Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

Aanhangsel van de Handelingen

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

3468

Vragen van het lid **Van Baarle** (DENK) aan de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties over *de huidige stand van zaken met betrekking tot de digitale beveiliging van overheidswebsites in Nederland* (ingezonden 14 juni 2021).

Antwoord van Staatssecretaris **Knops** (Binnenlandse Zaken en Koninkrijksrelaties) (ontvangen 5 juli 2021).

Vraag 1
Bent u bekend met het nieuwsbericht «Tientallen websites overheid voldoen niet aan veiligheidsrichtlijnen» van de NOS?[1]

Antwoord 1
Ja

Vraag 2, 8
Wat vindt u van het feit dat tientallen websites van de overheid, waaronder websites van de Belastingdienst, GGD's, veiligheidsregio's en waterschappen, niet voldoen aan de richtlijnen voor digitale beveiliging?
Bent u bekend met het feit dat de richtlijnen van het NCSC adviseren om de openbare pagina en de plek waar beheerders in kunnen loggen strikt van elkaar te scheiden? Wat gaat u hiermee doen?

Antwoord 2, 8
Voor de beveiliging van websites bij de overheid hanteren overheden bij het Rijk, provincies, waterschappen en gemeenten een basisnormenkader voor informatiebeveiliging. Het basisnormenkader is de Baseline Informatiebeveiliging Overheid (BIO)[2], die sinds januari 2019 van kracht is. De BIO stelt (in deel 1) dat voorafgaand aan het gebruik van een informatiesysteem een risicoafweging dient te worden gemaakt die vervolgens richtinggevend is voor het treffen van beveiligingsmaatregelen. Proportionaliteit is daarbij het uitgangspunt. Met andere woorden: gaat het om zeer vertrouwelijke informatie, dan worden andere afwegingen gemaakt dan wanneer het om openbare informatie gaat waarvan de beschikbaarheid belangrijk is.

[1] https://nos.nl/artikel/2384235-tientallen-websites-overheid-voldoen-niet-aan-veiligheidsrichtlijnen
[2] *Stcrt.* 2019, nr. 26526.

ah-tk-20202021-3468
ISSN 0921 - 7398
's-Gravenhage 2021

Het Nationaal Cybersecurity Centrum (NCSC) publiceert regelmatig adviezen in de vorm van richtlijnen. Ik ben hiermee bekend. Specifiek met betrekking tot deze zaak is dat de richtlijn «ICT beveiligingsrichtlijnen voor webapplicaties».[3] Voor de overheid kan deze richtlijn worden beschouwd als een nadere detaillering van de BIO voor het onderdeel webapplicaties.
Uiteindelijk is het resultaat dat een samenhangend pakket van maatregelen wordt vastgesteld en toegepast. Welke dat zijn, zal per geval verschillen. Dat is overigens niet vrijblijvend: over de staat van informatieveiligheid leggen de verschillende overheidsorganen verantwoording af aan hun controlerende organen, zoals Gemeenteraad, provinciale staten, etc.
Kortom, het is aan overheidsorganisaties om door het treffen van de verplichte maatregelen uit de BIO en aanvullende maatregelen, voortvloeiend uit een risicoafweging te bepalen hoe Wordpress veilig kan worden ingezet.

Vraag 3
Erkent u dat de overheid tekort heeft geschoten in het treffen van digitale beveiligingsmaatregelen tegen eventuele hackers?

Antwoord 3
Dat beeld deel ik niet, zie ook het antwoord onder vraag 2.

Vraag 4
Deelt u de mening dat de burgers erop zouden moeten kunnen vertrouwen dat overheden als de Belastingdienst, GGD's, veiligheidsregio's en waterschappen, vertrouwelijk en verantwoord met gevoelige gegevens omspringen? Zo nee, waarom niet?

Antwoord 4
Ik deel volledig uw mening dat de overheid vertrouwelijk en verantwoord met gevoelige gegevens moet omgaan. Burgers moeten ervan uit kunnen gaan dat de overheid zorgvuldig omgaat met hun gegevens.

Vraag 5
Deelt u de mening dat een overheidsorgaan pas aan (gevoelige) persoonsgegevensverzameling zou mogen doen als het de risico's voor de beveiliging van de informatie in kaart heeft gebracht en de digitale beveiliging afdoende is? Zo nee, waarom niet?

Antwoord 5
Ja.

Vraag 6
Bent u bekend met het feit dat het National Cyber Security Centrum (NCSC) als sinds 2014 waarschuwt voor 36 veiligheidsrisico's van Wordpress en dat desondanks 165 openbare overheidswebsites op Wordpress draaien? Wat is met deze waarschuwingen gedaan?

Antwoord 6
Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) is bekend met de meldingen van het NCSC. Bij de overheid worden de meldingen van het NCSC nauwlettend in de gaten gehouden door afzonderlijke overheidsorganisaties. De BIO stelt eisen aan het toepassen van (beveiligings)patches voor ernstige kwetsbaarheden in hard- en software. Overheidsorganisaties zijn zelf verantwoordelijk voor het toepassen van deze eisen. Bovendien zijn kwetsbaarheidswaarschuwingen aan de orde van de dag en worden die voor veel systemen gestuurd. Ik heb niet het beeld dat de hoeveelheid bekende kwetsbaarheden een exacte maatstaf is om de veiligheid van een product te beoordelen. Er spelen ook andere factoren mee zoals de aard, omvang en frequentie van onderzoeken naar een product.

[3] https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties

Vraag 7
Bent u bekend met het feit dat ook de website van de Informatiebeveiligingsdienst (IBD), dat gemeenten helpt bij cyberincidenten, draait op Wordpress? Wat vindt u hiervan?

Antwoord 7
Het is bekend bij het Ministerie van BZK dat de publieke website van de IBD, het Computer Emergency Response Team (CERT) van de Nederlandse gemeenten, draait op Wordpress. Voor de volledigheid meldt de Vereniging van Nederlandse Gemeenten (VNG) het Ministerie van BZK dat de beheeromgeving van deze website niet publiek is. De website van de IBD voldoet aan de eisen die de BIO daaraan stelt. De publieke website van de IBD ontsluit openbare informatie. Voor informatie met een hoger beschermingsniveau gebruikt de IBD andere middelen. Dit doet de IBD op basis van een uitgevoerde risicoanalyse, zoals ook de BIO voorschrijft. Verder voert de IBD periodiek penetratietesten uit op haar systemen, waaronder de website en op basis van de resultaten treft de IBD waar nodig maatregelen. Ik zie daarom geen bezwaar tegen het gebruik van individuele softwarepakketten, zoals Wordpress, als risicoafwegingen zijn gemaakt en maatregelen zijn getroffen.

Vraag 9
Bent u bereid om zo snel mogelijk de in de media genoemde overheidssites te laten voldoen aan de veiligheidseisen?

Antwoord 9
Gezien mijn beantwoording onder de gestelde vragen onder 2 t/m 8 is dat niet aan de orde. Het is de verantwoordelijkheid van elke organisatie zelf om de BIO, de verplichte overheidsmaatregelen en op basis van risicoafweging aanvullende maatregelen te implementeren.

Vraag 10
Welke beleidsmatige inspanningen wilt u verder doen om de digitale weerbaarheid van de overheidswebsites te vergroten?

Antwoord 10
In zijn algemeenheid geldt dat de overheid naast de verplichte maatregelen uit de BIO, diverse open standaarden implementeert zoals informatieveiligheidsstandaarden. De adoptie van deze informatieveiligheidsstandaarden wordt halfjaarlijks gemeten. Halverwege 2020 zijn achterblijvende overheidsorganisaties aangeschreven door het Forum Standaardisatie met adviezen ter verbetering.[4] De toepassing van de overige open standaarden van de «pas-toe-of-leg-uit» lijst van het Forum Standaardisatie wordt jaarlijks gemeten. De meest recente versie van deze Monitor Open standaarden 2020 is op 18 maart aangeboden aan uw Kamer.[5] Het beeld is dat het gebruik van de verplichte open standaarden verder toeneemt.
De wijze waarop in het algemeen het informatieveiligheidsbeleid bij de overheid gestalte krijgt, heb ik aan uw Kamer gemeld op 18 maart jl.[6] in de voortgangsbrief informatieveiligheid bij de overheid.

[4] De meting van de informatieveiligheidsstandaarden van september 2020 is te vinden op https://www.digitaleoverheid.nl/nieuws/beveiliging-internetdomeinen-overheid-vereist-voortdurende-aandacht/
[5] De monitor Open Standaarden, inclusief de informatieveiligheidsstandaarden, van september 2020 is te vinden op https://www.forumstandaardisatie.nl/publicaties/overige-publicaties
[6] *Kamerstuk* 26 643, nr. 749