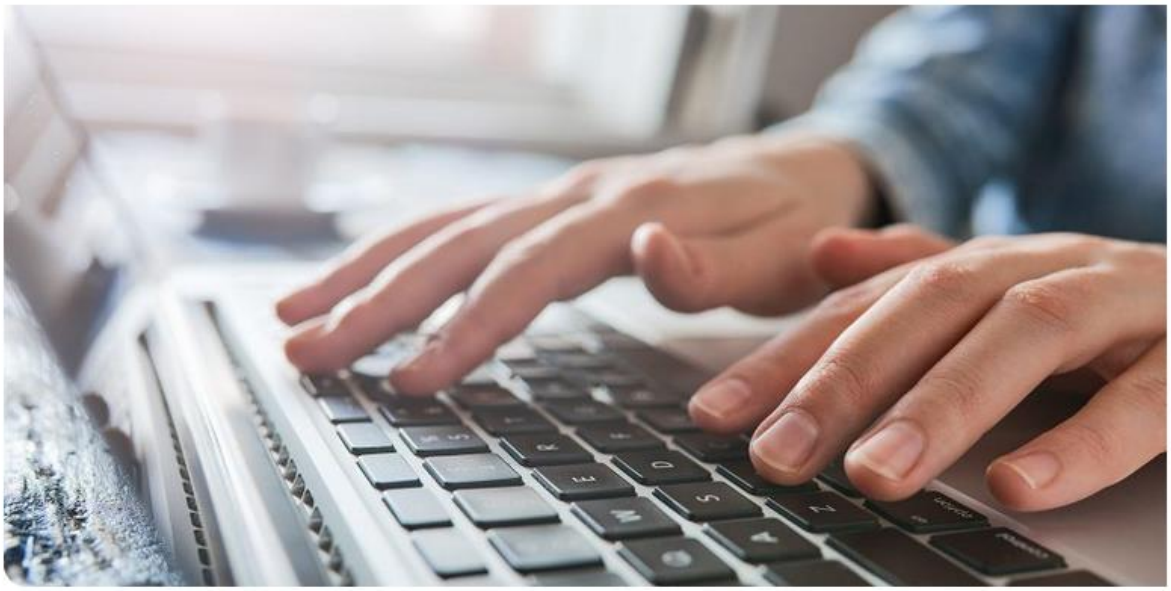
Tientallen websites overheid kwetsbaar voor hackaanvallen

Anton Mous

Leestijd: 2 minuten | Update: 16-06-2021



Overheidsinstanties negeren basale beveiligingsregels en vormen zodoende een groot beveiligingsrisico. Dat komt omdat de inlogpagina van hun website openbaar beschikbaar is. Zo maken ze het hackers eenvoudiger om de site te hacken. Het gaat om tientallen websites van de Nederlandse overheid.

Dat blijkt uit onderzoek van *Trouw*.

Openbare inlogpagina vergroot beveiligingsrisico's

Het dagblad schrijft dat de Rijksoverheid, een tiental gemeenten, vijf veiligheidsregio's, acht omgevingsdiensten, vier regionale GGD's, enkele waterschappen, FIOD, douane en de Belastingdienst 'een extra groot risico' lopen om te worden gehackt. Wat deze diensten met elkaar gemeen hebben, is dat hun website op WordPress draait. Het content management systeem werkt met een publiekelijk toegankelijke inlogpagina, waar men een gebruikersnaam en wachtwoord moet invullen om toegang te krijgen tot de back-end van een website.

Het feit dat de inlogpagina voor iedereen toegankelijk is, maakt ze kwetsbaar. Zeker als hackers technische hulpmiddelen gebruiken om gebruikersnamen te achterhalen en automatisch wachtwoorden in te voeren, net zolang totdat er een match is. Dit fenomeen noemen we ook wel *credential stuffing*. Dit gebeurde eind vorig jaar bij de gemeente Hof van Twente: hackers wisten het wachtwoord van een FTP-server te achterhalen ('Welkom2020') en zo toegang te krijgen tot de computersystemen van de gemeente.

De openbare inlogpagina is een bekend beveiligingsrisico bij WordPress. Het Nationaal Cyber Security Centrum (NCSC) waarschuwt al jaren voor het gevaar. Sinds 2014 heeft het NCSC 36 waarschuwingen gestuurd aan overheidsinstanties om het gevaar bespreekbaar te maken. Het adviesorgaan over cybersecurity heeft niet voor niets in zijn richtlijnen staan dat het onverstandig is om met een openbaar inlogscherm te werken.

WordPress is niet per definitie onveilig

Pieter Jansen, ethisch hacker en directeur van cyberveiligheidsbedrijf Cybersprint, noemt de bevindingen tegenover Trouw 'schokkend'. Hij denkt dat de IT- en security teams van de overheid geen of onvoldoende aandacht schenken aan het probleem. Marten van Dijk, hoofd van de onderzoeksgroep Computer Security van Centrum Wiskunde & Informatica, stelt dat de overheid op deze manier de cyberrisico's vergroot. Internetspecialist Jules Ernst onderzocht welke software overheden gebruiken om hun websites mee te bouwen. Van de 1.148 sites van de Rijksoverheid maken er 165 gebruik van WordPress.

Het gebruik van WordPress hoeft nog niet vanzelfsprekend te betekenen dat websites onveilig zijn. Om te beginnen kunnen sitebeheerders, redacteuren en ambtenaren die toegang hebben tot de site een sterk wachtwoord hanteren. Hoe sterker het wachtwoord, des te lastiger je het voor hackers maakt om in te breken. Een andere mogelijkheid om hackers te slim af te zijn, is door de URL van de openbare inlogpagina te veranderen.

Een woordvoerder van de Informatiebeveiligingsdienst (IBD) benadrukt dat het een goede zaak is dat er veel veiligheidsproblemen worden ontdekt in WordPress. Dat maakt het cms juist veiliger. Hij stelt dat 'de veiligste oplossing' niet het doel zou moeten zijn. "Het gaat erom dat je de risico's onderkent en dan zoveel maatregelen neemt dat die risico's acceptabel worden."

Van Dijk is het niet eens met deze uitleg. Hij zegt dat het de taak is van overheidsinstanties om onnodige risico's te voorkomen. "Als er een veiliger methode is om als overheid dezelfde dienstverlening aan te bieden, dan verdient die de voorkeur. Kies de allerveiligste optie."