Oldehoofsterkerkhof 2
Postbus 21000
8900 JA Leeuwarden
Telefoon 14058

Gemeente Leeuwarden

Zaaknummer: 2026-278975

Antwoord van burgemeester en wethouders op schriftelijke vragen als bedoeld in artikel 42, eerste lid, van het Reglement van Orde voor de vergaderingen van de raad der gemeente Leeuwarden, ingediend op 22 oktober 2026. De vragen zijn afkomstig van D66 en gaan over website storingen en het gebruik van PHP.

Vragen	**Antwoorden**
1. Op basis van wat voor soort feiten en argumenten werd de keuze gemaakt de website van de gemeente offline te halen? Kan hier ook eventueel een tijdspad bij gegeven worden, beginnend van de eerste signalen totdat uiteindelijk de website echt offline was?	Gemeente Leeuwarden wordt door de Informatie-beveiligingsdienst (IBD) geïnformeerd over actuele dreigingen. Deze specifieke dreiging is op woensdag 21 oktober 2026 om 09:20 uur per mail binnengekomen en om 11:31 uur gedeeld in onze security chat met de betrokken specialisten. Op basis van de eerste beoordeling van onze specialisten is om 11:52 uur door de sectormanager ICT besloten de betreffende leveranciers opdracht te geven de websites offline te halen. Vanaf dat moment zijn leveranciers direct begonnen met het offline halen. Omstreeks 13:38 uur kregen wij de bevestiging dat alles offline was. Tegelijkertijd had onze belangrijkste leverancier aangegeven al voorzorgsmaatregelen te hebben getroffen. Ze hadden toen al enkele risico's gemitigeerd op basis van de kennis die inmiddels voorhanden was. Na het beschikbaar komen van de beveiligingsupdate (patch), zijn de portalen en websites weer online gebracht. Dit gebeurde rond 23:30 uur op dezelfde dag, 21 oktober 2026.
2. In hoeverre is/was het college voorbereid op dit soort scenario's, waardoor veel maatschappelijke instanties niet of nauwelijks bereikbaar zijn en ze niet hun werk goed konden doen? Heeft het college dit soort, of van een ander soort, ‘doomscenario’s’ voorbereid voor hoe het college te werk moet gaan? Zo ja, op welke manier? Zo nee, waarom niet?	De gemeente Leeuwarden beschikt over een (Cyber)CrisisPlan. Hierin is uitgewerkt hoe de gemeente moet handelen in geval van bijvoorbeeld een ernstige hack. Zowel het College als de ambtelijke organisatie komen volgens dit plan in een crisisstructuur bij elkaar. Ze werken hierbij samen op basis van de BOB-systematiek 'Beeldvor-ming, Oordeelsvorming en Besluitvorming'. Hierbij staat het functioneren en de belangen van inwoners, bedrijven en de eigen organisatie centraal. Er wordt eveneens periodiek geoefend op basis van dit plan. In het geval van deze PHP kwetsbaarheid was het niet nodig de Crisisstructuur te activeren, gezien de direct uitgevoerde acties door zowel de ambtelijke organisatie als de leveranciers. Wel zijn burgemeester en wethouders uiteraard direct geïnformeerd.

3. Wat voor rol ziet het college voor zichzelf wanneer dit niet een tijdelijke storing is die snel opgelost kan worden, maar juist een langdurige waar eventueel veel chaos uit voortkomt?	Zie beantwoording vraag 2
4. Heeft de gemeente een ‘noodwebsite’ zoals die de gemeente Groningen heeft opgesteld voor eventuele toekomstige gevallen waar de ‘normale’ website als onveilig/niet beschikbaar wordt beschouwd? Zo ja, hoe worden de inwoners hierover geïnformeerd en hoe kunnen ze deze bereiken? Zo nee, waarom niet en ziet het college een mogelijkheid om er in de toekomst een te maken?	De gemeente beschikt niet over een speciale ’noodwebsite’ waarop we terug kunnen vallen wanneer de ‘live’ website uit de lucht is. In de werkinstructie voor het Klantcontactcentrum (KCC) staat wel vermeld dat in zo’n situatie gebruik kan worden gemaakt van een gearchiveerde kopie van de website op archiefweb.eu. Onze website wordt daar dagelijks gearchiveerd. Echter, deze versie is niet altijd beschikbaar, zoals bleek op woensdag 21 oktober 2026. Een van de geleerde lessen is dan ook dat we hiervoor een betere oplossing gaan ontwikkelen. Daarom zijn er inmiddels gesprekken gestart met contentbeheer om samen te werken aan een oplossing voor een betrouwbare ‘noodwebsite’ in de toekomst.
5. Het is gebleken dat de problemen in het PHP-programma werden ontdekt, mede door AI. Ziet de gemeente hier ook een kans om op eenzelfde soort manier onze eigen cyberveiligheid te versterken? Zo ja, op wat voor manieren? Zo nee, waarom niet?	Gemeente Leeuwarden volgt het normenkader Baseline Informatiebeveiliging Overheid (BIO) om de cyberveiligheid te versterken. Verder maakt gemeente Leeuwarden gebruik van geautomatiseerde scan software welke de omgeving continue scant op kwetsbaarheden. Daarnaast laten we de ICT-omgeving preventief controleren (pentesten) op kwetsbaarheden door externe onafhankelijke partijen. De inzet van AI ten behoeve van de cyberveiligheid heeft zeker onze interesse, echter vanuit de IBD (Informatiebeveiligingsdienst) zijn er nog geen handreikingen beschikbaar om dit betrouwbaar en uniform in te richten.
6. Volgens Cloudflare3 waren er al snel hackpogingen gedaan op basis van de problemen binnen PHP. Zijn er signalen dat er ook bij onze gemeente pogingen waren gedaan? Zo ja, wat zijn de eventuele consequenties hiervan?	De webserver logs van onze individuele websites laten zien dat er voor het uitvoeren van de patch (update) geen pogingen zijn gedaan om de kwetsbaarheid te misbruiken. Na het uitvoeren van de patch, vanaf 22 oktober, zijn er wel pogingen geregistreerd. Deze zijn echter succesvol afgewend. Ook van de leverancier van leeuwarden.nl en sdfryslan.nl hebben we de bevestiging gekregen dat er geen aanwijzingen zijn (op basis van de veiliggestelde logs) dat er misbruik of pogingen tot misbruik zijn geweest van de PHP-kwetsbaarheid.

Leeuwarden, 17 november 2026,

burgemeester en wethouders van Leeuwarden,

burgemeester.

secretaris.

**Dit document is rechtsgeldig digitaal ondertekend.*