



**TER BESLUITVORMING**

**Nota actief openbaar**

Ja

**Onze referentie**

**Datum**

7 december 2022

**Opgesteld door**

AIVD/CS/BO

**Samengewerkt met**

BZK/DGDOO, BZK/CZW,  
BZK/Cluster OIV,  
Defensie/MIVD,  
Defensie/DGB, J&V/NCTV,  
J&V/DGRR, BZ/DIE

**Bijlage(n)**

1

Aan Minister BZK  
Staatssecretaris BZK  
Van DGAIVD

# nota

Beslisnota Kamervragen over spionage met gebruik van Pegasus of vergelijkbare software

## Aanleiding

Op 10 november 2022 hebben Tweede Kamerleden Leijten en Jasper van Dijk (beiden SP) schriftelijke vragen gesteld over spionage met gebruik van Pegasus of vergelijkbare software. Deze vragen zijn gesteld naar aanleiding van een uitzending van het radioprogramma Argos op 5 november over dit onderwerp. Met deze nota wordt de beantwoording aan u beiden voorgelegd voor akkoord.

## Geadviseerd besluit

U wordt geadviseerd:

1. In te stemmen met de antwoorden;
2. *Voor MinBZK:* De antwoorden gezamenlijk met de minister van Justitie en Veiligheid, en mede namens de minister van Defensie, te ondertekenen;
3. In te stemmen met het verzenden van de antwoorden aan de Kamer.

## Kern

De Kamervragen van de leden Leijten en Jasper van Dijk zien enerzijds op het handelingsperspectief dat Nederlandse overheden hebben bij het mitigeren van de dreiging die uitgaat van binnendringsoftware zoals Pegasus, en anderzijds op de afwegingen die worden gemaakt ten aanzien van de inzet van de bevoegdheid tot binnendringen in een geautomatiseerd werk door opsporings-, inlichtingen- en veiligheidsdiensten.

## Toelichting

### *Inzet digitale weerbaarheid rijksoverheid*

In de beantwoording op vragen 1 tot en met 3 wordt ingegaan op hoe de verantwoordelijkheidsverdeling voor informatiebeveiliging binnen de Nederlandse overheid geregeld is. Het betreft een risico-gebaseerde aanpak op organisatieniveau. De Baseline Informatiebeveiliging Overheid (BIO) is hiervoor een belangrijke basis. Specifiek voor gerubriceerde informatie geldt het Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie (VIRBI). Om met gerubriceerde informatie te mogen werken worden er ook onder meer technische, facilitaire en organisatorische maatregelen genomen. Er worden ook specifieke middelen en netwerken ter beschikking gesteld om veilig met dergelijke informatie te kunnen werken.

Belangrijk is dat de kaders die gelden voor ambtenaren (voor zover relevant) ook moeten worden gehanteerd voor en door bewindspersonen zelf, waarbij de

handhaving en sanctionering echter uiteindelijk (anders dan bij ambtenaren) vooral een zaak is voor de politieke gremia (MR en Kamers). Bij hun aantreden krijgen bewindspersonen instructies over veiligheidsrisico's. In het 'Blauwe Boek' worden bewindspersonen gewezen op het Voorschrift Informatiebeveiliging Rijksdienst/Bijzondere Informatie (VIR-BI). Ook krijgen zij middelen aangeboden zoals telefoons, waaronder telefoons specifiek geschikt voor gerubriceerde communicatie.

**Onze referentie**

**Datum**

7 december 2022

#### *Afwegingen inzet bevoegdheid tot binnendringen in geautomatiseerd werk*

Desgevraagd wordt in de beantwoording inzicht gegeven in de juridische kaders en waarborgen rondom de inzet van de bevoegdheid tot binnendringen van een geautomatiseerd werk door opsporings-, inlichtingen- en veiligheidsdiensten. Ook wordt toegelicht wat de relevante ontwikkelingen daaromtrent zijn, zoals de evaluatie van de Wet computercriminaliteit III.

#### *Politieke context*

Sinds in de zomer van 2021 brede maatschappelijke aandacht ontstond voor binnendringsoftware, en meer specifiek voor Pegasus, zijn verschillende sets Kamervragen over het onderwerp gesteld. Het Europees Parlement heeft een onderzoekscommissie ingesteld. De rapporteur van deze commissie heeft op 8 november een conceptrapport gepubliceerd.

In de vragen van de leden Leijten en Jasper van Dijk wordt verwezen naar verschillende publicaties in landelijke media. Het gaat om een radiouitzending van het VPRO-programma Argos en om een artikel van RTL Nieuws.

#### *Proces*

Op vrijdag 2 december 2022 is de Kamer geïnformeerd dat het, met het oog op een zorgvuldige beantwoording, niet mogelijk is gebleken de vragen binnen de gebruikelijke termijn te beantwoorden.

#### *Financiële/juridische overwegingen*

Niet van toepassing

#### *Krachtenveld*

Niet van toepassing

#### *Strategie*

Niet van toepassing

#### *Uitvoering*

Niet van toepassing

#### *Communicatie*

Er is geen actieve communicatie voorzien. Bij eventuele vragen zal woordvoering plaatsvinden langs de lijn van de beantwoording van de Kamervragen.

#### **Informatie die niet openbaar gemaakt kan worden**

Niet van toepassing.