Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2011–2012

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 228 **BRIEF VAN DE MINISTER VAN VEILIGHEID EN JUSTITIE**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 19 maart 2012

Door middel van deze brief informeer ik uw Kamer, mede namens de Ministers van Economische Zaken Landbouw en Innovatie, Binnenlandse Zaken en Koninkrijksrelaties en Infrastructuur en Milieu over de beveiliging van Supervisory Control And Data Acquisition (SCADA)-systemen en de gebeurtenissen in de gemeente Veere. Dit conform mijn toezegging tijdens het AO Nationale Veiligheid d.d. 15 februari 2012 (Kamerstuk 29 517, nr. 59).

Beveiliging van SCADA-systemen

Uw Kamer heeft haar zorgen geuit over de beveiliging van SCADA-systemen naar aanleiding van de uitzending van ÉénVandaag over SCADA-systemen en de gebeurtenissen in de gemeente Veere. SCADA-systemen worden gebruikt voor het verzamelen, doorsturen, verwerken en visualiseren van meet- en regelsignalen van verschillende machines in (grote) industriële procescontrolesystemen. Deze systemen worden gebruikt in de vitale infrastructuur om processen aan te sturen. De beveiliging van SCADA-systemen is van groot belang. Inbreuken op SCADA-systemen raken ons direct. De aandacht van hackers voor de beveiliging van SCADA-systemen neemt de laatste tijd zichtbaar toe.

Een voorbeeld hiervan zijn de gebeurtenissen in de gemeente Veere. In de gemeente Veere had de hacker een pomp kunnen uitschakelen waardoor rioolwater niet kon worden afgevoerd. Dit had voor overlast en milieuverontreiniging kunnen zorgen. Hiermee was echter nog geen sprake van een bedreiging van de nationale veiligheid. Ook was er sprake van een systeem van checks and balances. Het betreft hier een mogelijke ingreep die de hoofdcentrale snel had kunnen signaleren waardoor er tijdig en adequaat geacteerd had kunnen worden door de betrokken partijen. In dit geval was de ernst van het incident relatief beperkt. Het toepassingsgebied van SCADA is zeer breed en varieert van zeer kritische vitale systemen en processen tot eenvoudige toepassingen. Het NCSC heeft een melding en de bijbehorende gegevens ontvangen van het programma

kst-26643-228
ISSN 0921 - 7371
's-Gravenhage 2012

ÉénVandaag. Het NCSC heeft hierop contact opgenomen met de gemeente, advies gegeven en ondersteuning aangeboden. Hiermee is adequate ondersteuning geboden.

Het beveiligen van dergelijke systemen is primair de verantwoordelijkheid van de eigenaren van de SCADA-systemen. De overheid houdt echter, gezien het grote belang dat door de overheid aan bepaalde sectoren wordt toegekend, toezicht op bepaalde sectoren. Met het oog hierop stelt de overheid naast de algemene wet- en regelgeving ook wet- en regelgeving op het sectorale niveau op. Deze sectorale wet- en regelgeving wordt opgesteld door de bij deze sectoren betrokken vakdepartementen. Ten aanzien van de financiële sector berust deze verantwoordelijkheid bijvoorbeeld bij het Ministerie van Financiën en ten aanzien van de telecommunicatiesector bij het Ministerie van Economische Zaken, Landbouw en Innovatie. Hierbij behoren dan ook de sectorale toezichthouders. Juist door hun specifieke focus op een bepaalde sector zijn de betrokken vakdepartementen en toezichthouders goed in staat om te weten wat er in de sector speelt. De minister van Veiligheid en Justitie heeft de regie op cyber security en de nationale veiligheid.

Geïnitieerde acties

De beveiligingsproblematiek met betrekking tot SCADA-systemen is bij ons bekend. GOVCERT.NL, tegenwoordig het Nationaal Cyber Security Centrum (NCSC), heeft hiervoor gewaarschuwd in het Cyber Security Beeld Nederland[1] en het Nationaal Trendrapport Cybercrime en Digitale Veiligheid 2010[2]. Ook de NCTV heeft de problematiek in eerdere publicaties reeds aangekaart. Om de weerbaarheid van de vitale sectoren te vergroten, zijn reeds maatregelen getroffen. Er is geoefend en er zijn penetratietesten gedaan. Deze acties maken deel uit van de Nationale Cyber Security Strategie.

In 2012 zal verder worden ingezet op de aansluiting van vitale sectoren bij het Nationaal Cyber Security Centrum. Daarnaast zal de huidige samenwerking tussen het NCSC en de zogeheten ISAC's, de overlegstructuren van vitale sectoren om informatie over cyber security te delen, de komende periode worden geïntensiveerd. Deze overlegstructuren worden in de loop van 2012 bij het NCSC ondergebracht. Door deze samenwerking en het delen van informatie kunnen problemen eerder worden aangepakt. Hoewel er in de komende periode nog veel moet gebeuren zijn er op dit vlak al een aantal grote stappen gezet, bijvoorbeeld in de vorm van de deelname van private partijen in de publiek-private ICT Response Board.

De aandacht van hackers en security onderzoekers voor de beveiliging van SCADA neemt de laatste tijd zichtbaar toe. Het Nationaal Cyber Security Centrum (NCSC) heeft mede daarom twee checklists opgesteld ten behoeve van de beveiliging van SCADA systemen. De eerste checklist zet alle punten uit het eerder gepubliceerde NCSC-Factsheet van 14 februari jl. op een rij en geeft handreikingen over hoe om te gaan met systemen online. Daarnaast is er ook een tweede checklist die organisaties kan helpen om zelf vast te stellen of hun SCADA omgeving afdoende beveiligd is op basis van maatregelen die als «good practice» beschouwd worden. Het NCSC draagt, waar mogelijk in samenspraak met bijvoorbeeld koepelorganisaties, zorg voor een adequate en actieve verspreiding van deze checklists, zodat zoveel mogelijk relevante partijen er kennis van kunnen nemen.

[1] Zie Kamerstukken 26 643, nr. 220.
[2] Zie Kamerstukken 28 684, nr. 292.

Tot slot

Concluderend, we zien dat systemen in toenemende mate afhankelijk zijn van het internet. Dit biedt kansen maar brengt daarnaast ook nieuwe risico's met zich mee. De eigenaar van een SCADA-systeem is zelf verantwoordelijk voor een passende beveiliging van het desbetreffende systeem. In het geval van de gemeente Veere was er weliswaar sprake van een betreurenswaardig incident, het betrof echter geen bedreiging van de nationale veiligheid. Het verhogen van de weerbaarheid van de vitale sectoren is een van de actielijnen van de Nationale Cyber Security Strategie. Hiermee blijft het Kabinet zich ervoor inzetten om Nederland digitaal veiliger te maken.

De minister van Veiligheid en Justitie,
I. W. Opstelten