Docnr1

RAPPORT

Van ‘brand meester’ naar ‘brandveilig’

Onderzoek naar de ICT-inbreuk bij het Openbaar Ministerie

Docnr1

Inhoudsopgave

HOOFDSTUK 1

1.1 Aanleiding 6
1.2 Instelling, opdracht en samenstelling 7
1.3 Doel en scope 7
1.4 Gevolgde aanpak 8
1.5 Leeswijzer en opbouw rapportage 8

HOOFDSTUK 2

2.1 Situatieschets van de gebeurtenissen rondom de inbreuk en het herstel van IV 9
2.2 Reflectie acute fase en herstel 12

HOOFDSTUK 3

3.1 Situatieschets van de historische gebeurtenissen en aanloop naar de inbreuk 13

HOOFDSTUK 4

4.1 Focus op de toekomst en het trekken van lessen 16
4.2 Reflectie op de toekomst 18

Bijlagen 21

Docnr1

Afkortingen en begrippen

Afkortingen	Betekenis
AD	Active Directory
BIO	Baseline Informatiebeveiliging Overheid
BKB	Bestuurlijke Ketenberaad
CIO	Chief Information Officer
CMT	Crisismanagementteam
CERT	Computer Emergency Response Team
CISO	Chief Information Security Officer
EDR	Endpoint Detection & Response
HBO	Hoog Beveiligde Omgeving
HovJ	Hoofdofficier van Justitie
IB	Informatiebeveiliging
IV	Informatievoorziening
IVOM	Directie Informatievoorziening OM
KA	Kantoorautomatisering
NCSC	Nationaal Cyber Security Centrum
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid
OM	Openbaar Ministerie
ORG	Interne kantoornetwerk
SOC	Security Operations Center

Begrippen
Assetmanagement is het systematisch beheren van alle IT-middelen gedurende hun volledige levenscyclus, met als doel inzicht, controle en risicobeheersing te waarborgen ter ondersteuning van onderzoek naar en beheersing van een inbreuk in een IT-systeem.
Citrix NetScaler is een geavanceerd netwerkapparaat (edge device) dat zorgt voor veilige en geoptimaliseerde levering van applicaties.
Edge device is een netwerkapparaat dat zich aan de rand van een netwerk bevindt en het verkeer tussen interne systemen en externe netwerken (zoals internet) verwerken of beveiligen.
Initial access betreft de eerste stap in een cyberaanval, waarbij een aanvaller een voet tussen de deur krijgt in het netwerk, systeem of de omgeving van het slachtoffer. Vanuit dit punt kan een aanvaller verdere acties in het IT-landschap van het slachtoffer uitvoeren.
Ketenpartners zijn de partners in alle ketens (Strafrechtketen, Vreemdelingenketen, Executieketen, etc.), waarbij we onderscheid maken tussen directe afnemers van de OM-gegevens (politie, CJIB, Justid) en indirecte partners zoals Justis, IND en DJI (die hun gegevens ophalen bij Justid).
Logging is het systematisch registreren van technische systeem- en applicatieactiviteiten in digitale logbestanden, zodat deze later kunnen worden geanalyseerd of gecontroleerd.
Monitoring is het doorlopend observeren van de werking en prestaties van IT-infrastructuur en software om afwijkingen vroegtijdig te detecteren en daarop te kunnen reageren.
Patch is een beveiligingsupdate voor een kwetsbaarheid waar nog geen eerdere oplossing voor beschikbaar was.
Performance issues betreft prestatieproblemen binnen IT-systemen, applicaties of infrastructuur waarbij de werking trager of instabieler is dan verwacht of afgesproken. Bijvoorbeeld lange responsetijden, hoge systeembelasting of capaciteitsproblemen.
Security issues betreft beveiligingsproblemen binnen IT-systemen, applicaties of infrastructuur waarbij de vertrouwelijkheid, integriteit of beschikbaarheid van gegevens en systemen in het geding is. Bijvoorbeeld kwetsbaarheden, ongeautoriseerde toegang of onvoldoende beveiligingsmaatregelen.
Web shell is een ongeautoriseerd programmaonderdeel op een webserver die een aanvaller via een webpagina toegang geeft tot bestanden of systemen. Een web shell wordt gebruikt als achterdeur.
Zero-day is een kwetsbaarheid in software of hardware die nog niet bekend is bij de leverancier of ontwikkelaar ervan en waarvoor nog geen patch beschikbaar is.

Docnr1

Preambule

In de voorliggende rapportage doet de Commissie evaluatie ICT-inbreuk Openbaar Ministerie verslag van haar bevindingen. Daarmee geeft zij antwoord op de vragen waarmee zij in december 2025 op pad is gestuurd. Centraal stond de vraag hoe het besluitvormingsproces is verlopen na de melding van een inbreuk via 'de voordeur' van de ICT-systemen: de Citrix NetScaler-omgeving. Een tweede vraag was of deze inbreuk voorkomen had kunnen worden en of de gevolgen ervan voorkomen of beperkt hadden kunnen blijven. In het verlengde van de genoemde vragen is gekeken welke lessen uit deze recente ervaringen kunnen worden getrokken.

Het risico van een dergelijk onderzoek is dat bevindingen niet altijd worden aangewend om van te leren, maar eerder om oordelen uit te spreken over verantwoordelijken. Eventuele verbeterpunten kunnen dan worden gezien als tekortkomingen, in plaats van als aansporing om zaken te verbeteren en aan te passen aan de actuele stand van zaken. Het is alsof iemand in de spiegel kijkt als een vorm van zelfreflectie, terwijl tegelijkertijd een ander meekijkt en vervolgens oordeelt en een beschuldigende vinger wijst. De commissie heeft getracht deze valkuil te vermijden. Deze rapportage moet in de eerste plaats worden gelezen als een poging om inzicht te bieden in de inbreuk, de omstandigheden waaronder deze plaatsvond en de vragen die dat oproept voor de toekomst.

Wat het Openbaar Ministerie (OM) is overkomen met deze inbreuk, is niet uniek. Regelmatig worden we opgeschrikt door dit soort digitale inbraken, bij publieke en private organisaties. We zullen ons als maatschappij moeten realiseren dat dit soort incidenten veelvuldig plaatsvindt. Het is onderdeel geworden van de ontwikkelingen op het gebied van cybercriminaliteit, digitale afhankelijkheden en geopolitieke spanningen.

Een cyberincident zoals hier onderzocht raakt zelden alleen de organisatie waar het plaatsvindt. De gevolgen werken door naar partners, leveranciers en organisaties waarmee digitale verbindingen bestaan. Dat geldt in het bijzonder voor het OM, dat opereert binnen een omvangrijke strafrechtketen met veel onderlinge afhankelijkheden, waarbij de politie en de rechtelijke macht de belangrijkste stakeholders zijn. Deze positie in de keten is van groot belang en de vraag wordt gesteld of het OM als relatief kleine organisatie (in vergelijking met beide genoemde stakeholders) deze centrale positie zelfstandig op adequate wijze kan invullen of dat bundeling van krachten en meer centrale regie op het gebied van IV noodzakelijk is.

In onze gesprekken met partijen in de omgeving van het OM die gevolgen van het incident hebben ervaren, kwam het belang van goede afstemming tussen partijen in de strafrechtketen duidelijk naar voren. Opvallend is dat veel partijen zich beroepen op hun specifieke en eigen karakter en rol en daarmee hun autonomie centraal lijken te stellen. Inhoudelijk is dat begrijpelijk en is ook voor de eigen rol van het OM van belang. Tegelijk roept het vragen op over samenwerking en afstemming op technisch en systemisch niveau.

Het beeld van een verzameling losse eilanden dat primair hun onafhankelijkheid centraal stelt, tegenover de vorming van een archipel waarin krachten worden gebundeld waar dat mogelijk is, biedt een bruikbare metafoor voor een aantal vraagstukken dat in deze rapportage aan de orde komt. Gezien vanuit het perspectief van de samenleving is dat van belang, omdat die het geheel zal bekijken en beoordelen op effectiviteit en betrouwbaarheid.

De spanning tussen het OM en het ministerie van Justitie en Veiligheid hoort bij de inrichting van onze rechtsstaat, maar raakt tegelijkertijd aan bredere vragen over verantwoordelijkheden, afhankelijkheden en sturing binnen complexe organisaties en ketens. Waar inhoudelijke en principiële scheidslijnen bestaan, kan wel gezocht worden naar samenwerking en afstemming op technisch en/of ander terrein.

Tot slot een opmerking over de rol van externe leveranciers. Moderne organisaties zijn in hoge mate afhankelijk van marktpartijen voor levering, beheer en onderhoud van hun digitale voorzieningen. Daarmee ontstaat een verwevenheid van verantwoordelijkheden die in tijden van crisis scherp zichtbaar kan worden. Ook dit vormt een belangrijk onderdeel van de context waarbinnen de inbreuk moet worden bezien.

Docnr1

De gebeurtenissen die in deze rapportage worden beschreven hebben grote gevolgen gehad voor het OM, voor organisaties in de strafrechtketen en voor de medewerkers die zich gedurende lange tijd hebben ingezet om de gevolgen ervan op te vangen. Een woord van grote waardering voor die inzet is daarom zeker op zijn plaats.

Deze rapportage bevat analyses, beschouwingen en aanbevelingen van de commissie. Heel in het kort zijn haar constateringen als volgt:

- Het OM is getroffen door een ernstige ('zero-day') inbreuk, zoals die in deze tijd vaker voorkomt bij verschillende organisaties.
- Het besluit om offline te gaan is begrijpelijk en in dit geval verstandig geweest.
- Het is mede aan de enorme inzet van vele medewerkers van het OM en andere organisaties te danken dat vele zaken doorgang hebben kunnen vinden en de keten niet is vastgelopen.
- Voorafgaand aan de inbreuk was de beveiliging van ICT-systemen onvoldoende, niet in de laatste plaats voor wat betreft het ontbreken van monitoring op cruciale systemen als Citrix NetScaler, waar het in het geval van het OM gaat om de ORG-omgeving.
- De beveiliging van ICT-systemen is geen bijzaak, maar een zeer belangrijke voorwaarde voor het goed functioneren van het primaire proces.
- Nauwere samenwerking en afstemming binnen de strafrechtketen, met erkenning van de inhoudelijke grenzen, is noodzakelijk.
- Leg de geleerde lessen en opgedane ervaringen n.a.v. de inbreuk vast zodat die gebruikt kunnen worden in de toekomst.

De titel van dit rapport wijst op de noodzaak om te investeren in brandveiligheid en dus preventie in plaats van regelmatig 'brandjes te moeten blussen' bij calamiteiten.

In de afgelopen jaren is 'de wekker meerdere malen afgegaan' en klonken waarschuwingen over de gebrekkige en verouderde ICT-systemen en de risico's die daarmee verbonden zijn. Het is alsof regelmatig 'de sluimerknop is ingedrukt' en noodzakelijke aanpassingen achterwege bleven. Dit veranderde met de aanstelling van de CIO als lid van het College, waarmee duidelijk werd dat er structurele aanpassingen nodig zijn en aandacht voor ICT-systemen tot op het hoogste niveau op de kaart zijn gezet. Daarmee zijn nog niet alle problemen opgelost, dat is het begin van een langer traject. Onze grote zorg hierbij is hoe ervoor te zorgen dat de uitvoeringskracht binnen het OM stevig vergroot wordt en de juiste prioritering van noodzakelijke aanpassingen en investeringen kan worden aangebracht. Het is zaak om dat ook in de komende jaren op goede en structurele wijze te borgen!

Drs. Jaap Smit

Voorzitter Onderzoekscommissie evaluatie ICT-inbreuk
Openbaar Ministerie

Docnr1

HOOFDSTUK 1

Inleiding

Het digitale dreigingslandschap verandert voortdurend en wordt steeds onvoorspelbaarder. Dat onderstreept ook het Cybersecuritybeeld Nederland 2025 van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). De NCTV ziet uiteenlopende aanvallen van statelijke actoren, cybercriminelen en andere kwaadwillenden. Geopolitieke onzekerheden hebben hun weerslag op het digitale domein: staten zetten eigen cyberprogramma's op of werken samen met private partijen en niet-statelijke actoren. Door verschuivingen in internationale verhoudingen kunnen digitale afhankelijkheden plotseling risicovoller worden dan voorheen werd gedacht.

Een cyberincident leidt vaak tot een organisatiebrede crisis die verder gaat dan alleen IT of security. De directe invloed op kritieke bedrijfsprocessen leidt tot uiteenlopende veiligheids- en bestuurlijke uitdagingen, maar ook tot operationele uitdagingen op het moment dat de continuïteit in het geding komt. Snelle besluitvorming met beperkte informatie is dan noodzakelijk. Een voorbeeld van een dergelijk besluit kan zijn om systemen af te sluiten en andere mitigerende maatregelen om vervolgschade te beperken.

Jaarlijks vinden vele cyberincidenten plaats variërend van phishing, DDoS-aanvallen tot kwetsbaarheden en ransomware. Ook zijn er afgelopen maanden veel incidenten gemeld waarbij er hacks hebben plaatsgevonden en waarbij waardevolle data buit is gemaakt. In recente jaren zijn Citrix NetScaler-omgevingen herhaaldelijk doelwit geweest van cyberaanvallen. Nieuwe en bekende kwetsbaarheden in deze omgeving vormen een aantrekkelijk doelwit voor statelijke actoren en criminele groeperingen. De impact hiervan is aanzienlijk, omdat Citrix NetScaler-systemen direct gekoppeld zijn aan het internet en dienen als toegangspoort tot kritische bedrijfsapplicaties.

Op 16 juli 2025 ontdekte het Nationaal Cyber Security Centrum (NCSC) sporen van misbruik op Citrix NetScaler-systemen in Nederland. Aanvallers hebben een web shell geplaatst door misbruik te maken van een kwetsbaarheid met kenmerk CVE2025-6543. Het NCSC stelde uiteindelijk vast dat meerdere vitale organisaties binnen Nederland succesvol zijn aangevallen via deze kwetsbaarheid. Uit later onderzoek bleek dat het ging om een zogenaamde 'zero-day'. Dit betekent dat de leverancier op het moment van misbruik van de kwetsbaarheid hierover nog niets bekend heeft gemaakt en er nog geen patch beschikbaar is.

1.1 Aanleiding

Op 16 juli 2025 ontving het Openbaar Ministerie (OM) een waarschuwing van het NCSC. Uit een scan van het NCSC bleek dat het OM mogelijk gecompromitteerd was. Bij nader onderzoek op 17 juli is een zogenaamde "web shell" aangetroffen op een Citrix NetScaler van het OM. Dit wees erop dat deze zeer waarschijnlijk was gecompromitteerd. Het OM koppelt dezelfde dag de interne systemen los van het internet om mogelijk verdere schade te beperken.

De impact hiervan op het OM en op partners en betrokkenen in en rond de strafrechtketen was groot. De minister van Justitie en Veiligheid en het College van procureurs-generaal (College) hebben daarom samen besloten een onderzoek te laten uitvoeren naar de ICT-inbreuk en gevolgen daarvan. Hiervoor is een onafhankelijke commissie samengesteld, te weten de *Commissie evaluatie ICT-inbreuk Openbaar Ministerie*.

Docnr1

1.2 Instelling, opdracht en samenstelling

De commissie is op 1 december 2025 formeel van start gegaan. De minister van Justitie en Veiligheid en het College van procureurs-generaal stelden in november 2025 de commissie evaluatie ICT-inbreuk Openbaar Ministerie in. De commissie heeft tot taak het onderzoeken van de ICT-inbreuk bij het OM zoals gemanifesteerd op 17 juli 2025. Het verzoek is geweest hierbij terug te blikken op het incident, te bekijken hoe de reactie van het OM hierop was en welke stappen het OM heeft gezet en welke risico's hierbij zijn gesignaleerd.

De commissie betrekt hierbij onder meer de complexiteit van de strafrechtketen en de onderlinge (digitale) afhankelijkheden, bij zowel de gevolgbestrijding als de uitvoering van de noodoplossingen.

Naar aanleiding van haar bevindingen is de commissie bevoegd aanbevelingen te doen, zoals over de wijze waarop incidenten in informatiebeveiliging in de toekomst zo veel mogelijk kunnen worden voorkomen en het vroegtijdig detecteren dan wel het beperken van de impact van (misbruik van) deze kwetsbaarheden, rekening houdend met de ketenorganisaties.

De commissie bestaat uit:

- De heer drs J. Smit, voorzitter, voormalig commissaris van de Koning in Zuid-Holland;
- De heer prof. dr. M.J.G. van Eeten, hoogleraar Cybersecurity aan de TU Delft;
- De heer drs. B. Voorbraak, algemeen directeur Logius.

De commissie is secretarieel bijgestaan door het COT Instituut voor Veiligheids- en Crisismanagement (COT) en het OM.

1.3 Doel en scope

Doel van dit onderzoek is het terugblikken op het incident dat zich manifesteerde op 17 juli 2025, inclusief de directe afhandeling daarvan. Hierbij is gekeken naar de reactie van het OM op het incident, de stappen die het OM zette en de wijze waarop het herstel is vormgegeven. Om de inbreuk bij het OM in de juiste context te plaatsen, is gekozen ook te kijken naar de fase voorafgaand aan het incident. Het doel hiervan is om zicht te krijgen op de context waarin het incident plaatsvond en hoe deze situatie kon ontstaan. Tot slot wordt gekeken naar reeds ingevoerde verbetermaatregelen en de richting die is bepaald voor toekomstige ontwikkelingen binnen het OM.

Gelijktijdig aan de inbreuk bij het OM vond elders in de strafrechtketen ook een inbreuk plaats in Citrix NetScaler-systemen, hier is besloten niet offline te gaan. Daar lagen andere afwegingen aan ten grondslag die voor dit onderzoek niet relevant waren.

Deze rapportage betreft geen verantwoordings- of technisch-forensisch onderzoek. Wel is waar mogelijk en zinvol gebruik gemaakt van inzichten van het uitgevoerde technisch-forensisch onderzoek.

1.4 Gevolgde aanpak

De commissie startte met het maken van een analyse van beschikbare documenten. Voorbeelden hiervan zijn besluitenlijsten van het College van procureurs-generaal, beleidsdocumenten, onderzoeksrapporten van externe partijen en tijdlijnen. Deze documenten zijn met de grootste zorgvuldigheid behandeld en uitsluitend ingezet om feiten scherp te krijgen en inzicht te krijgen in beschikbare informatie en gemaakte afwegingen. De rapportage is gebaseerd op die informatie, verkregen tijdens de periode waarin het onderzoek is uitgevoerd. Nieuwe of aanvullende informatie kan van invloed zijn op de inhoud en de geformuleerde conclusies.

De commissie heeft regelmatig overleg gevoerd om analyses te bespreken. Voor een verdiepend beeld zijn verschillende gesprekken gevoerd met betrokkenen. De commissie voerde 17 gesprekken met meerdere respondenten in de periode tussen december 2025 en augustus 2026. Om bevindingen te toetsen bij respondenten vond op 8 mei 2026 een reflectiesessie plaats en in juni zijn de voorlopige bevindingen gepresenteerd en getoetst op feitelijke juistheid. Dit alles leidde tot het opstellen van deze rapportage.

Docnr1

1.5 Leeswijzer en opbouw rapportage

Om de inbreuk en gevolgen zorgvuldig te analyseren, is gekozen voor een gefaseerde benadering. In hoofdstuk 2 beschrijven wij fase 1: de gebeurtenissen rondom de inbreuk en het herstel. Om deze gebeurtenissen in de juiste context te plaatsen, blikken wij in hoofdstuk 3 terug op de fase in aanloop naar het incident, benoemd als fase 0. Tot slot richten wij ons in hoofdstuk 4 op fase 2: de periode na de directe afhandeling van het incident en het trekken van lessen voor de toekomst, zowel voor het OM als voor de gehele strafrechtketen. In iedere fase is onderscheid gemaakt tussen het feitelijk schetsen van de situatie en geven wij vervolgens onze reflectie daarop.

Per fase zijn de bevindingen bekeken vanuit drie perspectieven: *techniek*, de *organisatiestructuur* en de *cultuur* van de organisatie. Daarbij is steeds gekeken hoe deze factoren een rol speelden tijdens het incident, in de aanloop naar het incident en bij de opvolging hiervan. In deze rapportage verwijzen we omwille van leesbaarheid naar 'incident' met het besef dat de inbreuk voor betrokkenen grote impact had en is ervaren als crisis.

Docnr1

HOOFDSTUK 2

Fase 1: Inbreuk en herstelproces

2.1 Situatieschets van de gebeurtenissen rondom de inbreuk en het herstel van IV

In dit hoofdstuk schetsen wij de gebeurtenissen rondom het ontdekken van de inbreuk en het herstel, ook wel fase 1 genoemd. We kijken naar de technische inrichting, de organisatiestructuur en de cultuur van de organisatie en de wijze waarop deze een rol hebben gespeeld tijdens het incident en het herstel.

2.1.1 Techniek

Op 16 juli 2025 waarschuwde NCSC het OM voor een mogelijk cyberincident met Citrix NetScaler-systemen. Het College van het OM besloot op 17 juli hierop de digitale omgeving van het OM af te sluiten van het internet. Het besluit is genomen vanwege een combinatie van factoren. Allereerst was het onduidelijk of interne netwerken waren gecompromitteerd en of data was geraakt of geëxfiltreerd – kortom, de aard en reikwijdte van de dreiging waren op dat moment volledig onbekend. Daarnaast beschikt het OM over zeer gevoelige informatie. Het was niet mogelijk om in kleinere segmenten offline te gaan. Het College was zich er daarbij van bewust dat de impact van het offline gaan op de strafrechtketen en alle betrokkenen in het strafproces groot zou zijn, al was niet duidelijk wat alle effecten zouden zijn.

Op het moment van de inbreuk is binnen het OM geen monitoring werkend op de kantoorautomatisering (ORG), waaronder ook de Citrix NetScaler-systemen vallen. Het gevolg hiervan is dat het OM Security Operations Center (SOC) op dat moment geen zicht had op de periode voor en na de inbreuk. Er viel niet vast te stellen wat precies was gebeurd en hoever de aanvallers waren binnengedrongen. Wel was er monitoring beschikbaar voor de Hoog Beveiligde Omgeving (HBO).

Nadat de Citrix NetScaler-systemen zijn losgekoppeld van het internet, startte op 18 juli 2025 het technisch-forensisch onderzoek door de gecontracteerde incidentresponsepartner van het OM: Deloitte. Deloitte vroeg logging van systemen op bij de externe leveranciers, waaronder de leverancier van de Citrix Netscaler-systemen. Dit onderzoek werd afgesloten op 7 augustus 2025. De analyse van de commissie is gebaseerd op het technisch-forensisch onderzoek van Deloitte. De commissie heeft geen aanvullend forensisch onderzoek uitgevoerd.

Volgens het forensisch onderzoek hebben de aanvallers een zogenaamde zero-day kwetsbaarheid in het Citrix NetScaler-systeem misbruikt. Hierdoor heeft men een "achterdeur" weten te plaatsen op het systeem. Dit is gebeurd op 19 juni of eerder – mogelijk zelfs al in mei. Deze kwetsbaarheid werd pas door Citrix publiek bekend gemaakt, en van een patch (beveiligingsupdate) voorzien, op 25 juni (CVE-2025-6543). De patch kan een voorafgaande inbreuk niet ongedaan maken. Hierdoor bleef de inbreuk bij het OM voortbestaan, ook na het toepassen van de patch. De inbreuk werd pas ontdekt op 16 juli door het NCSC. Dit betekent dat de aanvallers een kleine maand of langer toegang hebben gehad tot de gecompromitteerde NetScaler.

Het forensische rapport weet ook enkele andere activiteiten van de aanvaller te reconstrueren, met name verkeer tussen de NetScaler, de domaincontroller en de Exchange server (de e-mailomgeving). De beschikbare logbestanden tonen verdachte verbindingspogingen met de Exchange server, waarbij de actor op 20 juni 2025 succesvol kon inloggen met een gebruikersaccount. Uit de logbestanden bleek echter niet dat daadwerkelijk e-mails of andere mailboxgegevens zijn opgehaald.

Docnr1

Vanwege de beperkte logging op het ORG-netwerk kan het rapport geen duidelijkheid geven over de exacte toedracht van het incident. Naast de genoemde bevindingen kunnen er ook andere handelingen zijn geweest van de aanvaller in de periode dat deze toegang had tot de achterdeur op het NetScaler-systeem. Zoals gezegd was er wel logging voorhanden voor het HBO-netwerk. Bij de analyse van die logging vond men geen sporen van een inbreuk op dat netwerk.

De commissie constateert dat de feiten uit het forensisch rapport passen bij het volgende beeld, geformuleerd in termen van het MITRE ATT&CK framework. De inbreuk begon uit het verkrijgen van *initial access* door een aan een statelijke actor gelieerde partij. Vervolgens hebben de aanvallers *persistence* verkregen door het plaatsen van de "web shell". Daarna is *discovery* gedaan van het interne netwerk en pogingen tot *lateral movement* gesignaleerd naar de domeincontroller en de Exchange server. Het rapport beschrijft het testen van onderschepte gegevens, onder andere door in te loggen op de e-mailomgeving en gegevens van een specifieke gebruiker in te zien. Het lijkt erop dat de aanvallers niet zijn toegekomen aan vervolgstappen in het ORG-netwerk. Dit past bij het feit dat ook andere organisaties getroffen waren door aanvallen op dezelfde kwetsbaarheid en de aanvallers wellicht hun aandacht moesten verdelen. Het HBO-netwerk lijkt niet te zijn getroffen.

De impact van het besluit om offline te gaan, was op het moment dat dit genomen werd slechts deels te overzien. Enerzijds zou het offline halen van systemen leiden tot vooraf bekende verstoringen in het werkproces van het OM. Medewerkers konden bijvoorbeeld uitsluitend inloggen op kantoorlocaties, zij waren niet per mail bereikbaar en er was sprake van een beperkte functionaliteit van applicaties. Ook was vooraf duidelijk dat partners in de keten getroffen zouden worden door uitval van koppelingen. Anderzijds was de hoeveelheid en reikwijdte van de koppelingen van de OM-systemen in de strafrechtketen onbekend. Ook assetmanagement bleek tijdens het afsluiten een knelpunt, omdat onvoldoende inzichtelijk was welke IT-assets in gebruik waren en van welke processen zij afhankelijk waren. Dat betekent bijvoorbeeld dat een aantal onderdelen onbedoeld actief bleef, terwijl die onderdelen afgesloten hadden moeten worden met het offline gaan van het OM. Daarnaast werden er systemen offline gehaald die strikt genomen niet van het OM waren. Respondenten geven overigens aan dat ook wanneer de impact van het besluit volledig inzichtelijk was geweest, het offline gaan nog steeds de juiste keuze was.

Op 4 augustus, ruim twee weken na het ontdekken van de inbreuk, werd begonnen met het herstelproces. Het College stelde een reeks voorwaarden op waaraan de organisatie en het IT-landschap moesten voldoen voordat systemen weer live konden gaan. Hierbij was een inventarisatie gedaan van de bijbehorende risico's en mitigerende maatregelen, die uitmondde in een risico-inschatting en -acceptatie. Het College heeft daarin ook de belangen van de justitiabelen, de medewerkers en de maatschappij meegewogen. In de besluitvorming zijn aanbevelingen meegewogen vanuit o.a. AIVD, NCSC en de incidentresponsepartner van het OM.

Dit alles heeft geleid tot een zogenoemde plateauplanning (gecontroleerde, stapsgewijze opstart) met focus op primair processystemen en een werkwijze volgens een regiestructuur, onder aansturing van een Hoofdofficier van Justitie. De beveiligingsmaatregelen die moesten worden genomen alvorens een systeem weer online gebracht kon worden, het zogenaamde Plateau 0, waren:

- Het geheel vervangen van de gecompromitteerde Netscaler-infrastructuur ("greenfield");
- Het inrichten van Endpoint Detection & Response (EDR) monitoring op de kantoorautomatisering (voordat telewerken werd toegestaan);
- De HBO-omgeving loskoppelen van ORG;
- Het resetten van wachtwoorden voor de Active Directory (AD) van de kantoorautomatisering en HBO-omgeving.

Vervolgens werd bij de overgang naar elk volgend plateau ook een bijbehorend pakket beveiligingsmaatregelen geïmplementeerd, voordat koppelingen op systemen konden worden aangezet. Tegelijk werkte Team ICT aan een conceptplan voor livegang (op basis van de plateauplanning). In dit plan was aandacht voor 'harde' IT-vraagstukken en processystemen.

2.1.2 Organisatiestructuur

Het OM informeert in de avond van 17 juli 2025 de minister van Justitie en Veiligheid over het offline gaan vanwege diens verantwoordelijkheid voor het functioneren en de continuïteit van de justitiële keten. De minister informeert vervolgens de Tweede Kamer per brief over dit besluit[1].

Naast het besluit om offline te gaan, besloot het College op 17 juli 2025 tot het opstarten van een crisisorganisatie: het Crisismanagementteam (CMT) en tot het aanwijzen van de bestuurlijk CIO tot voorzitter daarvan. De crisisorganisatie van het OM schaalde op 18 juli 2025 officieel op. Vanaf dat moment startte dagelijks een voorbereidend-CMT, gevolgd

1 Minister van Justitie en Veiligheid, Kamerbrief Informatiebeveiliging OM, 17 juli 2025, Kamerstukken II 2024/25, 26643, nr. 1376.

Docnr1

door het CMT-overleg en aan het einde van de dag een digitaal overleg met de Hoofdofficieren van Justitie (HovJ's) en directeuren bedrijfsvoering en communicatie.

Tijdens het incident werden OM-medewerkers, parketleidingen en ketenpartners vanuit verschillende informatielijnen geïnformeerd. Nadat de situatie rondom het incident duidelijker werd, kwamen dagelijkse updates op gang en is geprobeerd de operatie en externe partijen waar mogelijk aan te haken. Door overleg binnen het Bestuurlijke Ketenberaad (BKB) kon het OM informatie delen met betrokken externe stakeholders, zoals het ministerie van Justitie en Veiligheid. Vanuit ketenpartners wordt echter een opmerking gemaakt over de grote mate van terughoudendheid van het OM in het delen van hoogvertrouwelijke informatie over het incident. De ketenpartners zijn immers eveneens gewend aan het werken met dit type informatie. In deze specifieke situatie bestond bij ketenpartners de behoefte om in een bepaalde setting meer van de hoogvertrouwelijke informatie te ontvangen. Dit stelde hen in staat de gevolgen voor hun werkprocessen en medewerkers in te schatten vanuit hun verantwoordelijkheid als werkgever.

Met betrekking tot het opstarten van het herstelproces in relatie tot het technisch-forensisch onderzoek, geeft een enkele respondent aan dat die van mening is dat herstelwerkzaamheden eerder hadden kunnen worden opgestart. In diens ogen zou vanwege de beperkte logging het technisch-forensisch onderzoek niet leiden tot een wezenlijk beter beeld van de inbreuk dan op dat moment bekend was. Het OM geeft hierbij aan dat de herstelwerkzaamheden begonnen zijn voor de definitieve uitkomsten van het onderzoek beschikbaar waren. Voor het College golden daarbij de vier eerder geformuleerde beveiligingsmaatregelen als leidend kader voor het herstelproces.

Na het afschalen van het CMT op 6 augustus is het Regieteam 'Stapsgewijze livegang' ingesteld, dit team verving de rol en taak van het CMT. Het Regieteam – bestaande uit vertegenwoordigers van Team Werkprocessen (Business), Team Informatievoorziening en Team ICT kwam eerst dagelijks, daarna drie keer per week en eind september nog eens per week bij elkaar. Het Regieteam bleef tot 29 september 2025 actief.

2.1.3 Organisatiecultuur

Het afsluiten van de organisatie had veel impact, zowel op het primaire proces binnen het OM als bij ketenpartners. Het effect op primaire processen zoals strafzaken, zittingen en de tenuitvoerleggingen van straffen is zo klein mogelijk gehouden door het volgen van noodprocessen. Daarbij lag de prioriteit bij het doorgaan van zittingen en behandelen van strafzaken. Er werd aanspraak gedaan op de vindingrijkheid, flexibiliteit en creatief handelen van OM en de ketenpartners. Het primaire proces bleef functioneren waardoor de maatschappelijke impact uiteindelijk beperkt bleef. De impact van de situatie op de strafrechtketen zelf was daarentegen groot. Organisaties als de rechtspraak, het CJIB, Slachtofferhulp, reclassering, Justid en de advocatuur hebben zich gedurende een lange periode intensief ingespannen om waar mogelijk bij te dragen aan het door laten gaan van de primaire processen in de ketens rond het OM en vertraging in de stapsgewijze livegang te beperken en in te lopen.

Het bleek een uitdaging om een goed beeld van de situatie te verkrijgen waarover ook gecommuniceerd kon en mocht worden. Alle externe communicatie – en een deel van de interne communicatie – diende zorgvuldig afgestemd te worden tussen OM en het ministerie. Het gevolg hiervan was dat communicatie trager was en beperkt bleef tot vooraf afgestemde mededelingen. Hierdoor hadden ketenpartners slechts beperkte informatie om hun eigen handelen op te baseren. Het informeren via de IV-lijn is richting ketenpartners voor zo ver mogelijk steeds gedaan. Vanuit de IV-organisatie van ketenpartners (politie) is ook kennis en ervaring ter beschikking gesteld aan het OM.

De communicatie via de CMT-lijn over de gevolgen voor de primaire processen bleef achter. Ketenpartners gaven aan dat belangrijke informatie hen niet of pas laat bereikte en dat telefonische bereikbaarheid gedurende het incident soms als onvoldoende werd gezien.

Respondenten geven aan dat de opgestelde voorwaarden waaraan moest worden voldaan voordat systemen weer live konden, zoals het installeren van EDR in de ORG-omgeving, in de praktijk lastig uitvoerbaar bleken en veel tijd vergden. Het inrichten van monitoring door het SOC bleek, anders dan EDR, niet binnen enkele maanden te kunnen worden geregeld. Dit werd mede veroorzaakt doordat leveranciers deze dienst buiten bestaande contractafspraken vonden gaan of omdat zij om andere redenen niet de relevante logging konden leveren.

Docnr1

Het CMT stelde een recovery plan vast, maar werd in de uitvoering verrast door de koppelingen in de keten die vooraf niet inzichtelijk waren. Enkele ketenpartners werden verrast door het moment waarop het CMT besloot af te schalen en de verantwoordelijkheid overdroeg aan het Regieteam. Bij verschillende ketenpartners waren op dat moment nog CMT's in werking om de effecten van het incident in goede banen te leiden. Voor hen was onvoldoende duidelijk dat het Regieteam ter vervanging van het CMT optrad.

2.2 Reflectie acute fase en herstel

Een inbreuk als deze komt in toenemende mate voor en organisaties zullen zich daar tegen moeten wapenen. Dit geldt des te meer voor het OM, gezien de gevoeligheid van de gegevens en de maatschappelijke rol van de organisatie. Het uitsluiten van een inbreuk is onmogelijk, maar het ontslaat een organisatie niet van de plicht om vooraf passende technische en organisatorische maatregelen te nemen die de gevolgen kunnen beperken.

Het adequate en weloverwogen improvisatievermogen van de organisatie bleek groot, met name door de vindingrijkheid en het flexibel en creatief handelen van medewerkers binnen het OM en de ketenpartners. Het is geruststellend dat het primaire proces handmatig doorgang kon vinden. Dankzij de veerkracht van het OM en ketenpartners is de maatschappelijke impact relatief beperkt gebleven, ondanks het feit dat de impact binnen de strafrechtketen groot was en de situatie veel van medewerkers heeft gevraagd. Op het moment van schrijven zijn bij sommige ketenpartners nog niet alle achterstanden ingelopen.

Het besluit om offline te gaan was verstandig, ook al was de impact hiervan vooraf onvoldoende scherp in beeld. Doordat de impact van het besluit vooraf niet volledig zichtbaar was, is ook de enorme informatiebehoefte wellicht onderschat. De werkwijze rondom afstemming van communicatie-uitingen tussen OM en ministerie werkte vertragend en begrenzend in wat gecommuniceerd kon worden, waardoor maar beperkt in de externe informatiebehoefte werd voorzien. Achteraf gezien had het ketenpartners geholpen om het besluit gepaard te laten gaan met snellere en uitgebreidere communicatie.

Het herstelproces begon pas meer dan twee weken na de inbreuk, op 4 augustus 2025. Die vertraging weerspiegelt een onderliggend dilemma voor het OM. De ene optie was de (tussen-)uitkomsten van het forensisch onderzoek af te wachten, om zodoende meer informatie te hebben over de aard en omvang van de inbreuk. Daarmee zou het herstelproces beter kunnen worden ingericht. Het nadeel daarvan is een latere start van het herstelproces. De andere optie was meteen te starten met het herstel, met als risico dat men handelt op basis van een onjuiste inschatting over de omvang van de inbreuk. De keuze om niet onmiddellijk met het herstel te beginnen is te begrijpen. Gezien het bijzondere en gevoelige type data waarover het OM beschikt, zijn zorgvuldigheid en betrouwbaarheid van groot belang. Een enkele respondent pleitte voor een eerdere start van het herstel, omdat vanwege de beperkte logging een volledig beeld hoe dan ook zou uitblijven, ook na het forensisch onderzoek.

Alles overziend concludeert de commissie dat het, na de melding van de inbreuk in Citrix NetScaler en de toen nog onbekende impact van offline gaan, begrijpelijk en navolgbaar is dat het OM besloot alle interne systemen los te koppelen van het internet.

Docnr1

HOOFDSTUK 3

Fase 0: Historie en aanloop naar de inbreuk

In dit hoofdstuk schetsen we de periode voorafgaand aan het incident, fase 0. Dit plaatst deze inbreuk in de juiste context. We kijken wederom naar de technische inrichting, de organisatiestructuur en de cultuur van de organisatie en de wijze waarop deze een rol hebben gespeeld in de aanloop naar het incident.

3.1 Situatieschets van de historische gebeurtenissen en aanloop naar de inbreuk

Het OM kampte al langere tijd met verouderde systemen. In 2023 informeerde de minister de Tweede Kamer hier al over per brief[2]. Voorafgaand aan de inbreuk, die zichtbaar werd op 16 juli 2025, vonden steeds kleine incidenten en verstoringen in de IT plaats. Dit waren geen beveiligingsincidenten, maar continuïteitsproblemen met applicaties en systemen. Het lukte het OM steeds deze incidenten ad hoc op te lossen, het spreekwoordelijk blussen van een brand. De middelen en capaciteit die benodigd waren in het blussen van deze branden, zorgden er echter voor dat structurele veranderingen of verbeteringen op het gebied van securitymaatregelen achterbleven. De problematiek is onder andere het gevolg van een langdurige achterstand in professionalisering van de IV. Er is wel geïnvesteerd in IV, maar onvoldoende in het inrichten van passende beveiligingsmaatregelen. Het verbeteren van IV, en in het bijzonder beveiliging, is een omvangrijk traject, dat nog een aantal jaar tijd en investeringen vergt.

3.1.1 Techniek

In de fase voor de inbreuk had het OM geen specifieke bescherming ingericht voor de Citrix NetScaler, anders dan

Daarnaast is elke Citrix NetScaler permanent vatbaar voor een zogenaamde 'zero-day' kwetsbaarheid. Er worden regelmatig zero-day kwetsbaarheden gevonden in Citrix NetScaler. Het enige antwoord op dit risico is zorgvuldig te monitoren wat er op en rondom de Citrix NetScaler gebeurt.

Van dergelijke monitoring was binnen het OM geen sprake. Monitoring vereist zowel logging van relevante systeemactiviteiten als tooling (software) waarmee deze gegevens kunnen worden geanalyseerd en afwijkingen of verdachte activiteiten tijdig kunnen worden gesignaleerd. Tot eind 2023 maakte het OM gebruik van een licentie van het ministerie van Justitie en Veiligheid voor de tooling (ArcSight) voor het monitoren van de kantoorautomatiseringsomgeving. In 2022 kondigde het ministerie aan om in december 2023 te stoppen met de dienstverlening, waarna het OM zelf verantwoordelijk zou worden voor het inrichten van tooling. Het ministerie stopt de licentie uiteindelijk om moverende redenen een maand eerder dan verwacht, namelijk november 2023.

Op dat moment heeft het OM nog geen alternatief georganiseerd. Pas in het najaar van 2024 wordt budget toegewezen voor het inrichten van monitoring op ORG, inclusief de Citrix NetScaler. Op het moment van de inbreuk in 2025 was tooling wel geïnstalleerd, echter was de logging nog niet ontsloten. Dit betekent dat er geen monitoring en logging van de kantoorautomatisering (ORG) beschikbaar was toen het OM op 17 juli de waarschuwing van het NCSC ontving. Het SOC had dus geen zicht op deze omgeving, inclusief de Citrix

2 Brief van de ministers van Justitie en Veiligheid en voor Rechtsbescherming, 15 februari 2023, Informatie- en communicatietechnologie (ICT) Kamerbrief 26 643 nr.

Docnr1

NetScaler-systemen. Het SOC beschikte wel over monitoring van de HBO-omgeving, waarvoor tooling was ingekocht en ingericht.

Respondenten geven aan dat het OM voor de inbreuk al jaren te maken heeft met instabiele, trage en verouderde ICT-systemen, zogenaamde performance issues. Zo vinden met regelmaat verstoringen plaats in systemen en zijn systemen op momenten onbereikbaar. Problemen in kritieke systemen veroorzaken vertragingen in het primaire proces van het OM. Het oplossen van de acute performance issues kreeg een hogere prioriteit dan structurele verbeteringen op informatiebeveiliging (IB).

3.1.2 Organisatiestructuur

In de periode voorafgaand aan het incident in juli 2025 ontbrak een structurele analyse en aanpak van de risico's rondom de digitale infrastructuur. Processen rondom dreigingsanalysen ontbraken of waren gebrekkig ingericht. Daarnaast was er binnen het OM geen vast risicomanagementproces georganiseerd, waardoor het analyseren, mitigeren en accepteren van risico's door het College onvoldoende plaatsvond.

Op 1 januari 2020 trad de Baseline Informatiebeveiliging Overheid (BIO) in werking. Alle Nederlandse overheidsinstanties werden hierdoor verplicht te voldoen aan de zogenaamde BIO-normen. Het hoofddoel hiervan is een betrouwbare, veilige overheid. Het OM voldoet op het moment van de inbreuk niet aan al deze normen. Het OM is hierin overigens niet uniek.

Naast de gebrekkige dreigingsanalyse en risicomanagementprocessen, had de Chief Information Security Officer (CISO) lange tijd geen centrale positie in de IV-organisatie. Tot kort voor de inbreuk was de positionering van de CISO onvoldoende verbonden met bestuurlijke en strategische processen, waardoor de invloed op prioriteiten, besluitvorming en organisatie-brede maatregelen beperkt bleef. Er bestond in die periode geen duidelijke lijn tussen de CISO en het College, met als gevolg dat belangrijke aandachtspunten op het gebied van IB niet structureel werden meegenomen in de strategische koers van de organisatie.

Hierin kwam verandering vlak voor de inbreuk, met de indiensttreding van de bestuurlijk CIO (per 1 maart 2025) en een nieuwe directeur IVOM (per 14 april 2025). In de periode daarna krijgt de CISO een periodieke afstemmingslijn. Het aanstellen van de bestuurlijk CIO was ingeven door de erkende noodzaak om de IV van het OM te verbeteren en voor te bereiden op de komst van het nieuwe Wetboek van Strafvordering.

Uit gesprekken met respondenten blijkt dat contracten met leveranciers niet altijd overeenkwamen met verwachtingen of behoeften van het OM. Zo beschikte de organisatie uitsluitend over productcontracten en niet over dienstcontracten. In deze contracten waren beveiligingsaspecten onvoldoende geborgd. De aard van de uitbesteding en behoeften van het OM vroegen juist om servicegerichte afspraken, zodat leveranciers ook verantwoordelijkheid dragen om continu hun diensten aan te passen aan de laatste stand van zaken. Hiermee ontstaat ook bij leveranciers een verhoogde aandacht aan beveiliging. Daarnaast werken leveranciers zo contractueel mee met het aansluiten van hun diensten op het SOC van het OM via het aanbieden van relevante logbestanden. Daarnaast zijn er bij het OM enkele contractmanagers beschikbaar, maar dit is ontoereikend voor het aantal contracten en de complexiteit ervan. Idem voor leveranciersmanagers, ondanks dat het overgrote deel van werkzaamheden extern is belegd.

De IT-organisatie werd vanuit verschillende hoeken gelijktijdig belast. Naast een aantal initiatieven voor het borgen van de continuïteit van de IV, liepen er ook binnen het portfolio meer dan 150 initiatieven met een IV-component, waardoor de druk op de uitvoeringskracht verdeeld werd over deze verschillende projecten. Eén van deze vele projecten is de transitie rondom Emma, het nieuwe digitaliseringsprogramma van het OM dat de uitvoering van het nieuwe Wetboek van Strafvordering moet gaan ondersteunen. Dit programma liep aanvankelijk 'naast' IVOM, maar vroeg ook capaciteiten en specifieke kennis vanuit IVOM en de leveranciers. Performance issues werden binnen de organisatie op ad hoc basis opgelost. Gezien de regelmaat van storingen had ook dit grote impact op de capaciteit. Daarnaast ging veel capaciteit naar de nieuwe organisatie van Informatievoorziening OM (IVOM).

3.1.3 Organisatiecultuur

Binnen de organisatie was tot op het niveau van de leiding bekend dat de IV-organisatie niet goed functioneerde. In de eerste helft van 2025 zijn hiervoor verschillende maatregelen getroffen, zoals de aanstelling van de bestuurlijk CIO en nieuwe directeur IVOM. Dit ging echter primair over performance issues binnen IV en het opleveren van nieuwe functionaliteiten zoals Emma en nog te weinig over security issues. De commissie herkent dat met deze verhoogde aandacht voor ICT er een aantal verbeteringen in gang is gezet, in het hoofdstuk over fase 2 wordt hier meer aandacht aan besteed. Deze verbeteringen hadden echter nog onvoldoende werking alvorens het OM werd geconfronteerd met de inbreuk dat onderwerp van onderzoek is in dit rapport.

Docnr1

Dieper in de organisatie heerste al langere tijd een gedeeld gevoel van onmacht ten aanzien van de ontwikkeling en staat van het IT-landschap, ook voor wat betreft de beveiliging. Signalen over de informatiebeveiligingsrisico's werden enerzijds onvoldoende opgemerkt door het College en anderzijds niet krachtig genoeg gecommuniceerd vanuit IVOM. Dit blijkt uit diverse voorbeelden die genoemd werden in de gesprekken. De CISO had geen direct overleg met de hoogste besluitvormers. Sommige respondenten gaven aan dat een rapportage over beveiligingsrisico's richting hogere organisatieniveaus werd aangepast waardoor deze aan scherpte verloor. Lager in de organisatie werd een bepaalde periodieke rapportage gestaakt omdat men het idee had dat deze niet gelezen werd; en dat staken leidde niet tot vragen van bovenaf. Door deze gebrekkige communicatie werd op bestuurlijk niveau het gevoel van urgentie onvoldoende ervaren en ontbrak de noodzakelijke prioriteitstelling op dit vlak. Dat vervolgens het inrichten van monitoring voor de ORG-omgeving uitbleef is een logisch gevolg van het feit dat de impact en daarmee samenhangende risico's op dat moment onvoldoende scherp in beeld waren.

3.1.4 Reflectie terugkijkend op de aanloop

Het beschermen van internet-facing systemen zoals Citrix NetScaler behoeft de allerhoogste prioriteit in de beveiliging van organisaties. *Edge devices*, zoals Citrix NetScaler, behoren al jaren tot de meest aangevallen systemen en zijn doelwitten van statelijke actoren en cybercriminelen. Hierin worden regelmatig zero-day kwetsbaarheden misbruikt. In de afgelopen vijf jaar zijn zeven zero-day kwetsbaarheden ontdekt bij Citrix NetScaler en heeft een scala aan Nederlandse organisaties te maken gehad met inbreuken. Uit de dreigingsanalyse had moeten blijken dat Citrix NetScaler doorlopend nauwkeurig gemonitord diende te worden op verdachte gebeurtenissen. Hieruit hadden beveiligingsmaatregelen moeten volgen ten aanzien van Citrix NetScaler. De langdurige afwezigheid van monitoring is een illustratie van onderschatting van het belang van goede beveiliging.

De onvolledige beveiliging van Citrix NetScaler is mede het gevolg van de nadruk op IT als 'instrument' voor het goed functioneren van het primaire bedrijfsproces en te weinig aandacht voor mogelijke kwetsbaarheden en veiligheidsrisico's van de gebruikte systemen. Deze focus weerspiegelt de organisatiecultuur waarin IV voornamelijk is gericht op het in standhouden en verbeteren van het primair proces. Dit patroon heeft invloed gehad op investeringen, besluitvorming en aandacht voor digitale voorzieningen en beperkte de mogelijkheden om de IV-organisatie strategisch te positioneren. Hierdoor ontstaat de spreekwoordelijke cultuur van "brandjes blussen" van IT-incidenten, zonder de mogelijkheid structurele verbeteringen of veranderingen door te voeren.

Het contractmanagement van het OM was onvoldoende scherp georganiseerd: contracten sloten vaak niet aan bij de verwachtingen, ook op het gebied van beveiliging. De capaciteit voor contractbeheer en leveranciersmanagement paste niet bij het grote aantal contracten en de omvang van extern belegde werkzaamheden.

Buiten contractmanagement was en is de druk op beschikbare IT-capaciteit hoog. Problemen met de performance van IV en het herstellen hiervan slokte veel tijd, energie en aandacht op. De honderden IV-initiatieven die liepen, waarvan Emma er één was, vraagt continu om een scherpe prioritering in inzet en capaciteit. Het primaire proces kreeg daarbij voorrang, dit is navolgbaar omdat de risicoafweging met betrekking tot het ontbreken van monitoring onvoldoende scherp was.

Deze capaciteitsdruk speelde overigens breder in de strafrechtketen. Ook andere organisaties richtten hun inzet primair op de eigen ontwikkeling, waardoor ook zij onvoldoende toekwamen aan gezamenlijke verbeteringen binnen de keten. Tijdens de inbreuk werd dit extra zichtbaar en voelbaar toen de hoeveelheid en complexiteit van de koppelingen van het OM naar de ketenpartners boven tafel kwamen. Uit 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 voldoende zijn gerealiseerd.

De keuze om op korte termijn technische problemen op te lossen waren steeds navolgbaar. Het leidde echter tot het ondersneeuwen van het belang en het daadwerkelijke realiseren van een adequate beveiliging. Signalen over de problematiek binnen de organisatie werden onvoldoende opgemerkt en zijn anderzijds onvoldoende krachtig gecommuniceerd.

Docnr1

HOOFDSTUK 4

Fase 2: Situatie en duiding richting toekomst

In dit hoofdstuk schetsen we welke stappen inmiddels zijn gezet en welke lessen verder richting toekomst te formuleren zijn. We richten ons primair op de periode na het afronden van het Regieteam op 29 september 2025. Ook hier kijken we eerst naar de technische inrichting, de organisatiestructuren en de verschillende culturen van zowel OM als ketenpartners.

4.1 Focus op de toekomst en het trekken van lessen

De bevindingen in de periode voorafgaand aan het incident (fase 0) en gedurende het incident (fase 1), vormen de basis waarop de analyse is uitgevoerd met het oog op de toekomst. Lessen die getrokken zijn omtrent het incident, zijn ook in de toekomst van toepassing. Sommige van deze geleerde lessen zijn al voor het incident ingevoerd, zoals het aanstellen van een bestuurlijke CIO. Andere zijn toegepast naar aanleiding van het incident. Met het oog op de toekomst zijn daarnaast andere en aanvullende lessen te trekken.

Zo leidde het incident tot onder meer extra werklast en oplopende voorraden bij het OM en ketenpartners en zorgde het offline gaan voor vertragingen in processen en communicatie. Nog steeds zijn de effecten daarvan merkbaar. Er zijn en worden nog steeds fors extra inspanningen geleverd door het OM en ketenpartners om de impact te beperken. Op 28 oktober 2025 vond een mini werkconferentie 'CTRL+Alt+Fwd' plaats op initiatief van de bestuurlijk CIO en de voorzitter van het Regieteam. Dat moment wordt gezien als stap richting toekomst.

De inzet en adequate creativiteit van veel medewerkers in de gehele strafrechtketen om de belangrijkste primaire processen via handmatige procedures werkbaar te houden, verdient waardering. Daarbij verdient het permanente aandacht en doorontwikkeling van een crisisstructuur zodat de organisatie(s) in staat zijn en blijven om tijdens grote IT-verstoringen hun maatschappelijke taak (met mogelijke beperkingen) te blijven uitvoeren. Hier zijn waardevolle lessen geleerd die niet verloren zouden mogen gaan voor de toekomst.

4.1.1 Techniek

Al voor het incident op 17 juli zette het OM stappen in het verbeteren van het IV-landschap en zijn intussen i-Plannen opgesteld bestaande uit een i-Visie en i-Strategie. Deze zijn gedeeld binnen de organisatie. Ook was het OM voor het incident begonnen met het inrichten van tooling en monitoring, na het incident is hier meer nadruk op gekomen en is hiermee verder gegaan. Hier is vooruitgang in geboekt.

Door het OM wordt gewerkt aan het herstellen en verbeteren van de ICT-infrastructuur. Dit is een meerjarig traject, ingestoken langs de lijn van vijf thema's. Digitale weerbaarheid is één van die thema's.

De komst van Emma, waarin veiligheidsmaatregelen in de architectuur zijn opgenomen, biedt niet de oplossing voor de beveiligingstekorten die geconstateerd zijn in de legacy-omgeving. Waar eerder werd gedacht dat het operationeel worden van Emma op korte termijn de functie van de legacy-omgeving deels zou kunnen overnemen, is inmiddels duidelijk dat die aanname niet meer klopt. De realisatie en ingebruikname van Emma is vertraagd. Beide omgevingen zullen de komende jaren parallel ingericht en onderhouden moeten worden. De legacy-omgeving zal dus ook van de nodige veiligheidsmaatregelen moeten worden voorzien. Het gevolg is dus een nog groter beslag op de toch al beperkte uitvoeringskracht die beschikbaar is voor de vele IT-projecten die lopen binnen het OM.

Docnr1

De verwachting is dat de komende tijd het aantal koppelingen in systemen op basis van de verbetermaatregelen eerder toeneemt dan afneemt. Respondenten geven aan dat het verminderen van het aantal koppelingen geen doel op zich is, maar dat deze koppelingen robuust moeten zijn.

4.1.2 Organisatiestructuur

De positionering van IV binnen de organisatie is aanzienlijk verbeterd. De verbeteringen begonnen al voor het incident en zijn daarna doorgezet. De bestuurlijk CIO is tijdelijk toegevoegd aan het College. Op korte termijn wordt gekeken of dit op deze wijze gehandhaafd wordt en ons advies is daartoe te besluiten. Ook de inrichting van IB is verbeterd. De CISO is anders gepositioneerd en meer betrokken bij besluiten in de organisatie. Ook is het portfoliomanagement, waar prioriteiten gesteld moeten worden beter ingericht.

Er is inmiddels stabiliteit in het management binnen IVOM dat bijdraagt aan kennis en bewustwording op dit onderwerp. Daarnaast is besloten om het programma Emma in te bedden binnen IVOM en onder te brengen in de directie Vernieuwing. Het is belangrijk de verschillende IVOM-onderdelen actief te blijven betrekken in verbeterplannen.

Het OM heeft te maken met een grote en aanhoudende uitdaging om de uitvoeringskracht te verkrijgen om de goede plannen die er liggen uit te voeren. Dit betekent dat de termijn waarop plannen gerealiseerd kunnen worden onder druk staat. De beperkte uitvoeringskracht betekent het maken van afwegingen. Het brengt het risico met zich mee dat i-Plannen niet automatisch op afzienbare termijn leiden tot de gehoopte verbetering. Respondenten spreken nadrukkelijk over beperkte uitvoeringskracht en niet over een capaciteitsprobleem. Het beeld ontstaat dat het OM beschikt over voldoende capaciteit, maar dat deze gerichter en scherper moet worden ingezet om plannen daadwerkelijk te realiseren. Gezien de omvangrijke opgaven waar het OM voor staat moeten soms lastige keuzes gemaakt worden in het uitvoeren van plannen. Tegelijkertijd bestaat de indruk dat intensievere samenwerking tussen en met de IV-organisaties van ketenpartners nog veel potentieel biedt. Hierdoor kunnen kennis en ervaring tussen de IV-organisaties worden uitgewisseld en kan een meer integraal beeld ontstaan. Het OM wordt gezien als een cruciale speler in de keten en ketenpartners kunnen de IV-organisatie van het OM waar en wanneer nodig versterken.

Het risicomanagementproces is nog onvoldoende expliciet gemaakt volgens respondenten. Het is essentieel om bewuste keuzes te maken over welke risico's het OM accepteert en welke actief moeten worden gemitigeerd. Dit vraagt om een duidelijke inrichting van rollen, verantwoordelijkheden en besluitvorming, zodat inzicht bestaat in zowel strategische als operationele risico's en de bijbehorende beheersmaatregelen. Daarnaast is het noodzakelijk om contractmanagement verder te professionaliseren. Informatiebeveiliging moet daarbij een integraal onderdeel zijn van contractafspraken, inclusief heldere eisen, toetsing en periodieke monitoring.

De verantwoordelijkheid voor securitymaatregelen is nog onvoldoende vastgelegd, waardoor onduidelijkheid ontstaat over aanspreekbaarheid en het risico toeneemt dat maatregelen niet structureel worden toegepast, gemonitord of geactualiseerd.

Ketenpartners in de strafrechtketen zijn van elkaar afhankelijk, systemen moeten hierop zijn ingericht. Binnen de strafrechtketen is geen centrale organisatie die de regie heeft op de samenwerking of het overzicht behoudt of stuurt op de ontwikkelingen binnen de keten. De keten is dermate complex dat geheel centrale regie onwenselijk is, maar een gedegen overzicht wel bijdraagt. Het brede gebrek aan uitvoeringskracht maakt dat de keten er niet in slaagt de link tussen de verschillende organisaties te leggen. Alle organisaties binnen de keten hebben hun capaciteit nodig om eigen processen draaiend te houden en aan te passen naar bijvoorbeeld veranderende wetgeving. Om de samenwerking binnen de keten te bevorderen is vervolgens te weinig uitvoeringscapaciteit, hierdoor komt het versimpelen van de keten nauwelijks van de grond. Daarnaast hebben sommige ketenpartners juist principiële overwegingen om bepaalde koppelingen niet te vereenvoudigen.

Docnr1

4.1.3 Organisatiecultuur

Het urgentiebesef is groot en de problemen worden breed erkend. Dit besef werd verder versterkt door de brandbrief van 20 november 2025. Het College van procureurs-generaal ontving een brief van het Comité OM Onder Druk, de brief is door 2850 medewerkers ondertekend. Zij stelden dat de ICT-problemen binnen het OM het resultaat zijn van jarenlange onvoldoende bestendige en consequente investeringen en eerdere bezuinigingen. Het OM liet in een reactie op de brandbrief weten te worden geconfronteerd met krappere financiële kaders door stijgende IV-kosten, het wegvallen van tijdelijke budgetten, niet-gecompenseerde claims, dalende instroom van zaken en rijksbrede bezuinigingen. Het College is hierover in gesprek met het ministerie, tegelijkertijd vraagt het OM-onderdelen maatregelen voor 2026 uit te werken.

Het College erkent in haar brief dat de recente ICT-inbreuk en jarenlange verstoringen veel impact hebben gehad op medewerkers en dat de focus op incidenten ten koste is gegaan van vernieuwing en strategische ontwikkeling. Ook is aangegeven dat hard gewerkt wordt aan structurele verbeteringen. Het College zegt toe transparanter te communiceren, vaker in gesprek te gaan met medewerkers en keuzes zorgvuldig en met oog voor de menselijke maat te maken.

Om de IV structureel te verbeteren, wordt gewerkt aan de uitvoering van de i-Visie, i-Strategie en i-Plan met aandacht voor betrouwbare dienstverlening, digitale weerbaarheid en modernisering van het IT-landschap. Er zijn al concrete stappen gezet, zoals extra servers en een nieuwe Outlook-omgeving, en er loopt een aanbesteding voor stabielere kantoorautomatisering. Het College benadrukt dat medewerkers beter geïnformeerd zullen worden over voortgang en keuzes.

Zoals vrijwel alle organisaties binnen de keten zich beroepen op hun eigen karakter en autonomie, doet het OM dat ook. Dit betekent dat organisaties ook alle eigen i-Plannen hebben en deze niet op elkaar zijn afgestemd. De commissie ziet nu wel eerste aanzetten om deze visies en plannen met elkaar te delen en op elkaar af te stemmen.

4.2 Reflectie op de toekomst

Al voor het incident zijn goede eerste stappen gezet om het IVlandschap maatschappelijk weerbaarder en robuuster te maken en de positionering van IV binnen de organisatie te versterken. De uitgevoerde stappen leidden in meer en mindere mate tot verbeteringen. Toch ziet de commissie dat de stappen die al in gang zijn gezet of die in gang gezet gaan worden nog niet toereikend zijn. De plannen verdienen extra uitwerking en concretisering, zoals het beleggen van verantwoordelijkheden en benoemen van tijdspaden.

Het grootste punt van zorg van de commissie is de beperkte uitvoeringskracht van het OM voor het verbeteren en moderniseren van de IT. Die beperkte uitvoeringskracht lag ten grondslag aan het langdurig opereren zonder monitoring op de ORG-omgeving. Er lag wel een plan, maar dit werd pas laat van geld en capaciteit voorzien. Dit is slechts één van de gevolgen. De zorgen over uitvoeringskracht spelen over de volle breedte van de IT-voorzieningen, niet alleen rondom beveiliging. Het verouderd landschap zorgt op allerlei manieren voor problemen. Tegenover de commissie voor Justitie en Veiligheid (J&V) van de Eerste Kamer omschreef de voorzitter van het College van procureurs-generaal het als "veel oude meuk".[3] Er wordt gewerkt aan het nieuwe plan Emma terwijl het bestaande ITlandschap tegelijkertijd ook in stand moet blijven.

Gegeven de enorme opgave waarvoor het OM staat, baart de beperkte uitvoeringskracht ons de meeste zorgen. Het is de vraag of en hoe de recente plannen, ook op het gebied van beveiliging, snel genoeg uitgevoerd kunnen worden. Hierdoor worden twee landschappen parallel beheerd en blijft de druk op de uitvoeringscapaciteit ook de komende jaren hoog.

De uitvoering vergt meerdere jaren en een verandering van een complex landschap kost simpelweg tijd. De beperkte uitvoeringskracht vraagt om duidelijk in de lijn belegde verantwoordelijkheden op het gebied van securitymaatregelen. In een volwassen IVorganisatie zijn governance, eigenaarschap en accountability expliciet belegd, zodat security integraal onderdeel is van sturing, planningencontrol en dagelijkse operatie. Dat betekent niet alleen het aanwijzen van een eigenaar op papier, maar ook het toewijzen van operationele verantwoordelijkheid voor de daadwerkelijke uitvoering, naleving en rapportage, zodat duidelijk is wie aanspreekbaar is op resultaat en continuïteit.

3 Verslag van de vergadering van de commissie voor Justitie en Veiligheid (J&V) op 23 september 2025, https://www.eerstekamer.nl/commissievergadering/20250923_j_v_2/verslag

Docnr1

De problemen met uitvoeringskracht spelen niet alleen binnen het OM, maar ook breder in de strafrechtketen. De uitvoeringscapaciteit voor verbeteringen is beperkt, de inzet ervan vraagt daarom om centrale afstemming en regie. Dit is ook in lijn met de rapporten van de Rekenkamer en het Adviescollege ICT-toetsing[4]. Organisaties richten zich tot elkaar wanneer zij iets verwachten, maar de capaciteit is onvoldoende om aan die gevraagde verwachtingen te voldoen. Het is zeker het onderzoeken waard om te kijken naar meer strategische en tactische samenwerking tussen de IV-organisaties van de ketenpartners; het OM wordt als cruciale organisatie in de keten gezien en het zorgen voor een adequaat ingerichte en werkende IV-organisatie binnen het OM is daarmee van groot belang.

Ook het aantal koppelingen zal hoog blijven en waarschijnlijk verder toenemen. Wel kunnen deze koppelingen zo worden ingericht dat het uitvallen van één onderdeel niet direct verstoringen veroorzaakt in andere delen van de keten. Betere segmentatie van systemen, verbonden via API's (Application Programming Interface), is daarbij wenselijk. Daarnaast moeten systemen beter om kunnen gaan met het opnieuw starten van het uitgevallen onderdeel. Zoals een ketenpartner benoemde: het opstarten zorgde voor meer problemen dan het afschakelen.

Het herinrichten van de koppelingen vereist afstemming tussen de ketenpartners. Voorgestelde wijzigingen stuiten soms op principiële bezwaren. De breed gehanteerde nadruk op het specifieke en eigen karakter van organisaties en hun onafhankelijkheid kan de noodzakelijke verbeteringen van koppelingen tussen de ketenpartners in de weg zitten.

De commissie ziet dat de juiste weg is ingeslagen. Positief is dat de achterstand in IV is onderkend en hier additionele financiële middelen voor vrij gemaakt worden. Het zal echter ruime tijd vergen om de achterstand weg te werken en het niveau van 'brandveilig' te hebben bereikt. Het OM moet dit voor de eigen organisatie bereiken, maar belangrijk is te blijven constateren dat het werken in de keten een eigen dynamiek kent met de grote uitdagingen die daarin spelen.

Tot slot de belangrijkste geleerde lessen voor de toekomst:

- Blijf investeren in fallback-opties, zoals handmatige werkprocessen, zodat bij grote IT-verstoringen de primaire processen snel kunnen worden voortgezet. Versterk daarmee de crisisstructuur en werk het Business Continuïteitsplan verder uit en periodiek bij. De commissie ziet in de samenwerking tussen Politie en OM een mooi voorbeeld waarop geïnvesteerd is in een gezamenlijke werkomgeving waarin medewerkers van beide organisaties al structureel samenwerken in operationele processen. In deze samenwerkingsvorm is het relatief eenvoudig om bij uitval van digitale systemen (hierbij hoeft niet alleen aan een cyberaanval gedacht te worden) handmatig de meest cruciale processen voortgang te blijven laten vinden.
- Ontwikkel voor de strafrechtketen een gezamenlijk Business Continuïteitsplan en richt de ketenarchitectuur zodanig in dat uitval van één ketenpartner beter kan worden opgevangen. Vergroot hiermee de robuustheid en continuïteit van de gehele keten.
- Bestendig de risicomanagementfunctie zodat beveiligingsrisico's adequaat worden meegewogen in de investeringsbeslissingen. Het portfolioproces wordt duidelijk vormgegeven; in dit proces zullen de beveiligingsrisico's een nadrukkelijk rol moeten spelen in prioritering.
- Maak een dreigingsanalyse en bepaal op basis hiervan de meest urgente investeringen voor informatiebeveiliging. De beperkte uitvoeringscapaciteit maakt prioritering cruciaal.
- Concretiseer de bestaande generieke plannen voor investeringen of maak aanvullende plannen voor urgente investeringen voor informatiebeveiliging, zodat ze uitgevoerd kunnen worden.
- Wijs nu middelen toe aan de meest urgente investeringen voor informatiebeveiliging, voor zover dat niet al is gebeurd.
- Beleg de verantwoordelijkheid voor het opleveren en beheren van beveiligingsfuncties expliciet bij specifieke afdelingen en managementfuncties binnen IVOM.
- Versterk de positie van sleutelfunctionarissen voor informatiebeveiliging binnen IV en veranker die tot op het hoogste niveau.
- Ga met ketenpartners in gesprek over de gedeelde afhankelijkheden. Maak van de verzameling losse eilandjes, die zich beroepen op hun specifieke en eigen karakter, een sterke archipel. Houd daarbij respect voor ieders verantwoordelijkheden, maar investeer gezamenlijk in collectieve kracht. Bekijk eigen strategieën, (i-)plannen, (beveiligings)architecturen en portfolio's steeds minder per organisatie afzonderlijk en steeds meer in onderlinge samenhang. Doe dit enerzijds om te voorkomen dat mogelijke besmetting via eigen kwetsbaarheden door

4 Rekenkamer (2026), "Resultaten verantwoordingsonderzoek 2025 ministerie van Justitie en Veiligheid", https://www.rekenkamer.nl/documenten/2026/05/20/vo-2025-jenv en Adviescollege ICT-toetsing (2026), "Advies ICT-aanpassingen invoering nWvSv, https://www.adviescollegeicttoetsing.nl/documenten/2026/05/12/advies-ict-aanpassingen-invoering-nwvsv

Docnr1

de keten heen kan 'overspringen'. Deze afstemming is anderzijds nodig om ketenbrede functionele ontwikkeling, zoals nieuwe wetgeving, integraal over de keten heen te kunnen besturen.

- Bewaak in de komende jaren op zorgvuldige wijze dat het functioneren van de legacy op orde blijft naast de verdere ontwikkeling van Emma.
- Versterk de uitvoeringskracht op het gebied van IV en ontwikkelingen en draag zorg voor voldoende financiële randvoorwaarden.
- Evalueer frequent tot op het hoogste niveau de voortgang van de ontwikkelingen rond IV en communiceer daarover naar de medewerkers.
- Creëer een organisatorische setting waarin hoogvertrouwelijke informatie met en tussen ketenpartners gedeeld kan worden om iedere ketenpartner in staat te stellen de risico's voor de eigen organisatie (processen, maar ook medewerkers) in te schatten.

Bijlagen

Respondentenoverzicht

Respondentenoverzicht
Bestuurlijk CIO Openbaar Ministerie
Directeur IVOM
Hoofd CIO-office
Directeur Parket-Generaal
Directeur Bedrijfsvoering Arrondissementsparket Oost-Nederland
(Voormalig) Hoofdofficier Arrondissementsparket Oost-Nederland
CISO OM
Teamlead SOC
Security en enterprise architecten IVOM
Extern responsteam Deloitte
CIO Justitie en Veiligheid
Directeur IV Justitie en Veiligheid
Directeur Executie CJIB
CIO CJIB
CIO DJI
Algemeen directeur IVO en CIO Rechtspraak
Lid Raad voor de Rechtspraak
Politie – Hoofd Operatie Eenheidsleiding
Politie – Operationeel Specialist Dienst Regionale Recherche
Nationale Politie

Documentenoverzicht

Documentenoverzicht
Besluitenlijsten m.b.t. afkoppelen systemen OM
i-Strategie, i-Visie en i-Plan Openbaar Ministerie
Documentatie m.b.t. crisisstructuur OM
Externe rapportages naar IT-landschap OM (voor de inbreuk)
Externe rapportages naar aanleiding van het incident
Kamerbrieven en Kamervragen omtrent de inbreuk • Kamerstuk 26643, nr. 1376. Datum 17 juli 2025. • Kamerstuk 26643, nr. 1377. Datum 23 juli 2025. • Kamerstuk 26643, nr. 1378. Datum 4 augustus 2025. • Kamerstuk 26643, nr. 1379. Datum 14 augustus 2025. • Kamerbrief 26643, nr. 1390. Minister van Justitie en Veiligheid. Onderzoek naar kwetsbaarheid ICT-systemen OM. Datum 3 september 2025. • Kamervragen De gevolgen van de hack bij het OM op de bedrijfsvoering. 2025Z17315. Gericht aan minister van Justitie en Veiligheid, ingediend door kamerlid Sneller. Datum 19 september 2025. • Antwoord op Kamervragen 2025Z17315. Datum 21 november 2025. • Kamervragen Het bericht '3000 medewerkers Openbaar Ministerie sturen brandbrief over ICT-problemen'. 2025Z20552. Gericht aan minister van Justitie en Veiligheid, ingediend door kamerlid Coenradie. Datum 26 november 2025. • Antwoord op Kamervragen 2025Z20552. Datum 13 januari 2026. • Kamervragen De aanhoudende ICT-problematiek bij het Openbaar Ministerie (OM). 2025Z20557. Gericht aan minister van Justitie en Veiligheid en staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties, ingediend door kamerlid Mutluer en kamerlid Kathmann. Datum 26 november 2025. • Antwoord op Kamervragen 2025Z20557.
Brandbrief Comité OM onder Druk: ICT-problematiek, werkdruk en aangekondigde bezuinigingen. Inclusief reacties OM.
Rekenkamer 2025 – Verantwoordingsonderzoek 2025 ministerie van Justitie en Veiligheid
Adviescollege ICT-toetsing 2026 – Advies ICT-aanpassingen invoeringen nWvSv