Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

> Retouradres Postbus 20011 2500 EA Den Haag

Aan de voorzitter van de Tweede Kamer der Staten-Generaal
Postbus 20018
2500 EA ’s-Gravenhage

Ministerie van Binnenlandse Zaken en Koninkrijkrelaties

Turfmarkt 147
Den Haag
Postbus 20011
2500 EA Den Haag
Nederland
www.linkedin.com/company/ministerie-van-bzk

Contactpersoon

Kenmerk
2022-0000550122

Uw kenmerk

Datum 7 oktober 2022
Betreft Hack bij ID-ware

Met deze brief wordt uw Kamer geïnformeerd over de recente ontwikkelingen rondom de hack op een leverancier in het kader van de uitgifte van Rijkspassen. In deze brief wordt ingegaan op de gevolgen voor de gebruikers van de Rijkspas en de genomen maatregelen en vervolgstappen.

ID-ware heeft een melding gemaakt bij de Rijksoverheid en Tweede Kamer van een hackaanval op de systemen van ID-ware. Het bedrijf is een Duitse leverancier met een dochter in Nederland, die een aantal producten en diensten levert aan onder meer de Rijksoverheid en de Eerste en Tweede Kamer. Dit betreft diensten rond Rijkspas, die leden van de Eerste en Tweede Kamer, de staf van die organisaties, en rijksambtenaren toegang verschaft tot de Kamergebouwen en rijkspanden.

Situatie

- Voor de Rijksoverheid voert ID-ware applicatiebeheer uit op de bij Rijksoverheid geïmplementeerde centrale Rijkspassystemen. Aan de Eerste en Tweede Kamer levert zij diensten voor het aanvragen en beheren van toegangspassen vanuit ID-ware’s eigen systemen.
- Op 21 september 2022 meldde ID-ware dat er een aanval heeft plaatsgevonden op haar systemen. Op 29 september 2022 zijn per brief de eerste resultaten gedeeld van onderzoek naar de aard van de aanval en de impact op de gegevens. Het ging om een aanval met ransomware, waarbij bestanden versleuteld worden om pas tegen betaling van losgeld weer beschikbaar te komen. Het bedrijf geeft aan dat de schade snel hersteld kon worden, maar dat gebleken is dat er een grote hoeveelheid bestanden naar buiten is gebracht.
- Onderzoek, waarbij ID-ware een securitybedrijf heeft ingeschakeld, heeft laten zien dat de databaseservers die gebruikt worden bij de uitgifte van passen niet geraakt zijn door de aanval. Of er gegevens van rijkspasgebruikers staan op de fileservers die wel geraakt zijn wordt onderzocht. Tot nu toe is bekend dat van bijna 3500 medewerkers van Rijksoverheid naam, rijkspasnummer en paraaf is gelekt vanuit de thuisbezorgservice van de kaart. Er kan uit onderzoek nog naar voren

komen dat andere gegevens van rijkspasgebruikers zijn gelekt. Er is geen sleutelmateriaal in beheer bij het bedrijf.
- Het bedrijf levert soortgelijke diensten aan andere klanten in Nederland en Duitsland en heeft hen eveneens op de hoogte gesteld. Ook is een melding gedaan bij Autoriteit Persoonsgegevens en heeft het bedrijf aangifte gedaan bij de politie.

Gevolgen
De persoonsgegevens die aanwezig zijn bij het bedrijf beperken zich tot de voor productie van de kaart noodzakelijke gegevens: naam, geboortedatum, geslacht, rijkspasnummer en pasfoto. Voor de meeste pasgebruikers zal dit, als toch blijkt dat deze gelekt zijn, een beperkte impact hebben, waarbij met name aan het risico van gebruik bij *phishing* moet worden gedacht. Niettemin betreur ik dit incident zeer, evenals de mogelijke gevolgen voor betrokken personen.

Met de gelekte informatie kan geen pas worden gefabriceerd die toegang tot gebouwen geeft, het hiervoor benodigde sleutelmateriaal wordt niet verwerkt bij ID-ware.

Maatregelen
Sinds de melding van het incident, heeft NCSC met partners, waaronder de politie, CISO Rijk, BVA Rijk en BVA's en CISO's Eerste en Tweede Kamer, een onderzoeksteam ingericht om de situatie te analyseren en impact te duiden.

Zowel het bedrijf als Rijkspasbeheer, Eerste en Tweede Kamer hebben een melding gedaan bij de Autoriteit Persoonsgegevens.

De interne systemen van Rijkspasbeheer, Eerste Kamer en Tweede Kamer zijn door de hack bij ID-ware niet geraakt, er is monitoring op de verbindingen.

De personen van wie is vastgesteld dat er gegevens zijn gelekt zijn persoonlijk geïnformeerd of worden een dezer dagen geïnformeerd.

Vervolg
Het NCSC en de hiervoor genoemde functionarissen en diensten van de getroffen organisaties zullen de situatie nauwlettend blijven monitoren en, indien daartoe aanleiding is, updates geven aan getroffen medewerkers, en/of tot advisering via hun website overgaan.

De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties
Digitalisering en Koninkrijksrelaties

Alexandra C. van Huffelen