Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

TER INFORMATIE

Nota actief openbaar
Ja

Onze referentie
2022-0000611081

Datum
9 november 2022

Aan Staatssecretaris BZK
Van CISO Rijk

nota

Nota update hackaanval ID-ware i.r.t. Rijkspas

Samengewerkt met
BVA Rijk

Bijlage(n)
1

Aanleiding

Op 7 oktober j.l. informeerde u de Eerste en Tweede Kamer over een hackaanval bij ID-ware, een bedrijf dat diensten levert voor de Rijkspasvoorziening en voor beheer van toegangspassen voor de Eerste Kamer en Tweede Kamer. U meldde hierin dat bevestigd was dat van bijna 3500 Rijksdienstmedewerkers persoonsgegevens zijn gelekt bij deze aanval, dat de interne systemen van Rijksoverheid en beide Kamers niet zijn getroffen en dat onderzoek nog liep. Inmiddels is het onderzoek afgerond. Met deze nota informeer ik u over de huidige stand van zaken.

Geadviseerd besluit

Kennisnemen van de actuele status rond de hack bij ID-ware en in te stemmen om de beide Kamers te informeren middels een brief.

Kern

- Bij de ransomware aanval op ID-ware, een bedrijf die diensten levert aan Rijkspas, is een grote hoeveelheid bestanden gelekt en via een website op het darkweb gepubliceerd. ID-ware was snel in staat om de systemen te herstellen, maar de gelekte bestanden konden niet meer teruggehaald worden. De respons op de aanval en het onderzoek heeft zich met name gericht op welke gegevens gelekt zijn en de gevolgen daarvan op medewerkers en veiligheid van personen en gebouwen.
- ID-ware heeft geen losgeld betaald aan de aanvallers.
- Het onderzoek dat ID-ware heeft uitgevoerd naar de gelekte gegevens is afgerond. Ook het NCSC heeft haar onderzoek afgerond.
- Er is nu bevestigd dat het aantal van 3500 gelekte gegevens van Rijkspasgebruikers naar beneden kan worden bijgesteld: bijna 3200 gegevens zijn nu geteld.
- Aanvullend heeft het NCSC geconstateerd dat van ca. 1300 pasgebruikers die een toegangspas tot de Tweede en/of Eerste Kamer hebben, gegevens zijn gelekt via logbestanden. Inmiddels hebben de Kamers deze personen hierover geïnformeerd.
- Ook is bevestigd dat gegevens van de Technische Universiteit Eindhoven en Hogeschool Utrecht bij dezelfde aanval zijn gelekt.
- Het technisch onderzoek door een extern securitybedrijf naar hoe de hack heeft plaatsgevonden en wat er is gebeurd was al eerder afgerond en is in concept gedeeld met klanten Rijkspas en de Tweede Kamer.

- Hiermee zijn de onderzoeken naar het incident afgerond en is de kans klein dat nog nieuwe datalekken worden ontdekt n.a.v. deze hackaanval.
- Hoewel de getroffen pasgebruikers van beide Kamers persoonlijk op de hoogte werden gebracht en de Rijksdienst nu niet verder geraakt is, adviseren we om de Kamers volledigheidshalve ook via een brief van de laatste ontwikkelingen op de hoogte te brengen.

Toelichting

- Het onderzoek naar de gelekte gegevens is uitgevoerd op gegevens die via z.g. leaksites beschikbaar zijn gekomen. Het gaat hierbij om een grote hoeveelheid bestanden (ca. 75.000) die zijn buitgemaakt tijdens de ransomwareaanval op ID-ware. Hierbij werd door een actor, waarvan de achtergrond niet bekend is, ingebroken op de systemen van ID-ware en werden fileservers met bestanden versleuteld. ID-ware had snel de systemen weer beschikbaar en ontdekte toen ook het datalek. U heeft over de hackaanval op 7 oktober j.l. de beide Kamers geïnformeerd[1].
- De bijna 3200 gegevens van Rijksmedewerkers die zijn gelekt bevatten naam, rijkspasnummer en paraaf die gebruikt werden in de thuisbezorgservice voor de Rijkspas. Dit betrof een proefproject en de gegevens waren tijdelijk opgeslagen.
- De ongeveer 1300 gegevens van medewerkers van Tweede en Eerste Kamer bevatten naam, geboortedatum, rijkspasnummer en in een aantal gevallen de pasfoto. Eerder hadden de Tweede Kamer en Eerste Kamer al de gebruikers van de pas gewaarschuwd. Nu het lek is bevestigd is dat inmiddels ook aan betrokkenen gecommuniceerd. Omdat er ook journalisten zijn in de groep van 1300 pashouders wordt hierover ook direct in de media over bericht (FD).
- ID-ware heeft op 28 oktober op haar website een verklaring geplaatst dat de onderzoeken zijn afgerond en getroffen organisaties zijn geïnformeerd[2].
- ID-ware heeft inmiddels maatregelen genomen die de kans op dit soort incidenten in de toekomst minimaliseren.CISO Rijk zal samenwerken met BVA Rijk en Rijkspasbeheer om te vergewissen dat de maatregelen en processen adequaat zijn voor de taak die ID-ware uitvoert.

Politieke context
De leden van de Tweede Kamer en Eerste Kamer zijn geïnformeerd over de hack en de gevolgen van de datalekken. Tijdens het debat van 2 november heeft u toegezegd de Kamer een update te sturen over het incident. Deze brief vervult die toezegging.

Communicatie
U wordt geadviseerd om de beide Kamers over de ontwikkelingen te informeren middels een brief.

---

1 https://www.rijksoverheid.nl/documenten/kamerstukken/2022/10/07/kamerbrief-hack-id-ware

2 https://www.id-ware.com/nl/over/nieuws/update-incidenten.html

Informatie die niet openbaar gemaakt kan worden

Motivering
In de openbaar gemaakte versie van deze nota zijn alle persoonsgegevens van ambtenaren geanonimiseerd.

Bijlagen

Volgnummer	Naam	Informatie
1	Brief update hackaanval ID-ware	De update voor de Kamers n.a.v. het afronden van het onderzoek van gelekte gegevens
2.	Kamerbrieven Hack bij ID-ware voor Eerste en Tweede Kamer	De brief die op 7 oktober 2022 aan de Kamers is gestuurd in verband met de hack bij ID-ware