Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2023–2024

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

1891

Vragen van het lid **Kathmann** (GroenLinks-PvdA) aan de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties over *de slechte beveiliging van gemeentelijke websites:* (ingezonden 5 maart 2024).

Antwoord van Staatssecretaris **Van Huffelen** (Binnenlandse Zaken en Koninkrijksrelaties) (ontvangen 3 juni 2024). Zie ook Aanhangsel Handelingen, vergaderjaar 2023–2024, nr. 1350.

Vraag 1
Kent u het bericht «Duizenden «vergeten» gemeentelijke websites in ontluisterende staat»?[1]

Antwoord 1
Ja, ik heb hier kennis van genomen.

Vraag 2
Deelt u de mening dat het zeer onwenselijk is dat van de 10.000 gemeentelijke websites slechts 28 procent aan de voor overheden verplichte beveiligingsstandaarden voldoet? Zo ja, waarom? Zo nee, waarom niet?

Antwoord 2
Ja, het is onwenselijk dat gemeentelijke websites niet voldoen aan de voor de overheden verplichte beveiligingsstandaarden. Uit de meest recente Meting Informatieveiligheidstandaarden overheid van Forum Standaardisatie blijkt echter dat 54% procent van de gemeentelijke websites voldoen aan de veiligheidsstandaarden[2]. Overheden hebben de verantwoordelijkheid richting de burger om online overheidsinformatie en diensten transparant, toegankelijk, betrouwbaar en veilig aan te bieden. Overheden hebben daarbij een voorbeeldfunctie als het gaat om de informatiebeveiliging. Een veilige website is daar onderdeel van.
Daarbij hoort onder meer dat overheden alle websites beveiligen volgens de wettelijke verplichte standaarden (Wdo)[3], en de informatieveiligheidsstandaarden van de «pas-toe-of-leg-uit»-lijst van het Forum Standaardisatie toepassen,

[1] Binnenlands Bestuur, 29 februari 2024, Duizenden «vergeten» gemeentelijke websites in ontluisterende staat (binnenlandsbestuur.nl).
[2] Meting Informatieveiligheidstandaarden overheid medio 2023 (forumstandaardisatie.nl)
[3] *Stb.* 2023, 179 | Overheid.nl

ah-tk-20232024-1891
ISSN 0921 - 7398
's-Gravenhage 2024

zoals ook is toegelicht in de beantwoording op eerdere Kamervragen.[4]
Overheden hebben zichzelf met het gezamenlijke beveiligingsnormenkader voor de gehele overheid, de Baseline Informatiebeveiliging Overheid (BIO), verplicht hun informatiesystemen, waaronder websites, te beveiligen. In de BIO wordt benadrukt dat de overheid de standaarden volgt die op de «pas toe of leg uit»-lijst van het Forum Standaardisatie staan.

Vraag 3
Deelt u de mening dat ook bij vergeten of niet meer gebruikte websites er wel degelijk een gevaar kan ontstaan dat in het geval die websites niet aan de verplichte veiligheidsstandaarden voldoen ze misbruikt kunnen worden om andere delen van een gemeentelijk netwerk binnen te dringen en daar schade te veroorzaken? Zo ja, waarom? Zo nee, waarom niet?

Antwoord 3
Ja, om websites veilig te houden moeten ze continu beheerd worden. Zodra websites niet meer beheerd worden ontstaat een grotere kans op misbruik van de website. Dat betekent dat een website bijvoorbeeld gebruikt kan worden door een kwaadwillende om zich voor te doen als een overheid, data te lekken of malware te verspreiden. Wat het exacte risico is bij het niet naleven van een standaard hangt af van de situatie en kan per website verschillen.

Vraag 4
Deelt u de mening dat overheden een voorbeeldfunctie hebben ook als het gaat om de beveiliging van websites en het nakomen van regels dienaangaande? Zo ja, wat gaat u doen om ervoor te zorgen dat gemeenten die voorbeeldfunctie gaan waarmaken? Zo nee, waarom niet?

Antwoord 4
Ja, overheden hebben een voorbeeldfunctie als het gaat om de beveiliging van websites en het volgen van de standaarden.
In opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties meet het Forum Standaardisatie halfjaarlijks de implementatie van de standaarden. Zoals ik in mijn Kamerbrief Digitalisering december 2023[5] heb toegelicht, blijkt uit de meest recente meting Informatieveiligheidstandaarden overheid medio 2023[6] dat 54% van de gemeten gemeentelijke websites voldoet aan de afgesproken websitestandaarden voor veilig en modern webverkeer (exclusief IPv6 en RPKI). Terwijl uit de meting blijkt dat gemeenten het beter doen dan in 2022 is er nog steeds een groep achterblijvers en volgt uit de meting dat er relatief slecht zicht is op domeinnamen van decentrale overheden.
In het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) zijn afspraken gemaakt tussen het Rijk, VNG, IPO en UvW om te sturen op de voortgang en knelpunten om zo per overheidsorganisatie de adoptie te versnellen. De voortgang zal twee keer per jaar geagendeerd worden in het OBDO.
Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties zet zich ook in voor beter domeinportfoliobeheer. Portfoliobeheer draagt niet alleen bij aan de veiligheid van een website, maar ook bij aan het naleven van wet- en regelgeving voor digitoegankelijkheid en het voorkomen van online tracking. In dit kader werkt het ministerie aan het Register Internetdomeinen Overheid (RIO). Vanaf eind 2023 zijn in het RIO de publieke internetdomeinen van de rijksoverheid geregistreerd. In 2024 krijgen medeoverheden de mogelijkheid hun (publieke) portfolio aan internetdomeinen op deze centrale plek vast te leggen. Het register kan gebruikt worden om te beoordelen of je te maken hebt met een overheidswebsite of niet.
Daarnaast steun ik het initiatief op basisbeveiliging.nl van de Internet Cleanup Foundation (ICF). Op deze website is met open data voor iedereen in te zien wat de stand is van de publiek meetbare digitale beveiliging van websites van overheidsorganisaties. Organisaties kunnen zich hieraan spiegelen en

---

[4] *Aanhangsel Handelingen II* 2022/23, 1167
[5] *Kamerstukken II* 2022/2023, 26 643, nr. 1112.
[6] Meting Informatieveiligheidstandaarden overheid medio 2023 (forumstandaardisatie.nl)

optrekken. ICF houdt ook regelmatig bijeenkomsten om te kijken welke websites van de overheid nog niet geïndexeerd zijn.
Om samen te werken aan een veiligere digitale samenleving vind ik het van belang dat beveiligingsonderzoekers kwetsbaarheden melden bij de desbetreffende overheidsorganisatie. Onbeheerde websites vallen daar ook onder. Onderzoekers kunnen de contactgegevens en afspraken vinden in een zogenaamde security.txt. Dit bestand moet verplicht publiek worden gepubliceerd. Daarnaast kunnen meldingen voor gemeenten ook direct gedaan worden via de Informatiebeveiligingsdienst (IBD).

Vraag 5
Deelt u de mening dat het onwenselijk is dat een van de redenen dat gemeenten laks omspringen met (de beveiliging van) vergeten of niet gebruikte websites is dat er niet gehandhaafd wordt op beveiligingseisen? Zo ja, wat gaat u doen om ervoor te zorgen dat er gehandhaafd wordt? Zo nee, waarom niet?

Antwoord 5
Het is onwenselijk dat gemeenten nog niet voldoen aan de verplichte beveiligingseisen. Zeker wanneer overheidsorganisaties niet aan de wettelijke verplichte veiligheidstandaarden voldoen. Zoals aangegeven in beantwoording van vraag 7 zijn gemeentes bezig met het implementeren van de standaarden. Vanuit het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties wordt hierop gemonitord[7] door een meting van het Forum Standaardisatie. In het kader van de Wet digitale overheid (Wdo) ben ik aan het verkennen hoe het toezicht op de wettelijke verplichte standaarden steviger kan worden ingericht. Door het niet toepassen van verplichte standaarden, lopen overheidsorganisaties een beveiligingsrisico.

Vraag 6
Wat gaat de Network and Information Security Directive (NIS2) voor gemeenten betekenen als het om de beveiliging van hun websites gaat? Hoeveel gemeenten voldoen nu al aan die richtlijn? Hoe groot acht u de kans dat gemeenten eind 2024 nog niet voldoen aan de NIS2? En wat zijn de gevolgen daarvan?

Antwoord 6
In lijn met bestaande toepassing van de Baseline Informatiebeveiliging Overheid (BIO), gaat de NIS2-richtlijn uit van de verantwoordelijkheid van organisaties zelf, zoals gemeenten, om passende en evenredige maatregelen te nemen voor het beveiligen van netwerk- en informatiesystemen. Waar de BIO zelfregulering is, leidt de toekomstige Cybersecuritywet (de implementatiewet van NIS2) tot een wettelijk verplichte zorgplicht.
Overheden, waaronder gemeenten, worden met de Cybersecuritywet verplicht om significante incidenten te melden bij het CSIRT en de toezichthouder. Ook kunnen gemeenten op vrijwillige basis incidenten die niet kwalificeren als significant, bijna-incidenten en cyberdreigingen melden bij het CSIRT. Deze incidenten en dreigingen kunnen gerelateerd zijn aan websites.
Tevens verplicht de Cybersecuritywet onafhankelijk toezicht. Voor de sector overheid is stelseltoezicht op informatieveiligheid nieuw. Het gegeven dat er toezicht komt, geeft overheidsorganisaties een extra prikkel om informatieveiligheid procesmatig in te richten. De beoogde toezichthouder voor NIS2 bij de overheid is de Rijksinspectie voor Digitale Infrastructuur (RDI) en zal beschikken over handhavingsbevoegdheden.
Het is tot slot niet goed mogelijk om betekenis te geven aan de vraag in hoeverre gemeenten voldoen aan NIS2 en de kans dat gemeenten eind 2024[8] nog niet voldoen aan de NIS2. Gemeenten passen immers momenteel de Baseline Informatiebeveiliging Overheid (BIO) toe binnen hun organisaties. Dit doen zij op basis van risicoafweging, passend bij hun eigen specifieke

[7] HTTPS en HSTS nulmeting op 1 juli 2023 (digitaleoverheid.nl)
[8] De implementatie van de NIS2 richtlijn via de Cyberbeveiligingswet heeft overigens vertraging opgelopen. De Minister van Justitie en Veiligheid heeft uw Kamer hierover op 31 januari jongstleden bericht. Zie *Kamerstukken II* 2023/24, 22 112, nr. 3868

situatie, en kan dus verschillen per gemeente. In deze aanpak is informatiebeveiliging geen einddoel, maar een continu proces waarin risicoanalyses worden geactualiseerd en maatregelen worden bijgesteld. Informatiebeveiliging is en blijft een cyclisch proces.

Vraag 7
Wat gaat u in overleg met gemeenten doen om ervoor te zorgen dat slecht beveiligde gemeentelijke websites die niet meer gebruikt worden uit de lucht worden genomen of beter beveiligd gaan worden? Kunt u de Kamer voor het komend zomerreces laten weten welke stappen er gezet zijn of gaan worden?

Antwoord 7
Samen met de VNG en IBD zorgen wij voor continue aandacht voor het goed beheren van websites. Zie ook de beantwoording op vraag 2 t/m 6 over de verschillende stappen die ik neem om overheidsorganisaties, waaronder ook gemeenten vallen, te ondersteunen in de toepassing van veiligheidstandaarden en het verbeteren van hun domeinportfoliobeheer.
Verder informeert de VNG-Informatiebeveiligingsdienst IBD gemeenten dagelijks over kwetsbaarheden en dreigingen en adviseert en ondersteunt op informatiebeveiligingsvraagstukken. De IBD monitort de websites en IT-infrastructuur van gemeenten en levert informatie over kwetsbaarheden direct, automatisch, door. Afhankelijk van de ernst neemt de IBD direct contact op met de gemeente. In april 2024 is de monitoringtool na een pilotfase uitgerold naar alle gemeenten.[9] De gemeenten hebben zelf ook toegang tot het portaal in de tool. Deze dienstverlening van de IBD is een aanvulling op de interne logging, monitoring en detectie door gemeenten zelf. Gemeenten kunnen hierbij onder andere gebruik maken van de monitoring en response diensten uit de raamcontracten die door VNG zijn afgesloten met diverse aanbieders.[10] Met de halfjaarlijkse Informatieveiligheidmeting van het Forum Standaardisatie worden de gemeenten periodiek extra geattendeerd, specifiek op websites, portalen en mailvoorzieningen.
Ik blijf uw Kamer ook informeren over deze stand van zaken. In de Verzamelbrief Waardengedreven Digitaliseren Q3 zal ik u informeren over de volgende halfjaarlijkse meting Informatieveiligheidstandaarden van het Forum Standaardisatie.

[9] Start monitoring External Attack Surface gemeenten – Informatiebeveiligingsdienst
[10] Raamovereenkomsten Monitoring & Response definitief gegund | VNG