Technische veiligheids- en inrichtingseisen voor webtoepassingen

Versie 2.0

Auteurs:
Cybersecurity Expert gemeente Tilburg
Web Expert gemeente Tilburg

GEMEENTE TILBURG

Inhoud

Versiebeheer

Versie	Datum	Auteur	Opmerking
0.1	26-07-2021	Cybersecurity Expert	Eerste opzet. Dit document is ontstaan uit een eerder document die opgesteld is door Wim van Iersel, Everett Manuel en Nino Camdzic.
0.2	15-09-2021	Cybersecurity Expert	Opmerkingen Sander Janssen en Steven Breepoel verwerkt. Toelichting toegevoegd.
0.9	06-10-2021	Cybersecurity Expert en Web Expert	Document ter review voorgelegd aan de opdrachtgever Sander Janssen en ISO Marius van Oers.
1.0	25-10-2021	Cybersecurity Expert en Web Expert	Opmerkingen verwerkt en document vastgesteld. Aangedragen als bijlage van Beleid Websites bij Sander Janssen. Daarmee wordt ook dit document jaarlijks herzien.
1.1	27-11-2023	Cybersecurity Expert en Web Expert	Updates en aanvullingen
1.2	30-11-2023	Cybersecurity Expert	Bronnen bijgewerkt
2.0	04-12-2023	Cybersecurity Expert en Web Expert	Vaststelling versie 2.0

Algemeen

In dit document worden de specifieke eisen benoemd die wij als gemeente Tilburg stellen aan een webtoepassing (intranetten, extranetten, websites, apps en webapplicaties). Het doel hiervan is om ervoor te zorgen dat de producten waarvoor we als gemeente verantwoordelijk zijn of waarvoor wij als verantwoordelijke worden gezien, voldoen aan de eisen die redelijkerwijs gesteld kunnen worden om de veiligheid en toegankelijk te garanderen.

Een webtoepassing wordt pas in gebruik genomen en toegestaan op de ICT-infrastructuur als deze voldoet aan de eisen. Om dit te kunnen garanderen wordt de webtoepassing eerst beoordeeld door het expertiseteam websites op de hieronder genoemde eisen.

De eisen zijn opgesteld aan de hand van:

- Internet.nl (VNG en Forum voor Standaardisatie);
- Richtlijnen Nationaal Cyber Security Centrum (NCSC);
- Open Web Application Security Project (OWASP): https://owasp.org/www-project-top-ten/;
- Securitybeleid gemeente Tilburg.

Veiligheidstest(en)

Wanneer een webtoepassing klaar is voor gebruik, stelt de leverancier gemeente Tilburg tijdig op de hoogte en in staat om een veiligheidstest uit te voeren ten behoeve van de oplevering en acceptatie van de webtoepassing. De leverancier richt, eventueel samen met de gemeente Tilburg, een testomgeving in waarmee de testen kunnen worden uitgevoerd.

De veiligheidstest wordt zowel in een testomgeving (indien aanwezig) als in de uiteindelijke productieomgeving afgenomen. De testomgeving wordt door de leverancier (tijdelijk) ter beschikking gesteld en de structuur daarvan is representatief voor de uiteindelijke systeemomgeving.

Technische eisen

Hieronder zijn de technische eisen benoemd waar websites en webapplicaties aan moeten voldoen.

1. Domeinnamen/DNS

Nr	Eis	Voldoet
1.1	Domeinnamen en DNS worden voor zover mogelijk beheerd door de gemeente Tilburg.	Ja/Nee
1.2	DNSSEC is ingeregeld door de gemeente Tilburg indien 1.1. van toepassing is. Anders wordt dit door de betreffende leverancier ingeregeld.	Ja/Nee
1.3	DANE is ingeregeld door de gemeente Tilburg indien 1.1. van toepassing is. Anders wordt dit door de betreffende leverancier ingeregeld.	Ja/Nee

2. HTTPS

Nr	Eis	Voldoet
2.1	De webapplicatie is uitsluitend te benaderen via HTTPS.	Ja/Nee
2.2	Certificaten worden geleverd door de gemeente Tilburg indien 1.1 van toepassing is. Anders wordt dit door de betreffende leverancier ingeregeld.	Ja/Nee
2.3	Het HTTPS certificaat is altijd minimaal een Organisatie-Validatie (OV) variant. Ongeacht of er wel of niet persoonsgegevens over de lijn gaan. Domein-Validatie (DV) certificaten (bijv. Let's Encrypt) worden niet geaccepteerd.	Ja/Nee
2.4	HTTP protocol moet doorverwijzen naar HTTPS.	Ja/Nee
2.5	Er worden alleen veilige TLS protocollen gebruikt.[1]	Ja/Nee
2.6	Er worden alleen veilige cipher suites gebruikt.[1]	Ja/Nee
2.7	De server dwingt zijn eigen cipher volgorde af.[1]	Ja/Nee
2.8	Er worden alleen veilige key exchange parameters gebruikt.[1]	Ja/Nee
2.9	Er worden alleen veilige hash functies voor de key exchange gebruikt.[1]	Ja/Nee
2.10	TLS-compressie staat uit.[1]	Ja/Nee
2.11	Secure renegotiation staat aan.[1]	Ja/Nee
2.12	Client-initiated renegotiation staat uit.[1]	Ja/Nee
2.13	0-RTT staat uit.[1]	Ja/Nee

[1] Raadpleeg de laatste versie van de NCSC-richtlijnen voor meer informatie: https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1/ICT-beveiligingsrichtlijnen+voor+Transport+Layer+Security+v2.1.pdf

3. Security Headers

Nr	Eis	Voldoet
3.1	Strict Transport Security (HSTS) staat aan: Minimale waarde van het max-age attribuut is 31536000.	Ja/Nee
3.2	Content-Security-Policy staat aan: er worden geen unsafe-inline en unsafe-eval gebruikt.	Ja/Nee
3.3	X-XSS-Protection staat aan.	Ja/Nee
3.4	X-Frame-Options staat aan.	Ja/Nee
3.5	X-Content-Type-Options staat aan.	Ja/Nee
3.6	Referrer-Policy staat aan. Aanbevolen policy-waarden: 1. Geen gevoelige informatie naar derde-partijen - no-referrer - same-origin 2. Gevoelige informatie naar derde-partijen alleen via beveiligde verbindingen (HTTPS) - strict-origin - strict-origin-when-cross-origin Niet aanbevolen policy-waarden: 1. Gevoelige informatie naar derde-partijen mogelijkerwijs via onbeveiligde verbindingen (HTTP) - no-referrer-when-downgrade (default policy van browsers) - origin-when-cross-origin - origin - unsafe-url	Ja/Nee
3.7	Aanbevolen: Security.txt moet aanwezig zijn in de juiste folder met minimaal contactgegevens van de betreffende contactpersoon m.b.t. security	Ja/Nee
3.8	Voor Cookies moeten de attributen Secure en HttpOnly aan staan. Van HttpOnly mag afgeweken worden als hier een legitieme reden voor is. Bijvoorbeeld: website analytics scripts. Als het Secure attribuut aanstaat, dan moet ook Secure prefix aanstaan.	Ja/Nee

4. Software stack

Nr	Eis	Voldoet
4.1	De webserver(s) draait niet onder system gebruiker. Er is een aparte gebruiker aanwezig voor de webserver met minimale rechten.	Ja/Nee
4.2	De software (inclusief plugins) is up to date.	Ja/Nee
4.3	Private keys staan gecodeerd op de webserver.	Ja/Nee
4.4	Alleen poorten 80 en 443 staan open voor de buitenwereld.	Ja/Nee
4.5	De beheeromgeving(en), zoals bijv. /wp-admin, is minimaal afgeschermd met 2Factor Authenticatie (2FA). Indien 2FA niet mogelijk is wordt de beheeromgeving(en) afgeschermd met een Access Control List (ACL). Zorg er ook voor dat na een max. aantal foutieve login pogingen de aanvaller geen nieuwe login pogingen meer kan doen.	Ja/Nee
4.6	De database(s) wordt niet ontsloten via internet.	Ja/Nee

4.7	Informatie over de gebruikte software van de website/ webapplicatie en de webserver is zoveel mogelijk verborgen. Voorbeeld: Server header, X-Powered-By header, etc.	Ja/Nee
4.8	De webserver is benaderbaar via IPv4 en IPv6.[2]	Ja/Nee

5. E-mail

5.1	DMARC dient ingericht te worden.	Ja/Nee
5.2	DKIM dient ingericht te worden.	Ja/Nee
5.3	SPF dient ingericht te worden.	Ja/Nee
5.4	Alleen poorten 25, 465, 587 en 2525 staan open voor de buitenwereld.	Ja/Nee

[2] Zie: https://forumstandaardisatie.nl/open-standaarden/ipv6-en-ipv4

Bijlage 1: Toelichting technische eisen

Nr	Eis	Uitleg
1.1	Domeinnamen	Dit geeft de gemeente Tilburg de mogelijkheid om een domein te parkeren waardoor een andere partij zich niet kan voordoen als gemeente Tilburg.
1.2	DNSSEC	DNSSEC maakt het lastig om de identiteit van een website te vervalsen.
1.3	DANE	DANE wordt gebruikt om de identiteit van een website te valideren.
2.1	HTTPS	Zonder HTTPS kan de verbinding afgeluisterd worden. Aanvallers kunnen alle gegevens die je doorgeeft aan een website ook zien. Zij kunnen hier vervolgens misbruik van maken. Potentieel kan er identiteitsfraude
2.3	Certificaat	Een OV certificaat voldoet aan de validatieprocedure die opgesteld is door de verstrekkers van certificaten: de Certificatie-Autoriteiten (CA's). Hiermee wordt gegarandeerd dat de identiteit van de website daadwerkelijk hoort bij de instantie die de gegevens ontvangt.
2.4	Doorverwijzen naar HTTPS	HTTP moet altijd doorverwijzen naar HTTPS omdat er géén gebruik mag worden gemaakt van een onveilige verbinding.
2.5 t/m 2.13	TLS	TLS is het protocol waarmee een verbinding beveiligd kan worden. Het TLS protocol moet echter goed geconfigureerd worden om een veilige verbinding te garanderen. NCSC geeft in haar beveiligings-richtlijnen aan wat de beste manier is om dat te doen.
3.1	HSTS	Strict Transport Security dwingt af dat alleen een veilige verbinding op een website gebruikt mag worden. Dit zorgt er verder voor dat er geen mogelijkheid voor een aanvaller ontstaat om een onveilige verbinding te initiëren, waardoor de aanvaller mogelijk gegevens zou kunnen stelen.
3.2	CSP	Content-Security-Policy (CSP) header maakt het mogelijk om malafide content te blokkeren op een website. Het is soms mogelijk voor aanvallers om malafide content in een website te injecteren (XSS). Deze malafide content kan bijvoorbeeld een stukje code zijn die een virus installeert bij de bezoeker van de website. Dit is zeer onwenselijk. Om dit te voorkomen kan je CSP inschakelen. CSP kan ook voorkomen dat je website opgenomen wordt in een malafide website (Frames). Het doel van aanvallers hier is om de gegevens van de gebruikers te stelen. CSP wordt momenteel alleen door moderne browsers ondersteunt.
3.3	X-XSS-Protection	X-XSS-Protection header doet hetzelfde als CSP alleen dan voor oudere browsers.
3.4	X-Frame-Options	X-Frame-Options header doet hetzelfde als CSP alleen dan voor oudere browsers.
3.5	X-Content-Type-Options	Deze header voorkomt dat malafide software automatisch geïnstalleerd kan worden. Dit gaat heel vaak gepaard met het injecteren van malafide scripts (XSS) in de webpagina.
3.6	Referrer-Policy	Deze header voorkomt dat derde partijen gebruikers kunnen traceren.
3.7	Security.txt	Op deze manier kunnen ethical hackers op een eenduidige manier de contactgegevens vinden om gevonden kwetsbaarheden op de juiste plek aan te kaarten.
3.8	Secure & HttpOnly	Het is belangrijk om cookies te beschermen. In cookies zijn vaak gegevens te vinden die alleen bedoeld zijn voor de huidige bezoeker van de website. Als een aanvaller toegang krijgt tot de cookies van een gebruiker dan kan een aanvaller zich voordoen als de legitieme gebruiker en kan alles op de website doen wat de legitieme gebruiker ook kan.

4.1	Gebruiker met minimale rechten	Aanvallers krijgen het soms voor elkaar om code uit te voeren op de server waarop de website draait. Deze code wordt dan uitgevoerd onder de gebruiker waaronder de webserver draait. Hoe minder rechten deze gebruiker heef hoe minder schade er aangericht kan worden.
4.2	Software up to date houden	Verouderde software of software die niet meer ondersteund wordt kan beveiligingslekken bevatten die misbruikt kunnen worden door aanvallers om de complete controle over de website over te nemen. Ze kunnen vervolgens de gebruiker gegevens stelen, malware verspreiden, etc.
4.3	Gecodeerde private keys	Private keys zijn een fundamenteel onderdeel van een veilige verbinding. Met de private key van je website kan je de veilige verbindingen decoderen. Als een aanvaller de private key van een website te pakken zou krijgen dan zou de aanvaller alle verbindingen naar je website kunnen afluisteren.
4.4	Hardening poorten	Poorten die onnodig open staan zijn een potentieel beveiligingsrisico omdat aanvallers dit mogelijk kunnen misbruiken om binnen te komen op de server.
4.5	Multi-Factory-Auth, Access Control List, Max aantal login pogingen	Een beheeromgeving van je website dient niet voor iedereen toegankelijk te zijn omdat het alleen bedoeld is voor de beheerders van de website. Men kan hier de content en de instellingen van de website wijzigen. Voor aanvallers is dit interessant omdat ze bijna de volledige controle van de website in handen kunnen krijgen. Dit kunnen ze vervolgens misbruiken om de gegevens van gebruikers te stelen, malware te verspreiden, etc.
4.6	Database niet publiekelijk toegankelijk	Databases bevatten vaak gevoelige gegevens die alleen toegankelijk zijn voor geautoriseerde gebruikers. Als een database ontsloten wordt aan het internet dan bestaat de kans dat aanvallers de database binnen kunnen dringen. Als de database in je interne netwerk staat dan wordt die kans aanzienlijk kleiner.
5.1	DMARC	DMARC geeft de verzendende partij de mogelijkheid om beleid te formuleren wat er met e-mails moet gebeuren wanneer de echtheidswaarmerken niet kloppen. Het geeft ook rapportagemogelijkheden voor legitieme en niet-legitieme uitgaande e-mailstromen. DMARC maakt het mogelijk om beleid in te stellen over de manier waarop een e-mailprovider om moet gaan met e-mail waarvan niet kan worden vastgesteld dat deze afkomstig is van het vermelde afzenderdomein. Hierdoor kunnen organisaties voorkomen dat anderen e-mails versturen namens het e-maildomein van de organisatie. Het gebruik van DMARC kan daarmee ingezet worden voor het verminderen en/of voorkomen van misbruik van de domeinnaam middels e-mail. Ook kan door het gebruik van de standaard worden voorkomen dat e-mailmailingen door e-mailproviders onterecht voor spam worden aangezien.
5.2	DKIM	Het gebruik van DKIM verkleint de kans op misbruik van e-mailadressen doordat ontvangers betrouwbaar echte e-mails van phishingmails of spam kunnen onderscheiden. Ook kunnen ontvangers controleren of de inhoud van de e-mail door derden is gemanipuleerd.

		DKIM is een techniek waarmee e-mailberichten kunnen worden gewaarmerkt. Een domeinnaamhouder kan in het DNS-record van de domeinnaam aan geven met welke sleutel e-mail namens de betreffende domeinnaam ondertekend moet worden. Een ontvangende mailserver kan de publieke sleutel in het DKIM-record van de domeinnaamhouder gebruiken om te controleren of de gebruiker van het betreffende domein, die een e-mail verstuurt, als afzender te controleren. Hierdoor kan de authenticiteit van de e-mail worden bepaald.
5.3	SPF	Het gebruik van SPF verkleint de kans op misbruik van e-mailadressen doordat ontvangers betrouwbaar echte e-mails van phishingmails of spam kunnen onderscheiden. SPF is een techniek waarmee een domeinhouder de IP-adressen van verzendende mailservers kan publiceren in de DNS. Een ontvangende mailserver kan deze IP-adressen gebruiken om te controleren of een e-mail daadwerkelijk afkomstig is van een verzendende mailserver van de betreffende domeinhouder.
5.4	Hardening poorten	Poorten die onnodig open staan zijn een potentieel beveiligingsrisico omdat aanvallers dit mogelijk kunnen misbruiken om binnen te komen op de server.