Gebruik van TLS en HTTP response headers

Datum: 30 oktober 2023

Door: Paddy Verberne

Versie: 1.7

Documenthistorie:

Datum	Versie	Auteur(s)	Toelichting
06-03-2018	0.9	Paddy Verberne	Conceptversie.
08-03-2018	1.0	Paddy Verberne	Eerste definitieve versie met kleine tekstuele wijzigingen en toevoegen OCSP-stapling en FS-ciphers.
25-10-2018	1.1	Paddy Verberne	Gewijzigd: maatregel 5 en maatregel 17. Toegevoegd: maatregel 18.
01-10-2019	1.2	Paddy Verberne	Geen TLS 1.0 en TLS 1.1 (maatregel 5). Feature-Policy toegevoegd (maatregel 6). Samesite toegevoegd (maatregel 10). Maatregel 12 aangescherpt. Maatregel 13 ingevoegd. Maatregel 20 uitgebreid met site van Mozilla. Voorbeelden bij conclusies verwijderd. HTTP headers -> HTTP response headers.
26-02-2020	1.3	Paddy Verberne	Maatregel 10 aangescherpt. Conclusie verwijderd.
27-02-2020	1.4	Paddy Verberne	Maatregel 19 met betrekking tot internet.nl toegevoegd.
21-09-2020	1.5	Paddy Verberne	Maatregel 5 puntiger geformuleerd. Maatregel 6 Feature-Policy naar Permissions-Policy. Maatregel 10 referentie naar “best practices” toegevoegd. Maatregel 12 uitgebreid.
08-04-2021	1.6	Paddy Verberne	Documentopmaak gewijzigd. Kleine tekstuele verbeteringen doorgevoerd. Maatregel 2 verduidelijkt. Maatregel 5 versimpeld. Maatregel 6 gebruik van X-Frame-Options genuanceerd. Nieuwe maatregel ingevoegd over het gebruik van Content-Security-Policy (maatregel 7).
23-10-2023	1.7 draft	Paddy Verberne	De naam ICT/A gewijzigd in ICT. De link bij maatregel 7 bijgewerkt. Nieuwe maatregel voor security.txt geïntroduceerd. Nieuwe maatregel voor RPKI geïntroduceerd. Afbeelding bij maatregel 20 (nu 22) bijgewerkt. Generiek gemaakt dat van maatregelen kan worden afgeweken mits overeengekomen met het intaketeam van ICT. Kleine tekstuele aanpassingen gedaan.
30-10-2023	1.7	Paddy Verberne	Maatregel voor security.txt uitgebreid zodat in voorkomende gevallen ook het security.txt-mechanisme van de leverancier kan worden ingezet.

Inleiding

Bij gemeente 's-Hertogenbosch wordt veel gebruik gemaakt van op web-technologie gebaseerde diensten. Denk hierbij aan websites, web-portals en mechanismes voor berichtenverkeer. Deze memo geldt voor alle diensten waarbij gemeente 's-Hertogenbosch verantwoordelijk is voor de exploitatie ervan, ongeacht waar deze is ondergebracht of hoe deze benaderbaar is. Het maakt dus niet uit of desbetreffende dienst is ondergebracht op het gemeentelijke netwerk of als SaaS-oplossing bij derden is ondergebracht.

De veiligheid van deze diensten is afhankelijk van vele factoren. Deze memo beperkt zich echter tot het uiteenzetten waaraan de beveiliging van de netwerkcommunicatie tussen aanbieder en afnemer van deze diensten moet voldoen en gaat dus niet over zaken zoals de veiligheid en beveiliging van de aangeboden applicatie.

Relevante technieken die bij het veilig maken van de netwerkcommunicatie worden gebruikt staan bekend onder de naam Transport Link Security (TLS) en HTTP response headers. Nieuwe versies van deze memo zullen worden gepubliceerd op het moment dat daar vanuit beveiligingsperspectief aanleiding toe is.

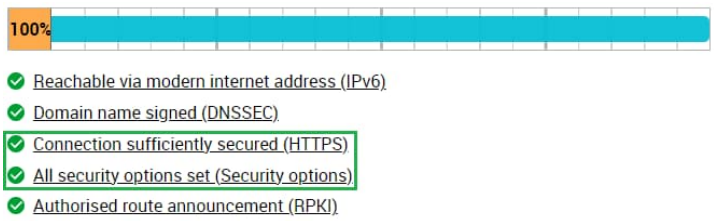
Van iedereen die voor een of meerdere genoemde diensten functioneel of technisch verantwoordelijk is, wordt verwacht dat deze de veiligheid van toegang tot deze diensten zoals bedoeld in deze memo op orde brengt en houdt. Toetsing van maatregelen is onderdeel van het intakeproces van ICT, waarin alle relevante disciplines zijn vertegenwoordigd.

Afwijkingen op de in dit document genoemde maatregelen, gebaseerd op de verplichte "Pas toe of leg uit" standaarden van Forum Standaardisatie en relevante publicaties van het NCSC, zijn alleen toegestaan na een schriftelijk akkoord van het intaketeam van ICT.

Maatregelen

1. Er wordt verplicht gebruik gemaakt van TLS. Als al gebruik wordt gemaakt van een niet-beveiligde verbinding, is deze alleen bedoeld om te verwijzen naar de met TLS beveiligde variant;
2. In geval van doorverwijzing moet de domeinnaam eerst zelf te verwijzen naar zijn HTTPS-variant, voordat deze eventueel doorverwijst naar een andere domeinnaam. Dit zorgt er ook voor dat een webbrowser de HSTS-policy kan accepteren. Een voorbeeld van een correcte verwijzing is: http://[www.]domein-a.nl -> https://[www.]domein-a.nl -> https://[www.]domein-b.nl;
3. Er wordt verplicht gebruik gemaakt van vertrouwde PKI-certificaten. Elke website geeft naast het certificaat waarmee de website wordt geïdentificeerd ook de nodige tussenliggende certificaten door. Gebruikers mogen niet worden geconfronteerd met foutmeldingen veroorzaakt door het niet juist inzetten van servercertificaten;
4. Voor verbindingen die vanaf het gemeentelijke netwerk naar websites worden gelegd en alleen voor medewerkers van gemeente toegankelijk zijn, geldt dat hier ook gebruik mag worden gemaakt van PKI-certificaten die door onze interne Certificate Authority (CA) zijn uitgeven;
5. Er wordt minimaal gebruik gemaakt van TLS versie 1.2;
6. Bij alle verbindingen (HTTP en HTTPS) met uitzondering van berichtenverkeer, worden de volgende HTTP response headers verplicht meegestuurd:
    - *X-Content-Type-Options*;
    - *X-Frame-Options* (niet verplicht als *frame-ancestors* in de *Content-Security-Policy* wordt gebruikt);
    - *X-Xss-Protection*;
    - *Content-Security-Policy*;
    - *Referrer-Policy*;
    - *Permissions-Policy*.;
7. De lijst van geldende aanbevolen instellingen voor de *Content-Security-Policy* is terug te vinden bij de testuitleg op de site https://internet.nl. Als aanscherping van deze maatregel geldt dat applicaties waarvoor een DigiD assessment van toepassing is geen van de waarden van *unsafe-eval* of *unsafe-inline* zijn toegestaan voor scripts of stylesheets (NOREA-Handreiking DigiD-assessment 4.0 (2023));
8. Bij beveiligde verbindingen (HTTPS) met uitzondering van berichtenverkeer, wordt verplicht ook de HTTP response header *Strict-Transport-Security* meegestuurd;
9. Het meesturen van HTTP response headers waaruit kan worden opgemaakt op welk platform de aangeboden dienst draait, zoals *Server* en *X-Powered-By*, is niet toegestaan, tenzij de werking van de dienst daardoor negatief wordt beïnvloed;
10. Voor alle meegestuurde HTTP response headers geldt dat de waarde ervan zodanig moet worden ingesteld dat een optimale beveiliging wordt bereikt zonder afbreuk te doen aan de functionaliteit van de geboden dienst;
11. Alle meegestuurde cookies zijn van het type secure, httponly en samesite en bevatten geen gevoelige informatie. Zie https://scotthelme.co.uk/tough-cookies/ voor de “best practices”. Voor samesite (https://web.dev/samesite-cookies-explained/) is gebruik van de optie “none” niet toegestaan;
12. Waar de gebruikte oplossing het toestaat, wordt gebruik gemaakt van OCSP-stapling, zodat het voor de afnemer van de dienst gemakkelijker is om de validiteit van het geboden TLS-certificaat te controleren;

13. Maak gebruik van ciphers die forward secrecy ondersteunen. Dit zorgt voor extra afluisterbescherming van versleuteld verkeer. Gebruik daarbij geen standaard Diffie-Hellman (DH) ciphersuites om onder andere CVE-2020-1968 (Raccoon Attack) te voorkomen. Let op: Het gaat hier alleen om DH-ciphersuites en niet om ECDH-ciphersuites;
14. Waar de gebruikte oplossing het toestaat, wordt geen gebruik gemaakt van op Cipher Block Chaining (CBC) gebaseerde ciphers;
15. Het gebruik van security.txt (RFC 9116) is verplicht. Gemeente 's-Hertogenbosch heeft daarvoor zelf een faciliteit ingericht. Het is de bedoeling dat verzoeken aan /.well-known/security.txt via een zogenaamde 302-redirect worden doorgeleid naar https://s-hertogenbosch.nl/.well-known/security.txt, tenzij de aangeboden dienst niet exclusief voor de gemeente bedoeld is. In dat geval is gebruik van een security.txt-mechanisme welke door de leverancier is ingericht van toepassing;
16. Om ongewenste omleidingen van verkeer te voorkomen wordt als onderliggende laag van de aangeboden dienst(en) verplicht gebruik gemaakt van RPKI. Dit 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 ongeldige routes;
17. Diensten die niet in productie zijn mogen niet door derden en niet via openbare netwerken zoals het internet benaderbaar zijn;
18. Voor diensten die niet in productie zijn geldt dat DNS-records hiervan niet mogen worden opgenomen in publiek benaderbare DNS-services;
19. Alle diensten worden voordat ze in productie worden genomen en daarna periodiek door een externe partij getest op kwetsbaarheden. Deze tests beperken zich niet tot TLS en HTTP response headers, maar zijn zeker ook bedoeld om de veiligheid van de aangeboden applicatie te testen;
20. Om te testen of de configuratie van TLS voldoet, kan gebruik worden gemaakt van een dienst van SSLLABS: https://www.ssllabs.com/ssltest/, waarbij als resultaat een minimale score "A" moet worden gehaald;
21. Om te testen of de configuratie van HTTP response headers voldoet, kan gebruik worden gemaakt van een dienst van Scott Helme: https://securityheaders.com/, waarbij als resultaat een minimale score "A" moet worden gehaald;
22. Op de site https://internet.nl/ kan de juiste implementatie van TLS en HTTP response headers worden gecontroleerd op "best practices" zoals aanbevolen door partijen uit de internetgemeenschap en de Nederlandse overheid. Als hier 100% wordt gescoord, dan wordt aan alle voorwaarden voldaan en zijn zaken met betrekking tot IPv6 en DNSSEC die buiten de scope van dit document vallen ook in orde. De voorwaarden voor het gebruik van IPv6 en DNSSEC staan vermeld in de gemeentelijke technische architectuur (TA), paragraaf 5.1. Voor TLS en HTTP response headers is het uitgangspunt dat de verbinding voldoende is beveiligd en dat alle applicatie-beveiligingsopties zijn ingesteld (zie afbeelding);



23. Als het testen van de configuratie van TLS en HTTP response headers niet mogelijk is via het internet, kan gebruik worden gemaakt van hulpprogramma's zoals curl (https://curl.haxx.se/)

en testssl.sh (https://testssl.sh/). Hoewel deze programma's geen score opleveren, kunnen ze wel een goede indicatie geven over de kwaliteit van desbetreffende configuratie;

24. Relevante documentatie die kan worden gebruikt om de configuratie van TLS en HTTP response headers in orde te maken:
    - https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices;
    - https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers;
    - https://wiki.mozilla.org/Security/Server_Side_TLS (gebruik minimaal "Intermediate compatibility").