Knops: ‘WordPress kan veilig worden ingezet door overheidsorganisaties’

Anton Mous

Leestijd: 4 minuten | Gepubliceerd: 06-07-2021

WordPress kan zonder problemen veilig worden ingezet door overheidsorganisaties. Zij maken een eigen risicoanalyse en bepalen aan de hand daarvan welke aanvullende beveiligingsmaatregelen noodzakelijk zijn. De site van de Informatiebeveiligingsdienst (IBD) draait weliswaar op WordPress, maar de beheeromgeving is niet publiekelijk toegankelijk. Daar is dan ook niets mis mee.

Dat schrijft staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties Raymond Knops in antwoord op schriftelijke vragen van DENK-Kamerlid Stephan van Baarle.

WordPress-websites lopen ‘extra groot risico’ om gehackt te worden

Begin juni onderzocht *Trouw* de beveiliging van overheidswebsites en andere politiek-bestuurlijk instanties. Het dagblad concludeerde dat de Rijksoverheid, een tiental gemeenten, acht omgevingsdiensten, vijf veiligheidsregio’s, vier regionale GGD’s, enkele waterschappen, de FIOD, douane en de Belastingdienst ‘een extra groot risico’ lopen om gehackt te worden.

Dat komt omdat de websites van deze organisaties op het content management systeem (CMS) WordPress draaien. In beginsel werkt het CMS met een publiekelijk toegankelijke inlogpagina. Beheerders en werknemers voeren hier hun gebruikersnaam en wachtwoord in. Dat iedereen toegang heeft tot de inlogpagina maakt de sites volgens Trouw extra kwetsbaar. Zeker als technisch onderlegde mensen tools gebruiken om automatisch gebruikersnamen en wachtwoorden in te voeren, totdat ze een match hebben.

Diverse experts schrokken van de bevindingen. Ze vermoedden dat de overheid geen of onvoldoende aandacht schenkt aan het probleem. Eén van hen is Marten van Dijk, hoofd van de onderzoeksgroep Computer Security van Centrum Wiskunde & Informatica. Hij zei dat de overheid op deze manier onnodig risico loopt. Om een idee te krijgen van de omvang: van de 1.148 overheidswebsites maken er 165 gebruik van WordPress.

Knops: 'Overheidsinstanties nemen goede beveiligingsmaatregelen'

Stephan van Baarle (DENK) schrok zich een hoedje toen hij de conclusies van het onderzoek in Trouw las. Het Tweede Kamerlid besloot schriftelijk een aantal vragen te stellen aan de staatssecretaris die verantwoordelijk is hiervoor, Raymond Knops. Het Kamerlid wilde van de staatssecretaris weten of hij vindt dat het kabinet tekort is geschoten in het treffen van digitale beveiligingsmaatregelen tegen hackers. Tevens vroeg hij waarom allerlei adviezen van het Nationaal Cyber Security Centrum (NCSC) over beveiligingsmaatregelen niet opgevolgd zijn. Tot slot pleitte hij ervoor om de inlogpagina strikt te scheiden van de openbare pagina's.

Staatssecretaris Knops heeft de afgelopen weken de tijd gevonden om de vragen van Van Baarle te beantwoorden. Om te beginnen vindt hij niet dat er tekort is geschoten bij de beveiliging van tientallen websites. Knops wijst erop dat de Rijksoverheid en lagere overheidsorganen het basisnormenkader Baseline Informatiebeveiliging Overheid (BIO) als uitgangspunt nemen. Daarin staat dat bij de keuze van een informatiesysteem of CMS een risicoafweging gemaakt dient te worden. De uitkomsten daarvan zijn richtinggevend voor het treffen van beveiligingsmaatregelen. Proportionaliteit is daarbij het uitgangspunt. Sites die vertrouwelijke informatie verwerken, maken een andere overweging dan sites die openbare informatie publiceren.

De richtlijnen die het NCSC regelmatig publiceert, zijn volgens de staatssecretaris een nadere invulling van de BIO. "Uiteindelijk is het resultaat dat een samenhangend pakket van maatregelen wordt vastgesteld en toegepast. Welke dat zijn, zal per geval verschillen", aldus staatssecretaris Knops. Hij benadrukt dat dit niet vrijblijvend is: overheidsorganen leggen immers verantwoordelijk af tegenover controlerende en toezichthoudende instanties.

Waarschuwingen van het NCSC zijn serieus genomen

De staatssecretaris deelt de mening van Van Baarle niet dat de overheid tekort is geschoten om voldoende digitale beveiligingsmaatregelen te treffen tegen hackers. Knops is van mening dat burgers erop moeten kunnen vertrouwen dat de overheid en andere politieke instanties vertrouwelijk en verantwoord met gevoelige gegevens omgaan. Dat kunnen ze ook, omdat de beveiligingsrisico's vooraf goed in kaart zijn gebracht.

Sinds 2014 heeft het NCSC voor 36 veiligheidsrisico's van WordPress gewaarschuwd. Van Baarle vroeg zich af wat er met deze waarschuwingen is gedaan, aangezien 165 websites van overheidsorganen op dit CMS draaien. Knops zegt at overheidsorganisaties de meldingen van het NCSC nauwlettend in de gaten houden. Ze zijn immers zelf verantwoordelijk voor de veiligheid van hun sites.

"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", aldus staatssecretaris Knops. Hij wijst erop dat er ook nog andere factoren meespelen om de veiligheid van een product te beoordelen, zoals aard, omvang en frequentie van onderzoek.

Staatssecretaris Knops heeft geen bezwaar tegen WordPress

Tot slot ziet de staatssecretaris het niet als een probleem dat de website van de Informatiebeveiligingsdienst (IBD) op WordPress draait. De site voldoet aan de eisen die de BIO daaraan stelt. Ook is er alleen openbare informatie te vinden. "Voor informatie met een hoger beschermingsniveau gebruikt de IBD andere middelen", zo zegt Knops. Zo voert de organisatie regelmatig penetratietesten en risicoanalyses uit, ook op de website. De Vereniging van Nederlandse Gemeenten (VNG) bevestigt dat de beheeromgeving niet publiekelijk toegankelijk is.

"Ik zie daarom geen bezwaar tegen het gebruik van individuele softwarepakketten, zoals WordPress, als risicoafwegingen zijn gemaakt en maatregelen zijn getroffen", concludeert de staatssecretaris. Knops ziet dan ook geen aanleiding om 'beleidsmatige inspanningen' te vergroten om de digitale weerbaarheid van overheidswebsites te vergroten.