26 643 Informatie- en communicatietechnologie (ICT)

36 800 IX Vaststelling van de begrotingsstaat van het Ministerie van Financiën (IXB) en de begrotingsstaat van Nationale Schuld (IXA) voor het jaar 2026

Nr. 1533 Brief van de minister van Financiën

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 18 juni 2026

Zoals ik schreef in mijn brief van 30 maart jl.[1] heeft het ministerie van Financiën op 19 maart jl. vastgesteld dat ongeautoriseerde toegang is verkregen tot een deel van de ICT-systemen. Bij de procedurevergadering van de commissie Financiën van 9 april jl. is verzocht om een vervolgbrief over de stand van zaken van dit incident. Met deze brief kom ik tegemoet aan dit verzoek van de Kamer.

Sinds de ontdekking van het cyberincident is er achter de schermen onverminderd hard gewerkt aan het weer veilig openstellen van onze systemen. Al snel konden we vaststellen dat de impact zich beperkte tot de systemen van het beleidsdepartement en dat de dienstverlening van de Belastingdienst, Douane en Toeslagen niet was geraakt. Inmiddels zijn de laatste restricties rond de systemen van het beleidsdepartement opgeheven en zijn alle systemen weer online en toegankelijk voor iedereen.

Ook kan ik melden dat belangrijke primaire processen van het ministerie, zoals de voorjaarsbesluitvorming, ondanks het incident doorgang hebben kunnen vinden. Dit is te danken aan onze (ICT-)medewerkers, het Security Operations Center (SOC), de ADR en getroffen directies, experts van Belastingdienst, SSC-ICT en de betrokken leverancier die samen hard hebben gewerkt om dit mogelijk te maken. In deze brief ga ik in op wat er is gebeurd, hoe het ministerie daarmee om is gegaan en wat dat betekent voor de toekomst, voor zover dit deelbaar is vanuit veiligheidsoverwegingen.

[1] Kamerstukken II 2025/26, 26 643, nr. 1498

**Wat is er gebeurd?**

We hebben inmiddels duidelijkheid over hoe de digitale inbraak is verlopen. Het ministerie heeft een eigen SOC, wat fungeert als centrale digitale alarmcentrale. Dit team van beveiligingsexperts bewaakt, detecteert en analyseert continu cyberdreigingen en IT-incidenten om de ICT-omgeving veilig te houden. Op 19 maart detecteerde het SOC vreemd gebruikersgedrag binnen het netwerk van het ministerie.

Net als andere departementen werkt het ministerie voor diverse digitale processen met externe leveranciers. Het was vrij snel duidelijk dat het incident een relatie had met de systemen die voor Financiën draaien bij een specifieke leverancier. In overleg met het SOC heeft de leverancier dezelfde dag mitigerende maatregelen genomen en bepaalde voorzieningen dichtgezet.

Na verder onderzoek bleek het om een geavanceerde inbraak te gaan. De actor heeft een *zero-day* kwetsbaarheid in de software die toegang tot de werkplekomgeving regelt misbruikt. Dit betekent dat de actor toegang had tot een kwetsbaarheid die tot dat moment nog onbekend was en waarvoor nog geen beveiligingsupdates bestonden. Met deze kennis heeft de leverancier van de getroffen software inmiddels maatregelen getroffen en op 27 maart al zijn klanten hierover geïnformeerd.

De inbraak heeft, mede doordat er tijdig mitigerende maatregelen zijn getroffen, geen schade aan de systemen tot gevolg gehad. Wel is het aannemelijk dat er door de inbraak gegevensdiefstal heeft plaatsgevonden. De betrokken medewerkers zijn hierover geïnformeerd en begeleid om de impact van het lek zo veel mogelijk te mitigeren. Het is naar verwachting niet te reconstrueren om welke bestanden het exact gaat. Daarnaast heeft de aangetaste integriteit van het systeem, vanwege de toegang van de actor, voor overlast gezorgd bij medewerkers en externe partners omdat systemen tijdelijk (en uit voorzorg) niet beschikbaar waren.

**Hoe zijn we ermee omgegaan?**

Binnen het ministerie werd de interne crisisorganisatie geactiveerd waarbij we ons organiseerden in een overleg met technische experts, evenals een bestuurlijke tafel die dagelijks bijeen kwam en regie voerde. Vanaf het begin werd hierbij samen opgetrokken met de leverancier, met externe beveiligingsexperts en met het Nationaal Cyber Security Centrum (NCSC).

De CISO en CIO (Chief Information Security Officer, Chief Information Officer) Rijk werden ingelicht, en er is melding gemaakt van het incident bij de Autoriteit Persoonsgegevens (AP). De datalekmelding bij de AP is binnen 72 uur na ontdekking van het incident gemaakt en daarmee binnen de wettelijke termijn uit de Algemene Verordening Gegevensbescherming (AVG). Er is regelmatig contact geweest met de AP om toelichting te geven of vragen te beantwoorden. Ook heeft het ministerie contact opgenomen met Team High Tech Crime (THTC) van de politie en is er aangifte gedaan.

Het NCSC heeft het Ministerie van Financiën en diens leverancier en beveiligingsexperts geadviseerd over mogelijke maatregelen, heeft ondersteuning geboden in het forensisch onderzoek en heeft daarnaast zijn netwerk ingezet om onderzoek te coördineren tussen verschillende partijen. Bovendien kon het NCSC met behulp van de gedeelde inzichten zowel nationale als internationale partners en organisaties geanonimiseerd informeren over de aanval, om de brede digitale weerbaarheid te verhogen.

In het kader van *responsible disclosure*[2] is als eerste de eigenaar van het kwetsbare systeem op een verantwoorde manier op de hoogte gesteld.

Er is vanuit veiligheidsoverwegingen extern beknopt gepubliceerd over het incident op het ministerie.

[2] Zie ook https://www.ncsc.nl/kwetsbaarhedenbeheer/belang-van-responsible-disclosure

Qua mitigerende maatregelen zijn onder meer zo snel mogelijk bepaalde voorzieningen dichtgezet om het risico op schade te beperken. Door het besluit om verbindingen naar bepaalde applicaties uit te zetten, konden medewerkers en externe partners tijdelijk niet meer inloggen bij voorzieningen zoals schatkistbankieren. Na forensisch onderzoek en controle op de data-integriteit bleek dat er geen indicatoren waren om aan te nemen dat de applicaties aangetast waren en dat deze met extra beveiligingschecks weer in gebruik genomen konden worden. Hierdoor konden de geraakte werkprocessen grotendeels weer doorgang vinden. Een andere maatregel die we hebben getroffen is dat de wachtwoorden van alle medewerkers van het beleidsdepartement preventief zijn gereset. Hierover zijn medewerkers op het intranet geïnformeerd.

**Wat betekent dit voor de toekomst?**

Op basis van het beschikbare forensisch materiaal kan geen uitsluitsel gegeven worden over de actor en de buitgemaakte gegevens. Bij dergelijke geavanceerde inbraken is het zelden mogelijk om erachter te komen wie of welke partij ervoor verantwoordelijk is.

Het ministerie evalueert het incident en verwerkt de inzichten in de continuïteits- en crisisplannen. Hoewel concrete maatregelen niet publiekelijk deelbaar zijn, heeft het incident ons veel geleerd over hoe we ons willen organiseren bij incidenten in de toekomst. De multidisciplinaire samenwerking tussen informatiebeveiligingsexperts, medewerkers met kennis van de primaire processen en externe specialisten was een aanpak die goed heeft gewerkt.

Bewustzijn van digitale veiligheid heeft continu aandacht binnen het Ministerie van Financiën. Daarom zetten wij in op digitale weerbaarheid van ambtenaren, processen én systemen. Hiermee zijn dit soort inbraken echter nooit geheel te voorkomen. Dit incident benadrukt het belang van deze trajecten.

We richten ons de komende tijd op de verdere uitbouw en professionalisering van het team dat verantwoordelijk is voor het monitoren, detecteren, loggen en afhandelen van digitale dreigingen en incidenten. Daarnaast worden ter bevordering van onze digitale weerbaarheid periodiek penetratietesten, crisisoefeningen en kwetsbaarheidsonderzoeken uitgevoerd.

Mocht uw commissie aanvullende vragen hebben over het incident, dan is het alsnog mogelijk om een aanvullende vertrouwelijke technische briefing te organiseren.

De minister van Financiën,
E. Heinen