Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2009–2010

Aanhangsel van de Handelingen

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

1102

Vragen van het lid **Heerts** (PvdA) aan de minister van Justitie over *onveilige webshops.* (Ingezonden 20 november 2009)

1
Kent u het artikel «Webshops zo lek als een mandje»?[1]

2
Was u op de hoogte van het feit dat maar 12 procent, of een klein percentage, van de webwinkels een veilige website hebben? Zo ja, wat heeft u met die kennis gedaan?

3
Als u niet op de hoogte was van deze dramatische cijfers, wat is in het algemeen uw mening daarover?

4
Is het waar dat webwinkels wettelijk verplicht zijn om persoonsgegevens te versleutelen? Hoe gaat dit versleutelen technisch in zijn werk? Kunnen deze webwinkels dit versleutelen eenvoudig toepassen?

5
Wie is verantwoordelijk voor de toezicht op deze webwinkels? Als er geen toezichthouder is, is dat een wenselijke situatie aangezien er sprake is van een wettelijke plicht? Als er wel een toezichthouder is, kan gezegd worden dat deze heeft gefaald?

6
Zijn er getallen bekent over het aantal klanten van deze webwinkels die slachtoffer zijn geworden van fraude door de laakbare houding van de webwinkels? Zo ja, kunt u die met de Kamer delen? Zo nee, wilt u daar naar laten kijken?

[1] AD, 18 november 2009.

Antwoord

Antwoord van minister **Hirsch Ballin** (Justitie) (ontvangen 24 december 2009) Zie ook Aanhangsel Handelingen, vergaderjaar 2009–2010, nr. 960

1
Ja.

2 en 3
Het onderzoek waarop bedoeld artikel is gebaseerd was mij niet eerder bekend. Uit het oogpunt van consumentveiligheid en consumentenvertrouwen acht ik het van belang dat webwinkels passende maatregelen nemen met het doel de persoonsgegevens van hun klanten op een goede manier te beschermen. Zij zijn daar wettelijk toe verplicht. Internetgebruikers hebben daarnaast ook een eigen verantwoordelijkheid. Om hen daarop te wijzen en hen van praktische tips te voorzien heb ik afgelopen zomer een Postbus 51 campagne Veilig Internetten gehouden.
Overigens wijs ik erop dat het aangehaalde onderzoek uitwees dat de betalingsgegevens (via iDeal) wel goed beveiligd zijn. De onbeveiligde informatiestroom betreft de overige gegevens, zoals de naam- en adresgegevens van de klant en de inhoud van de bestelling.
Ik acht de kans op misbruik van deze zogenaamde «telefoonboekgegevens» beperkt.

4
Ook webwinkels zijn op grond van artikel 13 Wet bescherming persoonsgegevens (Wbp) verplicht om de gegevens van klanten op een passende manier te beschermen. Wat passend is hangt onder andere af van de aard van de gegevens en de kosten van de te nemen maatregelen. In CPB-richtsnoeren is nader uitgewerkt dat het gebruik van het SSL-protocol daartoe een geëigend middel is.
Technisch gezien betekent de versleuteling dat er een beveiligde verbinding wordt gelegd tussen twee internetservers. Een webwinkel dient daartoe een beveiligingscertificaat aan te schaffen bij een externe partij. Bij gebruik van het Secure Socket Layer protocol (SSL, herkenbaar aan het slotje in de webbrowser) beschikt een website over een digitaal certificaat, een soort digitale handtekening. Dit certificaat dient als basis voor de versleuteling van het berichtenverkeer tussen website en gebruiker. Het versleutelen met SSL kan door website-eigenaren eenvoudig worden toegepast. SSL-certificaten kunnen worden aangeschaft bij een leverancier van

KVR38846
2009Z22176
0910tkkvr1102
ISSN 0921 - 7398
Sdu Uitgevers
's-Gravenhage 2010

digitale certificaten en vervolgens door de website-hoster op de website worden geplaatst. Dit vereist enige technische expertise die regulier aanwezig mag worden verondersteld bij website-hosters.

5
Het College bescherming persoonsgegevens (CBP) is aangewezen als toezichthouder op de naleving van de Wbp. Het betreft hier zogenaamd «ex post» toezicht: toezicht dat vormkrijgt door handhavend onderzoek aan de hand van vermoedens van overtredingen. Voor de keuze naar welke vermoedens handhavend onderzoek plaatvindt, maakt het CBP elk jaar een uitgebreide risico-analyse. Daarbij spelen de ernst en de hoeveelheid signalen die het CBP ontvangt een belangrijke rol. Ik heb geen aanwijzingen dat het CBP hierbij onzorgvuldig te werk is gegaan.

6
Het Meldpunt ID-fraude heeft in de eerste helft van 2009 26 meldingen ontvangen van personen die vermoeden dat hun gegevens via internet bij kwaadwillenden terecht zijn gekomen. Dit betreft zowel het verzamelen van identificerende gegevens op (semi-)openbare sites, zoals Hyves en LinkedIn, als het via niet legale weg verzamelen van gegevens (bijvoorbeeld door hacking en phishing). Mij zijn geen specifieke gegevens bekend over internetfraude via webwinkels, en ik zie geen aanleiding om naast de in mijn antwoord op vraag 5 genoemde werkzaamheden van het CBP hierover gegevens te verzamelen.