Bijlage 14: Gebruik van TLS en HTTP headers

Bij de gemeente 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 de gemeente 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. Als er een verwijzing wordt gedaan naar een ander domein, dan is gebruik van het volgende stramien verplicht: 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 alleen gebruik gemaakt van een combinatie van TLS versie 1.2 en 1.3. Gebruik van TLS versie 1.0 en 1.1 is geen valide optie en kan leiden tot connectieproblemen. Vanaf maart 2020 stopt de ondersteuning van deze protocollen zoals al geruime tijd aangekondigd door alle grote leveranciers van webbrowsers;
6. Bij alle verbindingen (http en https) met uitzondering van berichtenverkeer, worden de volgende HTTP headers verplicht meegestuurd:
    - X-Content-Type-Options;
    - X-Frame-Options;
    - X-Xss-Protection;
    - Content-Security-Policy;
    - Referrer-Policy.;
    - Feature-Policy
7. Bij beveiligde verbindingen (https) met uitzondering van berichtenverkeer, wordt verplicht ook de HTTP response header Strict-Transport-Security meegestuurd;
8. 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;
9. 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;
10. Alle meegestuurde cookies zijn van het type secure en httponly en bevatten geen gevoelige informatie. Hiernaast wordt gebruik van de optie samesite aangemoedigd;
11. 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;
12. Maak gebruik van ciphers die forward secrecy ondersteunen. Dit zorgt voor extra afluisterbescherming van versleuteld verkeer;