Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2011–2012

Aanhangsel van de Handelingen

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

1876

Vragen van de leden **Elissen** en **Van Bemmel** (beiden PVV) aan de minister van Veiligheid en Justitie over *het kwijtmaken van het archief van het Nationale Cyber Security Centrum* (ingezonden 17 februari 2012).

Antwoord van minister **Opstelten** (Veiligheid en Justitie) (ontvangen 19 maart 2012) Zie ook Aanhangsel Handelingen, vergaderjaar 2011–2012, nr. 1773.

Vraag 1
Bent u bekend met het bericht «Govcert kan niet bij eigen archief hackincidenten»?[1]

Antwoord 1
Ja.

Vraag 2
Hoe kijkt u tegen het feit aan dat het Nationaal Cyber Security Centrum (NCSC) niet meer bij de registraties van incidenten vóór 2009 kan komen? Past dit binnen het profiel van een lerende organisatie? Vindt u het belangrijk dat er (trend)onderzoek gedaan kan worden naar eerdere incidenten? Zegt deze manier van werken iets over de zorgvuldigheid van werken en/of de technische competenties van het NCSC en voorloper Govcert? Hoe worden kennis en kunde rond cyber security momenteel geborgd?

Antwoord 2
De registratie van incidenten van vóór 2009 is toegankelijk. Voor meer details per incident zijn echter wel extra handelingen nodig. Aangezien het reeds afgehandelde en in trendrapporten verwerkte zaken betreft, is dit mijns inziens aanvaardbaar.
Govcert.nl heeft tot 2012 jaarverslagen en trendrapporten uitgebracht, die mede gebaseerd zijn op de incidenten die sinds 2004 hebben plaatsgevonden. In die rapporten is gewaarschuwd voor bepaalde trends in kwetsbaarheden of risico's.
Het NCSC/Govcert.nl werkt zorgvuldig en beschikt over de benodigde technische competenties. De incidenten zijn zorgvuldig afgehandeld. Daarnaast heeft Govcert.nl, mede op basis van via deze incidenten opgedane kennis, jaarverslagen gepubliceerd en trendrapporten uitgebracht. Verder

[1] «Govcert kan niet bij eigen archief hackincidenten» (bron: http://webwereld.nl/nieuws/109551/govcert-kan-niet-bij-eigen-archief-hackincidenten.html)

ah-tk-20112012-1876
ISSN 0921 - 7398
's-Gravenhage 2012

worden jaarlijks vele ICT-beveiligingsadviezen met handelingsperspectief uitgebracht.

Vraag 3
Hebben zich vóór 2009 incidenten voorgedaan waarbij SCADA-systemen werden gehackt of misbruikt door onbevoegden? Zo ja, waarom is er niet eerder actie ondernomen om iets te doen aan de kwetsbaarheden die bijvoorbeeld in EenVandaag werden getoond?[2] Zo nee, waar baseert u dat op? Hoe weet u dat er geen SCADA-systemen werden gehackt of misbruikt door onbevoegden, aangezien het NCSC aangeeft niet over deze gegevens te beschikken?

Antwoord 3
Ja. ik ben mij al langer bewust van de kwetsbaarheid van SCADA-systemen en heb daarom hiervoor gewaarschuwd in publicaties zoals het Trendrapport Digitale Veiligheid 2010 en het Cyber Security Beeld Nederland.
Om de weerbaarheid van vitale sectoren te vergroten, zijn reeds maatregelen genomen. Er is geoefend en er zijn penetratietesten gedaan. Het verhogen van de weerbaarheid van de vitale sectoren is een van de actielijnen van de Nationale Cyber Security Strategie. Daarnaast heeft het NCSC naar aanleiding van de uitzending EenVandaag SCADA eigenaren extra gealerteerd over SCADA-beveiliging. Verder heeft het NCSC een checklist omtrent beveiliging van SCADA-systemen opgesteld om organisaties te helpen een juiste en bewuste keuze te maken voor een passend beveilingsniveau. Eigenaren van SCADA-systemen zijn zelf verantwoordelijk voor de beveiliging van hun SCADA-systemen.

Vraag 4
Wat vindt u ervan dat Govcert/NCSC informatie die zij op basis van de Wet Openbaarheid van bestuur (Wob) zou moeten verstrekken, niet verstrekt omdat de informatie op dusdanige wijze is opgeslagen dat deze niet meer eenvoudig geraadpleegd kan worden? Gaat u vanuit de eigen verantwoordelijkheid van de overheid ervoor zorgen dat deze gegevens zo snel mogelijk toegankelijk worden gemaakt? Zo ja, doet u dit om aan de ene kant te leren van incidenten en aan de andere kant om de indiener van het Wob-verzoek alsnog tegemoet te komen? Zo nee, waarom bent u niet bereid dit te doen?

Antwoord 4
Zoals ik bij antwoord 2 heb aangegeven, is de informatie toegankelijk. Voor meer gedetailleerde informatie zijn extra, arbeidsintensieve handelingen nodig.
Bij het Wob-verzoek waarnaar u verwijst, heeft verzoeker uitdrukkelijk ingestemd met de openbaarmaking van informatie vanaf 2009 alsook dat hij zijn bezwaar zou intrekken als hem informatie vanaf 2009 zou worden verstrekt. De desbetreffende informatie is openbaar gemaakt. Dat verzoeker thans om hem moverende redenen andere gedachten daarover heeft, betreur ik omdat het bestuursorgaan zich aan de gemaakte afspraak heeft gehouden.

Vraag 5
Hoe beoordeelt u de situatie dat een onderdeel van de overheid dat goed met techniek zou moeten kunnen omgaan, niet meer over de eigen historische gegevens kan beschikken? Had Govcert in uw beleving met open standaarden moeten werken? Had Govcert in uw beleving met het overgaan naar een nieuwe database de historische gegevens moeten migreren? Zo nee, waarom is er geen gebruik gemaakt van open standaarden? Waarom zijn er geen gegevens gemigreerd of is er geen virtualisatie toegepast om de gegevens alsnog te kunnen gebruiken?

Antwoord 5
Zoals weergegeven in antwoord 2 beschikt het NCSC/Govcert.nl over de eigen historische gegevens in een database. Deze database is gebaseerd op open source software, open standaarden dus.

[2] «Sluizen, gemalen en bruggen slecht beveiligid» (bron: http://www.eenvandaag.nl/binnenland/39770/sluizen_gemalen_en_bruggen_slecht_beveiligd)

Migratie van gegevens is op grond van de Archiefwet verplicht wanneer de duurzaamheid van de gegevens niet langer gegarandeerd kan worden. Zoals ook wordt weergegeven in antwoord 7, is dat hier niet aan de orde. De gegevens zijn veilig gesteld. Uit doelmatigheidsoverwegingen is er voor gekozen om de oude gegevens niet te migreren en te virtualiseren.

Vraag 6
Denkt u dat er een precedentwerking van deze zaak uitgaat en dat andere overheidsonderdelen nu ook gegevens op dusdanige wijze gaan opslaan dat deze niet meer gemakkelijk te delen zijn? Vindt u daarnaast dat de wijze van archiveren van Govcert vergelijkbaar is met het opslaan van de gegevens in een container om deze vervolgens af te laten zinken? Zo nee, waarom niet?

Antwoord 6
Nee, zie verder het antwoord op de vraag 2.

Vraag 7
Vindt u dat er naar de letter én de geest van de Wob is gehandeld? Had Govcert en heeft het NCSC in uw beleving een verplichting dan wel een verantwoordelijkheid om de incidentengegevens van de periode voor 2009 toegankelijk te houden? Voldeed Govcert en voldoet het NSCS aan de archiefwet? Zo ja, waarom vindt u dat? Kunt u uitsluiten dat deze manier van obstructie, waaronder het slecht toegankelijk maken van gegevens en het eerdere bericht dat de gegevens zoek waren, strafbaar is? Zo nee, welke maatregelen gaat u treffen om herhaling van dit soort situaties te voorkomen?

Antwoord 7
De Wob bevat regels voor de openbaarmaking van informatie over bestuurlijke aangelegenheden en niet over het beheer en de toegang tot overheidsarchieven. Die regels zijn opgenomen in de Archiefwet. De Erfgoedinspectie heeft als toezichthouder op de Archiefwet vastgesteld dat de incidentmeldingen van Govcert van de periode vóór 2009 zijn gearchiveerd in een database. Deze database wordt in een beveiligde beheersomgeving beheerd. De database is voldoende toegankelijk conform de archiefwettelijke eisen die zijn gesteld voor op termijn vernietigbare archieven.

Vraag 8
Kunt u deze vragen vóór 15 maart 2012 beantwoorden zodat de antwoorden bij het algemeen overleg over cyber security en privacy kunnen worden betrokken?

Antwoord 8
Ja.