Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2016–2017

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

230

Vragen van het lid **De Caluwé** (VVD) aan de Minister van Binnenlandse Zaken en Koninkrijksrelaties over *het artikel «Gluren in privégegevens»* (ingezonden 27 september 2016).

Antwoord van Minister **Plasterk** (Binnenlandse Zaken en Koninkrijksrelaties) (ontvangen 18 oktober 2016).

Vraag 1
Kent u het artikel «Gluren in privégegevens», over overheidspersoneel dat in digitaal beschikbare privégegevens kijkt?[1]

Antwoord 1
Ja.

Vraag 2
Heeft u inzicht in het aantal gevallen dat overheidspersoneel is betrapt op het ongeoorloofd bekijken, dan wel doorspelen van privégegevens? Zowel op landelijk niveau, als decentraal?

Antwoord 2
Organisaties in het openbaar bestuur zijn zelf verantwoordelijk voor registratie van integriteitsschendingen. Zij kunnen daarbij gebruik maken van het modelformulier dat mijn ministerie daartoe samen met de koepelorganisaties heeft vastgesteld. Op dat formulier valt het onbevoegd raadplegen van vertrouwelijke registers of deze raadplegen voor andere doeleinden dan waarvoor deze zijn bestemd, in de grotere categorie van «lekken en misbruik van informatie». Daaronder vallen ook andere vormen van lekken en misbruik van informatie, van verlies of diefstal van informatiedragers als ook het achterhouden van informatie.
In de Jaarrapportage Bedrijfsvoering Rijk, die jaarlijks aan de Tweede Kamer wordt gezonden, zijn cijfers van de ministeries over integriteitsschendingen opgenomen, uitgesplitst naar type. In de Jaarrapportage 2015 staat dat er dat jaar bij het Rijk 34 schendingen zijn geconstateerd in de genoemde grotere categorie op een totaal van 557 geconstateerde schendingen (TK 31 490, nr. 205).

[1] Telegraaf van zondag 25 september 2016

ah-tk-20162017-230
ISSN 0921 - 7398
's-Gravenhage 2016

Uit de voorlopige uitkomsten van de Monitor Integriteit en Veiligheid Openbaar Bestuur 2016, die ik later dit jaar aan de Kamer zal toesturen, valt op te maken dat in 2015 bij 11% van de onderzochte overheidsorganisaties in het openbaar bestuur een of meer schendingen zijn geregistreerd van lekken en misbruik van informatie.

Vraag 3
Op welke wijze wordt ervoor zorg gedragen dat overheidspersoneel ervan doordrongen is dat het bekijken en/of delen van privégegevens ongeoorloofd is?

Antwoord 3
Bij de introductie van nieuwe medewerkers en via bewustwordingsprogramma's op het gebied van privacy, informatiebeveiliging en integriteit, worden medewerkers er regelmatig van op de hoogte gebracht dat het bekijken en/of delen van diverse typen gevoelige gegevens ongeoorloofd is als dit niet strikt noodzakelijk is voor de uitvoering van de taak van de medewerker. Voor overheidspersoneel geldt op grond van de Ambtenarenwet de geheimhoudingsplicht. In de ambtseed of belofte die ambtenaren afleggen bij indiensttreding wordt daar expliciet aandacht aan besteed. Ook in gedragscodes wordt aandacht besteed aan informatiebescherming en het omgaan met vertrouwelijk informatie. Schendingen blijven in het algemeen niet zonder consequenties en kunnen tot rechtspositionele maatregelen leiden in geval van geconstateerd plichtsverzuim.

Vraag 4
Is het mogelijk te achterhalen of er ongeoorloofd is gekeken in privégegevens? Zo ja, wordt dit op regelmatige wijze gecheckt en op welke wijze? Zo nee, waarom is dit niet mogelijk?

Antwoord 4
Het is conform de privacywetgeving niet toegestaan om werknemers ongericht (digitaal) te observeren. Uit logginggegevens moet eerst blijken of er sprake is van een gerechtvaardigd vermoeden van niet-geautoriseerde handelingen. Deze kunnen vervolgens aanleiding geven voor nader persoonsgericht onderzoek.

Vraag 5
Wordt er gecontroleerd op het verstrekken van inlogcodes en wachtwoorden en op het niet delen van deze codes? Zo ja, hoe? Zo nee, waarom niet?

Antwoord 5
Het delen van gebruikersnaam en wachtwoorden is niet toegestaan. Dit wordt aangemerkt als integriteitsschending. Ook hiervoor geldt dat enkel gerichte controle mogelijk is bij een concrete verdenking.

Vraag 6
Bent u bekend met hetgeen gesteld is in het artikel, dat het soms maanden duurt voordat een nieuwe medewerker eigen inlogcodes krijgt? Zo ja, waarom duurt dit zo lang?

Antwoord 6
Indien een medewerker in verband met de functie of specifieke werkzaamheden een screening of veiligheidsonderzoek moet ondergaan, kan het om die reden langer duren voordat hij of zij voor specifieke gegevenssystemen eigen inlogcodes krijgt.

Vraag 7
Op welke wijze gaat u voorkomen dat privégegevens onveilig zijn, op het moment dat iedere burger zijn zaken met de overheid vanaf 2017 grotendeels digitaal kan afhandelen?

Antwoord 7
Wanneer een overheidsorganisatie persoonsgegevens verwerkt, dient die organisatie op basis van artikel 13 Wet bescherming persoonsgegevens een passend beveiligingsniveau te garanderen. De richtsnoeren van het College

bescherming persoonsgegevens (thans Autoriteit persoonsgegevens) uit 2013 die hierop van toepassing zijn, schrijven voor dat de bewaker encryptie (versleuteling) toe dient te passen bij verzending van persoonsgegevens via het internet. De organisatie is zelf verantwoordelijk voor het naleven van de wettelijke eisen om de persoonsgegevens te beschermen. De autoriteit Persoonsgegevens ziet daarop toe.
Bovenop deze wettelijke plicht hebben overheden zich gecommitteerd aan een op de Code voor Informatiebeveiliging (NEN-ISO(IEC 27002:2007 nl) gebaseerde baseline per sector of overheidslaag, zoals NEN7510 (in de zorg), BIR (voor het Rijk), BIG (voor gemeenten), BIWA (voor waterschappen), of IBI (voor provincies). Ik ben voornemens om tot een baseline informatiebeveiliging (BIO) voor de gehele overheid te komen, die de huidige baselines binnen de overheid vervangt. Dat voornemen wordt gedragen door alle overheidslagen. Naar verwachting zou deze BIO in 2017 gereed moeten zijn waardoor vanaf 2018 vervanging van de huidige baselines door de BIO plaats kan vinden.
Op 19 september heeft het Nationaal Beraad Digitale Overheid besloten dat nieuw aangekochte of ontwikkelde e-mailservers (voor e-mailverkeer) bij gemeenten en andere overheden voortaan moeten voldoen aan de e-mailbeveiligingsstandaarden STARTTLS en DANE. Gebruik van deze en andere standaarden (zoals TLS, DKIM+SPF en DNSSEC) is één van de schakels in de bestrijding van phishing en de beveiliging van persoonsgegevens. Het Nationaal Beraad heeft de open standaarden toegevoegd aan de verplicht toe te passen «pas-toe-of-leg-uit»-lijst met open standaarden. Door het Nationaal Beraad is eerder al een adoptie-impuls afgesproken, met het streefbeeld om alle voornoemde beveiligingsstandaarden die op de pas-toe-of-leg-uit-lijst staan – daar waar van toepassing – uiterlijk eind 2017 te hebben geïmplementeerd.