> Retouradres Postbus 96810 2509 JE Den Haag

Demo Gemeente
T.a.v. de Gemeentesecretaris
Meneer J. Janssen
Postbus 101
3434 AB Demo Gemeente

Bureau Forum Standaardisatie

Bezoekadres:
Wilhelmina v Pruisenweg 52
2595 AN Den Haag

Postbus 96810
2509 JE Den Haag

www.forumstandaardisatie.nl
info@forumstandaardisatie.nl

Inlichtingen bij
Robin Gelhard

Datum	15 mei 2020
Betreft	Internetveiligheidrisico's voor gemeente Demo

Geachte meneer Janssen,

In het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO)[1] is afgesproken om met behulp van moderne internetveiligheidstandaarden websites en e-mail van overheidsorganisaties beter te beveiligen. Juist in de huidige onzekere tijden ligt cybercriminialiteit op de loer en is betrouwbare informatie nog noodzakelijker. Forum Standaardisatie monitort in opdracht van de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties de naleving van deze overheidsbrede afspraken en heeft daarbij als taak het delen van resultaten en aanspreken van achterblijvende partijen[2].

Forum Standaardisatie voert ieder halfjaar een meting uit onder overheidsorganisaties naar de implementatie van de afgesproken internetveiligheidstandaarden. Uw gemeente maakt onderdeel uit van onze metingen.

Uit onze laatste meting (maart 2020) van uw domein **demogemeente.nl** komen de volgende risico's naar voren:

- **Onveilige verbinding website:** uw organisatie loopt het risico dat criminelen uitgewisselde websitegegevens kunnen onderscheppen, afluisteren of manipuleren.
- **Onveilige verbinding e-mail:** uw organisatie loopt het risico dat criminelen e-mails kunnen onderscheppen, afluisteren of manipuleren.
- **Vatbaar voor e-mailvervalsing (spoofing):** risico dat criminelen uw overheidsdomeinen kunnen misbruiken als afzenddomein voor bijvoorbeeld phishingaanvallen.

In de tabel ziet u welke maatregelen in uw organisatie al dan niet zijn getroffen[3]:

Vertrouwelijkheid webverkeer				Vertrouwelijkheid e-mailverkeer			Voorkomen van e-mailvervalsing		
DNSSEC	TLS	HTTPS	HSTS	STARTTLS	DNSSEC	DANE	DKIM	DMARC	SPF

[1] Zie: https://www.digitaleoverheid.nl/governance-digitale-overheid/. In het OBDO zijn ook de gemeenten vertegenwoordigd.
[2] Zie: https://wetten.overheid.nl/BWBR0040727/2018-03-16.
[3] De afkortingen in de tabel betreffen standaarden die, mits goed geïmplementeerd, helpen om bovenstaande risico's te voorkomen.

Datum
15 mei 2020

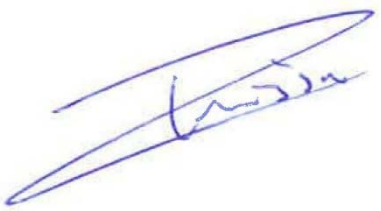
Het borgen van veilige informatie-uitwisseling tussen uw gemeente met burgers, bedrijven en medeoverheden is van belang voor de betrouwbaarheid van de (digitale) overheid. Vanwege de tweezijdigheid van deze informatie-uitwisseling liggen de risico's van misbruik niet alleen bij uw organisatie, maar ook bij partijen waar u digitaal mee communiceert. Uw organisatie heeft een zorgplicht naar burgers, bedrijven en medeoverheden om de digitale veiligheid op orde te brengen.

In de bijlage voorzien wij u van concreet advies om de geconstateerde risico's te (laten) mitigeren. Dit advies is opgemaakt met het meetinstrument Internet.nl[4], dat u helpt te testen of uw internet up-to-date is.

Slechts een deel van de overheidsorganisaties voldoet niet aan de internetveiligheidstandaarden, waaronder uw organisatie. Om ook volledig aan de afgesproken standaarden te kunnen voldoen is het van belang, dat u er bij uw dienstverlener op aandringt om de standaarden spoedig te implementeren. En daarbij vraagt om een concrete planning. Stap eventueel over naar een andere leverancier die wel voldoet aan de afgesproken standaarden.

Wanneer gaat u aan de slag de zwakke schakels in uw ICT te minimaliseren? Forum Standaardisatie hoort graag wanneer uw organisatie gaat voldoen en kan desgewenst advies geven. Heeft u hulp nodig? Of heeft u andere vragen? Laat het ons weten via info@forumstandaardisatie.nl of kijk op onze website forumstandaardisatie.nl.

Met vriendelijke groet,



Larissa Zegveld, Voorzitter Forum Standaardisatie

Bijlage: Advies informatieveiligheid voor uw domein, flyer 'Pas toe of leg uit'-lijst.

[4] Internet.nl is een initiatief van Platform Internetstandaarden (PLIS) dat een samenwerkingsverband is van partijen uit de internetgemeenschap en de Nederlandse overheid.

Bijlage 1: Advies informatieveiligheid voor het domein demogemeente.nl

Hieronder treft u een overzicht van hetgeen wij geconstateerd hebben met bijbehorende acties die u uit dient te laten voeren. Uw IT-dienstverlener kan hiermee aan de slag. Voor nadere technische informatie omtrent de constateringen kunt u de site testen op www.internet.nl.

Onveilige verbinding website: uw organisatie loopt het risico dat criminelen uitgewisselde websitegegevens kunnen onderscheppen, afluisteren of manipuleren.

Actie: Zorg ervoor dat de domeinnaam is ondertekend met een geldige DNSSEC-handtekening.
Een domeinnaamhouder kan met DNSSEC een digitale handtekening toevoegen aan DNS-informatie. Aan de hand van deze handtekening kan een internetgebruiker (onderwater en volledig automatisch m.b.v. speciale software) de inhoud en de ontvangen DNS-informatie
Actie: Zorg ervoor dat gebruik wordt gemaakt van HTTPS. En dat HTTPS veilig is geconfigureerd conform de 'ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) v2.0' van het Nationaal Cyber Security Centrum.
HTTPS zorgt voor het gebruik van HTTP over een met TLS beveiligde verbinding. Dit betekent dat het webverkeer door middel van een certificaat wordt versleuteld.

Actie: Zorg ervoor dat de webserver bezoekers automatisch doorverwijst van HTTP naar HTTPS op dezelfde domeinnaam (m.b.v. 301/302 redirect) óf dat deze ondersteuning biedt voor alleen HTTPS en niet voor HTTP.
HTTPS zorgt voor het gebruik van HTTP over een met TLS beveiligde verbinding. Dit betekent dat het webverkeer door middel van een certificaat wordt versleuteld.

Actie: Zorg ervoor dat gebruik wordt gemaakt van het HSTS beveiligingsmechanisme.
HSTS zorgt ervoor dat een webbrowser, na het eerste contact over HTTPS, bij vervolgbezoek de website altijd direct over HTTPS opvraagt. HTTPS zorgt voor het gebruik van HTTP over een met TLS beveiligde verbinding. Dit betekent dat het webverkeer door middel van een certificaat wordt versleuteld.

Onveilige verbinding e-mail: uw organisatie loopt het risico dat criminelen e-mails kunnen onderscheppen, afluisteren of manipuleren.

Actie: Zorg ervoor dat gebruik wordt gemaakt van STARTTLS en dat STARTTLS veilig is geconfigureerd conform de 'ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) v2.0' van het Nationaal Cyber Security Centrum.
STARTTLS maakt het mogelijk om SMTP-verkeer tussen mailservers over een met TLS versleutelde verbinding te laten lopen. Dit betekent dat het mailverkeer door middel van een certificaat wordt versleuteld.

Actie: Zorg ervoor dat de domeinnaam van de mailserver is ondertekend met een geldige DNSSEC- handtekening.
Een domeinnaamhouder kan met DNSSEC een digitale handtekening toevoegen aan DNS-informatie. Aan de hand van deze handtekening kan een internetgebruiker (onderwater en

volledig automatisch m.b.v. speciale software) de inhoud en de ontvangen DNS-informatie valideren. Hierdoor is met grote waarschijnlijkheid vast te stellen dat het antwoord van de DNS onderweg niet is gemanipuleerd door derden.

Actie: Zorg ervoor dat de mailserver DANE toepast.
DANE, dat voortbouwt op DNSSEC, geeft zekerheid over de identiteit van de ontvangende mailserver. Dit voorkomt dat een aanvaller zich kan uitgeven als ontvangende-mailserver, waardoor hij het mailverkeer kan onderscheppen. Daarnaast dwingt DANE het gebruik van TLS af. Dit voorkomt dat een aanvaller de opzet van STARTTLS kan blokkeren, om zo toegang tot de onversleutelde berichten te krijgen.

Vatbaar voor e-mailvervalsing (spoofing): risico dat criminelen uw overheidsdomeinen kunnen misbruiken als afzenddomein voor bijvoorbeeld phishingaanvallen.

Actie: Zorg ervoor dat DKIM wordt toegepast.
DKIM is een techniek waarmee e-mailberichten kunnen worden gewaarmerkt. Het gebruik van DKIM verkleint de kans op misbruik van e-mailadressen doordat ontvangers betrouwbaar echte e-mails van phishingmails of spam kunnen onderscheiden. Ook kunnen ontvanger
Actie: Zorg ervoor dat DMARC wordt toegepast en dat de syntax van het DMARC-record correct is en dat deze een voldoende strikte policy bevat (p=quarantine of p=reject) om misbruik van het domein door phishers en spammers tegen te gaan. Het is van belang dat een strikt DMARC-beleid stapsgewijs wordt ingevoerd om te voorkomen dat deze e-mails onterecht als spam worden gemarkeerd of niet meer aankomen. Forum Standaardisatie biedt een handreiking aan in de vorm van een stappenplan om tot een strikt DMARC-beleid te komen (zie onze website bij DMARC-standaard).
DMARC is een techniek om valse e-mails of SPAM tegen te gaan. DMARC maakt het mogelijk om beleid in te stellen over de manier waarop een e-mailprovider om moet gaan met e-mail waarvan niet kan worden vastgesteld dat deze afkomstig is van het vermelde afzenderdomein. Hierdoor kunnen organisaties voorkomen dat anderen e-mails versturen namens het e-maildomein van de organisatie. Mogelijk zijn er externe partijen die legitieme mailings met uw internetdomein als afzender versturen.