Overzicht streefbeeldafspraken en metingen informatieveiligheidstandaarden

Binnen de overheid zijn er adoptieafspraken over standaarden voor internetveiligheid en informatieveiligheid. Forum Standaardisatie meet ieder halfjaar de voortgang.

Over de afspraken

Op dit moment is de afspraak dat alle websites van de overheid een beveiligde verbinding moeten hebben en hiervoor moeten de standaarden HTTPS en HSTS (conform de richtlijnen van het NCSC) worden toegepast. Daarnaast dienen domeinnamen beveiligd te zijn met de standaard DNSSEC. Voor mail is de afspraak dat ter voorkoming van phishing de standaarden SPF, DKIM en DMARC worden ondersteund en dat voor het voorkomen van het afluisteren van mailverkeer de standaarden STARTTLS en DANE worden toegepast. Na het instellen van de mailstandaarden dienen DMARC en SPF vervolgens zodanig geconfigureerd te worden dat phishing van mail actief wordt bestreden.

Dit betekent dat voor deze standaarden niet het tempo van 'pas toe of leg uit' wordt gevolgd (i.e. wachten op een volgend investeringsmoment en dan de standaarden implementeren) maar dat actief wordt ingezet op implementatie van de standaarden op de korte termijn. Hieronder vindt u een overzicht van de gemaakte afspraken met een verwijzing naar de onderliggende notitie.

STREEFBEELD	WELKE STANDAARD GEADOPTEERD	VERWIJZING AFSPRAAK
EIND 2017 en verder	TLS/HTTPS: beveiligde verbindingen van websites DNSSEC: domeinnaambeveiliging SPF: anti-phishing van email DKIM: anti-phishing van email DMARC: anti-phishing rapportages	Streefbeeld afspraak voorgelegd mei 2015. Herbevestiging afspraak streefbeeld eind 2017.
EIND 2018	HTTPS en HSTS conform de NCSC richtlijn: beveiligde verbindingen van websites	Opname HTTPS en HSTS conform NCSC op de lijst inclusief de aanvulling van de streefbeeldafspraak Herbevestiging realisatiedatum in het Digiprogramma 2018.
EIND 2019	STARTTLS en DANE: encryptie van mailverkeer SPF en DMARC: het instellen van strikte policies voor deze emailstandaarden.	OBDO notitie: instemmen met aanvullende streefbeeld afspraak voor e-mailstandaarden

Wat is afgesproken

De afspraken over bovenstaande standaarden luiden als volgt:

Streefbeeldafspraak voor eind 2017:

- TLS wordt toegepast bij alle overheidswebsites waarbij burgers en of bedrijven gegevens moet invoeren, of waarbij gegevens vooringevuld zijn;
- DNSSEC wordt gebruikt voor elke domeinnaam waarmee een overheidsorganisatie met burgers en/of bedrijven communiceert
- DMARC, SPF en DKIM deze 'e-mail' standaarden worden toegepast voor alle ovverheidsdomeinnamen of deze nu wel of niet gebruik maken van mail.

Streefbeeldafspraak voor eind 2018:

- De afspraak is dat alle overheidswebsites HTTPS en HSTS inclusief de veilige configuratie conform NCSC uiterlijk eind 2018 hebben ingevoerd. Dit als aanvulling op de al bestaande adoptie-impuls van het Nationaal Beraad. Dit is herbevestigd in het Digiprogramma 2018 waar staat dat eind 2018 alle overheidswebsites voorzien zijn van HTTPS en HSTS.

Streefbeeldafspraak voor eind 2019:

- Voor eind 2019 is er een streefbeeldafspraak voor de adoptie en configuratie van een aantal IV-standaarden specifiek voor e-mail. (STARTTLS en DANE en SPF en DMARC).
- STARTTLS en DANE: standaarden voor de beveiliging van mailverkeer middels encryptie zodat derden niet kunnen meelezen.
- Het instellen van strikte policies voor SPF en DMARC. Zolang dat niet is ingesteld weet de ontvanger nog niet wat te doen met verdachte e-mail. De configuratie moet op orde zijn. *(Opm: Actieve policies zijn ~all en –all voor SPF, en p=quarantine en p=reject voor DMARC)*

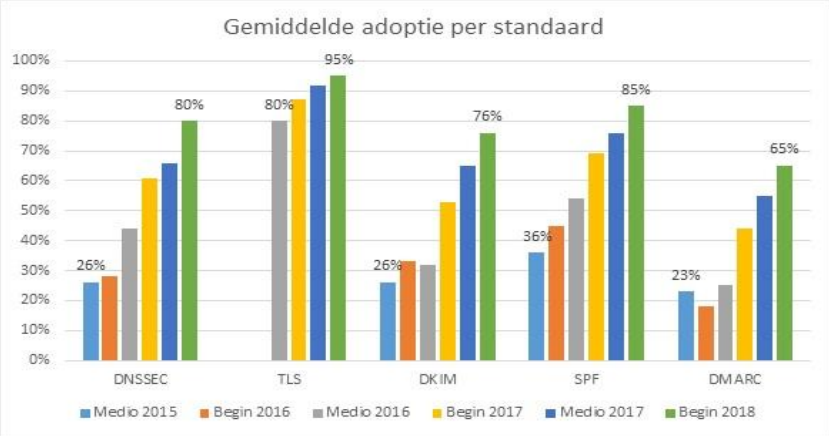
Over de meting

Forum Standaardisatie voert ieder halfjaar een meting uit op de implementatie van informatieveiligheidstandaarden bij overheidsorganisaties. Sinds 2015 biedt het Platform Internet Standaarden de mogelijkheid om via de website internet.nl domeinen te toetsten op het gebruik van internet- en veiligheidstandaarden die op de 'pas toe of leg uit' lijst van Forum Standaardisatie staan. In datzelfde jaar is Forum Standaardisatie gestart met een halfjaarlijkse meting van overheidsdomeinen op het voldoen aan deze standaarden.

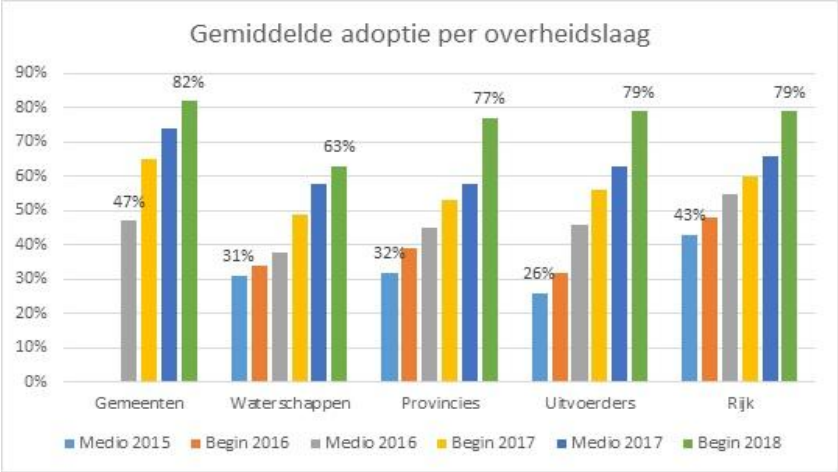
De metingen hebben ertoe geleid dat het Nationaal Beraad in mei 2015 en het OBDO in april 2018 de ambitie uitspraken om bovenstaande standaarden versneld te adopteren. Ieder half jaar wordt een nieuwe meting uitgevoerd. Januari 2018 was de eindmeting over de eerste streefbeeldafspraak over TLS, DNSSEC, SPF, DKIM en DMARC. Sinds april ligt de lat iet hoger en zijn de metingen uitgebreid met de nieuwe streefbeeldafspraken. De eerset meting conform de nieuwe afspraken is medio juli 2018.

Meetresultaten

De resultaten van de halfjaarlijkse metingen zijn te vinden op https://magazine.forumstandaardisatie.nl/nl_NL/overview.html Begin 2018 is de laatste meting uitgevoerd. De gemiddelde adoptiegraad was ten tijde van de eerste meting 35%, de laatste meting geeft een adoptiepercentage aan van ruim 80%.



Per overheidslaag uitgesplitst zien we het volgende:



Meer informatie over welke domeinen zijn getoetst en hoe de meting tot stand is gekomen kunt u vinden in ons magazine over de IV-meting. De laatste meting is te vinden op: https://magazine.forumstandaardisatie.nl/nl_NL/5425/79258/cover.html

Om welke domeinen gaat het?

In de IV meting toetsen we de volgende groepen domeinen:

• De domeinen van de overheidsorganisatie die direct of indirect vertegenwoordigd zijn in het OBDO, zoals Ministeries, uitvoerders (de Manifestpartijen), Gemeenten, Provincies en Waterschappen en partijen die behoren tot Klein LEF

•De domeinen die horen bij voorzieningen van de Generieke Digitale Infrastructuur.

•De meest bezochte domeinnamen van overheden (en uitvoerders), denk hierbij ook aan een domeinnaam als politie.nl

Zelf meten?

Wilt u zelf uw domeinnaam meten ga naar www.internet.nl. Wilt u uw domeinnaam getoetst zien worden in de IV-meting of heeft u hier vragen over, neem dan contact op via info@forumstandaardisatie.nl