**2009Z20759**

Vragen van het lid Algra (CDA) aan de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties over het kraken van websites. (Ingezonden 6 november 2009)

1
Heeft u kennisgenomen van het artikel over het veel te makkelijk kraken van websites van de overheid? 1)

Antwoord 1
Ja

2
Wat wordt er gedaan om websites van de overheid te beschermen tegen inbrekers?

Antwoord 2
Het beveiligen van websites tegen inbrekers is een verantwoordelijkheid van de eigenaren van die websites. Overheidswebsites worden beschermd tegen inbrekers door het goed implementeren van beveiligingsmaatregelen en het controleren daarop. Dat is bij het gegeven voorbeeld in onvoldoende mate gebeurd. Mede daarom heb ik in mijn toespraak op het Govcertcongres en in het aangehaalde artikel aangekondigd dat ik laat onderzoeken in hoeverre er gekomen kan worden tot een meldplicht voor ICT-incidenten bij de (rijks)overheid en audits op genomen maatregelen. Daarnaast heeft Govcert het Raamwerk Beveiliging Webapplicaties ontwikkeld, waarin geadviseerd wordt hoe met de beveiliging van websites om te gaan.

3
Is het waar dat het beveiligen van websites geen topprioriteit is van de overheid?

Antwoord 3
Nee, zoals gesteld in het artikel neemt het gebruik van Internet-websites als communicatie en transactiemiddel voor de overheid toe. Een belangrijke voorwaarde hierbij is dat dit gebruik veilig en betrouwbaar plaats kan vinden.

4
Welke voorvallen van diefstal van privé-gegevens via overheidswebsites zijn bekend?

Antwoord 4
Vooralsnog zijn mij geen voorvallen van diefstal van privé-gegevens via overheidswebsites bekend.

5
Waarom is er sprake van een verslechtering van de beveiliging ten opzichte van een jaar geleden, zoals in het artikel door de directeur van HMS-management wordt beweerd en lijkt te worden bevestigd door ICT adviesorgaan Govcert? 2)

Antwoord 5
In het algemeen signaleert Govcert in haar Trendrapport 2009 dat de veiligheid van het internet als geheel verslechtert, Daarbij ging het met name om de internetinfrastructuur en over netwerkverkeer van besmette computers.[1] Ik heb echter geen indicatie dat de beveiliging van overheidswebsites verslechtert.

6
Waarom hebben overheidssites geen digitaal slot?

Antwoord 6
Websites kennen geen universeel digitaal slot. De beveiliging van een website bestaat uit een samenstel van maatregelen, gericht op de bescherming tegen risico's van incidenten en misbruik. Bij de overheidswebsites is het de bedoeling dat de informatie breed beschikbaar is voor burgers en professionals. Daarom is het van belang om de juiste maatregelen op de juiste plaats toe te passen. Het gebruik van SSL bij overheidswebsites en het voorkomen van kwetsbaarheden (zoals in het artikel in Trouw genoemde SQL-injecties) zijn voorbeelden van dergelijke specifieke maatregelen. Overheidssites maken gebruik van diverse beveiligingsmaatregelen. Indien ondanks

[1] Trendrapport 2009 (http://www.govcert.nl/render.html?it=156).

deze maatregelen toch incidenten plaatsvinden, is Govcert.nl beschikbaar om samen met de getroffen overheidsorganisatie snel in te grijpen en mogelijke schade voor burgers en overheid te beperken.

7
Op welke manier bent u voorbereid op het risico dat het ICT-apparaat van de overheid voor een groot deel wordt platgelegd?

Antwoord 7
Het Voorschrift Informatiebeveiliging voor overheidsorganisaties binnen de Rijksdienst verplicht tot een risicoafweging. Op basis van deze afweging nemen deze organisaties onder eigen verantwoordelijkheid voor hun systemen passende maatregelen.
De mate waarin bedrijfsprocessen afhankelijk zijn van ICT en de mate waarin ze daarbij kwetsbaar zijn, speelt een belangrijke rol. Het kabinet bevordert het risicobewustzijn, ook bij de medeoverheden, via organisaties zoals GOVCERT.NL, het Nationaal Adviescentrum Vitale Infrastructuur (NAVI) en tot en met 2009 ook via het programma Nationale Infrastructuur CyberCrime (NICC) en biedt daarmee ook overlegstructuren om informatie, kennis en ervaringen met elkaar te delen. Zie tevens het antwoord op de Vragen van het lid Gerkens (SP) aan de minister van Binnenlandse Zaken en Koninkrijksrelaties over uitval ICT (TK 2008-2009 aanhangsel 1903).

8
Wat doet u om op het terrein van beveiliging tegen computerhackers binnen de overheid een mentaliteitsverandering tot stand te brengen?

Antwoord 8
Een belangrijk instrument hiervoor zijn de beveiligingsadviezen van Govcert en de veelvuldige overleggen die zij heeft met ICT-verantwoordelijken binnen de departementen, op zowel operationeel als tactisch en strategisch niveau. Daarnaast vraag ik in voorkomende gevallen, zoals bij de in het artikel genoemde SSL-problematiek, ook de CIO's van de departementen om bijzondere aandacht aan problemen te geven. Ten derde zullen de aangekondigde onderzoeken naar meldplicht en audits een positieve bijdrage leveren aan mentaliteitsverandering, daar waar dat nodig is.

1) Trouw, 5 november 2009: "Een, twee, drie - en gekraakt is de website"
2) Zie noot 1)