Commissie V&J

Ministerie van Veiligheid en Justitie
Aan de minister
Postbus 20301
2500 EH DEN HAAG

Plaats en datum: Den Haag, 8 november 2012
Betreft: Nieuwsbericht van ICS-CERT dat hackers zich richten op Scada-systemen
Ons kenmerk: 2012Z19016/2012D41634

Geachte heer Opstelten,

In de procedurevergadering van de vaste commissie voor Veiligheid en Justitie van 7 november 2012 is gesproken over een nieuwsbericht van 26 oktober 2012 van webwereld.nl dat hackers hun pijlen richten op scada-systemen. De commissie heeft besloten om u een reactie te vragen op dit nieuwsbericht. De commissie ziet deze reactie graag tijdig tegemoet zodat deze nog kan worden geagendeerd voor het algemeen overleg over de voortgang van de Nationale Cyber Security Strategie op 29 november 2012. Volledigheidshalve heb ik het nieuwsbericht bijgevoegd.

Bij deze breng ik u het besluit van de commissie over.

Hoogachtend,

De griffier van de vaste commissie voor Veiligheid en Justitie,

D.S. Nava

BIJLAGE: Nieuwsbericht Webwereld.nl

Tweede Kamer der Staten-Generaal
Postbus 20018
2500 EA Den Haag

T. 070-3182211
E. cie.vj@tweedekamer.nl

BIJLAGE: Nieuwsbericht Webwereld.nl
http://webwereld.nl/nieuws/112252/hackers-richten-pijlen-op-kerncentrales.html

Gepubliceerd: Vrijdag 26 oktober 2012
Auteur: Henk-Jan Buist

Hackers storten zich op SCADA-systemen, waarschuwt ICS-CERT. Deze industriële pc's die onder meer kerncentrales aansturen, zitten vol kwetsbaarheden en exploittools maken misbruik ervan erg makkelijk.

Hacktivisten en andere hackers richten hun pijlen op industriële systemen die kritieke infrastructuur zoals kerncentrales, waterbedrijven, rioolinstallaties en sluizen aansturen. Daarvoor waarschuwt de beveiligingsdienst van industriële systemen ICS-CERT. De plc's van SCADA-systemen zijn makkelijk te misbruiken door exploittools die maandenlang ongepatchte gaten openwrikken. Bovendien gebruiken hackers zoekmachine Shodan om snel kwetsbare systemen op te sporen.

Snoodaards besnuffelen SCADA
"ICS-CERT neemt een verhoogde interesse waar van malafide groepen, waaronder hacktivisten en anarchisten, voor industriële apparaten", stelt de dienst in een waarschuwingsbericht (PDF). De dienst ziet dat zwakke SCADA-systemen worden geïdentificeerd door hackers en de adressen daarvan worden gepubliceerd op verschillende sites. "Leden van deze groepen vragen anderen de machines te bekijken of zich er toegang toe te verschaffen."

SCADA-systemen zijn vaak zo lek als een mandje en via een beveiligingstool zijn de kwetsbaarheden in honderden van deze besturingssystemen eenvoudig te misbruiken. Juist omdat SCADA-systemen kritieke infrastructuur aanstuurt als stroom- en watervoorziening is een stevige beveiliging gewenst. Maar de besturingssystemen zitten vol bugs en backdoors.

Via de tool CoDeSys zijn backdoors te openen naar verschillende industriële controlesystemen die een internetverbinding hebben. De tool is bedoeld om plc's eenvoudig op afstand te herprogrammeren. Veel SCADA-systemen vereisen hiervoor niet eens dat de gebruiker logincredentials gebruikt en laten wie dat ook maar wil binnen, vertelt een beveiligingsonderzoeker aan Ars Technica.

Industriële systemen wijdopen
Verschillende backdoors in SCADA-systemen zijn breedgedocumenteerd. Veiligheidsdienst ICS-CERT, die de beveiliging van industriële systemen in de gaten houdt, waarschuwt bijna dagelijks voor een nieuwe kwetsbaarheid. De dienst gebruikt als standaardadvies om kritieke systemen niet aan een internetverbinding te hangen.

ICS-CERT waarschuwt dat onder meer plc's van fabrikanten GE, Rockwell Automation, Schneider Electric en Koyo te misbruiken zijn met de tool waar de dienst in februari ook al eens melding van maakte. "Bezitters van deze systemen moeten niet aannemen dat hun industriële controlesystemen veilig zijn of dat ze een configuratie gebruiken waarbij geen actieve internetverbinding aanwezig is", aldus de dienst.

De makers van SCADA systemen zijn notoir laks in het beveiligen van hun besturingssystemen. ICS-CERT stelt dat beveiligingsproblemen in industriële systemen extra gevaarlijk zijn geworden met de komst van de zoekmachine Shodan twee jaar geleden. Shodan indexeert kwetsbare servers en op deze manier kunnen hackers de gaten in SCADA-systemen sneller misbruiken.

Veiliger besturingssysteem
De fabrikanten van industriële systemen vertrouwden in het verleden op security-through-obscurity. Maar nu kwetsbaarheden op straat liggen, expoittools verkrijgbaar zijn en ip-adressen van SCADA-machines online verschijnen, ligt die tijd ver achter ons. Na Stuxnetdat zich richtte op industriële centrifuges voor het verrijken van uranium, werd in de beveiligingswereld hard gezocht naar personeeldat gespecialiseerd is in SCADA-systemen.

Beveiligingsbedrijf Kaspersky werkt naar eigen zeggen al tien jaar aan een veilig besturingssysteem voor industriële systemen. Eugene Kaspersky onthulde eerder deze maand officieel plannen voor dit OS, maar hoe het precies gaat werken en wanneer het moet uitkomen blijft onduidelijk.

Tweede Kamer der Staten-Generaal
Postbus 20018
2500 EA Den Haag

T. 070-3182211
E. cie.vj@tweedekamer.nl