Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2026–2027

Vragen gesteld door de leden der Kamer

2026Z22802

Vragen van het lid **Kathmann** (PRO) aan de Staatssecretaris van Economische Zaken en Klimaat en de Minister van Justitie en Veiligheid over *het offline halen van belangrijke websites door een cyberkwetsbaarheid* (ingezonden 22 oktober 2026).

Vraag 1
Kunt u reageren op het nieuws dat verschillende overheidswebsites offline zijn gehaald vanwege het risico op hacks?[1]

Vraag 2
Welke websites van de overheid en belangrijke instanties zijn (tijdelijk) offline gehaald? Welke gevolgen heeft dit (gehad) voor burgers en organisaties?

Vraag 3
Wat gaat u doen om problemen die ontstaan als gevolg van het (tijdelijk) offline halen van deze websites op te lossen? Bij welke belangrijke processen, zoals inloggen met DigiD of het maken van een online afspraak, is hier mogelijk sprake van?

Vraag 4
Wanneer waren de kwetsbaarheden bekend?[2] Hoeveel tijd zat er tussen de ontdekking en het openbaar maken van deze informatie? Is er een aanleiding om te denken dat de kwetsbaarheid is misbruikt door hackers?

Vraag 5
Hoe heeft u gereageerd om zo snel mogelijk het risico op hacks te voorkomen? Welke afstemming vindt er plaats om de reactie met alle getroffen overheden en bedrijven te coördineren?

Vraag 6
Welke rol heeft het Nationaal Cyber Security Center (NCSC) in het ondersteunen van overheden en organisaties die wellicht dezelfde kwetsbare programmeertaal gebruiken, maar hier geen weet van hebben?

---

[1] NOS Nieuws, 21 oktober 2026. nos.nl/artikel/2636055-websites-van-overheid-en-in-onderwijs-offline-vanwege-lek-risico-op-hacks

[2] Dit betreft twee risico's die geconstateerd zijn in de programmeertaal PHP

Vraag 7
Hoe wordt actuele en belangrijke informatie met de juiste partijen gedeeld als de website van het NCSC zelf ook offline is gehaald? Waar kunnen burgers en organisaties betrouwbare informatie in dit geval vinden?

Vraag 8
Ligt er een plan klaar voor het tijdig beschermen van belangrijke websites en instanties zodra een dergelijke kwetsbaarheid wordt gevonden? Zo ja, wat is het beleid hiervoor?

Vraag 9
Ziet u, gezien het groeiende aantal kwetsbaarheden, storingen en cyberaanvallen, aanleiding om bestaande wetten en beleid aan te scherpen? Zo ja, wat moet aangepast worden en op welke termijn gaat u hier voorstellen voor doen?

Vraag 10
Kunt u deze vragen afzonderlijk van elkaar en zo spoedig mogelijk beantwoorden?