Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties

Aan de Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA Den Haag

www.rijksoverheid.nl
www.facebook.com/minbzk
www.twitter.com/minbzk
www.linkedin.com/company/ministerie-van-bzk

Kenmerk
2021-0000337059

Uw kenmerk
2021Z10260

Datum	6 juli 2021
Betreft	Verzoek van de vaste Kamercommissie voor Digitale Zaken om een reactie op het bericht 'Overheden negeren basale beveiligingsregels, tientallen websites gevoelig voor hacks'

Tijdens de procedurevergadering van de vaste commissie voor Digitale Zaken van de Tweede Kamer op 9 juni jl. is verzocht om een reactie op het bericht van Trouw over "Overheden negeren basale beveiligingsregels, tientallen websites gevoelig voor hacks". Deze brief bevat de gevraagde reactie.

Ik vind het van groot belang dat informatieveiligheid goed is geregeld en dat burgers en inwoners veilig hun zaken kunnen doen met de digitale overheid. Het artikel van Trouw stelt dat publieke webpagina's, waarin je een gebruikersnaam en wachtwoord moet invullen, de hele wereld toegang verschaffen tot de inlogpagina's voor het beheer van websites. Daarmee zou het de kans vergroten dat kwaadwillenden kunnen inbreken.

Kaders en richtlijnen
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)[1], dat 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. Uiteindelijk is het resultaat dat een samenhangend pakket van maatregelen wordt vastgesteld en toegepast. Dat is niet vrijblijvend. Over de staat van informatieveiligheid leggen de verschillende overheidsorganen verantwoording af aan hun controlerende organen, zoals Gemeenteraad, Provinciale Staten, etc.

Onderdeel van het pakket van maatregelen zijn acties die altijd moeten worden toegepast (BIO, deel 2). Een tweetal daarvan biedt een belangrijke bijdrage aan de veiligheid van publieke webpagina's waarin je een gebruikersnaam en

1 Stcrt. 2019, nr. 26526.

wachtwoord moet invullen. Dat zijn het verplichte gebruik van tweefactorauthenticatie. Als dat niet aan de orde is, dan worden eisen gesteld aan de complexiteit van de wachtwoorden. De BIO schrijft ook voor dat (beveiligings)patches voor ernstige kwetsbaarheden in hard- en software binnen een week moeten worden toegepast en dat in de tussentijd op basis van een expliciete risicoafweging mitigerende maatregelen getroffen moeten worden.

Het Nationaal Cybersecurity Centrum (NCSC) publiceert regelmatig adviezen in de vorm van richtlijnen. Specifiek met betrekking tot het bericht van Trouw is dat de richtlijn "ICT beveiligingsrichtlijnen voor webapplicaties".[2] Voor het onderdeel "operationeel beleid voor platformen en webservers" doet de richtlijn van het NCSC de volgende aanbeveling: "Overweeg de invoering van sterke authenticatiemechanismen voor de toegang tot systemen. Deze mechanismen kenmerken zich door het gebruik van ten minste twee factoren voor authenticatie." Overigens kan bovengenoemde richtlijn van het NCSC voor de overheid worden beschouwd als een nadere detaillering van de BIO voor het onderdeel webapplicaties.

Tot slot hanteert de overheid eveneens de Coordinated Vulnerability Disclosure (CVD)[3], een leidraad van het NCSC, om de veiligheid van informatiesystemen, waaronder ook websites, verder te stimuleren. Het doel van CVD is om bij te dragen aan de veiligheid van ICT-systemen door kennis over kwetsbaarheden te delen. Eigenaren van ICT-systemen kunnen dan kwetsbaarheden (laten) verhelpen vóórdat deze actief misbruikt kunnen worden door derden.

<u>De constateringen</u>
Publieke webpagina's waarin het volstaat om met een gebruikersnaam en wachtwoord in te loggen, voldoen niet zonder meer aan de overweging uit de hierboven genoemde richtlijn van het NCSC. Zoals eerder gemeld in deze brief, is beveiliging het resultaat van een risico-afweging om wat voor informatie het gaat. Ook gaat het bij beveiliging om de samenhang van getroffen maatregelen en niet om het richten op slechts één maatregel. Dat kan betekenen dat bij een authenticatie met alleen gebruikersnaam en wachtwoord op andere plaatsen in het systeem aanvullende maatregelen zijn getroffen (segmentering, beperking van rechten, etc.). Welke dat zijn, zal per geval verschillen.

Dat betekent dat het NCSC dit gebruik van Wordpress op zich niet afraadt. 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.

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

3 https://www.ncsc.nl/documenten/publicaties/2019/mei/01/cvd-leidraad

Ook meldt Trouw dat het NCSC sinds 2014 overheden 36 waarschuwingen heeft gestuurd over veiligheidskwesties bij Wordpress. 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.

De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,

drs. R.W. Knops