Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2012–2013

# 26 643 Informatie- en communicatietechnologie (ICT)

**Nr. 261**

## BRIEF VAN DE MINISTER VAN VEILIGHEID EN JUSTITIE

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 3 december 2012

In de procedurevergadering van de vaste Kamercommissie voor Veiligheid en Justitie van 7 november jl. is de Minister van Veiligheid en Justitie, naar aanleiding van een brief van het lid Gesthuizen (SP), verzocht om te reageren op het op 26 oktober jl. op de website www.webwereld.nl verschenen nieuwsbericht: «hackers richten pijlen op kerncentrales».

In het nieuwsbericht «hackers richten pijlen op kerncentrales» wordt ingegaan op een waarschuwing van ICS-CERT (het op Industriële Controle Systemen, ofwel ICS, gerichte Computer Emergency Response Team van de Amerikaanse overheid). De waarschuwing[1] van ICS-CERT d.d. 25 oktober jl. is een update op een eerder advies van ICS-CERT. In deze waarschuwing wordt ingegaan op de toegenomen interesse van onder andere hacktivisten voor industriële controlesystemen (ICS), zoals Supervisory Control And Data Acquisition (SCADA)-systemen en het gebruik van de internet-zoekmachine SHODAN om dergelijke aan het internet gekoppelde systemen te vinden.

In het artikel wordt ten onrechte de suggestie gewekt dat hacktivisten zich hiermee specifiek op kerncentrales zouden richten. In de waarschuwing van ICS-CERT wordt consequent gesproken over industriële controlesystemen. Deze systemen worden in diverse sectoren toegepast. Daarmee is niet gezegd dat er geen sprake is van kwetsbaarheden in dergelijke systemen of dat er geen toegenomen aandacht bestaat van hacktivisten voor industriële controlesystemen. Deze problematiek is bij ons bekend en daar wordt naar gehandeld.

In mijn brief[2] d.d. 19 maart jl. heb ik dan ook aangegeven dat in de afgelopen jaren het Nationaal Cyber Security Centrum en haar voorganger regelmatig hebben gewaarschuwd voor kwetsbaarheden in industriële controlesystemen. Hierbij heb ik ook aangegeven dat de beveiliging van deze systemen primair de verantwoordelijkheid is van de eigenaren hiervan. In dezelfde brief heb ik ook aangegeven dat op de

[1] Zoals gepubliceerd op: http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-12-046-01A.pdf

[2] Zie Kamerstukken 26 643, nr. 228

kst-26643-261
ISSN 0921 - 7371
's-Gravenhage 2012

website www.ncsc.nl diverse concrete informatie- en adviesproducten beschikbaar zijn om eigenaren te helpen bij de beveiliging van industriële controlesystemen. Die publicaties verwijzen tevens naar de adviezen van, onder andere, ICS-CERT.

In het Cyber Security Beeld Nederland-2[1] (CSBN-2) dat ik op 6 juli jl. aan uw Kamer heb aangeboden is eveneens uitgebreid aandacht besteed aan de kwetsbaarheden in industriële controlesystemen. Tevens is in het CSBN-2 ingegaan op de toegenomen aandacht van cyberonderzoekers voor kwetsbaarheden in industriële controlesystemen en het feit dat hacktivisten op zoek lijken naar kennis over dergelijke systemen en de beveiliging daarvan.

Hierbij wil ik nogmaals benadrukken dat in het artikel onterecht de suggestie wordt gewekt dat de dreiging specifiek op kerncentrales is gericht. De dreiging is gericht op industriële controlesystemen die in diverse sectoren worden toegepast. Specifiek voor de nucleaire sector kan ik echter aangeven dat deze begin 2013 beschikt over een door de Minister van Economische Zaken vastgestelde Design Basis Threat (DBT) Cyberdreigingen. Deze is aanvullend op de reeds op grond van de Kernenergiewet verplichte DBTs voor dreigingen van fysieke aard. Mede op grond van internationale aanbevelingen (w.o. van de zijde van het Internationaal Atoomagentschap, IAEA) is deze specifieke ICT DBT-uitwerking ontwikkeld. Hiermee kunnen de Nederlandse nucleaire installaties een adequaat en proportioneel beveiligingsbeleid voeren op het vlak van ICT. De implementatie van een DBT door de nucleaire sector is verplicht. Gezien de ontwikkelingen binnen het digitale domein worden de werking en strekking van deze DBT naar verwachting frequent geëvalueerd.

De beveiligingsvraagstukken rondom industriële controlesystemen zijn mij bekend en hiervoor is dan ook reeds meerdere malen gewaarschuwd. Het NCSC zal onverminderd aandacht blijven vragen voor deze vraagstukken en de concrete kwetsbaarheden. Met de aansluiting van de ISACs (Information Sharing and Analysis Centres) van de verschillende vitale sectoren bij het NCSC zal de uitwisseling van kennis over dreigingen, kwetsbaarheden en de oplossingen hiervoor alleen maar toenemen.

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

[1] Zie Kamerstukken 26 643, nr. 245