Advies inzake de digitale veiligheid van Industrial Automation & Control Systems (IACS) in de vitale infrastructuur van Nederland

CSR
Cyber Security Council
Cyber Security Raad

Advies inzake digitale veiligheid van Industrial Automation & Control Systems (IACS) in de vitale infrastructuur van Nederland

Gericht aan:

De minister van Justitie en Veiligheid
De staatssecretaris van Economische Zaken en Klimaat
De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties
De overige ministers en staatssecretarissen wiens aanbieders van vitale diensten onder de Wbni vallen
De bevoegde autoriteiten

CSR
Cyber Security Council
Cyber Security Raad

24 april 2020

CSR-advies 2020, nr. 2

Excellentie,

Hierbij ontvangt u het advies van de Cyber Security Raad (hierna de raad) over de digitale veiligheid van Industrial Automation & Control Systems (IACS)[1] in de vitale infrastructuur van Nederland.

Beschermen wat van ons is

De digitalisering van productieprocessen neemt de komende jaren verder toe en daarmee groeit de afhankelijkheid van ICT en IACS in onze samenleving. Vitale productie- en ICT-processen moeten daarom goed worden beschermd. IACS zijn veelal op ICT-gebaseerde meet- en regelsystemen die gebruikt worden voor de aansturing van onze productieprocessen. IACS zijn daarmee van cruciaal belang voor de continuïteit van de (vitale) infrastructuur; een verstoring van de vitale infrastructuur kan grote ontwrichtende gevolgen hebben voor de samenleving en het vertrouwen in digitalisering. Het kan leiden tot uitval van systemen en objecten die onze maatschappij en samenleving laten functioneren. IACS zorgen er bijvoorbeeld voor dat onze sluizen en bruggen functioneren, energie en gas worden gedistribueerd, drinkwater wordt gereinigd, nucleair materiaal wordt verwerkt, treinen op bestemming komen, containers worden vervoerd en liften functioneren. De huidige Corona-crisis onderstreept de urgentie van cybersecurity van IACS; vitale diensten moeten kunnen blijven functioneren.

Er is voortdurend aandacht nodig om de IACS van de vitale processen op orde te houden of te brengen. Een belangrijke constatering daarbij is het feit dat niet-vitale processen verweven zijn met vitale infrastructuur en dat IACS vaak indirect gekoppeld zijn aan het internet, waardoor de impact van een intentionele of niet-intentionele verstoring op de gehele keten omvangrijk kan zijn. Het is daarom raadzaam om ons te focussen op vitale sectoren en niet alleen op vitale aanbieders. Onderzoeken door de Wetenschappelijke Raad voor het Regeringsbeleid (WRR)[2] en de Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek (TNO)[3] vragen aandacht voor de risico's van (nieuwe) ketenafhankelijkheden voor IACS op sectoraal én cross-sectoraal niveau. Daarbij mag ook de internationale component niet uit het oog worden verloren. De afhankelijkheid van veel vitale processen, zoals bij energie, stopt niet bij de landsgrens. Cascade-effecten kunnen zowel in een land als over en weer tussen landen plaatsvinden. Ook daar moeten we in ons land op ingesteld zijn.

In het kader van de bescherming van onze vitale infrastructuur spelen IACS een essentiële rol en verdienen daarom structureel onze aandacht. Doordat IACS steeds meer gebruikmaken van generieke ICT-middelen, worden daarmee ook standaard ICT-problemen in de industriële automatisering geïntroduceerd. Het uitbuiten van de kwetsbaarheden in IACS, kan tot grote economische schade en maatschappelijke ontwrichting leiden. Desondanks gaat in Nederland de meeste aandacht naar cybersecurity van ICT. Tot op heden zijn er in Nederland en veel andere landen geen IACS-gerelateerde cyberincidenten in de vitale infrastructuur geweest met grote impact. We kunnen echter niet achteroverleunen en denken dat het niet zo'n vaart zal lopen. Buiten de vitale infrastructuur in

[1] Voor dit advies is in 2019 voorbereidend onderzoek uitgevoerd door Gartner in opdracht van de CSR.
[2] Wetenschappelijke Raad voor het Regeringsbeleid (2019) *Voorbereiden op digitale ontwrichting*, WRR-Rapport 101, Den Haag
[3] Adviesrapport 'Intersectorale afhankelijkheden: buitenlandse methoden en mogelijke toepasbaarheid in Nederland' (2013), TNO, Uitgevoerd in opdracht van het (toenmalige) Ministerie van Veiligheid en Justitie en het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC)

Nederland (NotPetya[4]) en buiten West-Europa (BlackEnergy[5] en Stuxnet[6]) zijn wel voorbeelden bekend van ontwrichtende uitval van IACS. Dichterbij huis heeft NotPetya in het Verenigd Koninkrijk voor aanzienlijke schade gezorgd.

De toenemende connectiviteit van IACS[7] in combinatie met verouderde systemen (legacy) maken de vitale infrastructuur kwetsbaar voor onopzettelijke uitval en voor kwaadwillende actoren. Het is dan ook voorstelbaar dat er in de toekomst gecoördineerde, gelijktijdige aanvallen zullen plaatsvinden op de vitale infrastructuur. In Nederland waarschuwt de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) dat statelijke actoren proberen om zich toegang te verschaffen tot onze vitale processen[8].

Het is belangrijk dat we beschermen wat van ons is; we moeten slagvaardig kunnen blijven reageren op misstanden en/of cyberaanvallen.

We hebben onze zaken niet in alle gevallen voldoende op orde

We moeten ons realiseren dat het dreigingslandschap voortdurend in beweging is. Door nieuwe dreigingen en ketenafhankelijkheden kan blijken dat bepaalde objecten kwetsbaarder worden, waardoor andere of extra maatregelen nodig zijn. Dit zorgt vervolgens voor de noodzaak om andere of extra middelen en mensen vrij te maken die de benodigde maatregelen in lijn brengen met de geïdentificeerde risico's. Dit maakt cyberweerbaarheid een zaak van de boardroom. Onderzoeken van verschillende instanties rondom IACS laten zien dat dit in praktijk niet altijd in voldoende mate het geval is. Zo blijkt uit onderzoek van de Algemene Rekenkamer[9] dat de digitale weerbaarheid van onze waterkeringen op dit moment niet conform planning loopt, terwijl de overheid hierin een regie- en voorbeeldrol heeft. De Wet Beveiliging Netwerk en Informatiesystemen (Wbni) beschrijft de wetgevende taken van de betrokken ministeries[10] en definieert de bevoegde autoriteiten[11] voor alle vitale sectoren. De Wbni legt de verantwoordelijkheid voor het managen van risico's van externe afhankelijkheden van derde partijen bij de individuele aanbieder van de essentiële dienst. Hierdoor ontstaat een beperkt inzicht in de risico's en afhankelijkheden tussen overheid en bedrijfsleven in de verschillende vitale sectoren.

Met ander woorden, er is geen volledig beeld over de dreigingen en risico's in onze vitale sectoren en het is daarmee onbekend of we ons voldoende kunnen beschermen.

Daarnaast blijkt ook dat we onvoldoende zijn voorbereid op de gevolgen van uitval van IACS. Het Cybersecuritybeeld Nederland 2019[12] en het adviesrapport 'Voorbereiden op digitale ontwrichting'

[4] Varianten van Petya zijn voor het eerst waargenomen in maart 2016. Zij verspreidden zich via bestanden die met e-mails werden meegestuurd. In juni 2017 werd een nieuwe variant van Petya (NotPetya) gebruikt voor een wereldwijde cyberaanval, waarbij voornamelijk Oekraïne het doelwit was.

[5] BlackEnergy-malware werd in 2016 gebruikt bij aanvallen tegen energiecentrales. Door de aanvallen kwamen ongeveer 700.000 mensen in Oekraïne een paar uur zonder stroom te zitten.

[6] Stuxnet is een schadelijk computerprogramma. Het bestaan van deze geavanceerde worm werd ontdekt in juni 2010 door een fabrikant van antivirussoftware uit Wit-Rusland. Het programma beïnvloedt de werking van bepaalde Siemens-apparatuur op schadelijke wijze.

[7] Online Discoverability and Vulnerabilities of ICS/SCADA Devices in the Netherlands (2019), Universiteit Twente, uitgevoerd in opdracht van het Wetenschappelijk Onderzoek en Documentatiecentrum (WODC)

[8] Jaarverslag AIVD 2018, Algemene Inlichtingen- en Veiligheidsdienst, 2019

[9] Digitale dijkverzwaring: cybersecurity en vitale waterwerken (2019), Algemene Rekenkamer

[10] Dit betreft het ministerie van Justitie en Veiligheid en het ministerie van Economische Zaken en Klimaat

[11] De Wbni (artikel 4.1) definieert als bevoegde autoriteiten: Ministerie van Economische Zaken en Klimaat (Agentschap Telecom), Ministerie van Financiën (De Nederlandse Bank N.V.), Ministerie van Infrastructuur en Waterstaat (Inspectie Leefomgeving en Transport) en Ministerie Volksgezondheid, Welzijn en Sport (Inspectie Gezondheidszorg en Jeugd).

[12] Cybersecuritybeeld Nederland (CSBN) 2019, Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), 2019

van de WRR[13] laten zien dat Nederland onvoldoende voorbereid is op een eventuele digitale ontwrichting en de (wettelijk verankerde) ondersteuning die benodigd is als deze mogelijkheid zich voordoet. De raad acht dit een ongewenste situatie en is van mening dat:

De Nederlandse samenleving moet kunnen vertrouwen op de veiligheid en continuïteit van de vitale infrastructuur. De cyberweerbaarheid van IACS van de vitale aanbieders moet op het vereiste niveau worden gebracht dat passend en proportioneel is gelet op de dreigingen en risico's.

[13] Wetenschappelijke Raad voor het Regeringsbeleid (2019) *Voorbereiden op digitale ontwrichting*, WRR-Rapport 101, Den Haag

ADVIEZEN

De overheid onderkent de noodzaak van effectief toezicht op digitale veiligheid om blijvend te werken aan een hoog niveau van digitale weerbaarheid en continuïteit. De cyberweerbaarheid van de vitale sectoren verschillen in volwassenheidsniveau. In opdracht van de raad heeft Gartner onderzoek gedaan naar de aard en omvang van de IACS-problematiek. De belangrijkste aanbevelingen uit het onderzoek zijn dat de beheerders van IACS[14] behoefte hebben aan een meer ketengerichte samenwerking binnen de vitale sectoren, betere informatie-uitwisseling en op bepaalde terreinen ondersteuning nodig hebben bij de inkoop van IACS. TNO onderschrijft deze uitkomsten in het onderzoek naar succesfactoren voor digitaal veilige IACS[15].

De volgende drie maatregelen zorgen in onderlinge samenhang voor meer inzicht, overzicht en robuustheid van de IACS en verhogen daarmee de cyberweerbaarheid van ons land:

1. **Vitale sectoren beschikken zonder uitzondering over een eigen sectoraal IACS-controleraamwerk. Waar nodig wordt het toezicht proportioneel versterkt.**
2. **De kennis over IACS wordt gebundeld en het delen van (geclassificeerde) IACS-dreigingsinformatie wordt beter gefaciliteerd.**
3. **Beheerders van IACS worden bij het inkoopproces beter ondersteund.**

Ad 1. Vitale sectoren beschikken zonder uitzondering over een eigen sectoraal IACS-controleraamwerk. Waar nodig wordt het toezicht proportioneel versterkt.

Het grote belang van de continuïteit van vitale aanbieders in combinatie met de toename van de digitale dreigingen vraagt om structurele aandacht voor de cyberweerbaarheid. In de beleidsreactie op het CSBN 2019 geeft het kabinet aan dat het veiligheidsniveau van vitale sectoren op orde moet zijn. Ook beheerders van IACS moeten dus doorlopend op de hoogte zijn van de stand van zaken van de cyberweerbaarheid van hun organisatie. Beheerders van IACS hebben aangegeven dat er behoefte is aan een helder en gedragen kader van te nemen cyberweerbaarheidsmaatregelen[16]. Het raamwerk moet beschrijven wat van de organisaties verwacht mag worden om hun IACS cyberweerbaar te houden. Gezien de aard en complexiteit van de problematiek is samenwerking bij het opstellen van het raamwerk tussen (sectorale) toezichthouders, de beheerders en leveranciers van IACS, noodzakelijk en de sleutel tot succes.

[14] Beheerders van IACS zijn alle organisaties die verantwoordelijk zijn voor het beheer van IACS in vitale processen. Dit kunnen zowel vitale aanbieders zijn als bedrijven aan wie delen van vitale processen zijn uitbesteed.
[15] Adviesrapport 'Succesfactoren voor digitaal veilige Operationele Technologie (2019), TNO
[16] Dit is een van de conclusies uit het voorbereidend onderzoek dat in 2019 is uitgevoerd door Gartner in opdracht van de CSR.

Normalisering, certificering en standaardisering in de sectoren en in de markt moeten centraal staan in de raamwerken. Inmiddels wordt het belang hiervan ook in Europees verband gezien en opgepakt. De Cyber Security Act[17] zal hierin een belangrijke rol gaan vervullen. De toezichthouder(s) kunnen betrokken worden in het proces waarbij de markt, beleid en uitvoeringsinstanties deze kaders ontwikkelen. Het gezamenlijk opstellen van een sectorspecifiek IACS-controleraamwerk zorgt voor meer uniformiteit en draagvlak en houdt rekening met de specifieke manier van werken binnen de sector. De raad adviseert om bij het opstellen van sectorale IACS-controleraamwerken aansluiting te zoeken bij lopende Europese initiatieven.

Het raamwerk kan ook de minder 'volwassen' beheerders van IACS helpen bij het beter inrichten van de (digitale) beveiliging van hun systemen. Een aantal vitale sectoren in Nederland, waaronder nucleair en watervoorziening hebben zelfstandig al een eigen sectoraal controleraamwerk ontwikkeld. Op basis van die kennis en ervaring kan een aanpak worden ontwikkeld waarbij alle vitale sectoren toewerken naar een eigen IACS-controleraamwerk. Laten we vooral samen gebruikmaken van wat er al is.

De raad baseert het advies mede op de aanpak in het Verenigd Koninkrijk en Duitsland waar sectorale controleraamwerken voor vitale sectoren al succesvol worden toegepast. Op basis van die ervaringen verdient het aanbeveling om de sectorale IACS-controleraamwerken in de toekomst te laten beoordelen door een onafhankelijke derde partij.

De raad adviseert de bevoegde autoriteiten in samenwerking met de sectorale toezichthouders en de beheerders van IACS, te zorgen voor de invoering van de sectorale IACS-controleraamwerken in alle vitale sectoren.

Versterken toezicht cyberweerbaarheid

De raad is voorstander van een actieve invulling van toezicht binnen de wettelijke kaders (Wbni). Hierbij is het van belang dat voor iedereen duidelijk is hoe dit toezicht is geregeld en welke consequenties er zijn verbonden aan het schenden van regels. De toezichthouders kunnen de IACS-controleraamwerken als uitgangspunt nemen voor het toezicht en daarop reflecteren zodat dit in een continue verbetercyclus terecht komt en de verantwoordelijkheid daar blijft waar het thuishoort, namelijk bij de bedrijven en instellingen zelf. Op basis van ieder sectoraal IACS-controleraamwerk kan, waar nodig, het toezicht proportioneel worden versterkt.

De raad acht het noodzakelijk dat alle vitale sectoren binnen nu en maximaal twee jaar over een sectoraal IACS-controleraamwerk beschikken en hierover rapporteren aan de aangewezen toezichthouders en dat zij daarop kunnen toetsen.

Ad 2. De kennis over IACS wordt gebundeld en het delen van (geclassificeerde) IACS-dreigingsinformatie wordt beter gefaciliteerd.

Het feit dat kennis- en informatiedeling een steeds terugkerend probleem is als het gaat om de cyberweerbaarheid van onze samenleving, baart de raad zorgen. In 2017 heeft de raad uitgebreid aandacht gevraagd voor dit onderwerp en geadviseerd dat er een landelijk dekkend stelsel van informatieknooppunten moet worden gevormd dat ervoor moet zorgen dat informatie over

[17] The EU Cybersecurity Act: https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act

cybersecurity voor alle bedrijven en organisaties in Nederland op eenvoudige wijze toegankelijk is.[18] Dit jaar constateerden de NCTV[19] en de WRR[20] dat de huidige informatievoorziening nog steeds niet op het juiste niveau is. De huidige informatie-uitwisseling wordt gekenmerkt door een zekere mate van vrijheid omdat het verstrekken van relevante informatie niet altijd verplicht is of binnen de vigerende wet- en regelgeving niet mogelijk is. Partijen zijn vaak huiverig om informatie te delen als dit niet door de wet verplicht wordt gesteld. Het uitwisselen van specifieke informatie is een gevoelige zaak vanwege concurrentie, wettelijke beperkingen, nationale veiligheid en de dubbelrol van de overheid, die verkregen informatie ook kan gebruiken voor controles. De gebrekkige informatie-uitwisseling geldt in zelfs een grotere mate voor informatie-uitwisseling over IACS.

Bundeling van de schaars aanwezige IACS-kennis

Kennisontwikkeling over IACS is noodzakelijk om te kunnen garanderen dat de vitale aanbieders voldoende cyberweerbaar zijn en daarmee de continuïteit en integriteit kan worden geborgd. Specialisten op het gebied van Informatietechnologie (IT) en Operationele Technologie (OT) kunnen het zich niet veroorloven om in verschillende werelden te opereren. De krachten van deze tot nu toe veelal gescheiden werelden moeten worden gebundeld.

Alle betrokken stakeholders, waaronder het Nationaal Cyber Security Centrum (NCSC), de (sectorale) toezichthouders, en de beheerders van IACS binnen de vitale sectoren moeten daarom over voldoende kennis beschikken om met elkaar, en met andere landen, de dialoog aan te gaan. Diverse andere landen beschikken bij de toezichthouders en bij specialistische afdelingen van het NCSC gericht op IACS over medewerkers die elk door middel van sectorspecifieke opleidingen kennis hebben van vitale sectoren. De raad vindt dat dit voorbeeld in ons land moet worden gevolgd. De sectorale toezichthouders, waaronder het Agentschap Telecom en het NCSC moeten over voldoende deskundigen beschikken om binnen de (wettelijke) taken en verantwoordelijkheden bij te dragen aan de cyberweerbaarheid van IACS in de vitale sectoren. In de praktijk blijkt dat de kennis over IACS schaars is, daarom dient de aanwezige kennis volop worden benut. Publieke en private organisaties kunnen elkaar daarin versterken. Onder coördinatie van het NCSC dient er daarom een formeel, publiek-privaat netwerk van deskundigen te worden opgericht. Ook de leveranciers van IACS dienen, waar mogelijk, onderdeel uit te maken van dit netwerk. Deskundigen moeten elkaar ook buiten hun sector gemakkelijk weten te vinden. Het verdient daarom aanbeveling om de Information Sharing & Analysis Centers (ISAC's) langs deze cross-sectorale lijn verder te optimaliseren en kennisdeling omtrent IACS verder te stimuleren.

Inrichten van 'trusted channels' tussen overheid en vitale infrastructuur

Naast kennisdeling is ook het delen van dreigingsinformatie over IACS van cruciaal belang. Het delen van deze dreigingsinformatie is extra gevoelig, omdat er statelijke actoren bij betrokken kunnen zijn en de uitval van IACS kan leiden tot maatschappelijke ontwrichting en aanzienlijke aansprakelijkheden. Een van de obstakels bij informatiedeling is het feit dat hoog geclassificeerde dreigingsinformatie alleen onder strenge voorwaarden kan worden gedeeld. Het delen van dergelijke informatie kan alleen plaatsvinden als er onderling vertrouwen is tussen de beheerders en leveranciers van IACS en ook de overheidsinstanties als het NCSC en de inlichtingendiensten die informatie delen. De raad pleit ervoor om, naast de reguliere wijze van informatie-uitwisseling binnen het landelijk dekkend stelsel van informatieknooppunten, 'trusted channels' te realiseren voor het delen van geclassificeerde

[18] CSR Advies 2017, nr. 2 'Naar een landelijk dekkend stelsel van informatieknooppunten, advies inzake informatie-uitwisseling met betrekking tot cybersecurity en cybercrime'
[19] Cybersecuritybeeld Nederland (CSBN) 2019, Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), 2019
[20] Wetenschappelijke Raad voor het Regeringsbeleid (2019) *Voorbereiden op digitale ontwrichting*, WRR-Rapport 101, Den Haag

(dreigings)informatie door alle overheidsinstanties (NCTV, AIVD/MIVD, NCSC en toezichthouders) met individuele beheerders binnen vitale sectoren. Een instrument om het doel te bereiken is het aanstellen van een Security Liaison Officer (SLO). De SLO is vertrouwenspersoon binnen een organisatie met IACS in een vitaal proces en is in het bezit van een veiligheidsscreening[21], zoals beschreven in de wet veiligheidsonderzoeken.

Structureel beleggen van cyberoefeningen

Het bundelen van schaarse kennis en het verbeteren van de informatievoorziening zijn randvoorwaarden voor het vergroten van de cyberweerbaarheid bij beheerders van IACS. Daarnaast levert het structureel uitvoeren van gezamenlijke cyberoefeningen, ook over de landsgrenzen heen, een belangrijke bijdrage aan het robuust maken van de cyberweerbaarheid. Er zullen voor IACS meer sectorspecifieke oefeningen moeten worden ontwikkeld en uitgevoerd waarbij ook aandacht is voor cross-sectorale en internationale afhankelijkheden; oefening baart kunst en dat geldt ook voor cyberweerbaarheid.

Ad 3. Beheerders van IACS worden bij het inkoopproces beter ondersteund.

De aanschaf van IACS in de vitale sector maakt slechts een klein (financieel) deel uit van een infrastructuurproject. Dat resulteert er vaak in dat een partij die in dat fysieke component is gespecialiseerd een onderaannemer heeft voor de IACS. Het zekerstellen van continuïteit en integriteit vraagt van zowel vraag- als aanbodkant een benadering waarbij IACS wordt gezien als kritiek onderdeel waarin cyberweerbaarheid contractueel moet worden geborgd. Organisaties hebben daarin volgens de raad behoefte aan ondersteuning op een aantal gebieden: het ontwikkelen van standaard contractclausules, het delen van informatie over kwetsbaarheden in IACS en het onder voorwaarden kunnen uitsluiten van specifieke leveranciers. Dit blijkt uit het onderzoek van Gartner. Beheerders geven aan behoefte te hebben aan ondersteuning vanuit de overheid bij het maken van de juiste cybersecurityafspraken met leveranciers gedurende het inkoopproces en het gebruik van de systemen. Cybersecurityvoorwaarden moeten standaard in de contractvoorwaarden worden opgenomen, bijvoorbeeld over de security van ontwerpprincipes, de mate van het updaten van producten door leveranciers en ook voorwaarden over de betrouwbaarheid van de leverancier zelf. Certificering zou gezien het internationale karakter van de meeste leveranciers bij voorkeur op Europees niveau moeten plaatsvinden. Dit sluit aan bij de ambitie van de Nederlandse Cybersecurity Agenda (NCSA)[22] en de Roadmap Digitaal Veilige Hard- en Software[23] waarin de Nederlandse overheid actief wil bijdragen aan standaarden en certificering die Europees (Mondiaal) breed worden geaccepteerd en de cyberweerbaarheid bevorderen. Ook de onlangs in werking getreden EU Cybersecurity Act[24] draagt hieraan bij.

Uitsluiting van specifieke leveranciers

In het advies inzake 5G[25] heeft de AIVD de risico's voor innesteling in de Nederlandse vitale infrastructuur voor mogelijke sabotagedoeleinden bevestigd. Op basis van objectieve criteria biedt het advies van de AIVD-beheerders van IACS de mogelijkheid om specifieke leveranciers binnen

[21] Deze functionaliteit bestaat reeds in verschillende EU landen en is ook in de European Program for Critical Infrastructure Protection (EPCIP) richtlijn beschreven.
[22] Nederlandse Cybersecurity Agenda: Nederland digitaal veilig, Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), namens Rijksoverheid, 2018
[23] Roadmap Digitaal Veilige Hard- en Software, Ministerie van Economische Zaken en Klimaat en Ministerie van Justitie en Veiligheid, 2018
[24] The EU Cybersecurity Act: https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act
[25] Advies Nationale Veiligheid en Veiling 5G, Algemene Inlichtingen- en Veiligheidsdienst, 2019

telecommunicatie uit te sluiten van inkoop. Uit de eerder afgekondigde voorzorgsmaatregel van het kabinet over Kaspersky antivirussoftware waarbij bedrijven in de vitale infrastructuur werden gewezen op de overwegingen van het kabinet om geen gebruik meer te maken van deze software, blijkt het noodzakelijk om met objectieve criteria[26] te komen om het wettelijk mogelijk te maken om leveranciers uit te sluiten bij aanbestedingen. De raad adviseert daarom vergelijkbare risicoanalyses te maken binnen de vitale processen om ook deze beheerders van IACS vanuit de overheid de juridische handvatten te geven om bepaalde leveranciers uit te kunnen sluiten van deelname bij aanbestedingen van deelprocessen binnen specifieke sectoren.

Inrichten steunpunt IACS

De raad is van mening dat de bovengenoemde ondersteuning transparant en makkelijk toegankelijk moet zijn voor beheerders van IACS. De raad adviseert aan het NCSC om, in samenwerking met de overige toezichthouders en andere relevante partijen een (virtueel) steunpunt IACS in te richten. Het steunpunt heeft onder andere tot doel de beheerders van IACS te ondersteunen bij hun inkoopproces met relevante kennis op het terrein van cybersecurity en het verzamelen en delen van meldingen van kwetsbaarheden van leveranciers en beheerders. In Duitsland zijn afspraken tussen overheid en IACS-leveranciers vastgelegd in een Charter-of-Trust. Ook dit zou het steunpunt tot taak moeten hebben. Het steunpunt dient ook juridische obstakels te identificeren bij het delen van informatie over IACS. Alle relevante cybersecurity-informatie moet worden gedeeld om het handelingsperspectief te bieden aan (nog niet-geïnformeerde) beheerders van IACS. Op deze wijze kunnen leveranciers van IACS zich van elkaar onderscheiden en neemt het vertrouwen in deze systemen toe.

[26] De volgende criteria zijn gehanteerd in het Besluit Veiligheid en Integriteit Telecommunicatie:
a. een staat, entiteit of persoon is waarvan bekend is of waarvoor gronden zijn te vermoeden dat deze de intentie heeft een in Nederland aangeboden elektronisch communicatienetwerk of -dienst te misbruiken of uit te laten vallen, of.
b. nauwe banden heeft met of onder invloed staat van een staat, entiteit of persoon als bedoeld onder a, of een entiteit of persoon is ten aanzien van wie er gronden zijn om dergelijke banden of invloed te vermoeden.

GERICHTE ADVIEZEN

De adviezen zijn gericht op de overheid en via de overheid op het bedrijfsleven. Alleen als er beter wordt samengewerkt tussen de publieke en private sector kan de cyberweerbaarheid van IACS in de vitale processen worden verhoogd en kan de Nederlandse samenleving vertrouwen op de veiligheid en continuïteit van de vitale infrastructuur. De raad adviseert daarom dat:

De ministers en staatssecretarissen wiens aanbieders van vitale diensten onder de Wbni vallen:

1. Ervoor zorgdragen dat elke vitale sector binnen twee jaar over een sectoraal IACS-controleraamwerk beschikt en daarover aan de toezichthouders rapporteert.
2. De mogelijkheden onderzoeken om de sectorale controleraamwerken te laten toetsen door een onafhankelijke derde partij.

De minister van Justitie en Veiligheid en de staatssecretaris van Economische Zaken en Klimaat, gezamenlijk:

3. Binnen één jaar een (virtueel) steunpunt IACS realiseren waar leveranciers en beheerders van IACS binnen vitale sectoren IACS-specifieke kwetsbaarheden kunnen melden en advies kunnen krijgen over cyberweerbaarheid bij de aanschaf (en vervanging) van deze systemen.

De minister van Justitie en Veiligheid:

4. Ervoor zorgdraagt dat binnen het Nationaal Cyber Security Centrum (NCSC) binnen twee jaar voldoende specialistische sectorspecifieke deskundigheid wordt ontwikkeld over IACS.
5. Binnen twee jaar een formeel publiek-privaat netwerk van IACS-deskundigen realiseert en stimuleert dat Information Sharing & Analysis Centers (ISAC's) op gelijk volwassenheidsniveau komen en langs cross-sectorale lijn worden doorontwikkeld.
6. Elke twee jaar binnen de vitale infrastructuur minimaal één IACS-georiënteerde oefening laat plaatsvinden gericht op specifiek één vitaal proces. Minstens iedere vier jaar moeten ook cross-sectorale en internationale afhankelijkheden in deze oefening worden meegenomen.

De minister van Justitie en Veiligheid en de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties, gezamenlijk:

7. Binnen één jaar in samenwerking met de vitale sectoren trusted channels realiseren.

Alle bevoegde autoriteiten:

8. Op basis van de sectorale controleraamwerken, waar nodig, proportioneel het toezicht versterken.
9. Binnen twee jaar beschikken over toezichthouders met voldoende specialistische sectorspecifieke deskundigheid over IACS.

’s-Gravenhage,

Namens de Cyber Security Raad,

Hans de Jong
Covoorzitter CSR

Pieter-Jaap Aalbersberg
Covoorzitter CSR