Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Voorzitter van de Tweede Kamer der Staten-Generaal

Postbus 20018

2500 EA Den Haag

DGDOO/DS

Kenmerk
2022-0000679272

Uw kenmerk
2022-0000254001

Datum	23 december 2022
Betreft	Beantwoording Kamervraag lid Van Ginneken (D66) over het bericht ''Kritiek op niet naleven securityregels overheidswebsites: ''geen rocketscience''''.

Hierbij bied ik u, mede namens de minister van Justitie en Veiligheid, de beantwoording aan op de schriftelijke vragen die zijn gesteld door de het lid Van Ginneken (D66) over het bericht 'Kritiek op niet naleven securityregels overheidswebsites: 'geen rocketscience'''. Deze vragen zijn ingezonden op 30 november 2022 met kenmerk 2022Z23575.

De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties
Digitalisering en Koninkrijksrelaties

Alexandra C. van Huffelen

2022Z23575
(Ingezonden op 30 november 2022)

Vragen van het lid Van Ginneken (D66) aan de minister van Justitie en Veiligheid en de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties over het bericht 'Kritiek op niet naleven securityregels overheidswebsites: 'geen rocketscience''.

Vraag 1
Klopt het bericht dat de helft van de domeinnamen van de Rijksoverheid niet voldoet aan verplichte securitystandaarden? [1]

Antwoord
Ja.

Forum Standaardisatie meet twee keer per jaar in hoeverre een set internetdomeinen van de overheid voldoet aan de relevante informatieveiligheidsstandaarden van de 'pas toe of leg uit'-lijst. Over de gemeten standaarden zijn implementatieafspraken met een deadline gemaakt: de zogenoemde 'streefbeeldafspraken'. Uit de meest recente meting blijkt dat de helft, 50%, van alle Rijksoverheid- domeinnamen voldoet aan de streefbeeldafspraken voor webdomeinen.

De internetdomeinen van de overheid moeten aan **al** deze standaarden voldoen, en deze moeten ook nog correct geconfigureerd zijn om mee te tellen in het percentage dat geheel voldoet. De toepassing van deze standaarden is primair de verantwoordelijkheid van iedere overheidsorganisatie zelf en het niet volledig voldoen kan ook als reden hebben dat de standaarden onjuist zijn geconfigureerd.

Vraag 2
Klopt het bericht dat minder dan de helft voldoet aan de verplichte e-mailstandaarden?

Antwoord
Nee. Uit de meest recente meting blijkt inderdaad dat e-mailstandaarden achterblijven, maar beter presteren dan webstandaarden bij de Rijksoverheid. 55% van de Rijksoverheid voldeed aan de e-mailstandaarden. Ik vind het onacceptabel dat overheden dit niet op orde hebben en zal per brief, via de koepelorganisaties[1], alle overheden oproepen zo snel mogelijk de standaarden te implementeren.

Vraag 3
Hoe verklaart u het niet voldoen aan deze minimale verplichtingen gezien dit al in 2019 en 2021 had moeten plaatsvinden? Mede omdat het hier vaak om niet hele

1 Voorzitter van de Tweede Kamer der Staten-Generaal

Postbus 20018

2500 EA Den Haag

ingewikkelde technische ingrepen gaat die belangrijk zijn voor onze digitale veiligheid?

Antwoord
Of de adoptie van de standaarden ingewikkeld is, verschilt per standaard, maar ook per wijze waarop ICT bij een organisatie is ingeregeld. Zo is bijvoorbeeld de adoptie (en 'strenge' configuratie) van de anti-email-phishing standaard DMARC[2] ingewikkelder, wanneer meerdere externe partijen namens die organisatie mail versturen (bijv. ten behoeve van mailinglijsten en enquêtes). Ook zijn veel organisaties afhankelijk van hun externe leverancier. Zo biedt de meest gebruikte cloudmail-provider van de overheid default geen IPv6[3] en geen DANE[4]. Voor het Rijk is Strategisch Leveranciersmanagement Microsoft, Google Cloud en Amazon Web Services (SLM), belegd binnen het ministerie van Justitie en Veiligheid (JenV), verantwoordelijk voor de communicatie met de leveranciers. JenV vraagt samen met Forum Standaardisatie al sinds 2019 aandacht voor de implementatie van de standaarden. De implementatie van deze standaarden is door Microsoft steeds in tijd opgeschoven. SLM en Forum Standaardisatie hebben Microsoft opnieuw gewezen op de verplichting voor de Nederlandse Overheid deze standaard toe te passen en hebben Microsoft gevraagd de huidige ultieme invoerdatum van juli 2023 hoe dan ook te garanderen.

Het blijft belangrijk dat overheden hun leverancier aanspreken op tekortkomingen en zo nodig overstappen naar een leverancier die de standaard wel goed ondersteunt. Maar ook bij ingewikkelder implementatie is adoptie zeker mogelijk, getuige het groot aantal organisaties dat hun internetdomeinen wel binnen het afgesproken tijdspad op orde heeft gebracht. Ik verwacht dan ook van alle organisaties dat ze alsnog aan de regels gaan voldoen.

Vraag 4
Welke rol speelt het tekort aan IT'ers bij de Rijksoverheid om te voldoen aan de implementatie van verplichte securitystandaarden? Welke andere oorzaken ziet u?

Antwoord
Het tekort aan IT'ers bij de Rijksoverheid speelt in zekere zin een rol om te voldoen aan de implementatie van verplichte securitystandaarden. Ook het Rijk heeft namelijk te maken met een tekort aan IT'ers en dat draagt bij aan het tijdig handelen. Echter kunnen we niet causaal vaststellen dat een tekort aan IT'ers bijdraagt aan het niet voldoen aan de gemaakte afspraken. Zoals onder vraag 3 toegelicht, kunnen andere oorzaken ook bijdragen aan een onvoldoende toepassing van de standaarden zoals afhankelijkheid van externe leveranciers en/of een gebrekkig domeinbeleid.

---

2 DMARC (Domain-based Message Authentication, Reporting and Conformance) is een verificatieprotocol voor e-mail.

3 Internet Protocol versie 6 (IPv6) maakt communicatie van data tussen ICT-systemen binnen een netwerk, zoals internet, mogelijk. De standaard bepaalt dat ieder ICT-systeem binnen het netwerk een uniek nummer (IP-adres) heeft.

4 DANE staat voor DNS-based Authentication of Named Entities en is een protocol voor het veilig publiceren van publieke sleutels en certificaten.

Vraag 5
Hoe beoordeelt u het feit dat pas 55% van de provincies alle anti-phishingstandaarden volledig geadopteerd heeft en 81% van de gemeentes? Hoe gaat u ervoor zorgen dat ook lagere overheden voldoen aan hun verplichtingen voor een veilige digitale omgeving?

Antwoord
Ik blijf mij inzetten voor een veilige en betrouwbare overheid op het internet. In de beantwoording van Kamervragen over cookies op overheidswebsites[5] van 1 november jl., heb ik aangekondigd medeoverheden en rijksoverheidsorganisaties per brief te wijzen op het belang te voldoen aan geldende wet- en regelgeving. In diezelfde brief zal ik eveneens aandacht vragen voor de implementatie van de informatieveiligheidsstandaarden.
Die brief bied ik aan de Vereniging van Nederlandse Gemeenten, het Interprovinciaal Overleg, de Unie van Waterschappen, de CIO Rijk, de Manifestgroep en Klein Lef aan. In die brief spreek ik de diverse overheden aan op hun verantwoordelijkheid om zich te houden aan de gemaakte afspraken. Indien een overheidsorganisatie het IT-beheer heeft uitbesteed, is het van belang de ICT-dienstverlener formeel te verzoeken om ondersteuning van de betreffende standaarden, en daarbij te wijzen op beschikbare how-to's en te vragen om een concrete planning.
Als de huidige leverancier te weinig medewerking verleent, moeten overheden overwegen om over te stappen naar een leverancier die wel voldoet aan de afgesproken standaarden. Om geschikte leveranciers te vinden kan informatie uitgewisseld worden met collega-overheden die leveranciers hebben die wel de afgesproken standaarden ondersteunen.

Vraag 6
Met het oog op het principe van ‘goed voorbeeld doet goed volgen’, acht u het pijnlijk als verantwoordelijk minister dat het ministerie van Justitie en Veiligheid op dit moment het minst goed aan deze standaarden voldoet? Wanneer verwacht u dit opgelost te hebben?

Antwoord
Het is belangrijk dat het ministerie van JenV zo spoedig mogelijk voldoet aan de verplichte open informatieveiligheiddstandaarden van Forum Standaardisatie. Na het kerstreces wordt uw Kamer door de minister van JenV geïnformeerd over de termijn waarop de standaarden zijn geïmplementeerd. Deze implementatie en het beheer van e-mail-en webdomeinen moet in de ICT-agenda’s van de JenV-onderdelen worden gepland. Domeinbeheer is noodzakelijk opdat het ministerie van JenV blijft voldoen aan deze standaarden.

[1] AG Connect, 25 november 2022, Kritiek op niet naleven securityregels overheidswebsites: ‘geen rocketscience’ (https://www.agconnect.nl/artikel/kritiek-op-niet-naleven-securityregels-

5 Tweede Kamer der Staten-Generaal, 2021-2022, 2022Z14322

overheidswebsites-geen-rocketscience)