Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

TER INFORMATIE

Nota actief openbaar
Ja

Onze referentie
2022-0000550131

Datum
6 oktober 2022

Opgesteld door

Samengewerkt met
BVA Rijk, CISO's Eerste Kamer en Tweede Kamer, NCSC

Bijlage(n)
1

Aan Staatssecretaris BZK
Van CISO Rijk

nota

01. Nota bij Kamerbrief Hack bij ID-ware

Aanleiding

Leverancier ID-ware heeft gemeld slachtoffer te zijn geweest van een hackaanval. ID-ware levert toegangspassen voor de Rijksdienst en de Eerste en Tweede Kamer. Eerder informeerde ik u over de situatie, de mogelijke impact en de ondernomen acties tot nu toe. Inmiddels zijn in concept resultaten van onderzoek bij het bedrijf in vertrouwen gedeeld en op basis hiervan informeert u de Tweede Kamer

Geadviseerd besluit

U wordt geadviseerd om akkoord te gaan met de inhoud van de brief en snel na het informeren van medewerkers van beide Kamers en Rijksoverheid de brief te zenden naar de Tweede Kamer.

Kern

- ID-ware heeft gemeld slachtoffer te zijn geweest van een ransomwareaanval op hun systemen. De getroffen systemen konden snel hersteld worden vanwege een goede actuele back-up. Wel is geconstateerd dat een grote hoeveelheid gegevens door de aanvaller zijn buitgemaakt.
- Lopend onderzoek, waarbij ID-ware een securitybedrijf heeft ingeschakeld, moet uitsluitsel geven of en welke gegevens van klanten zijn gelekt. Tot nu toe is bevestigd van een groep van iets minder dan 3500 medewerkers van Rijksoverheid naam, rijkspasnummer en paraaf in de gelekte gegevens voorkomen. Voorlopige conclusies wijzen erop dat er het hierbij blijft.
- Een incidentteam met CIO Rijk in regie, beide Kamers en NCSC is sinds 30 september actief, daarbij zijn sinds 3 oktober ook politie en inlichtingendiensten betrokken en communicatie is voorbereid voor verschillende scenario's. Dit moment is nu aangebroken: verder wachten op conclusies geeft meer zekerheid of er echt niet meer meer gegevens gelekt zijn, maar draagt niet wezenlijk bij aan het beeld.
- Ik adviseer u om kort nadat medewerkers van Eerste en Tweede Kamer en Rijksoverheid zijn geïnformeerd ook de Tweede Kamer te informeren vanuit uw verantwoordelijkheid voor de Rijksdienst.

Toelichting

ID-ware levert diensten voor uitgifte en beheer van toegangspassen aan Rijksoverheid, Eerste Kamer en Tweede kamer.

ID-ware geeft aan in de nacht van 16 op 17 september slachtoffer te zijn geworden van een ransomwareaanval[1]. Daarbij zijn enkele servers onklaar gemaakt. Toen het werd ontdekt is externe hulp ingeschakeld om de aanval te stoppen en voor herstel en onderzoek. Met actuele en goed werkende back-ups konden de beschadigde servers hersteld worden. Geconstateerd is dat de database servers met productiegegevens niet geraakt zijn. De aanval heeft zich gericht op de file servers van het bedrijf met hierin losse bestanden. Als reactie hebben Eerste Kamer en Tweede Kamer ook de netwerkverbindingen met ID-ware verbroken. De verbindingen worden bij alle partijen gemonitord op misbruik (incl. Rijkspasbeheer).

Het onderzoek wijst uit dat er een grote hoeveelheid bestanden zijn verkregen door de aanvaller. Op darkweb is door de aanvaller een lijst met bestandsnamen gepubliceerd. Op dit moment wordt nagegaan of persoonsgegevens of andere klantgegevens zijn gelekt. Tot nu toe is bevestigd door Rijkspasbeheer dat van 3500 medewerkers van de Rijksoverheid naam, rijkspasnummer en paraaf bij de gelekte gegevens zaten. Deze zijn afkomstig van de thuisbezorgdienst van de Rijkspas. Er zijn hierbij geen huisadressen gelekt.

Er zijn door ID-ware, Eerste Kamer, Tweede Kamer en Rijkspasbeheer al meldingen bij de Autoriteit Persoonsgegevens over een mogelijk lek gedaan. De politie heeft een aangifte opgenomen, gedaan door ID-ware.

Politieke context

Het bekend worden van de aanval bij leden van de Kamers zal vrijwel zeker tot vragen leiden.

Communicatie
Er is een communicatieoverleg waarin de voorbereiding voor communicatie is getroffen. Richting medewerkers wordt actief gecommuniceerd.

Informatie die niet openbaar gemaakt kan worden

[redacted]

[1] Bij een ransomware aanval dringt de aanvaller binnen in het netwerk van de organisatie om vervolgens gegevens te versleutelen. Het slachtoffer krijgt pas weer toegang tot de gegevens als er een bedrag aan losgeld is betaald. Meestal wordt bij de aanval ook gegevens naar buiten gebracht om aan te kunnen tonen dat de organisatie echt getroffen is of in tweede instantie geld te eisen om te voorkomen dat de gegevens gepubliceerd worden.

[redacted]

Onze referentie
2022-0000550131

Datum
6 oktober 2022

Motivering
In de openbaar gemaakte versie van deze nota zijn

- om veiligheidsredenen gevoelige gegevens niet opgenomen;
- alle persoonsgegevens van ambtenaren geanonimiseerd.

Bijlagen

Volgnummer	Naam	Informatie
1	Kamerbrief Hack bij ID-ware	