GEMEENTE HOORN

Gemeente Hoorn
Nieuwe Steen 1
Postbus 603
1620 AR Hoorn
T 0229 25 22 00
www.hoorn.nl
Contactpersoon
F. van den Berg
Zaaknummer: 3093239
Bijlagen: -

Fractie Eenhoorn
A. van Beusekom

Hoorn, 13-11-2026

Onderwerp: Beantwoording artikel 36-vragen van fractie Eenhoorn over Cyberveiligheid

Beste meneer/ mevrouw,

U heeft vragen gesteld over Cyberveiligheid. In deze brief leest u de antwoorden op uw vragen.

Vraag 1 Inzicht in het gebruik van PHP
Is het college op de hoogte van de recent gemelde kwetsbaarheden in PHP? Kan het college aangeven of de gemeente Hoorn, haar websites, digitale dienstverlening en interne ICT-systemen gebruikmaken van PHP, rechtstreeks of via software en diensten van externe leveranciers? Heeft de gemeente hiervan een actueel en volledig overzicht?

Antwoord
Het college is op 21 oktober 2026 geïnformeerd over de wereldwijd gemelde beveiligingskwetsbaarheden in PHP. Direct zijn maatregelen getroffen en uw raad is hierover geïnformeerd via de raadsbrief van 22 oktober 2026.

De gemeente Hoorn maakt voor een deel van haar digitale voorzieningen gebruik van systemen en toepassingen die gebaseerd zijn op PHP, zowel rechtstreeks als via leveranciers. Op basis van een risicoanalyse en informatie van leveranciers is beoordeeld welke systemen mogelijk geraakt konden worden. De mogelijke risico's zijn daarmee in beeld gebracht en passende maatregelen zijn getroffen.

Het verkrijgen en onderhouden van een volledig en actueel overzicht van alle applicaties, componenten en afhankelijkheden binnen de gemeentelijke ICT-omgeving blijft een continu proces.

Vraag 2 Risicoanalyse en kwetsbare systemen
Heeft de gemeente onderzocht of haar eigen systemen of de systemen van leveranciers kwetsbaar zijn voor de recent gemelde PHP-kwetsbaarheden? Zo ja, wat zijn de uitkomsten en welke maatregelen zijn of worden genomen? Zo nee, wanneer wordt dit onderzoek uitgevoerd?

Antwoord
Direct nadat de kwetsbaarheden bekend werden, heeft de gemeente beoordeeld welke eigen systemen en systemen van leveranciers mogelijk geraakt konden worden. Daarbij is gebruikgemaakt van informatie en adviezen van het Nationaal Cyber Security Centrum (NCSC) en is contact onderhouden met betrokken leveranciers.

Uit deze beoordeling bleek dat het intranet en enkele themawebsites mogelijk kwetsbaar waren. Deze zijn uit voorzorg tijdelijk offline gehaald. De gemeentelijke website Hoorn.nl is online gebleven omdat deze geen gebruik maakt van PHP.

Vraag 3 Beveiligingsupdates en leveranciers
Welke afspraken heeft de gemeente met haar ICT-leveranciers over het tijdig installeren van beveiligingsupdates, het melden van kwetsbaarheden en het beheersen van cyberrisico's? Kan het college bevestigen dat betrokken leveranciers de kwetsbaarheden beoordelen en waar nodig passende maatregelen treffen, zoals het installeren van patches of het tijdelijk uitschakelen van kwetsbare systemen?

Antwoord
De gemeente maakt met haar ICT-leveranciers afspraken over informatiebeveiliging, het tijdig installeren van beveiligingsupdates, het melden van beveiligingsincidenten en kwetsbaarheden en het beheersen van cyberrisico's. Deze afspraken zijn vastgelegd in contracten, verwerkersovereenkomsten en de daarbij behorende beveiligingseisen. De leveranciers moeten kwetsbaarheden actief monitoren, risico's beoordelen en passende maatregelen treffen om de veiligheid en continuïteit van hun dienstverlening te waarborgen.

Het college kan bevestigen dat betrokken leveranciers de kwetsbaarheden hebben beoordeeld en waar nodig maatregelen hebben getroffen. Nadat de benodigde updates beschikbaar kwamen, zijn deze geïnstalleerd, zijn controles uitgevoerd en konden de tijdelijk getroffen maatregelen worden opgeheven.

Vraag 4 Raadsinformatie en continuïteit van de dienstverlening
De gemeente Hoorn maakt gebruik van iBabs wat mogelijk door de gemelde kwetsbaarheden kan worden geraakt? Zo ja, is de gemeente hierover door de leverancier geïnformeerd en zijn de betreffende systemen of diensten tijdelijk uitgeschakeld of aangepast? Welke maatregelen zijn beschikbaar om de continuïteit en toegankelijkheid van raadsinformatie en gemeentelijke dienstverlening te waarborgen wanneer een systeem uit veiligheidsoverwegingen offline moet worden gehaald?

Antwoord
De gemeente is op 21 oktober 2026 door de leverancier van iBabs geïnformeerd dat de applicatie niet was geraakt door de gemelde PHP-kwetsbaarheid. De continuïteit en toegankelijkheid van raadsinformatie zijn hierdoor niet onderbroken.

Mocht een systeem voor raadsinformatie in de toekomst uit veiligheidsoverwegingen tijdelijk niet beschikbaar zijn, dan wordt beoordeeld welke alternatieve werkwijzen nodig zijn om raadsleden toegang te blijven bieden tot de benodigde informatie en vergaderingen zoveel mogelijk doorgang te laten vinden.

Vraag 5 Inwoners, gegevensbescherming en verantwoording
Op welke wijze borgt het college dat eventuele kwetsbaarheden tijdig worden opgespoord en dat mogelijke gevolgen voor persoonsgegevens, vertrouwelijke informatie en de dienstverlening aan inwoners worden beperkt? Indien een beveiligingsincident of datalek wordt vastgesteld, welke procedures gelden dan voor de afhandeling, melding bij de

bevoegde instanties en, indien noodzakelijk, informatievoorziening aan betrokken inwoners en de gemeenteraad?

Antwoord
Het college borgt de digitale veiligheid van de gemeente door te werken volgens de Baseline Informatiebeveiliging Overheid (BIO2), periodiek risicoanalyses uit te voeren en beveiligingsmaatregelen continu te actualiseren. Daarnaast ontvangt de gemeente via onder meer het Nationaal Cyber Security Centrum (NCSC), de Informatiebeveiligingsdienst (IBD) en leveranciers informatie over actuele dreigingen en kwetsbaarheden, zodat tijdig passende maatregelen kunnen worden genomen.

Wanneer een beveiligingsincident wordt vastgesteld, wordt onderzoek gedaan naar de aard, omvang en mogelijke gevolgen daarvan en de oplossingen hiervoor. Het uitgangspunt is dat dat transparant wordt gecommuniceerd wanneer zich een incident voordoet.

Bij een datalek, wordt gehandeld volgens de wettelijke verplichtingen uit de Algemene verordening gegevensbescherming (AVG) en de Cyberbeveiligingswet. Indien vereist wordt melding gedaan bij de Autoriteit Persoonsgegevens en worden betrokkenen geïnformeerd. Ook melden we significante cyberincidenten bij de aangewezen instanties. Afhankelijk van de aard en impact van het incident wordt ook de gemeenteraad geïnformeerd.

Vraag 6 Is de 3,5 miljoen begroot voor blootstelling van de gemeente aan cyberaanvallen, afdoende net als de acties die hieruit voortkomen? Wat gaat u hier mee doen? Gezien de huidige situatie?

Antwoord
De € 3,5 miljoen is geen budget maar een inschatting van de mogelijke financiële gevolgen van een cyberincident. Dit risico is opgenomen in de paragraaf Weerstandvermogen en risicobeheersing.

Om de risico's zo klein mogelijk te maken, investeren we in 2027 investeren extra in de versterking van onze digitale weerbaarheid. Hiermee beperken wij zoveel mogelijk zowel de kans op een cyberaanval als de financiële en operationele impact daarvan.

Wij blijven de ontwikkelingen en dreigingen monitoren en beoordelen periodiek of de omvang van het opgenomen risico en de getroffen maatregelen nog passend zijn. Als de uitkomsten daartoe aanleiding geven, passen wij de risico-inschatting of maatregelen aan en informeren wij de raad hierover via de paragraaf Weerstandvermogen en risicobeheersing.

Met vriendelijke groet,

Burgemeester en wethouders van Hoorn

de secretaris de burgemeester