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 's-Gravenhage

Directie Cyber Security

Schedeldoekshaven 200
2511 EZ Den Haag
Postbus 20301
2500 EH Den Haag

Ons kenmerk

287556

Uw kenmerk

2012Z11855

Bij beantwoording de datum en ons kenmerk vermelden.

Wilt u slechts één zaak in uw brief behandelen.

Datum 31 juli 2012
Betreft Brief beantwoording kamervragen aanpak van cyberspionage

Hierbij zenden wij u de antwoorden op de schriftelijke vragen over de waarschuwing van het Industrial Control Sytem Cyber Emergency Response Team van het lid Gesthuizen (SP). Deze vragen zijn ingezonden op 13 juni 2012 met kenmerk 2012Z11855.

De Staatssecretaris van Veiligheid en Justitie,

F. Teeven

Vragen van het lid Gesthuizen (SP) aan de minister van Veiligheid en Justitie over de waarschuwing van het Industrial Control System Cyber Emergency Response Team (ingezonden 13 juni 2012; 2012Z11855)

Datum
31 juli 2012

1
Wat is uw reactie op de waarschuwing van het Industrial Control System Cyber Emergency Response Team?

Antwoord
De waarschuwing van de Amerikaanse ICS-CERT acht ik waardevol. ICS-CERT brengt jaarlijks vele waarschuwingen en adviezen uit. Het Nationaal Cyber Security Centrum (NCSC) is bekend met deze producten en maakt ook gebruik van de informatie uit deze producten en verwerkt deze in haar publicaties.
In een door het NCSC uitgebrachte factsheet over de beveiliging van SCADA/ICS systemen is verwezen naar de informatie op de website van ICS-CERT.

2
Wordt er in Nederland gebruik gemaakt van de in de memo genoemde SCADA en ICS gerelateerde web- en softwareapplicaties van Siemens, bijvoorbeeld in de chemische-, olie- en gasindustrie, in de sectoren voedsel- en watervoorziening of andere sectoren, zoals de gezondheidszorg en defensie? Zo ja, op welke schaal en in welke sectoren?

3
Zijn de bedrijven en organisaties in Nederland, die deze kritieke systemen beheren, op de hoogte van de in de memo vermelde "cross-site scripting", "path traversal, XML Injection" en "buffer overflow" problemen in relatie tot de vermelde Siemens applicaties? Zo nee, waarom niet?

4
Hebben deze bedrijven de specifieke aanbevolen stappen ter beveiliging van de systemen en ter voorkoming van zowel manipulatie op afstand als manipulatie door derden van deze systemen al genomen? Zo nee, waarom niet? Wanneer verwacht u dat deze bedrijven en organisaties de maatregelen wel genomen hebben?

Antwoord
Het is niet bekend of en in welke mate er in Nederland gebruik wordt gemaakt van de genoemde SCADA en ICS gerelateerde web- en software applicaties van Siemens.

In mijn brief van 19 maart jl[1] heb ik aangegeven dat het NCSC ten aanzien van de beveiliging van SCADA/ICS systemen adviseert en een factsheet en checklists heeft gepubliceerd en deze actief heeft verspreid binnen de overheid en de private vitale sectoren. In de factsheet wordt verwezen naar informatie op de website van ICS-CERT. Daarnaast wordt in de factsheet ingegaan op de veiligheidsrisico's die het aansluiten van SCADA/ICS-systemen op het internet met zich meebrengt. Ook is in het door het NCSC gepubliceerde Raamwerk Beveiliging Webapplicaties hierover uitgebreid aandacht besteed. Deze publicaties gaan ook in op de problemen zoals benoemd in vraag 3.

[1] *Zie Kamerstukken 2011-2012, 26643, nr 228.*

De aansluiting bij het NCSC van de Information Sharing and Analysis Centres (ISACs) van diverse (vitale) private sectoren zal de advisering richting die sectoren en de kennisdeling versterken.

Zoals ik in mijn brief van 19 maart jl. aangaf zijn organisaties zelf primair verantwoordelijk voor de beveiliging van hun systemen, maar houdt de overheid, gezien het grote belang dat door de overheid aan bepaalde sectoren wordt toegekend, toezicht op bepaalde sectoren (onder andere de sector telecom en financiën). 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. Hierbij behoren dan ook de sectorale toezichthouders.

5
Weet u of de bedrijven en organisaties, die deze kritieke systemen beheren, de meer algemene aanbevelingen in de memo hebben toegepast, waaronder de loskoppeling van deze systemen en software van het internet waar mogelijk, de scheiding van deze systemen en software van de interne bedrijfsnetwerken door middel van firewalls en het gebruik van VPNs (Virtual Private Networks) om veilige verbindingen met deze applicaties te garanderen? Zo nee, waarom niet? Wanneer denkt u dat de bedrijven en organisaties deze maatregelen wel genomen hebben?

Antwoord
Het NCSC is geen toezichthouder die beveiligingsarrangementen van organisaties opvraagt. Het NCSC heeft een advies en incident respons rol richting overheid en vitale sectoren.