Bijlage 13: **Gebruik van TLS en HTTP headers**

Bij gemeente ’s-Hertogenbosch wordt veel gebruik gemaakt van op webtechnologie 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. Relevante technieken die bij het veilig maken van de netwerkcommunicatie worden gebruikt staan bekend onder de naam Transport Link Security (TLS) en HTTP headers. Onderstaande maatregelen op dit gebied zijn hierbij vereist:

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 en/of stylesheets (https://www.norea.nl/download/?id=8904);
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 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” alleen toegestaan na expliciete toestemming van het intaketeam van ICT/A;
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. Diensten die niet in productie zijn, mogen niet door derden en niet via openbare netwerken zoals het internet benaderbaar zijn, tenzij door het intaketeam van ICT/A anders is overeengekomen;
16. Voor diensten die niet in productie zijn, geldt dat DNS-records hiervan niet mogen worden opgenomen in publiek benaderbare DNS-services, tenzij door het intaketeam van ICT/A anders bepaald;
17. 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 headers, maar zijn zeker ook bedoeld om de veiligheid van de aangeboden applicatie te testen;
18. 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;
19. Om te testen of de configuratie van HTTP headers voldoet, kan gebruik worden gemaakt van een dienst van Scott Helme: https://securityheaders.io/ , waarbij als resultaat een minimale score “A” moet worden gehaald;
20. 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);

21. Indien 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;
22. Relevante documentatie die kan worden gebruikt om de configuratie van TLS en HTTP 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”).