SaaS maatregelen gemeente Zaanstad

Richtlijnen voor technische en organisatorische beheersmaatregelen bij SaaS-oplossingen

Wijzigingsprocedure
Het document wordt door de afdeling Informatiebeveiliging beheerd. Het wordt minimaal eens per jaar geactualiseerd en wanneer nodig herzien. Na een herziening wordt de nieuwe versie opnieuw vastgesteld.

Gerelateerde documenten

■ ICT-Beveiligingsrichtlijnen voor webapplicaties	NCSC
■ Baseline Informatiebeveiliging Overheden (BIO)	IBD
■ Aansluitvoorwaarden ICT	Gemeente Zaanstad

Doel
Dit document dient ter ondersteuning van de informatiebeveiliging van de gemeente Zaanstad. Het geeft richtlijnen die voor de informatiebeveiliging bij SaaS-oplossingen nodig zijn en stuurt hiermee de selectie van nieuwe SaaS-leveranciers.

Doelgroep
De richtlijnen kennen twee doelgroepen. Het is enerzijds geschreven voor de proceseigenaar bij de gemeente, in hoedanigheid van bijvoorbeeld de opdrachtgever, projectleider of product-owner. Anderzijds geeft de SaaS-leverancier, aan de hand van de richtlijnen in paragraaf 3.1 en 3.2, inzage in het beveiligingsniveau van de SaaS-oplossing. Deze tabellen dienen door de SaaS-leverancier ingevuld te worden.

Inhoud

1 Informatiebeveiligingseisen SaaS-systemen

1.1 Wat is SaaS

SaaS, oftewel Software As A Service, heeft betrekking op software die als online dienst wordt aangeboden. Er wordt ook van webservices of web-based api's gesproken. De SaaS-leverancier is eigenaar van de software en biedt dit in licentievorm aan met een daarbij behorend dienstniveau en beheer.

Het Informatiebeveiligingsbeleid is gebaseerd op de Baseline Informatiebeveiliging Gemeenten, vanaf 01-01-2020 de Baseline Informatiebeveiliging Overheid, en wordt gebruikt als basis voor de beoordeling van processen en informatiesystemen op aanwezige risico's. Dit document geeft invulling aan zowel de technische als organisatorische beheersmaatregelen die voor alle SaaS-systemen geldt.

1.1.1 Waarom een specifieke set maatregelen voor SaaS-systemen?

SaaS-systemen worden in regel afgenomen van leveranciers die van buiten het gecontroleerde netwerk van de gemeente opereren en van daaruit hun diensten aanbieden. Een dergelijke oplossing biedt zowel kansen als risico's.

De uitbesteding via SaaS-oplossingen ontslaat de gemeente zich niet van haar verantwoordelijkheid om zorgvuldig met (gevoelige) gegevens om te gaan die zij in bezit heeft. Wanneer de gemeente besluit een dienstverlening via een SaaS-oplossing uit te besteden, is het van belang om inzicht te krijgen in het beveiligingsniveau dat van toepassing is bij de leverancier. Dat leidt tot een bewustere omgang met risico's, kennis van genomen maatregelen en in sommige gevallen de nog te treffen maatregelen.

Deze richtlijnen zijn opgesteld om de risico's van SaaS-systemen voor de gemeente zodanig te verminderen dat eventuele rest-risico's acceptabel blijven.

2 SaaS-maatregelen

Om de eerder genoemde risico's van SaaS-systemen te kunnen verminderen volgt de gemeente de volgende bestaande kaders voor SaaS-systemen:

- De maatregelen uit ICT Beveiligingsrichtlijnen voor web-applicaties (NCSC)
- De maatregelen die de ICT-Infra organisatie stelt en voor SaaS-oplossingen van belang zijn. Het gaat hier vooral om de technische implementatie.

Bovendien staat bewustwording op het gebied van informatiebeveiliging ook bij een SaaS-oplossing centraal. Verschillende normeringen die voor de gemeente van toepassing zijn, verplichten een organisatie om beveiliging doorlopend aandacht te geven. Bewustwording wordt daarom ook in dit document opgenomen.

2.1 Informatiebeveiligingskader voor SaaS-systemen

Net als alle andere gemeenten hanteert de gemeente Zaanstad de Baseline Informatiebeveiliging Gemeente (BIG) als kader voor diens Informatiebeveiliging.
Vanaf 1 januari 2020 wordt de BIG vervangen door de Baseline Informatiebeveiliging Overheid (BIO). Voor onderstaande maatregelen heeft dat geen invloed daar de genoemde maatregelen compliant zijn aan het BIO Basis Beveiligings Niveau (BBN) 2. Dit is ook in overeenstemming met het baseline niveau van de BIG.

Om de set aan beveiligingsmaatregelen begrijpelijk en toepasbaar te maken, is de keuze gemaakt om een selectie te maken uit de richtlijn "ICT-beveiligingsrichtlijnen voor webapplicaties " van het Nationaal Cyber Security Centrum (NCSC). Deze norm is vastgesteld door het ministerie van Binnenlandse Zaken en Koninkrijksrelaties in overleg met Logius, Rijks auditdienst en NCSC. De beveiligingsrichtlijnen van NCSC zijn breed toepasbaar voor ICT- oplossingen die gebruikmaken van webapplicaties zoals ook SaaS-oplossingen.

Het Informatiebeveiligingskader voor SaaS-systemen geeft aandacht aan de eerder genoemde risico's die zich bij SaaS-oplossingen kunnen voordoen.
Dit Informatiebeveiligingskader is van toepassing voor SaaS-systemen die de Baselinetoets BIG/BIO tot en met BIV rating 1-2-2 (BIO BBN 2) scoren. Wanneer er een hogere BIV rating gescoord wordt, dienen aanvullende maatregelen genomen te worden of er moet een uitgebreide analyse worden uitgevoerd.

2.2 Maatregelen bij ICT

Bij interne systemen van de gemeente behoort een deel van de technische beveiligings controls tot het uitvoeringsgebied van ICT. Het moet helder zijn welke controls bij ICT van toepassing zijn, zowel in generieke zin als eventueel per beveiligingsniveau.

Voor SaaS-systemen geldt dat de SaaS-leverancier zelf verantwoordelijk is voor de te nemen beveiligings- en continuïteitsmaatregelen. Bij SaaS-diensten is er vaak minder ruimte om specifieke maatregelen van procesniveau te treffen omdat de dienst niet bij ons in beheer is. Dit betekent dat er op voorhand gekeken moet worden of de SaaS-dienstverlening een voldoende beveiligingsniveau biedt.

In specifieke gevallen zal er Service Level Agreement (SLA / DAP) opgesteld kunnen worden. Hierin komen ook afspraken in terug die van invloed zijn op de informatiebeveiliging, zoals de beschikbaarheid, rapportages, backup & restorepolicy en uitwijkmogelijkheden. Vaker zal de SaaS-leverancier echter een Service Level Commitment aanbieden en zullen er geen specifieke SLA afspraken gemaakt kunnen worden. De gemeente weegt dan bij de voorselectie van de SaaS-leverancier af of deze maatregelen bij de SaaS-leverancier voldoende geborgd worden.

2.3 Bewustwording en kwetsbaarhedentest

De gemeente verwacht van SaaS-leveranciers een actuele kennis op het gebied van risico's, kwetsbaarheden en security. Voor SaaS-applicaties kan de OWASP Top Ten (2017) als startpunt voor bewustwording dienen. Voorts zijn er verschillende alternatieven op het gebied van bewustwording, waaronder het NCSC of het NIST.

Bovendien dient elke SaaS-applicatie minimaal (maar niet uitsluitend) te worden getest op de meest voorkomende kwetsbaarheden uit het OWASP Top Ten (2017) document waarmee aangetoond kan worden dat deze kwetsbaarheden bij de productie versie niet meer aanwezig zijn;

- A1 – Injection (SQL, LDAP, OS)
- A2 – Broken authentication and session management
- A3 – Sensitive Data Exposure
- A4 – XML External Entities (XXE)
- A5 – Broken Access Control
- A6 – Security Misconfiguration
- A7 – Cross-site Scripting
- A8 – Insecure Deserialzation
- A9 – Using components with known vulnerabilities
- A10 – Insufficient Logging & Monitoring

3 Informatiebeveiligingskader SaaS

De tabellen onder 3.1 en 3.2 worden door de beoogd SaaS-leverancier ingevuld en waar nodig van uitleg voorzien.

3.1 Beleidsdomein

Code NCSC	Maatregel	Aanwezig Ja/Nee/NVT	Uitleg indien niet aanwezig of NVT
B.05[1]	In een contract met een derde partij voor de uitbestede levering of beheer van een (web)applicatie (als dienst) zijn de beveiligingseisen en -wensen vastgelegd en op het juiste (organisatorische) niveau vastgesteld.		
U/TV.01	De inzet van identiteit- en toegangsmiddelen levert betrouwbare en effectieve mechanismen voor het vastleggen en vaststellen van de identiteit van gebruikers, het toekennen van de rechten aan gebruikers, het controleerbaar maken van het gebruik van deze middelen en het automatiseren van arbeidsintensieve taken.		
U/TV.01	Wachtwoorden worden gebruikt op basis van de geldende beveiligingseisen uit de BIO[2] en worden eenrichting-versleuteld (hash en salt) opgeslagen.		
U/WA.02	Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten.		
U/WA.03	De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt.		
U/WA.04	De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren.		
U/WA.05	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacy bevorderende en crypto grafische technieken.		
U/WA.05	Gevoelige (vertrouwelijke) gegevens worden beschermd door gebruik te maken van cryptografische technieken in de database, bestanden en/of communicatie.		
U/PW.02	De webserver garandeert specifieke kenmerken van de inhoud van de protocollen.		
U/PW.03	De webserver is ingericht volgens een configuratie-baseline (zie tabel 2)		
U/PW.05	Het beheer van platformen maakt gebruik van veilige (communicatie)protocollen voor het ontsluiten van beheermechanismen en wordt uitgevoerd conform het operationeel beleid voor platformen.		
U/NW.04	De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van protectie- en detectiemechanismen.		

[1] B.05 wordt door de gemeente Zaanstad ingevuld. De overige items worden door SaaS-leverancier ingevuld.
2 Zie BIO maatregel 9.4.3.1

U/NW.05	Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd.		
U/NW.06	Voor het configureren van netwerken is een hardenings richtlijn beschikbaar.		
C.02	Leverancier is ISO27001 gecertificeerd met betrekking op de te leveren dienstverlening. Indien de leverancier niet ISO 27001 gecertificeerd is kan een kwaliteitshandboek voldoen. Hiervan zijn alle onderdelen van de ISO 27001 uitgewerkt en heeft een externe auditor vastgesteld dat de opgenomen PDCA cyclus gelijkwaardig is van opzet als de ISO 27001 voorschrijft. Alternatieven voor een ISO27001 certificering is een SOC 2 of SOC 3 Assurance rapportage.		
C.03	Vulnerability assessments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT componenten van de webapplicatie (scope).		
C.04	Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope). Specifiek: een penetratietest is uitgevoerd bij ingebruikname, door onafhankelijke derde partij. Alternatief is het kunnen overhandigen van een TPM van maximaal 1 jaar.		
C.06	In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht.		
C.07	De loggings- en detectie-informatie (registraties en alarmeringen) en de condities van de beveiliging van ICT systemen worden regelmatig gemonitord (bewaakt, geanalyseerd) en de bevindingen gerapporteerd.		
C.08	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.		
C.09	Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches tijdig zijn geïnstalleerd in de ICT voorzieningen.		
C.10	Herstelmaatregelen, waaronder back-up en recovery procedures, zijn geïmplementeerd en worden periodiek getest.		

3.2 Uitvoerend domein (technisch)

Maatregel nr.		Aanwezig Ja/Nee/NVT	Uitleg indien niet aanwezig of NVT
T.01	Algemeen Leverancier maakt gebruik van webservices of web-api's die hoofdzakelijk via het http applicatie-protocol versleuteld worden aangeboden. Non-http applicatie-protocollen worden alleen in overleg toegestaan.		
T.02	Versleuteling Dataverkeer wordt versleuteld met PKI-certificaten, conform de richtlijnen van het NCSC (TLS 1.2 of hoger). Voor domeinnamen eindigend op zaanstad.nl worden PKI-Overheidscertificaten gebruikt. HTTPS verkeer verloopt over poort 443.		
T.03	Architectuur De oplossing van de SaaS-leverancier is horizontaal en/of verticaal schaalbaar. Het systeem is in staat om schommelingen in gebruik, binnen de marges van de gebruiksvoorwaarden, adequaat op te vangen.		
T.04	Communicatie met gemeentelijke infrastructuur vindt alleen plaats via de daarvoor bestemde gateways en api-services.		
T.05	Output, exports, of gecreëerde bestanden worden via de frontend van de leverancier benaderbaar gemaakt.		
T.06	Data van de gemeente mag niet voor andere gebruikers beschikbaar komen. In geval van multi-tenancy oplossingen mogen api-services en netwerkservices shared zijn, maar data niet. De data blijft alleen per tenant toegankelijk..		
T.07	Kantooromgeving Er is zowel bij leverancier als afnemer geen mogelijkheid voor het gebruik van shares, ftp, remote access of Citrix.		
T.08	Geleverde diensten zijn compatible met browsers waaronder Microsoft Edge en Firefox[3]. Specifieke client-applicaties of plugins zijn niet noodzakelijk om de SaaS-diensten te kunnen afnemen (zero footprint)		
T.09	Indien SaaS-dienst output voor kantoortoepassingen levert, zijn deze compatible met MS Office 2016 of hoger		
T.10	Toegangsbeveiliging Burgerauthenticatie verloopt via DigiD, ketenauthenticatie via e-Herkenning EH-2 of EH-3		
T.11	Voor alle andere gebruikers leveren de SaaS-diensten two-factor authenticatie (2FA). In situaties waar geen two-factor authenticatie mogelijk is, wordt halfjaarlijks het wachtwoord vernieuwd.		
T.12	SAML2.0 wordt als SSO authenticatie- en delegatieprotocol gebruikt.		
T.13	Netwerken Leverancier heeft netwerksegmentatie geïmplementeerd waarbij omgevingen met verschillende beveiligingsniveaus van elkaar gescheiden worden. Onder andere de kantoor-, acceptatie-, en productie omgevingen.		

[3] Huidige versie en vorige versie (n-1).