Ministerie van Justitie en Veiligheid

> Retouradres Postbus 20301 2500 EH Den Haag

Directie Informatievoorziening en Inkoop

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

Aan de Voorzitter van de Tweede Kamerder Staten-GeneraalPostbus 200182500 EA DEN HAAG

Ons kenmerk
3438601

Bij beantwoording de datum en ons kenmerk vermelden. Wilt u slechts één zaak in uw brief behandelen.

Datum 16 juli 2021
Onderwerp Informatiebeveiligingsincident

Op 30 juni jl. werd aan mij een datalek binnen mijn ministerie gemeld. Het gaat om persoonsgegevens van een groot aantal medewerkers van JenV-organisaties en een kleiner aantal medewerkers van andere organisaties. Deze data zijn via een voormalige extern medewerker onterecht terechtgekomen bij twee andere overheidsorganisaties waarvoor hij opdrachten uitvoerde. Onderstaand ga ik nader in op het lek. Het geconstateerde datalek is na de ontdekking direct gemeld bij de Autoriteit Persoonsgegevens. Meteen na het ontdekken en vermelding ervan aan mij is een drietal onderzoeken op mijn verzoek gestart, ook dat licht ik onderstaand toe.

Op dit moment heb ik geen indicatie dat deze data door onbevoegden zijn ingezien of gebruikt. Het onderzoek dat hierover uitsluitsel moet geven, is nog niet afgerond. De betreffende data zijn na ontdekking verwijderd dan wel onbruikbaar gemaakt bij de twee overheidsorganisaties en bij de betreffende medewerker. Ik betreur het incident zeer en neem dit hoog op.

Wat is gelekt en hoe
Een voormalige externe medewerker bij mijn ministerie heeft –tegen de regels in- een analysetool gekopieerd van JenV naar een eigen werkomgeving en vervolgens naar twee andere overheidsomgevingen. Deze medewerker voerde bij mijn ministerie kwaliteitscontroles uit op toegangsdiensten, zoals de Rijkspas. De medewerker geeft aan dat hij de tool wilde kopiëren, daarbij zijn ook de daaraan gekoppelde data gekopieerd. Het gaat om persoonsgegevens van circa 65.000 medewerkers, waarvan een klein deel niet bij J&V-organisaties werkt. Het datalek bevat persoonsgegevens zoals naam, organisatie, soort dienstverband, ID/paspoortnummer, Rijkspasnummer, mailadres, geboorteplaats en –datum, geslacht en nationaliteit. Het datalek bevat geen privéadressen of telefoonnummers of wachtwoorden.

Het datalek bij mijn ministerie is ontdekt door de GGD GHOR doordat zij de gekopieerde data tijdens een routinecontrole op het netwerk (waar het naartoe was gekopieerd) aantroffen. Zij hebben dat direct aan mijn ministerie gemeld, en daarna is de data ook aangetroffen bij het OM en bij de eigen werkomgeving van betrokkene.

Lopende onderzoeken

Directie
Informatievoorziening en Inkoop

Datum
16 juli 2021

Ons kenmerk3438601

Het is bij mijn ministerie nadrukkelijk verboden om vertrouwelijke of privacygevoelige informatie op onveilige apparatuur te verwerken, zoals op privémiddelen. Deze informatie moet altijd met grote zorgvuldigheid worden behandeld en die zorgvuldigheid is hier met voeten getreden. Afspraken hierover zijn vastgelegd in de gedragsregeling voor de digitale werkomgeving en de regels voor extern ingehuurd personeel. Ik vind het zeer kwalijk dat het verplaatsen van de analysetool (inclusief persoonsgegevens) alsnog plaats heeft kunnen vinden. Ik heb direct opdracht verstrekt aan de Accountantsdienst Rijk (ADR) om een audit te doen naar dit informatiebeveiligingsincident en verbetermaatregelen voor te stellen. De ADR doet onderzoek naar de werkprocessen, systemen en waarborgen binnen het departement. Dit is gericht op het identificeren van beveiligingsrisico's en verbetermogelijkheden, teneinde incidenten in de toekomst te voorkomen.

De data zijn, zoals gezegd, veiliggesteld voor nader onderzoek en daarna direct verwijderd, dan wel onbruikbaar gemaakt op de plekken waar het niet hoorde te staan. De betrokkene verleende hierbij alle medewerking. Mijn ministerie heeft Fox-IT ingeschakeld om forensisch onderzoek uit te voeren. Doel van dit onderzoek is een technische reconstructie om te bepalen of meer personen buiten JenV toegang hebben gehad tot het gegevensbestand.

Verder heb ik het Integriteitsbureau van DJI gevraagd een onderzoek te doen naar de feitelijke handelingen rond dit incident op de werkvloer.

In totaal lopen nu dus drie onderzoeken naar dit informatiebeveiligingsincident. Op advies van de beveiligingsautoriteit van mijn ministerie wordt op basis van de uitkomsten van deze onderzoeken bekeken of nadere stappen moeten worden ondernomen.

Informeren van betrokkenen
Alle personen die voorkomen in het datalek worden vandaag geïnformeerd, evenals de bestuurders van de getroffen organisaties. Voor de medewerkers is ook een centrale mailbox geopend waar zij terecht kunnen met vragen over dit incident.

Tot slot
Ik wacht nu de uitkomsten van genoemde onderzoeken af alvorens een besluit te nemen over de vervolgstappen. Uiteraard zal ik desgewenst uw Kamer daarover informeren.

De Minister van Justitie en Veiligheid,

Ferd Grapperhaus