



> Retouradres Postbus 20301 2500 EH Den Haag

Aan de Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Onze referentie
7766851

Bijlage(n)
1

Datum 8 oktober 2026
Betreft Aanbieding & reactie rapport ICT-inbreuk OM

Inleiding

Mijn ambtsvoorganger heeft in een brief van 23 januari 2026 de stand van zaken toegelicht van de externe commissie die door het College van procureurs-generaal en mijn ambtsvoorganger is ingesteld om de aanpak van de ICT-inbreuk bij het OM in juli 2025 te evalueren.¹ De commissie kreeg als opdracht mee om enerzijds terug te kijken op het incident, de getroffen maatregelen en de impact op de keten en anderzijds te onderzoeken wat er moet gebeuren om dergelijke incidenten in de toekomst te voorkomen.

Deze commissie heeft inmiddels haar werkzaamheden afgerond en bijgaande rapportage op 26 augustus 2026 opgeleverd. De commissie, die ik zeer erkentelijk ben voor haar werkzaamheden, bestond uit:

- Jaap Smit, oud-commissaris van de Koning van Zuid-Holland.
- Michel van Eeten, hoogleraar op het gebied van cybersecurity aan de TU Delft.
- Bert Voorbraak, algemeen directeur bij Logius, het agentschap van het ministerie van BZK dat digitale diensten levert aan overheden.

In deze brief reageer ik op de bevindingen en licht ik enkele andere ontwikkelingen met betrekking tot de ICT van het OM toe. Een paar passages in het rapport zijn onleesbaar gemaakt omdat openbaarmaking van deze informatie risico's met zich meebrengt op aantasting van de informatiebeveiliging van het OM.

Inhoud rapport

Reactie op incident

In het rapport concludeert de commissie in grote lijnen dat het OM adequaat ("begrijpelijk en in dit geval verstandig") op het incident heeft gereageerd door alle interne systemen los te koppelen van het internet. Het incident betrof een

¹ Kamerstukken II, 2025-2026, 26643, nr. 1455.

zogenaamde 'zero-day' inbreuk. Een zero-day kwetsbaarheid is een zwakke plek in software of hardware die nog niet bij de ontwikkelaars ervan bekend is.² Omdat de ontwikkelaars of fabrikant er nog geen weet van hebben, is er nog geen beveiligingsoplossing voor. Het is daardoor niet mogelijk om dergelijke inbreuken te voorkomen.

Onze referentie
7766851

Datum
8 oktober 2026

Beveiliging ICT

De commissie constateert echter ook dat de beveiliging van de ICT-systemen voorafgaand aan de ICT-inbreuk onvoldoende was. Dit komt onder meer tot uiting in het ontbreken van een permanente monitoring op een cruciaal systeem als de Citrix NetScaler (geavanceerd netwerkkapparaat dat zorgt voor veilige en geoptimaliseerde levering van applicaties) binnen de kantooromgeving, waardoor verdachte activiteiten of afwijkingen meteen kunnen worden gesignaleerd. Inmiddels is deze monitoring wel aanwezig.

De commissie stelt dat in de afgelopen jaren 'de wekker meerdere malen is afgegaan' en dat er waarschuwingen klonken over de gebrekkige en verouderde ICT-systemen en de risico's die daarmee verbonden zijn. Noodzakelijke aanpassingen bleven lange tijd achter. Hierin kwam verandering vlak voor de inbreuk, met de indiensttreding van een bestuurlijk Chief Information Officer (per 1 maart 2025) en een nieuwe directeur voor de informatievoorziening (per 14 april 2025).

De ontstane situatie is volgens de commissie mede het gevolg van de nadruk op IT als 'instrument' voor het goed functioneren van het primaire bedrijfsproces. Deze focus weerspiegelt een organisatiecultuur waarin IV voornamelijk is gericht op het in stand houden en verbeteren van het primaire proces. De druk op de ICT-capaciteit was hoog en bij prioritering kreeg het primaire proces voorrang. Ook bij andere ketenorganisaties speelde dit. Uit de gesprekken met respondenten blijkt dat er ideeën waren voor functionele en beveiligingsmaatregelen in de keten, maar dat deze door beperkte uitvoeringskracht en onvoldoende gezamenlijke sturing niet of niet tijdig zijn gerealiseerd. De keuzes voor korte-termijn-oplossingen voor technische problemen waren steeds navolgbaar. Het leidde echter tot het ondersneeuwen van het belang en het daadwerkelijke realiseren van een adequate beveiliging. Signalen over de (beveiligings-)problematiek binnen de organisatie werden langere tijd onvoldoende opgemerkt en zijn anderzijds onvoldoende krachtig gecommuniceerd.

De positionering van de informatievoorziening binnen de OM-organisatie is volgens de commissie ondertussen aanzienlijk verbeterd. De verbeteringen begonnen al voor het incident en zijn daarna doorgezet.

Toekomst

De commissie stelt dat al voor het incident goede eerste stappen zijn gezet om het IV-landschap maatschappelijk weerbaarder en robuuster te maken en de positionering van IV binnen de organisatie te versterken. Toch ziet de commissie dat de stappen die al in gang zijn gezet of die in gang gezet gaan worden nog niet toereikend zijn. Het zal ruime tijd en capaciteit vergen om de achterstand weg te werken en het niveau van 'brandveilig' te hebben bereikt. Ook stelt de commissie dat de organisaties binnen de strafrechtketen hun inzet primair richten op de eigen ontwikkeling waardoor zij minder toekomen aan gezamenlijke verbeteringen

² <https://www.ncsc.nl/kwetsbaarhedenbeheer/wat-is-een-zero-day>

binnen de keten. De keten is dermate complex dat geheel centrale regie onwenselijk is, maar een gedegen overzicht wel bijdraagt. De commissie adviseert om met de ketenpartners in gesprek te gaan over de gedeelde afhankelijkheden en van de verzameling losse eilandjes, die zich beroepen op hun specifieke en eigen karakter, een sterke archipel te maken.

Onze referentie
7766851

Datum
8 oktober 2026

Het rapport wordt afgesloten met een aantal geleerde lessen voor de toekomst. Belangrijke elementen daarin zijn dat gewerkt dient te worden aan businesscontinuïteit en risicobeheersing, zowel intern OM als in ketenverband. De commissie adviseert daarnaast om te investeren in het op orde brengen van de informatiebeveiliging en de organisatie ervan daarop aan te passen. Ook adviseert de commissie om frequent tot op het hoogste niveau de voortgang van de ontwikkelingen rond de IV te evalueren.

Reactie op rapport

Het rapport geeft duidelijk aan dat de aandacht voor de beveiliging van de ICT bij het OM voorafgaand aan het incident onvoldoende was. Inmiddels zijn op verschillende geconstateerde knelpunten, zoals de hiervoor genoemde monitoring en de positie van de voor beveiliging van de ICT verantwoordelijke functionarissen binnen de organisatie, belangrijke verbeteringen gerealiseerd. Sommige verbeteringen waren al voor al voor het incident gerealiseerd. Tegelijkertijd constateert de commissie dat het OM er met deze verbeteringen nog niet is. Het is het begin van een langer traject om de achterstand op ICT-gebied weg te werken. Ik deel deze constatering volledig.

De komende jaren moet het OM een grote inhaalslag maken op de ontwikkeling van de ICT, waaronder de informatiebeveiliging. Hiervoor krijgt het OM op grond van het coalitieakkoord 50 miljoen euro per jaar extra ter beschikking. Ik vind het noodzakelijk dat de voortgang van de ontwikkeling van de ICT – conform de bevindingen in het rapport – goed wordt gemonitord. Ik zal hiervoor samen met de voorzitter van het College van procureurs-generaal een onafhankelijke reviewboard benoemen met deskundigen die beschikken over ruime ervaring en expertise op het gebied van informatievoorziening, ICT en organisatieverandering. De reviewboard zal meerdere keren per jaar advies uitbrengen aan mij en de voorzitter van het College. De reviewboard zal worden gevraagd om expliciet aandacht te hebben voor de door de commissie geconstateerde ontwikkelpunten. De adviezen van de reviewboard en de reactie van het OM zal het OM elk jaar via het jaarbericht toelichten. Ik zal uw Kamer deze jaarberichten zoals gebruikelijk met mijn reactie toezenden.

De reviewboard zal bestaan uit de volgende leden:

- Arco Groothedde, bestuurder bij woningcorporatie Eigen Haard en onder meer voormalig algemeen directeur van Translink (bedrijf achter OV-chipkaart en OV-pay).
- Nathan Ducastel, directeur bij VNG-Realisatie en ambassadeur van de Nederlandse digitaliseringsstrategie.
- Bianca Rouwenhorst, directeur Informatiebeleid en CIO bij het Ministerie van Volksgezondheid, Welzijn en Sport.
- Jan Willem Duijzer, onder meer voormalig CIO bij de Rechtspraak.
- Richard van Breukelen, onder meer voormalig directeur ICT Belastingdienst en voormalig programmadirecteur ICT bij de politie.

Naast de inzet van de reviewboard zal ik de Audit Dienst Rijk vragen om een onderzoek uit te voeren naar de aanpak die het OM hanteert om met betrekking tot de Baseline Informatiebeveiliging Overheid (het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen).

Onze referentie
7766851

In het rapport wordt ook aandacht besteed aan de afhankelijkheden op het gebied van de ICT binnen de strafrechtketen en de noodzaak voor ketenorganisaties om goed samen te werken. Ik zal deze bevinding meenemen bij de uitwerking van de motie Mutluer,³ waarin de regering wordt verzocht te onderzoeken hoe de centrale regie op ICT binnen de justitiële keten kan worden versterkt. Ik zal u hierover dit jaar nader informeren.

Datum
8 oktober 2026

Tijdens het commissiedebat strafrechtketen op 8 september 2026 heb ik toegezegd in deze brief ook in te zullen gaan op de aansluiting van het OM bij het Shared Service Center-ICT (SSC-ICT) van de Rijksoverheid. Het SSC-ICT is een centrale eenheid binnen de Rijksoverheid, die IT-diensten levert aan andere delen van het Rijk. Het proces om de standaard werkplekken, waar het overgrote deel van de medewerkers bij het OM gebruik van maakt, aan te laten sluiten bij het SSC-ICT loopt. Hiermee wordt het OM minder afhankelijk van commerciële dienstverleners en wordt de kennis behouden. Ik kan nog niet kan aangeven wanneer de aansluiting is gerealiseerd, maar de inzet is om dit zo spoedig mogelijk te doen.

De Minister van Justitie en Veiligheid,

D.M. van Weel

³ Kamerstukken II, 2025-2026, 36800 VI, nr. 52.