Ministerie van Veiligheid en Justitie

> Retouradres Postbus 20301 2500 EH Den Haag

Aan de Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

NCTV

Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl

Kenmerk
NCTV/5726950/12

Bijlagen
1

Datum 16 maart 2012
Betreft Beantwoording vragen van de leden Hachi en Schouw (beiden D'66) over de risico's van software voor het op afstand besturen van industriële processen (ingezonden 1 februari 2012)

Hierbij bied ik u, mede namens de Minister van Binnenlandse Zaken en Koninkrijksrelaties, de antwoorden aan op de schriftelijke vragen die zijn gesteld door de leden Hachi en Schouw (beiden D'66) over de risico's van software voor het op afstand besturen van industriële processen. Deze vragen werden ingezonden op 1 februari 2012 met het kenmerk 2012Z01694.

De Minister van Veiligheid en Justitie,

I.W. Opstelten

2012Z01694

Datum
16 maart 2012

Antwoorden op de vragen van de leden Hachchi en Schouw (beiden D66) aan de ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Veiligheid en Justitie over de risico's van software voor het op afstand besturen van industriële processen (ingezonden 1 februari 2012)

Kenmerk
NCTV/5726950/12

Vraag 1
Hebt u kennisgenomen van het artikel "Scada-beveiliging een structureel probleem" Joost Schellevis? 1)

Ja.

Vraag 2
Onderschrijft u de stelling van de schrijver dat, anders dan in het Cybersecuritybeeld Nederland 2011 wordt gesuggereerd, het niet nodig is om over uitzonderlijk geavanceerde software te beschikken om een aanval op een beheerssysteem van bijvoorbeeld een riolering te laten slagen?

Ja. Het is niet nodig om over uitzonderlijk geavanceerde software te beschikken om een aanval op een beheerssysteem van bijvoorbeeld een riolering te laten slagen. In het Cyber Security Beeld Nederland (CSBN) 2011 is niet anders gesuggereerd.

Het CSBN gaat enerzijds in op generieke risico's van SCADA-systemen en anderzijds op de specifieke mogelijkheid van een gerichte aanval met een variant op de Stuxnet malware om een vitaal proces te verstoren. Over dit laatste stelt het CSBN dat het ontwikkelen van een variant op Stuxnet om op soortgelijke wijze SCADA-systemen van andere vitale processen te verstoren 'diepgaande kennis vereist van het aan te vallen proces'.

Vraag 3
Welke veiligheidseisen worden er gesteld aan Scada-systemen, zowel bij de overheid als in de commerciële sector? Hoe wordt hier toezicht op gehouden? Indien er toezicht gehouden wordt, wat is dan het beeld dat toezichthouders hebben van de veiligheid van de systemen?

Organisaties binnen de overheid en de commerciële sector zijn zelf verantwoordelijk voor hun SCADA-systemen.

Het NCSC adviseert de overheid en de commerciële sector over veiligheid van SCADA-systemen. Zo heeft het NCSC een checklist[1] 'security on-line SCADA-systemen' ontwikkeld . Deze adviezen zijn gezonden aan vitale organisaties bij de overheid en in de commerciële sector.

Toezicht op de veiligheid van SCADA-systemen ligt bij sectorale toezichthouders, die vallen onder de relevante vakdepartementen. Naast algemene wet- en regelgeving bestaat er op het sectorale niveau relevante wet- en regelgeving met daarbij voor de diverse sectoren van toepassing zijnde verplichtingen. Deze wet- en regelgeving laat zich veelal kenmerken door de specifieke focus op de sector.

[1] *Zie: www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/factsheets*

Vraag 4
Onderschrijft u de waarschuwing voor het gevaar van USB-sticks? Kunnen in cruciale industriële infrastructuren, zoals de kerncentrale van Borssele, datadragers van buitenaf, zoals usb sticks, vrij ingevoerd worden? Bestaan hier beveiligingsprotocollen voor?

Ik onderschrijf de waarschuwing voor het gevaar van USB-sticks. Het NCSC/Govcert.nl heeft in adviezen over informatiebeveiliging gewezen op de risico's die zijn verbonden aan het gebruik van USB-sticks.

(Vitale) organisaties zijn zelf verantwoordelijk voor het uitvoeren van de adviezen van het NCSC, het opstellen van beveiligingsprotocollen en de naleving daarvan. Het valt nooit helemaal uit te sluiten dat datadragers van buitenaf worden ingevoerd. Met betrekking tot het door u aangehaalde voorbeeld van de kerncentrale Borssele merk ik op dat de beveiliging van de centrale in algemene zin een hoge prioriteit kent. Zo heeft in het najaar 2011 een stresstest safety door de vergunninghouder van de kerncentrale Borssele plaatsgevonden. Hierin is ondermeer onderzocht of, en zo ja op welke wijze, cyberaanvallen op onder meer sturingssystemen van de kerncentrale uitgevoerd kunnen worden. Geconcludeerd is dat de systemen in de kerncentrale goed uitgerust is om dit soort aanvallen te kunnen weerstaan.

Vraag 5
Hoe beoordeelt u de veiligheidsrisico's van Scada-systemen die rechtstreeks op het internet zijn aangesloten?

Het aansluiten van Industriële Controle Systemen(ICS) zoals SCADA op het internet vergroot de veiligheidsrisico's. Voor alle systemen die een koppeling hebben met het internet geldt dan ook, dat hierbij uiterste zorgvuldigheid betracht dient te worden. De beveiliging van dergelijke systemen is een verantwoordelijkheid van ieder betrokken bedrijf of organisatie. Zoals gezegd zal het NCSC intensief samenwerken met de vitale sectoren om de kennis over SCADA-systemen en de beveiliging daarvan op een hoger niveau te brengen.

Vraag 6
Is er op Europees niveau aandacht voor de veiligheidsrisico's van Scada-systemen? Zo ja, welke activiteiten worden er op dit gebied ontplooid? Zo nee, bent u bereid hier aandacht voor te vragen?

Ook op Europees niveau is er aandacht voor de veiligheidsrisico's van procesbesturingsystemenen en lopen er al diverse activiteiten.
- Het Europees Agentschap voor Netwerk- en Informatiebeveiliging (ENISA) heeft aandacht voor de beveiliging van ICS, organiseert bijeenkomsten hieromtrent en brengt publicaties uit over dit onderwerp;
- Euroscsie: een informatie-uitwisselingverband tussen Europese overheidsorganisaties en Computer Emergency Response Teams (CERTs), Europese (onderzoeks)instellingen zoals ENISA, CERN, JRC, en grote bedrijven/organisaties met als doel de kennis op dit vakgebied met elkaar te delen;
- Vanuit een gezamenlijk initiatief van Alliander en TNO wordt onder de naam European Network for Cyber Security (ENCS) een initiatief uitgewerkt om tot een test- en trainingsfaciliteit te komen gericht op de beveiliging van SCADA-systemen. ENCS zal medio dit jaar starten.

Joost Schellevis, 30 jannuari 2012; http://tweakers.net/reviews/2465/all/scada-beveiliging-een-structureel-probleem.html

Datum
16 maart 2012

Kenmerk
NCTV/5726950/12