AUTORITEIT
PERSOONSGEGEVENS

Datum
9-5-2023

Ambtsbericht

Onderwerp
Informatievoorziening voor de beantwoording van de Kamervragen van het lid Slootweg (CDA) over het bericht "Steekspel rond mysterieuze datadiefstal; Bedrijven delen data van klanten met hun leveranciers, maar hoe veilig is dat?"

Het lid Slootweg (CDA) heeft Kamervragen gesteld aan de Staatssecretaris van Koninkrijksrelaties en Digitalisering over het bericht "Steekspel rond mysterieuze datadiefstal; Bedrijven delen data van klanten met hun leveranciers, maar hoe veilig is dat?". Dit ambtsbericht dient ter verschaffing van informatie aan het ministerie van Binnenlandse Zaken en Koninkrijksrelaties voor de beantwoording van de vragen 2, 5, 6 en 7.

Vraag 2
Kunt u een update geven van het datalek bij Nebu en het aantal klanten en bedrijven en organisaties dat in Nederland getroffen is?

Informatie voor beantwoording van vraag 2:
Elk jaar ontvangt de Autoriteit Persoonsgegevens (AP) ruim 20.000 datalekmeldingen[1]. Van een datalek is sprake wanneer er ongeoorloofde of onbedoelde toegang tot persoonsgegevens heeft plaatsgevonden. Maar ook als deze gegevens ongewenst zijn vernietigd, verloren, gewijzigd of verstrekt. In Nederland geldt een meldplicht voor datalekken. Dit houdt in dat organisaties (zowel bedrijven als overheden) direct een melding moeten doen bij de AP zodra zij een ernstig datalek hebben. Dit kunnen zij melden via het meldformulier datalekken. De gevolgen voor slachtoffers van een datalek kunnen groot zijn. De gelekte gegevens kunnen namelijk door cybercriminelen worden ingezet voor internetfraude. Slachtoffers wordt daarom geadviseerd om alert te zijn op phishing. Bij phishing worden mensen naar valse websites gelokt om daar nog meer gegevens buit te maken.

De AP heeft tot nu toe 172 datalekmeldingen ontvangen die te maken hebben met het datalek bij IT-leverancier Nebu.

Vraag 5
Deelt u de mening dat het gevaar op datalekken vooral in de keten zit van partijen die samenwerken met bedrijven zoals IT-leveranciers, onderzoeksbureaus en andere partijen met wie (klant)data wordt gedeeld?

Informatie voor beantwoording van vraag 5:
In 2021 waarschuwde de AP in haar datalekkenrapportage al voor datalekken bij IT-leveranciers. IT-leveranciers leveren bijvoorbeeld softwarediensten, digitale werkplekken of opslagruimte aan organisaties. Dat leidt tot een clustering van persoonsgegevens op de servers van deze leveranciers.

[1] Zie de datalekrapportages van de AP: Rapportages klachten en datalekken | Autoriteit Persoonsgegevens

Hierdoor zijn zij een gewild doelwit voor cyberaanvallen door criminelen: er valt hier veel te halen. Op basis van de ontvangen datalekmeldingen schat de AP in dat cyberaanvallen bij IT-leveranciers in 2021 minimaal 7 miljoen slachtoffers hebben gemaakt.

Vraag 6
Welke verantwoordelijkheid hebben bedrijven en (overheids)organisaties volgens u om digitaal verantwoord ondernemen in de keten te waarborgen?

Informatie voor beantwoording van vraag 6:
Als een organisatie gebruik maakt van een IT-leverancier, dan blijft de organisatie verantwoordelijk voor de beveiliging van de persoonsgegevens. Daarnaast zijn organisaties ook verantwoordelijk voor het melden van een datalek aan de AP én aan de slachtoffers. Het is daarom belangrijk dat organisaties alleen IT-leveranciers inschakelen die genoeg garanties geven voor passende technische en organisatorische beveiligingsmaatregelen. Organisaties zijn verplicht om in overeenkomsten afspraken te maken over de verwerking van persoonsgegevens en de beveiliging daarvan. Organisaties kunnen periodiek controleren of de IT-leverancier deze zogeheten verwerkersovereenkomsten naleven.

Wat betreft de beveiliging van netwerk- en informatiesystemen wijst de AP graag op de aankomende nieuwe Netwerk- en Informatiebeveiligingsrichtlijn (NIB2). Deze richtlijn komt bovenop de al bestaande Netwerk- en Informatiebeveiligingsrichtlijn (NIB1). NIB2 zal naar verwachting worden verwerkt in Nederlandse wetgeving door een aanpassing van de Wet Beveiliging Netwerk- en Informatiesystemen (Wbni). Als gevolg van NIB2 krijgen meer vitale sectoren, van de voeding en farmaceutische tot de ruimtevaart en datacenters, te maken met wettelijke verplichtingen voor de beveiliging van hun systemen. Bovendien ziet de AP in de richtlijn een uitbreiding van de meldplicht datalekken. Namelijk een doorzendplicht vanuit andere toezichthouders naar de AP. Regulering, en bijbehorend toezicht, zal gepaard moeten gaan met een forse uitbreiding van de personele capaciteit van de digitale toezichthouders. In de Nederlandse Cybersecuritystrategie 2022-2028 worden al structurele gelden vrijgemaakt om in te spelen op aankomende regelgeving. Met het oog op de datalekken meldplicht en de meldingen aan de AP van andere toezichthouders is het opvallend dat de AP hier niet in is meegenomen.

Vraag 7
Schiet de huidige regelgeving niet tekort als een externe partij waar een datalek plaatsvindt niet meewerkt aan onderzoek en geen informatie deelt over het datalek? Hoe kan een externe partij gedwongen worden om informatie te delen, zodat consumenten weten waar zij aan toe zijn? Deelt u de mening dat de consument in dit geval onvoldoende wordt beschermd?

Informatie voor beantwoording van vraag 7:
Externe partijen zijn op basis van de Algemene verordening gegevensbescherming (AVG) verplicht om organisaties zo snel mogelijk te informeren over een datalek. Organisaties moeten namelijk zo spoedig mogelijk een datalekmelding doen aan de AP en de slachtoffers van het datalek (dus de consument) informeren. De AVG vergroot hiermee de digitale weerbaarheid van slachtoffers van datalekken. Aan deze slachtoffers moet handelingsperspectief geboden worden, bijvoorbeeld door te adviseren over de wijziging van hun wachtwoorden van gebruikersaccounts.