NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Toelichting:

Op 12 juni 2018 heeft NOREA een Update 2018 Handreiking bij DigiD-assessments 2.0 gepubliceerd. Voortschrijdend inzicht omtrent de kwetsbaarheden en technische beveiliging van websites hebben aanleiding gegeven voor deze update. We onderkennen hierbij dat DigiD Assessments reeds zijn uitgevoerd of gestart en dat verantwoordelijke partijen tijd nodig hebben om (additionele) maatregelen te implementeren. De NOREA werkgroep DigiD assessments beveelt IT-auditors aan om bij de uitvoering van DigiD Assessments onderstaande maatregelen te onderkennen om zodoende de verantwoordelijke partij daar waar relevant te kunnen adviseren om deze maatregelen te treffen. Deze maatregelen zijn voor de DigiD Assessment 2019 nog niet verplicht, maar deze worden mogelijk wel onderdeel van het raamwerk voor 2020 en zijn gebaseerd op de laatste inzichten omtrent de kwetsbaarheden en technische beveiliging van websites .

#	Normtekst	Aanbeveling bij de normstelling
U/WA.05	De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken.	De NOREA werkgroep DigiD assessment heeft kennis genomen van de recente update van het NCSC voor de TLS beveiliging. Zie hiervoor: https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls De beschikbaarheid van TLS 1.3 en publicatie van de vernieuwde richtlijnen van het NCSC zijn aanleiding om de richtlijnen voor TLS aan te scherpen. Hierbij beveelt NOREA aan om configuraties uit te faseren die in de toekomst onvoldoende veilig zijn. Concreet is het advies minimaal TLS 1.2 of hoger gecombineerd met minimaal 128 bits cipher suites te gaan gebruiken en TLS 1.0 en 1.1 niet meer te ondersteunen.
U/PW.03	De webserver is ingericht volgens een configuratie-baseline.	HTTP security headers bieden steeds meer en fijnmazigere controle over de toegang tot en het delen van informatie. Het correct gebruik van security headers levert een extra beschermingslaag op. De NOREA werkgroep DigiD assessments adviseert de onderstaande HTTP responseheaders. • X-Frame-Options (niet nieuw) De X-Frame-Options header voorkomt dat de pagina in een iFrame wordt geladen, waarmee gegevens kunnen worden gestolen, pagina's worden aangepast of gebruikers worden misleid. Aanbevolen waarden: deny of sameorigin • Strict-Transport-Security (HSTS) HTTP Strict Transport Security (HSTS) zorgt ervoor dat browsers alleen over TLS communiceren met de webapplicatie. Door het forceren van HTTPS beschermt deze header gebruikers tegen afluisteren en Man-in-the-Middle (MitM)-aanvallen. HSTS voorkomt het gebruik van gemengde HTTP en HTTPS inhoud, beschermt tegen fouten van webservers zoals het laden van JavaScript via een onveilige verbinding en voorkomt dat gebruikers waarschuwingen over ongeldige certificaten kunnen negeren.

#	Normtekst	Aanbeveling bij de normstelling
		Aanbevolen waarde: max-age=31536000; includeSubDomains • X-Content-Type-Options De X-Content-Type-Options header voorkomt dat de browser het MIME-type van een bestand bepaalt op basis van kenmerken (sniffing). Wanneer deze header is ingesteld op nosniff, vertrouwt de browser het MIME-type dat door de server wordt meegegeven en zal de browser de bron blokkeren als deze fout is. Dit voorkomt spoofing van resources zoals CSS stylesheets en Javascript-bestanden die over HTTP worden verstuurd. Aanbevolen waarde: nosniff • Content-Security-Policy (aangescherpt) De Content-Security-Policy (CSP) geeft de browser instructies over welke resources vanaf welke locatie mogen worden ingeladen en hoe deze mogen worden gebruikt. Een CSP kan fijnmazige instructies bevatten per soort resource, zoals afbeeldingen, stylesheets en scripts. Bij het gebruik van een CSP zijn standaard de uitvoering van inline scripts en de eval()-functie uitgeschakeld. Deze onveilige methoden kunnen echter worden toegestaan door 'unsafe-inline' en 'unsafe-eval' op te nemen in de CSP, waardoor de effectiviteit van deze header geminimaliseerd wordt. Aanbevolen waarden zijn: default-src ‘self’; frame-src ‘self’; frame-ancestors ‘self’; Sta geen onveilige configuratie toe door het gebruik van 'unsafe-inline' (tenzij gebruik wordt gemaakt van een nonce) en 'unsafe-eval'. Het is niet toegestaan bronnen beginnend met http:// te whitelisten. • Referrer-Policy De Referrer-Policy beperkt het ongevraagd delen van privacygevoelige informatie bij het doen van verzoeken aan, en bij het doorsturen van de gebruiker naar, een andere website. Gebruik de instelling ‘same-origin’, zodat de referrer-header alleen wordt meegestuurd bij verzoeken binnen het eigen domein. Dit voorkomt het lekken van privacygevoelige informatie bij omleiden naar externe domeinen. De striktere instelling ‘no-referrer’ kan ook worden gebruikt, zodat de referrer-header nooit wordt meegestuurd.