beoordeeld of alle autorisaties juist en actueel zijn. Hierover wordt een rapportage uitgebracht aan de verantwoordelijk systeemeigenaar en de ISO of CISO.

5.4 Toetsing effectiviteit

1. Per DigiD-aansluiting wordt de effectiviteit van de genomen maatregelen en procedures (werking) periodiek getoetst op tenminste het volgende:
    1. de beoordeling van de autorisaties (U/TV.01)
    2. de incidentenprocedure en een overzicht van de incidenten (U/WA.02)
    3. de beoordeelde releases (C.08)
2. Deze toetsingen op werking zijn verder uitgewerkt in het beleid audits, assessments & testen.

Technisch

1. Voor wat betreft de DigiD aansluitingen wordt door de SWO uitsluitend gebruik gemaakt van cloudapplicaties welke door SaaS leveranciers worden geleverd. Derhalve wordt een groot deel van de door Logius verplichte normen ingevuld door de SaaS-leverancier die hiervan middels een jaarlijkse, door een onafhankelijk auditor opgestelde, TPM-verklaring verantwoording over aflegt.

[8] Voor toewijziging rol zie bijlage Toewijzing rollen organisatie Informatieveiligheid & Privacy - SWO
[9] Voor toewijziging rol zie bijlage Toewijzing rollen organisatie Informatieveiligheid & Privacy - SWO

Bijlage 1: TLS/SSL certificaat

Transport Layer Security (TLS) en diens voorganger Secure Sockets Layer (SSL), zijn encryptie-protocollen die de communicatie tussen computers (zoals bijvoorbeeld op het internet) beveiligen. Lastig is dat een standaardisatiecommissie op een gegeven moment een nieuwe naam voor SSL heeft geïntroduceerd, namelijk TLS, en opnieuw bij versie 1.0 is begonnen.

Het doel van de TLS-protocollen is tweeledig. De server door middel van een certificaat geauthentiseerd zodat de gebruiker zeker kan zijn dat de gevonden server ook inderdaad is wie hij zegt te zijn (authenticatie). Daarnaast wordt de communicatie tussen beide partijen versleuteld door gebruik te maken van cryptografie (encryptie).

Op dit moment zijn de volgende versies van SSL en TLS in omloop:

Versie	Omschrijving	Ondersteuning gestopt	Veilig
SSL v2.0	Was al jaren kwetsbaar, niemand gebruikt dit.		Onveilig
SSL v3.0	Wordt nog steeds ondersteund door zeer veel servers, maar blijkt "lek" te zijn. SSL wordt niet langer als sterke cryptografie beschouwd.	Juni 2015	Onveilig
TLS v1.0	Minimale verschillen met SSL v3.0. TLS 1.0 wordt niet langer als sterke cryptografie beschouwd.	30 juni 2018 door Payment providers.	Onveilig
TLS v1.1	Tussenversie. Geen lekken maar bepaalde cryptografie wordt niet als veilig beschouwd en wordt daarom steeds minder ondersteunt.	Browser ondersteuning tot uiterlijk maart 2020	Veilig, mits juist geïmplementeerd. Niet meer ondersteund.
TLS v1.2	Actuele versie, ondersteund door alle moderne webbrowsers en servers		Veilig
TLS v1.3	Sinds 19 oktober 2015 was er een concept beschikbaar van TLS 1.3. In maart 2018 is deze versie definitief gemaakt. Dit wordt steeds beter door browsers en servers ondersteunt.		Veilig