Antwoord

van Gedeputeerde Staten

op vragen van

E.F.A. Zevenbergen (VVD) en E.N.W. Hoogland (VVD)
(d.d. 8 augustus 2019)

Nummer
3539

Onderwerp
SCADA

Aan de leden van Provinciale Staten

Toelichting vragensteller
Onlangs is bekend geworden dat nog steeds tientallen Nederlandse IT-systemen van kritische infrastructuur onvoldoende beveiligd zijn[1]. In opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum van het ministerie van Justitie en Veiligheid werd door de Universiteit van Twente (UT) onderzocht of de geconstateerde gebreken uit het verleden zijn opgelost. Helaas stelde de UT vast dat de beveiliging van industriële IT-omgevingen een veronachtzaamd onderwerp blijft, terwijl de beveiliging van die omgevingen van levensbelang kan zijn voor zowel de mens als de onderneming of overheid zelf.

Sinds 20015 zijn in Zuid-Holland alle systemen die te maken hebben met water op afstand bedienbaar gemaakt. Denk daarbij aan bruggen en sluizen en de bediening daarvan. Maar met SCADA wordt nog veel meer publieke en industriële systemen aangestuurd binnen onze provincie. De VVD-fractie maakt zich zorgen over de geconstateerde zwakheden in kritieke systemen en vraagt zich af of dit ook in Zuid-Holland voorkomt.

Uiteraard heeft de VVD-fractie er begrip voor dat delen van de antwoorden omwille van de veiligheid gerubriceerd zijn.

Toelichting GS:
De beantwoording van de gestelde vragen wordt gedaan tegen de achtergrond van de gegeven toelichting. De beantwoording gaat in op de beveiliging van systemen in beheer van de provincie voor de besturing van kritische infrastructuur.

[1] https://www.compact.nl/articles/beveiliging-van-industriele-it-omgevingen/ https://tweakers.net/nieuws/155770/onderzoekers-zestig-slecht-beveiligde-nederlandse-scada-systemen-op-internet.htm.

1. *Wanneer was de laatste inventarisatie van de IT-systemen in provinciaal beheer en hoeveel van die IT-systemen worden aangestuurd met SCADA?*

Antwoord
ICS, Industriële Controle Systemen is een verzamelbegrip voor verschillende soorten controlesystemen en instrumentarium die worden gebruikt voor industriële procesbesturing. Een ICS systeem dat gebruik maakt van een computer en een netwerk om op afstand te besturen wordt een SCADA systeem genoemd.
"SCADA, afkorting van Supervisory control en data acquisition, is het verzamelen, doorsturen, verwerken en visualiseren van meet- en regelsignalen van verschillende machines in grote industriële systemen. Een SCADA systeem bestaat uit een computer met daarop SCADA-software.. Een SCADA systeem vergemakkelijkt het uitwisselen van meetgegevens, het zichtbaar maken van gegevens voor de menselijke operator, het beïnvloeden van deze systemen (sturing) en het verwerken van meetgegevens toto rapporten of alarmering." (bron Wikipedia)

Uit een onderzoek van de Universiteit van Twente (Online discoverability and vulnerabilities of ICS/SCADA devices in the Netherlands van 2019) in opdracht van het Ministerie van Justitie en veiligheid blijkt dat 60 van de 989 op het openbare internet gevonden en onderzochte ICS/SCADA systemen kwetsbaar zijn voor bekende zwakke beveiligingspunten (CVE's) zoals genoemd in Hoofdstuk 4 van het onderzoeksrapport. De onderzoekers stellen onder andere voor dat belangrijke Industrial control systems en SCADA's niet meer via het openbare internet te bereiken zouden moeten zijn. Die zouden door firewalls, vlan's of vpn's verborgen moeten worden, zodat kwaadwillende, eventueel buitenlandse hackers er niet bij kunnen. Uiteindelijk willen de onderzoekers een compleet separaat internet opzetten voor kritieke infrastructuur.
Sinds 9 november 2018 is de Wet beveiliging netwerk- en informatiesystemen (Wbni) van kracht. De Wbni is erop gericht de digitale weerbaarheid van Nederland te vergroten, de gevolgen van cyberincidenten te beperken en zo maatschappelijke ontwrichting te voorkomen. In deze wet worden de processen geïdentificeerd die als vitaal (kritiek) worden onderscheiden.

Vitale infrastructuur in beheer bij de provincie betreft op grond van die definitie alleen de vier provinciale sluiscomplexen. Deze sluiscomplexen zijn niet verbonden met het openbare internet en worden lokaal bediend en zijn dus geen onderwerp waarop het onderzoek en de kritiek/zorg van de Universiteit van Twente betrekking op heeft.

De Dienst Beheer Infrastructuur van de provincie heeft de volgende (niet vitale/kritieke infrastructurele) ICS/SCADA systemen in gebruik.

1. Verkeersmanagementsysteem voor het op afstand besturen van verkeerslichten, dynamische route informatiepanelen en camera's
2. Centrale Objectbedieningssysteem voor het op afstand bedienen van bruggen
3. Managementsysteem voor het op afstand besturen van pompen en gemalen
4. Managementsysteem voor het besturen van Openbare verlichting

Bovengenoemde systemen zijn dan wel niet vitaal/kritisch op grond van de Wbni maar het is maatschappelijk zeer ongewenst als deze niet beschikbaar zijn door het illegaal inbreken in computers of computernetwerken of door het omzeilen van beveiligingsmaatregelen (hacken).
De Volkskrant heeft op grond van de WOB informatie van ons verkregen over de beveiliging van deze systemen. De brief aan De Volkskrant (PZH-2019-687321032) van 3 april 2019 is als bijlage bijgevoegd.

2. *Heeft de provincie de constateringen uit het verleden i.r.t. SCADA geïmplementeerd om de beveiliging van deze IT-systemen te verbeteren?*

Antwoord
In Hoofdstuk 5 van het onderzoeksrapport van de Universiteit van Twente worden de maatregelen tegen “bekende zwakke beveiligingspunten” waarop u doelt uiteengezet. Dit zijn inderdaad maatregelen die zijn geïmplementeerd in de provinciale ICS/SCADA systemen.

3. *Wanneer heeft de provincie haar laatste veiligheidsscan uitgevoerd op de IT-systemen die aangestuurd worden met SCADA? Welke kwetsbaarheid van deze IT systemen is uit deze veiligheidsscan naar voren gekomen? Zijn deze IT-systemen naar uw mening voldoende beveiligd? Zo niet, welke maatregelen heeft u voorgenomen om de beveiliging wel op orde te brengen?*

Antwoord
Op basis van eigen risicoanalyses, door audits van de provinciale Eenheid Audit en Advies en externe gespecialiseerde bedrijven wordt ons beleid getoetst aan de beveiligingsnorm en worden de geïmplementeerde maatregelen getest op opzet en bestaan.
Over de geconstateerde kwetsbaarheden kunnen wij u in openbaarheid niet informeren. Beveiliging is een constante wedloop van het treffen van maatregelen om te voorkomen dat systemen worden gehackt. Er worden daarom voortdurende aanvullende maatregelen getroffen om te komen tot voldoende beveiliging.

Indien gewenst kunnen statenleden mondeling nader worden geïnformeerd over de in het rapport genoemde kwetsbaarheden en de toegepaste risico beperkende maatregelen.

4. *Hoeveel systemen zijn te vinden door buitenstaanders, bijvoorbeeld doormiddel van een eenvoudige portscan? Hoe vaak zijn veiligheidsincidenten met deze IT-systemen geconstateerd? Zijn deze incidenten onderzocht? Wat waren de uitkomsten en wat zijn de mogelijke gevolgen van deze lekken? Waarom zijn deze lekken niet eerder gedicht?*

Antwoord
Provinciale systemen zijn voor buitenstaanders niet (eenvoudig) te vinden. Hoe kritischer het systeem hoe uitgebreider het pakket aan maatregelen om hackers buiten te houden. Zonder in detail te treden; er worden regelmatig pogingen gedaan om provinciale systemen te hacken. Tot op dit moment heeft men geen toegang kunnen verkrijgen tot de genoemde systemen.

5. *Heeft u contact met het NCSC over kwetsbaarheid van IT-systemen die aangestuurd worden met SCADA? Bent u bereid om uw kennis te delen met andere overheden zoals gemeentes en waterschappen?*

Antwoord
Het NCSC werkt in opdracht van de Rijksoverheid ten behoeve van de uitvoering van de Wet beveiliging netwerk- en informatiesystemen (Wbni). De werkzaamheden van het NCSC richten zich dus in hoofdzaak op voor de in de wet onderscheiden vitale infrastructurele processen. De provinciale betrokkenheid bij die processen is zeer gering. Wij nemen wel kennis van NCSC nieuwsbrieven en publicaties. Het NCSC informeert de provincie indien zij kennis hebben van specifieke provinciale dreigingen. De provincie werkt onder andere samen met Rijkswaterstaat aan een uitbreiding van de Baseline informatiebeveiliging Overheid (BIO) met een onderdeel dat specifiek ingaat op de beveiliging van Operationele techniek aangestuurd door ICS/SCADA systemen. De BIO is het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen (Rijk, gemeenten, provincies en waterschappen). Desgevraagd zijn wij altijd bereid onze kennis te delen met andere overheden. Door het uitvoeren van audits bij gemeenten die gebruik maken van ons ICS/SCADA netwerk delen wij indirect onze kennis in deze.

6. *Wat gaat u met de kennis van nu doen om deze IT-systemen in de toekomst veilig te houden?*

Antwoord
We gaan een Cyber Security Management Systeem (CSMS) op grond van norm NEN-EN-IEC 62443 invoeren. Op die wijze gaan wij de noodzakelijke voortdurende verbetering goed organisatorisch borgen. Dit CSMS is op dit moment ingericht voor 1 van de systemen en zal ingericht worden voor alle systemen die hier zijn besproken.

Den Haag, 3 september 2019

Gedeputeerde Staten van Zuid-Holland,
secretaris, voorzitter,

drs. H.M.M. Koek drs. J. Smit