Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

> Retouradres Postbus 20011 2500 EA Den Haag

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal
Postbus 20018
2500 EA Den Haag

DGDOO
CRD/IB

Turfmarkt 147
2511 DP Den Haag
Postbus 20011
2500 EA Den Haag
www.rijksoverheid.nl

Onze referentie
2026-0000605661

Bijlage(n)
0

Datum	25 november 2026
Betreft	Beantwoording Kamervragen over verouderde software bij de overheid naar aanleiding van het PHP-lek

Hierbij bied ik u, mede namens de staatssecretaris van Digitale Economie en Soevereiniteit, de antwoorden aan op de schriftelijke vragen die zijn gesteld door het lid El Boujdaini (D66) over verouderde software bij de overheid naar aanleiding van het PHP-lek. Deze vragen werden ingezonden op 29 oktober 2026, met kenmerk 2026Z23405.

De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,

Eric van der Burg

2026Z23405

DGDOO
CRD/IB

Onze referentie
2026-0000605661

Vragen van het lid El Boujdaini (D66) aan de staatssecretarissen van Binnenlandse Zaken en Koninkrijksrelaties en van Economische Zaken en Klimaat over verouderde software bij de overheid naar aanleiding van het PHP-lek (ingezonden 29 oktober 2026)

1. Bent u bekend met het bericht dat PHP alleen voor de vier nog ondersteunde versies een reparatie heeft uitgebracht, terwijl naar schatting zestig tot zeventig procent van de PHP-servers op oudere versies draait?[1]

Ja.

2. Hoe zorgt de Baseline Informatiebeveiliging Overheid 2 (BIO2) ervoor dat software die helemaal geen updates meer krijgt, op tijd wordt vervangen?

De Baseline Informatiebeveiliging Overheid (BIO2) eist dat organisaties tot passende maatregelen komen om risico's te beheersen. Onder andere eist de BIO2 dat organisaties een inventaris bijhouden van systemen en hun onderhoudsstatus, dat systemen up-to-date worden gehouden en dat ontdekte kwetsbaarheden tijdig worden verholpen. Wanneer het niet mogelijk is om aan deze eisen te voldoen, omdat software 'end of life' is en geen updates meer ontvangt (BIO beheersmaatregel 8.19), moet de organisatie passende maatregelen treffen. Aangezien de BIO2 geldt als minimumeis voor informatiesystemen van de overheid, is een gevolgtrekking dat het systeem moet worden vervangen, of dat middels een comply-or-explain hier gemotiveerd van afgeweken wordt. Tot het systeem is vervangen zal de organisatie passende mitigerende maatregelen moeten treffen om het risico te beheersen.

3. Hebben controles zoals ENSIA, de Auditdienst Rijk of de Algemene Rekenkamer de afgelopen jaren verouderde software bij de overheid aan het licht gebracht? Wat is daar vervolgens mee gedaan?

Vanuit de Algemene Rekenkamer is onder andere in de hoogrisicolijst[1], gepubliceerd op 20 mei 2026, het risico "Niet-weerbare ICT, verouderde systemen en leveranciers-afhankelijkheid vormen risico (5-FOB-Ontvangsten-Doel/Bedrijfsvoering)" benoemd, waarbij specifiek aandacht is voor verouderde systemen. De opvolging van en de terugkoppeling over dergelijke risico's en overige tekortkomingen verloopt middels de jaarlijkse verantwoordingscyclus. Zoals als antwoord op vraag 2 toegelicht hebben overheidsorganisaties zelf de verplichting om verouderde software in kaart te brengen en de risico's hiervan te beheersen.

Daarnaast bevat ENSIA een algemene vragenlijst over de Baseline Informatiebeveiliging Overheid; op die manier leggen organisaties verantwoording af over de wijze waarop ze de risico's van verouderde software beheersen. De beantwoording van deze vragenlijst en de opvolging was tot dusver een interne aangelegenheid van gemeenten voor de verantwoording aan hun College en de Gemeenteraad. Vanaf de inwerkingtreding van de Cyberbeveiligingswet (Cbw) gebruikt de Rijksinspectie Digitale Infrastructuur (RDI) de ENSIA verantwoording over de BIO als een van de bronnen voor haar toezicht.

[1] Hoogrisicolijst - Hoge risico's voor Nederland, stand voorjaar 2026 | Algemene Rekenkamer

4. Hoeveel systemen van de overheid draaien op dit moment op software die geen beveiligingsupdates meer krijgt, en is dat overzicht volledig?

Het ministerie van BZK heeft geen centraal overzicht van alle systemen van de overheid die geen beveiligingsupdates meer krijgen. De verantwoordelijkheid voor individuele systemen ligt bij organisaties zelf.

5. Gaan de Inkoopeisen Cybersecurity Overheid en de Algemene Beveiligingseisen voor Rijksoverheidsopdrachten ook over de onderliggende software in een product, zoals PHP, of alleen over het product zelf?

De Inkoopeisen Cybersecurity Overheid (ICO) kunnen ook betrekking hebben op onderliggende software, maar dat is niet vanzelfsprekend. De ICO ondersteunen opdrachtgevers bij het formuleren van cybersecurityeisen aan ICT-producten en -diensten. Of componenten zoals PHP daadwerkelijk onder de contractuele afspraken vallen, hangt af van de eisen die de opdrachtgever, op basis van een risicoafweging, in de overeenkomst opneemt.

De Algemene Beveiligingseisen voor Rijksoverheidsopdrachten (ABRO) hebben een andere primaire doelstelling: het beschermen van nationale veiligheidsbelangen bij daarvoor aangewezen opdrachten. De eisen betreffen onder meer de beveiliging van de opdrachtnemer, diens ICT en informatie. Zij zijn niet primair opgezet als generieke productspecificatie voor softwarecomponenten. Afhankelijk van de opdracht kunnen beveiligingseisen echter ook gevolgen hebben voor de keuze van welke technologie gebruikt kan/zal worden en welke leveranciersketen in een specifiek geval acceptabel is.

6. Hoe vaak is de afgelopen jaren gehandhaafd op deze inkoopeisen, bijvoorbeeld toen een leverancier zijn product niet meer bijwerkte?

Overheidsbrede cijfers hierover zijn niet beschikbaar. Daardoor kan niet worden aangegeven hoe vaak opdrachtgevers leveranciers hebben aangesproken op het uitblijven van beveiligingsupdates.

7. Hoe wordt bij de Cyberbeveiligingswet getoetst of organisaties weten welke verouderde onderdelen er in de software van hun leveranciers zitten?

De Cyberbeveiligingswet (Cbw) stelt verplicht dat rekening wordt gehouden met de algemene kwaliteit van de producten en de staat van de digitale weerbaarheid van haar leveranciers en dienstverleners, met inbegrip van hun veilige ontwikkelingsprocedures (Artikel 21, lid 4 onder b Cbw). Verder behoort een entiteit onder de Cbw vastgesteld beleid te hebben voor het beheer van haar bedrijfsmiddelen die zij voor haar werkzaamheden of voor het verlenen van haar diensten gebruikt. De entiteit legt dat beleid schriftelijk vast en past dat beleid aantoonbaar toe (Artikel 16 van het Cyberbeveiligingsbesluit). Ten slotte bevat voor de overheidssector de Cyberbeveiligingsregeling Overheid (Cbro) specifieke regels, waaronder de verplichting de BIO2 toe te passen. Daarom verwijs ik u verder naar het antwoord op de vragen 2 en 3.

8. Hoe wordt de veiligheid geborgd van systemen die de overheid al jaren gebruikt, nu de eisen uit de Cyber Resilience Act alleen gelden voor producten die vanaf december 2027 op de markt komen?

De essentiële cybersecurity-eisen van de Cyber Resilience Act (CRA) voor digitale producten gaan inderdaad in vanaf 11 december 2027. Wel is het zo dat er nu al op grond van de CRA een meldplicht geldt voor misbruikte kwetsbaarheden en incidenten, ook voor producten die al op de markt gebracht zijn.

De beveiliging van bestaande systemen blijft in de eerste plaats de verantwoordelijkheid van de overheidsorganisatie die deze gebruikt. De Cyber Resilience Act (CRA) stelt verplichtingen aan fabrikanten van producten met digitale elementen, maar neemt de verantwoordelijkheid van gebruikers voor het beheer van hun systemen niet over.

Ook zonder de CRA zijn er (veiligheids)eisen aan systemen die de overheid gebruikt. Voor de beveiliging van bestaande overheidssystemen blijft het eigen risicobeheer bepalend. De BIO2 biedt daarvoor een normenkader. Voor organisaties die onder de Cyberbeveiligingswet vallen, gelden daarnaast toepasselijke wettelijke verplichtingen voor de beveiliging van netwerk- en informatiesystemen.

Een normenkader en/of zorgplicht betekenen niet automatisch dat alle verouderde software en onderliggende afhankelijkheden bekend zijn. Softwarecomponenten kunnen zijn verwerkt in producten die externe leveranciers ontwikkelen en onderhouden. Daardoor beschikt de opdrachtgever niet altijd zelfstandig over de informatie of de mogelijkheden om kwetsbaarheden te verhelpen.

Overheidsorganisaties moeten daarom gedurende de gehele gebruiksperiode van digitale producten zicht houden op de ondersteuning van systemen, relevante leveranciersafhankelijkheden en de mogelijkheden om risico's te beperken. Wanneer ondersteuning of beveiligingsupdates ontbreken, moet op basis van de feiten en risico's worden beoordeeld welke maatregelen nodig zijn. Dat kan variëren van aanvullende beveiliging en beperking van gebruik tot vervanging of beëindiging van de voorziening. Indien er niet genoeg essentiële informatie aanwezig is, moet dat eerst worden onderzocht; het accepteren van voorgenoemde risico's is geen vervanging voor naleving van toepasselijke verplichtingen.

De verdere ontwikkeling van de ICO en het leveranciersmanagement richten zich mede op het ondersteunen van de in de voorgaande paragraaf benoemde afwegingen gedurende de levenscyclus. Daarbij is ook aandacht voor afhankelijkheden en kwetsbaarheden die meerdere overheidsorganisaties kunnen raken.

9. Blijft er, ondanks deze Europese regels, een gat over dat Nederland zelf moet dichten? Zo ja, hoe wilt u dat doen en op welke termijn?

Voor veiligheid van digitale producten biedt de CRA vanaf 11 december 2027 een sluitend kader. Daarnaast regelt de netwerk- en informatiebeveiligingsrichtlijn (NIS2) de interne cybersecurityhuishouding van belangrijke en kritieke entiteiten. Alle nationale en Europese regels zijn een deel van de puzzel om producten, diensten en organisaties zo veel mogelijk digitaal veilig te houden. Daarnaast is het overheidsbeleid dat er risicogebaseerd te werk gegaan wordt, en dat concrete maatregelen op basis van een risicoanalyse genomen worden. Aanvullende regels zijn hierdoor onder meer gesteld in

de BIO2 en de diverse ministeriële regelingen onder de Cbw. Hiermee wordt op dit moment vanuit de overheid het nodige gedaan om producten, diensten en organisaties zo veilig mogelijk te houden.

10. Is de ondersteuning door de Informatiebeveiligingsdienst genoeg voor gemeenten, provincies en waterschappen om verouderde software zelf op te sporen en te vervangen?

De Informatiebeveiligingsdienst (IBD) is onderdeel van de Vereniging van Nederlandse Gemeenten (VNG), en ondersteunt gemeenten bij digitale veiligheid en privacy. Zij geeft hiervoor kennisproducten uit en voorziet in kennisdeling onderling.

11. Kunt u deze vragen afzonderlijk van elkaar en voor het commissiedebat Online veiligheid en cybersecurity beantwoorden?

De vragen zijn afzonderlijk van elkaar en zo spoedig mogelijk beantwoord.

[1] PHP-lekken tonen risico van onzichtbare afhankelijkheid, IO+ d.d. 22 oktober 2026; https://ioplus.nl/nl/posts/php-lekken-tonen-risico-van-onzichtbare-afhankelijkheid