Een rapport voor het

Ministerie van Justitie en Veiligheid

Onderzoek Cybersecurity voor Industrial Automation en Control Systems

21 augustus 2019
Engagement: 330051524

Gartner®

Inhoud

1 Managementsamenvatting

Tot op het moment van het schrijven van dit rapport zijn er bij de organisaties in de vitale sectoren (energie-, gas-, water-, distributie- en waterkeringen etc.) binnen Nederland en West-Europa geen grote IACS (Industrial Automation Control Systems) problemen geweest als gevolg van een cyber aanval. Buiten de vitale sectoren en buiten West-Europa zijn er wel diverse voorbeelden bekend van uitval van IACS-systemen en de daaraan gekoppelde productiemiddelen.

Een cyber aanval op IACS-systemen kan leiden tot incidenten met grote impact. Daarom is het noodzakelijk dat de overheid toeziet op de (IACS) veiligheid binnen de vitale sectoren. De overheid heeft behalve een controlerende taak, ook een informatie verschaffende taak, ook als het gaat over het risico van aanvallen door statelijke actoren.

Voor de selectie van de sectoren die deel uitmaken van de vitale infrastructuur in scope van dit onderzoek is in overleg met de opdrachtgever (Cyber Security Raad) gebruik gemaakt van de indeling die de NCTV heeft opgesteld[1]. Aangezien de focus van het voorliggend onderzoek is gericht op IACS-systemen zijn de sectoren waarbij IACS-systemen een bovengemiddeld belang heeft ook meegenomen.

Uit het voorliggend onderzoek blijkt dat de vitale sectoren de mogelijke IACS (legacy) gerelateerde problemen in kaart hebben gebracht en maatregelen hebben genomen om eventuele risico's zoveel als mogelijk te mitigeren. Dit betekent niet dat er niets meer hoeft te gebeuren: Nog niet alle organisaties binnen de vitale sectoren zijn klaar met het uitvoeren van geplande verbeterinitiatieven. Binnen de organisaties in de vitale sectoren zijn de strategische lijnen uitgezet en geven CISO's (of equivalent daarvan) aan dat er voldoende budget beschikbaar wordt gesteld om risico's te mitigeren. Uit het onderzoek blijkt ook dat het (internationaal) oefenen en voorbereiden op aanvallen belangrijk blijft.

Ondanks dat er nog geen IACS-incidenten zijn geweest met grote impact, betekent dit niet dat er geen knelpunten zijn of dat nieuwe maatregelen niet nuttig of nodig zijn. De belangrijkste knelpunten en verbetermogelijkheden zoals deze naar voren zijn gekomen in het voorliggend onderzoek betreffen:

- **Het verbeteren van de samenwerking binnen elk van de sectoren:** Dit kan door het gezamenlijk (evt. met of zonder de toezichthouder) opstellen van een sector-specifiek IACS beveiligingsraamwerk, het stimuleren en faciliteren van ISAC's (Information Sharing and Analysis Centres) en het gezamenlijk oefenen van sector-specifieke IACS aanvalscenario's, zowel nationaal alsook internationaal.
- **Het verbeteren van informatie-uitwisseling:** Als een (beperkt) aantal beveiligingsmedewerker(s) binnen de bedrijven in de vitale sectoren over voldoende security clearance beschikt, is het eenvoudiger (voor bv. de AIVD) om vertrouwelijke informatie over dreigingen te delen.
- **Het toepassen van standaardcontractclausules:** Niet alle huidige IACS contracten (binnen de vitale sectoren) bevatten voldoende mogelijkheden om de leverancier (en de onderaannemers) te verplichten om langere tijd te zorgen voor veilige IACS-systemen.
- **Het mogelijk maken van uitzonderingen bij aanbestedingen:** Het is nu niet mogelijk om enkel en alleen op basis van een advies minister van Justitie en Veiligheid een partij uit te sluiten voor een aanbesteding. Onderzoek of dit kan worden opgelost door een uitzonderingsbepaling te maken voor de vitale sectoren.

[1] https://www.nctv.nl/organisatie/nationale_veiligheid/vitale_infrastructuur/index.aspx

Uit literatuurstudie en op basis van gehouden interviews blijkt niet dat er grote beleidsaanpassingen nodig zijn om de vitale sectoren veilig te houden. Wel blijft aandacht nodig voor het op tijd uitvoeren van de geplande operationele maatregelen voor de verbetering van de IACS-systemen. Verder kan door de invoering van een aantal verbetermogelijkheden (zie hierboven en H8) de digitale weerbaarheid van de vitale sectoren nog verder verbeterd worden.

2 Scope en afbakening

2.1 Aanleiding en doelstelling

Tijdens de CSR vergadering van 14 december jl. is het CSR Werkprogramma 2018 - 2019 vastgesteld. In dit werkprogramma is een vijftal onderwerpen opgenomen waarvoor de raad verschillende producten en adviezen ontwikkelt. Een van deze onderwerpen is Industrial Automation & Control Systems (hierna: IACS).

De CSR heeft daarom onderzoek laten uitvoeren naar de aard en omvang van de IACS cybersecurity problematiek in de vitale infrastructuur van Nederland en inzicht verkrijgen in de ontwikkelingen binnen de EU, NAVO en bij gelijksoortige organen. Daarnaast wil de raad met dit onderzoek inzicht krijgen in mogelijke maatregelen en oplossingen. Hierbij gaat het minder om maatregelen en oplossingen op operationeel niveau, maar vooral om strategische oplossingen. De uitkomsten van dit onderzoek kunnen door de CSR gebruikt worden bij het verstrekken van een advies aan de regering en private partijen.

In het kader van de bescherming van de vitale infrastructuur speelt industriële automatisering een essentiële rol. Doordat steeds meer gebruik wordt gemaakt van generieke ICT-middelen worden ook de standaard ICT-problemen in de industriële automatisering geïntroduceerd. De combinatie van verouderde systemen (legacy) en kwetsbaarheden in IACS maken van de vitale infrastructuur een potentieel doelwit voor cybercrime en -aanvallen[1].

In het voorliggend onderzoeksrapport ligt de nadruk op het inzichtelijk krijgen van de heersende problematiek van IACS in de vitale infrastructuur (d.w.z. infrastructuur in eigendom van en beheerd door bedrijven in de vitale sectoren zoals gedefinieerd door de NCSC[2]) van Nederland als het gaat om cybersecurity. Het bieden van strategische maatregelen en oplossingen om de huidige problematiek te mitigeren staat hierbij centraal.

2.2 Definitie IACS in het kader van dit onderzoek

Met IACS zijn in dit onderzoek die systemen (bestaande uit hard- en software) bedoeld die als meet- en regelsystemen die voor de aansturing van industriële processen of gebouwbeheersystemen worden gebruikt. De IACS-systemen kunnen op afstand fysieke apparaten bedienen en/of controleren d.m.v. van het monitoren van de toestand van deze apparaten en de toestand en werking van het fysieke apparaat kunnen veranderen. Ook de bescherming van het netwerk en de apparatuur die gebruikt wordt bij het aanpassen van de configuratie van de IACS-software is meegenomen in dit onderzoek.

2.3 Onderzoeksvragen

De CSR heeft Gartner gevraagd een analyse uit te voeren naar de huidige problematiek van IACS in de vitale infrastructuur van Nederland als het gaat om cybersecurity. De hoofdvraag is:

Wat is de aard en omvang van de problematiek rondom Industrial Automation & Control Systems in de vitale infrastructuur van Nederland en wat is de internationale dimensie hiervan?

[1] https://www.ncsc.nl/documenten/publicaties/2019/juni/12/cybersecuritybeeld-nederland-2019

[2] Zie https://www.nctv.nl/organisatie/nationale_veiligheid/vitale_infrastructuur/index.aspx

Bovenstaande hoofdvraag is verder uitgewerkt door de CSR in onderstaande zeven onderzoeksvragen[1]:

1. Wat is de aard en omvang van de huidige problematiek van IACS in de vitale infrastructuur van Nederland als het gaat om cybersecurity?
   - Waardoor wordt de problematiek veroorzaakt?
   - Hoelang blijft de problematiek spelen zowel nu als in de toekomst?

Om bovenstaande vragen te beantwoorden heeft Gartner literatuuronderzoek uitgevoerd om zo de meest voorkomende alsook de problemen met de grootste impact te identificeren. Met het expert panel is in een workshop[2] besproken of dit inderdaad de belangrijkste problemen zijn. Vervolgens heeft Gartner met diverse experts[3] uit verschillende organisaties binnen de vitale sectoren interviews uitgevoerd waarin aan de experts is gevraagd of zij verwachten dat de problematiek blijft bestaan. De voorgestelde maatregelen zijn dan ook mede gebaseerd op de input vanuit deze interviews.

2. Welke gevolgen kan de problematiek hebben op de continuïteit van de bedrijfsvoering binnen de vitale infrastructuur en de nationale veiligheid?

Met het expert panel is tevens besproken wat de belangrijkste reeds bestaande c.q. toegepaste mitigerende maatregelen zijn. Het antwoord hierop is gebruikt bij het bepalen van het advies of het zinvol of nodig is om bepaalde maatregelen verplicht te stellen. In die gevallen waaruit blijkt dat de kans van optreden beperkt is en de impact zeer groot, heeft dit gevolgen voor het gewenste kosten- en inspanningsniveau. Verder heeft het benodigde kosten- en inspanningsniveau in relatie tot het risico ook gevolgen voor het advies. Soms worden niet preventieve, maar reactieve maatregelen voorgesteld omdat preventieve maatregelen een te hoge inspanning en of kosten met zich meebrengen (Het incident wordt niet voorkomen, maar de impact kan worden beperkt).

3. Ondervinden omringende landen nadelen van de problematiek in Nederland? En ondervindt Nederland nadeel van de problematiek in omringende landen?

Voor de interviews zijn ook experts van buitenlandse organisaties uitgenodigd[6]. Ook de maatregelen die buitenlandse overheden hebben geformuleerd zijn in het voorliggend rapport besproken. Deze maatregelen zijn bijvoorbeeld verwerkt in de voorgestelde maatregelen

4. Welke ontwikkelingen zijn er op het terrein van IACS binnen de EU, NAVO en soortgelijke organen? En wat betekent dat voor de Nederlandse aanpak?

Organisaties zoals ANSI/ISA (verantwoordelijk o.a. voor de ANSI/ISA/IEC 62443-standaard “Cyber security for Industrial Automation and Control Systems”) en ook NAVO-vertegenwoordigers zijn uitgenodigd en gesproken. Dit om ervoor te zorgen dat niet alleen de input van de ons omringende landen maar ook bredere internationale ontwikkelingen zijn meegenomen in het voorliggend adviesrapport.

5. Welke strategische maatregelen en oplossingen zijn er beschikbaar? Welke rollen en taken hebben stakeholders bij mogelijke strategische maatregelen en oplossingen?

---

[1] De onderzoeksvragen zijn door de CSR geformuleerd in Offerteaanvraag onderzoek naar Industrial Automation & Control Systems (IACS) tbv Ministerie van Justitie en Veiligheid (MJenV), Cyber Security Raad (CSR), kenmerk 10100026552

[2] Bijeenkomst CSR klankbordgroep ICS op 21 november 2018

[3] Voor lijst geïnterviewden, zie bijlage

De IEC 62443 norm geeft een framework voor veilig werken met IACS. . Het platform Industrieel Platform Cybersecurity – NEN maakt hier al gebruik van. Het industrie-breed implementeren van internationale standaarden is niet eenvoudig. De (internationale) ervaringen van de geïnterviewde bedrijven[1] zijn tevens meegenomen in voorstellen in het voorliggend adviesrapport.

6. Zijn er maatregelen of *best practices* in omringende landen die als voorbeeld kunnen dienen? En welke geïmplementeerde oplossingen hadden onvoldoende effect?

Naast hierboven genoemde Nederlandse organisaties met ervaring in de toepassing van internationale standaarden en raamwerken is onderzoek gedaan naar wat buitenlandse organisaties doen. Op deze manier is een goed beeld ontstaan van hetgeen buurlanden van Nederland doen op het gebied van bescherming van de vitale infrastructuur. Verder heeft op EU-niveau TIBER-EU hier al ervaring mee opgedaan (in eerste instantie is dit raamwerk gericht op de financiële sector, maar de *lessons learned* zijn zeker bruikbaar voor de meer industriële vitale sectoren).

7. Wat zijn de (beschikbaarheids)risico's op het primaire proces en wat is het kostenniveau van de te nemen maatregelen?

Extra maatregelen kosten extra geld. Ook is het aanpassen van oude systemen niet zonder risico en zorgt mogelijk voor extra downtime of benodigd aanvullende personele inzet. Om de impact van deze maatregelen te bepalen zijn de maatregelen ook besproken worden met de leveranciers (d.w.z. bedrijven die zelf IACS software en apparaten waar IACS software op draait maken en leveren). Ook het verwachte kostenverschil bij de keuze voor preventieve versus reactieve maatregelen is in de analyse meegenomen, zodat dit kan dienen als input voor beleidskeuzes.

2.4 Leeswijzer

Het voorliggend rapport is als volgt ingedeeld:

Hoofdstuk 1.	Managementsamenvatting
Hoofdstuk 2.	Scope en afbakening In dit hoofdstuk is de scope afgebakend in termen van vitale infrastructuur in Nederland en inzet van IACS per vitale industrie. Welke sectoren vallen wel in scope en welke niet? Wat is IACS die binnen de scope van deze studie valt? Uitgangspunt hierbij is de lijst met sectoren zoals beschreven door het NCTV, Categorie A. (Zie bijlage voor referentie)
Hoofdstuk 3.	Aard en omvang van de heersende problematiek Wat is de mate van inzet van IACS per sector? Welke issues spelen er en zijn deze verschillend per sector of zijn deze gemeenschappelijk tussen de verschillende sectoren?
Hoofdstuk 4.	Mogelijke impact verstoring IACS binnen vitale infrastructuur en nationale veiligheid Wat is de impact van verstoringen in de vitale infrastructuur op de maatschappij, economie en nationale veiligheid? Kan een verstoring in een sector zich verspreiden naar een (of meerdere) andere sectoren? Tevens zijn in dit hoofdstuk internationale voorbeelden van impact van verstoringen van vitale infrastructuur beschreven.

[1] Zie bijlage A

Hoofdstuk 5.	Invloed van en op het buitenland van problemen met IACS in de vitale infrastructuur In dit hoofdstuk is ingegaan op de mogelijke effecten van verstoringen in het buitenland op de vitale infrastructuur in Nederland en andersom. Wat merkt Nederland van verstoringen in de vitale infrastructuur van onze buurlanden (waaronder ook het Verenigd Koninkrijk en Noorwegen i.v.m. de verwevenheid van de vitale infrastructuur)? Wat merken de buurlanden bij een verstoring van de Nederlandse vitale infrastructuur?
Hoofdstuk 6.	Internationale ontwikkelingen op het gebied van IACS In dit hoofdstuk is ingegaan op internationale ontwikkelingen op het gebied van IACS. Wat zijn de bestaande IACS-toepassingen? Welke van de oplossingen zijn al volwassen, welke nog niet en naar welke oplossingen wordt nog onderzoek verricht? Welke ontwikkelingen binnen EU en NAVO zijn relevant (o.a. TIBER-EU)?
Hoofdstuk 7.	Best practices uit andere landen/sectoren Hoe is de bovenstaande IACS-problematiek in andere landen en of sectoren in andere landen aangepakt? Wat zijn de hiermee opgedane ervaringen? Wat zijn de *best practices* uit verschillende sectoren?
Hoofdstuk 8.	Beschikbare strategische maatregelen en oplossingen Gegeven de geconstateerde problematiek, wat zijn mogelijke strategische maatregelen en oplossingen? Tot welke scenario's kunnen de oplossingen gecombineerd worden? Welke mitigerende maatregelen zijn mogelijk om de impact of kans van optreden van geconstateerde risico's te beperken? Welke maatregelen zijn kostenefficiënt?

2.5 Vitale infrastructuur in scope van dit onderzoek

Voor de selectie van de sectoren die deel uitmaken van de vitale infrastructuur is in overleg met de opdrachtgever (Cyber Security Raad) gebruik gemaakt van de indeling die de NCTV heeft opgesteld[1]. Aangezien de focus van het voorliggend onderzoek is gericht op IACS-systemen zijn de sectoren waarbij IACS-systemen een bovengemiddeld belang heeft ook meegenomen (zie Tabel 1). Zie bijlage A voor een overzicht van de uitgenodigde organisaties.

Er is hierbij onderscheid gemaakt tussen een categorie A en categorie B om recht te doen aan de diversiteit van impact die een incident kan hebben op de vitale infrastructuur.

Categorie A:

- Economische gevolgen: > Ca. 50 miljard euro schade of ca. 5,0 % daling reëel inkomen;
- Fysieke gevolgen: Meer dan 10.000 personen dood, ernstig gewond of chronisch ziek;
- Sociaal maatschappelijke gevolgen: Meer dan 1 miljoen personen ondervinden emotionele problemen of ernstig maatschappelijke overlevingsproblemen, en
- Cascade gevolgen: Uitval heeft als gevolg dat minimaal twee andere sectoren uitvallen.

Categorie B:

[1] https://www.nctv.nl/organisatie/nationale_veiligheid/vitale_infrastructuur/index.aspx

- Economische gevolgen: > Ca. 5 miljard euro schade of ca. 1,0 % daling reëel inkomen;
- Fysieke gevolgen: Meer dan 1.000 personen dood, ernstig gewond of chronisch ziek, en
- Sociaal maatschappelijke gevolgen: Meer dan 100.000 personen ondervinden emotionele problemen of ernstig maatschappelijke overlevingsproblemen.

De volgende sectoren hebben alleen activiteiten van categorie B en hebben een beperkte inzet van IACS. Deze worden daarom niet meegenomen in de analyse:

- IT/Telecom;
- Transport;
- Financieel;
- Openbare Orde Veiligheid;
- Digitale overheids-processen, en
- Inzet Defensie.

Sector	Vitale processen	Categorie	In scope van IACS analyse
Energie	Landelijk transport en distributie elektriciteit	A	Ja
	Regionale distributie en productie elektriciteit	B	Ja. Energiecentrales maken op grote schaal gebruik van IACS
	Gasproductie, landelijk transport en distributie gas	A	Ja
	Regionale distributie gas	B	Nee
	Olievoorziening	A	Ja
Drinkwater	Drinkwatervoorziening	A	Ja
Water	Keren en beheren waterkwantiteit	A	Ja
Chemie	Grootschalige productie/verwerking en/of opslag (petro)chemische stoffen	B	Ja. De sector maakt veel gebruik van IACS
Nucleair	Opslag, productie en verwerking nucleair materiaal	A	Ja. De sector maakt veel gebruik van IACS. De IACS issues bij het opwekken van elektriciteit zijn niet wezenlijk anders dan bij andere type energiecentrales.

Tabel 1 Overzicht van vitale sectoren in scope van dit onderzoek

De vitale infrastructuur in het buitenland heeft ook invloed op Nederland. Andersom heeft de vitale infrastructuur in Nederland ook invloed op het buitenland. Aangezien Nederland (Ministerie van Financiën) eigenaar is van de grensoverschrijdende netwerken voor gas en energie (TenneT en Gasunie) is het voor deze sectoren niet nodig geweest om buitenlandse experts uit te nodigen maar zijn de afhankelijkheden, invloeden en de internationale samenwerking met de Nederlandse experts besproken.

De impact van waterkering (bv. sluizen) vanuit Duitsland is heel beperkt: Omdat Nederland stroomafwaarts ligt, heeft een mogelijk verkeerd gesloten sluis vooral (en eerst) impact op Duitsland. Daarom zijn er geen interviews gepland met Duitse waterwering organisaties.

2.6 Aanpak

De geformuleerde onderzoeksvragen zijn beantwoord op basis van een literatuurstudie, een workshop met experts, interviews en twee schriftelijke feedbackrondes. De workshop met de klankbordgroep IACS was er vooral op gericht om de strategische en beleidsimplicaties van de (operationele) problematiek te verhelderen. De volgende stap in de analyse bestond eruit om te onderzoeken of en welke structurelere (beleids)aanpassingen nodig zijn. Tot slot zijn de conclusies van het rapport aan de CSR-begeleidingsgroep gepresenteerd.

In de volgende paragrafen is elk van de stappen van het onderzoek verder toegelicht.

2.6.1 Literatuurstudie

Op basis van literatuur, openbare bronnen en Gartner Research heeft Gartner een eerste antwoord op de vragen geformuleerd. De uitkomsten van dit literatuuronderzoek zijn tevens gebruikt bij de voorbereiding van de expert workshop.

2.6.2 Expert workshop

Ter voorbereiding van de expert workshop is de door CSR ten behoeve van dit onderzoek opgestelde lijst met vragen door Gartner aangevuld op basis van een eerste risico- en impactanalyse waarbij gekeken is naar aspecten op o.a. het gebied van definitie, meerwaarde/ investeringen, politiek (o.a. transparantie), kosten, beperkingen, security, wetgeving, (internationale) marktontwikkelingen, techniek, ontsluiting en implementatie.

De expert workshop met de klankbordgroep IACS[1] was primair gericht op het verkrijgen van inzicht in de huidige IACS-problematiek binnen de uitgenodigde organisaties. Hierbij zijn ook beleidsvraagstukken aan de orde gekomen. Verder is deze workshop gebruikt voor het aanscherpen van de vragen en mogelijke toekomstscenario's en het delen van de uitkomsten uit de literatuurstudie. De discussies en resultaten van de workshop zijn meegenomen in de aanbevelingen in het voorliggende rapport.

2.6.3 Interviews

Gartner heeft in overleg met de CSR klankbordgroep de CSR experts geïnterviewd. In elk van de interviews zijn de voor de expert relevante onderzoeksvragen aan bod gekomen. De lijst van geïnterviewde personen en organisaties is bijgesloten in bijlage A.

[1] Bijeenkomst CSR klankbordgroep ICS op 21 november 2018.

2.6.4 Analyse en aanbevelingen

De focus van de expert workshop en de interviews lag in eerste instantie bij het ophalen en valideren van risico's en mogelijke (operationele) oplossingen. Aanvullend heeft Gartner een analyse uitgevoerd van welke strategische en beleidsmatige maatregelen mogelijk zijn.

De geïnventariseerde problematiek vormt de basis voor de (beleids)adviezen in dit rapport en kunnen worden gebruikt ter bespreking met de relevante organisatie (zoals beleidsmedewerkers van het Ministerie van Justitie en Veiligheid). De adviezen in dit rapport kunnen door de CSR gebruikt worden bij het verstrekken van advies aan de regering en private partijen.

3 Mate van gebruik van IACS binnen vitale sectoren

Omdat de focus van dit rapport op strategische maatregelen en oplossingen voor de verbetering van de beveiliging van IACS ligt, wordt in dit hoofdstuk alleen een aantal *voorbeelden* genoemd met betrekking tot de inzet van IACS. Zonder inzicht in het gebruik van IACS is het moeilijk om de invloed van deze systemen te beoordelen bij incidenten.

Op basis van de interviews kan gesteld worden dat de vitale sectoren de mogelijke IACS (legacy) gerelateerde kwetsbaarheden in kaart gebracht hebben en maatregelen genomen hebben om de risico's zoveel te mitigeren. Dit betekent niet dat er niets meer hoeft te gebeuren.Nog niet alle organisaties zijn klaar met het uitvoeren van de geplande verbeterinitiatieven[1]. Maar binnen de organisaties in de vitale sectoren zijn de strategische lijnen uitgezet en geven de CISO's (of equivalent daarvan) aan dat er voldoende budget beschikbaar wordt gesteld om de risico's te mitigeren. Verder blijft het (internationaal) oefenen en voorbereiden op aanvallen belangrijk.

Ook is het proces van risicoclassificatie van de objecten (bv. IACS van een sluis of transformatorhuisje) niet statisch, omdat door nieuwe dreigingen of andere veranderingen kan blijken dat bepaalde objecten belangrijker worden, waardoor extra maatregelen nodig zijn. Dit zorgt vervolgens voor de noodzaak om extra middelen en mensen vrij te maken om benodigde maatregelen in lijn te brengen met de geïdentificeerde risico's. Er is dus voortdurend aandacht nodig om de IACS-systemen van de vitale sectoren op orde te houden of brengen, omdat zoals in dit hoofdstuk beschreven is, de impact van een incident groot kan zijn.

Onderstaand overzicht van inzet van IACS-systemen per sector geeft een aantal (niet uitputtende) voorbeelden waaruit blijkt dat IACS-systemen heel belangrijk zijn voor de respectievelijke sector en dat de impact bij verkeerde aansturing (veroorzaakt door een fout of bewust handelen) kan zorgen voor grote verstoringen, maatschappelijke onrust en impact op bv. gezondheid, veiligheid of milieu.

3.1 Voorbeeld 1: IACS inzet binnen de energiesector

Binnen de energiesector wordt veel gebruik gemaakt van IACS-systemen. Verder is het de verwachting dat dit nog verder gaat toenemen door het gebruik van "smart grids", waarbij auto's geladen (of zelfs ontladen) worden binnen de parameters die de gebruiker ingegeven heeft. Ook het gebruik van wind- en zonenergie zorgt voor een wisselend aanbod van elektriciteit. Via IACS-systemen wordt ervoor gezorgd dat de spanning op het electriciteitsnet constant blijft. Verder worden deze IACS-systemen ook ingezet om bij onderhoud delen spanningsloos te maken, zodat onderhoud veilig kan gebeuren. Ook bij incidenten (bv. een probleem met een transformator) kan de stroom anders gerouteerd worden, zodat de eindgebruikers hier geen last van hebben.

De impact bij verkeerde aansturing (veroorzaakt door een fout of bewust handelen) kan ervoor zorgen dat (delen van) het elektriciteitsnetwerk zonder spanning komt te staan (black-out). Verder is het mogelijk dat de spanning hoger of lager wordt dan 230V, waardoor aangesloten apparaten ook fysiek beschadigd kunnen raken (voltage surge/spike). Een

[1] Rapport Algemene rekenkamer: 'digitale dijkverzwaring: cybersecurity en vitale waterwerken' https://www.rekenkamer.nl/publicaties/rapporten/2019/03/28/digitale-dijkverzwaring-cybersecurity-en-vitale-waterwerken

ander probleem dat kan ontstaan betreft frequentie-fluctuatie, waardoor o.a. klokken en timers niet meer goed functioneren. Als het meet gedeelte niet goed functioneert kan dit ervoor zorgen dat er niet of niet tijdig ingegrepen kan worden bij afwijkingen.

Bij normaal gebruik zorgen de IACS-systemen ervoor dat dit niet kan optreden, maar als deze niet bruikbaar zijn, of juist bewust verkeerde stuurinformatie krijgt, dan zijn dit mogelijke gevolgen.

3.2 Voorbeeld 2: IACS inzet bij de gasvoorziening

Voor de gasvoorziening worden IACS-systemen ingezet voor de aansturing van pompen, het afsluiten van onderdelen voor onderhoud en het controleren van de hoeveelheid getransporteerd gas. Gasunie heeft een uitgebreid netwerk (o.m. de gasrotonde, waarbij verschillende aanbiedende partijen aardgas kunnen leveren aan diverse afnemers. Ook worden IACS-systemen ingezet bij de besturing van de grote ondergrondse opslagfaciliteiten zodat de gasstromen van minuut tot minuut gebalanceerd kunnen worden.

De impact bij verkeerde aansturing (veroorzaakt door een fout of bewust handelen) kan ervoor zorgen dat de gasdruk te hoog of te laag wordt, waardoor apparaten niet meer functioneren. Ook kan dit ervoor zorgen dat de gasvoorziening uitvalt, waardoor huishoudens of industrie zonder gas komen te zitten.

3.3 Voorbeeld 3: IACS inzet bij de drinkwatervoorziening

Ook bij de drinkwatervoorziening worden IACS-systemen ingezet voor routering, distributie en het zorgen voor beschikbaarheid van het drinkwater. Ook hier kan ervoor gezorgd worden dat een pompstation of pijp bij onderhoud of incidenten afgeschakeld kan worden. Behalve inzet van IACS-systemen voor de beschikbaarheid van water, worden deze ook (beperkt, maar in toenemende mate) ingezet voor het meten van de waterkwaliteit. De pH en de troebelheid van het water wordt automatisch gemeten. De verwachting is dat in de toekomst er meer geautomatiseerde waterkwaliteitsmetingen worden uitgevoerd. Nu worden deze metingen vooral uitgevoerd door laboratoria.[1]

De impact bij verkeerde aansturing (veroorzaakt door een fout of bewust handelen) kan ervoor zorgen dat er (korte tijd) onvoldoende gezuiverd water naar de eindgebruikers gepompt wordt. Verder kan verkeerde aansturing ervoor zorgen dat de druk te laag is, zodat gebruikers geen of onvoldoende water ontvangen.

3.4 Voorbeeld 4: IACS inzet bij de waterkeringen

Ook voor de besturing van waterkeringen zijn IACS-systemen heel belangrijk. Vrijwel alle waterkeringen, bedienbare bruggen en sluizen kunnen op afstand bediend worden. Ook de besturing van tunnels (van verlichting tot pompen) is grotendeels geautomatiseerd. Ook hoog- en laagwatermetingen nodig voor het (geautomatiseerd) sluiten van bijvoorbeeld stormvloedkeringen maken gebruik van IACS-systemen.

De impact bij verkeerde aansturing (veroorzaakt door een fout of bewust handelen) kan ervoor zorgen dat bruggen opengaan zonder noodzaak (evt. zonder dat de slagbomen aangestuurd worden), of dat pompen op het verkeerde moment aan- of uitgeschakeld worden, zodat polders te veel of te weinig water krijgen. Ook kunnen er onveilige situaties

[1] http://www.vewin.nl/Waterspiegelartikelen/09-Sensoring%20drinkwaterkwaliteit%20stap%20verder%20door%20project%20SAWA%2004-2013.pdf

ontstaan in tunnels als de verlichting of de pompen niet functioneren, zodat de tunnel afgesloten moet worden.

3.5 Voorbeeld 5: IACS inzet bij kerncentrale

De besturing van de kerncentrale is zo ingericht dat menselijk ingrijpen tot een minimum beperkt blijft. Dit betekend dat IACS-systemen heel belangrijk zijn voor de centrale. Behalve voor de besturing en monitoring van het proces wordt IACS ook ingezet voor het meten van vitale plekken in het primaire circuit door gebruik te maken van thermokoppels. Deze zorgen voor een real time registratie van temperatuursveranderingen, zodat uitspraken gedaan kunnen worden over o.a. metaalmoeheid (leidend tot aantasting van structurele integriteit) van het primaire circuit[1]. Doordat de apparatuur blootgesteld wordt aan straling, is het nodig om de omgevingscondities exact te meten. Met deze informatie kan een restlevensduur berekend worden. Componenten die niet meer voldoen, kunnen zo op tijd vervangen worden. Ook wordt er gebruik gemaakt van geluidsdetectie, om afwijkingen (slijtage) snel te vinden door het gemeten geluid te vergelijken met de referentiewaarden.

De impact van verkeerde aansturing kan significant zijn. Wel is het zo dat alle belangrijke systemen redundant zijn uitgevoerd, zodat uitval van een onderdeel (incl. de besturing) niet direct tot een probleem leidt. Verder is een volledig losstaand systeem aanwezig dat zelfstandig kan besluiten tot een afschakeling van het proces (ReaktorSchnell-Abschaltung, RESA) bij bepaalde parameters. De regelstaven vallen dan in de reactor, de neutronen die de kernsplijting op gang houden, worden geabsorbeerd en de kettingreactie stopt onmiddellijk.

3.6 Voorbeeld 6: IACS inzet bij Defensie Pijplijn Organisatie

De NAVO heeft in Europa een uitgebreid netwerk liggen ten behoeve van transport en opslag van kerosine. De kerosine wordt door dit netwerk vanuit verschillende raffinaderijen en opslagterminals (o.a. in Rotterdam) afgeleverd aan civiele en militaire luchthavens en een viertal depots. Transport gebeurt middels een uitgebreid stelsel van ondergrondse pijpleidingen.

Alhoewel de civiele luchtvaart veruit de grootste gebruiker is, wordt dit netwerk om strategische redenen beheerd door de Defensie Pijpleiding Organisatie (DPO), een onderdeel van de NAVO. Het ondergrondse pijpleidingenstelsel van de DPO is verbonden met vergelijkbare stelsels in België, Luxemburg, Duitsland en Frankrijk.

Besturing van dit geheel (pompen, kleppen en andere onderdelen) gebeurd vanuit een centrale kamer middels IACS-systemen die volledig gescheiden zijn van het ICT-netwerk van Defensie. Elk van de pompstations beschikt daarnaast over een lokaal bedieningspaneel. Dit is een bewuste ontwerpkeuze van de NAVO en DPO, omdat er op deze manier geen mogelijkheid bestaat om vanuit het ICT-domein het IACS-besturing over te nemen.

Installatie van nieuwe softwareversies en -patches voor IACS-systemen binnen dit netwerk kent een aantal veiligheidsmaatregelen: Ten eerste moet de te installeren software door een zgn. ‘wasstraat’ waar het gecontroleerd wordt op afwezigheid van bekende problemen. Ten tweede moet, vanwege het gescheiden karakter van het netwerk, de installatie altijd lokaal gebeuren, onder toezicht van een DPO-medewerker. Tot slot moeten alle leveranciers een ABDO-status hebben en hun medewerkers een MIVD-screening voordat zij voor DPO werkzaamheden mogen verrichten.

[1] Een blik in de Bol (2017), uitgave van EPZ.

3.7 Conclusie

Dankzij IACS-systemen is het mogelijk om met beperkte menskracht complexe infrastructuur te besturen en te monitoren. Binnen de vitale sectoren wordt veel gebruik gemaakt van IACS-systemen. Dit wordt gebruikt om mechanische, elektrische of hydraulische apparatuur aan te sturen, zoals kleppen, relais, pompen, bruggen, sluisdeuren, slagbomen etc.

Behalve voor de normale operatie wordt het IACS-systeem vaak ook gebruikt om medewerkers te attenderen op bijzondere situaties, waarvoor zij handmatige acties moeten uitvoeren. Zo kan het zijn dat een klep vastzit en dat ondanks het stuursignaal voor het openen van de klep, het monitordeel constateert dat de klep dicht blijft. Ook bij situaties die de veiligheid van het systeem of de omgeving betreffen, kan het IACS-systeem een waarschuwing geven, dat zou kunnen leiden tot het (al dan niet handmatig) uitschakelen van (onderdelen van) de installatie.

IACS-systemen zijn dus heel belangrijk voor de vitale infrastructuur. Daarom is het goed om te onderzoeken wat er kan gebeuren als er een incident optreedt. Dit wordt beschreven in het volgende hoofdstuk.

4 Mogelijke impact IACS-incidenten in vitale sectoren

In dit hoofdstuk wordt beschreven wat de mogelijke impact kan zijn van verstoring van IACS-systemen.

Bij het bepalen wat de impact van verstoringen in de vitale infrastructuur op de maatschappij, economie en de nationale veiligheid zou kunnen zijn, is het noodzakelijk om eerst te onderzoeken welke verstoringen er recent al hebben plaatsgevonden. De hier genoemde lijst is niet uitputtend[1], maar toont verschillende typen incidenten. Bij de keuze van de incidenten is ervoor gekozen om alleen voorbeelden te nemen uit de vitale sectoren, waarbij er schade ontstond. Bij het laatste voorbeeld is de schade beperkt gebleven, maar door de grote mogelijk impact (nucleair incident) is deze toch opgenomen.

Vanuit de (internationale) literatuur zijn er twee voorbeelden bekend waarbij statelijke actoren via digitale kanalen (hetzij direct via internet of via een besmette laptop van een medewerker) binnen gedrongen zijn in vitale infrastructuur en daarbij bewust schade hebben veroorzaakt via IACS-systemen.

Daarnaast zijn er diverse[2] voorbeelden bekend waarbij er op systemen was binnengedrongen, maar waarbij de IACS infrastructuur niet het doelwit was. Wel geeft dit aan dat de IACS-systemen kwetsbaar zijn voor ongewenste beïnvloeding via digitale kanalen[3].

Buiten de vitale sectoren zijn er nog recentere voorbeelden van vergelijkbare aanvallen bekend, zoals bij het Deense Maersk, Amerikaanse farmaceut Merck, Russische oliegigant Rosneft, Brits advertentiebedrijf WPP, en het Spaanse voedselbedrijf Mondelez[4].

4.1 Cyberaanval op het elektriciteitsnetwerk van Oekraïne

4.1.1 De aanval is uitgevoerd met relatief eenvoudige middelen

In december 2015 heeft een cyberaanval op een regionaal Oekraïens elektriciteitsdistributiebedrijf geleid tot een verstoring van de dienstverlening aan ongeveer 225.000 klanten.

De storingen waren te wijten aan de onbevoegde toegang van derden tot een van de computers en SCADA-systemen van het bedrijf. Zeven 110 kV en 23 35 kV-onderstations werden gedurende drie uur afgesloten.

---

[1] Andere relevante hacks op vitale infrastructuur, https://thehackernews.com/2017/06/electric-power-grid-malware.html

[2] CyberX Labs, *Global IACS & IIoT Risk Report* from: https://cdn2.hubspot.net/hubfs/2479124/Report%20-%20Global%20IACS%20&%20IIoT%20Risk%20Report.pdf, Hoofdstuk 4.3

[3] Behalve de hier genoemde voorbeelden zijn er ook andere bekend (zoals Triton, GreyEnergy en CrashOverRide), maar omdat niet bekend is of deze gebruikt zijn bij aanvallen op vitale infrastructuur, zijn deze hier niet geanalyseerd.

[4] https://www.ad.nl/rotterdam/wereldwijde-hack-legt-bedrijven-en-rotterdamse-terminal-plat~a60dd307/

De aanval werd o.a. uitgevoerd door Microsoft Office-documenten te sturen naar medewerkers met daarin een macro die zorgde voor de installatie van de malware. Deze malware zorgde er vervolgens voor dat de aanvallers de computers van medewerkers konden overnemen (remote admin). Verder werden via deze malware ook gebruikersnamen en wachtwoorden gestolen, waarmee het mogelijk was om ook via VPN-toegang te krijgen tot het netwerk.

4.1.2 Met betere monitoring en security awareness zou aanval waarschijnlijk niet hebben kunnen plaatsvinden

Voor deze aanval was het niet nodig om gebruik te maken van speciale *zero day exploits* of andere (on)bekende veiligheidsproblemen.

De aanval zou waarschijnlijk niet succesvol zijn geweest als de operators op de hoogte waren geweest van de risico's van office macro's. Verder zou de implementatie van onder andere Security Monitor technologie bij hebben kunnen dragen aan een vroegtijdige detectie van de aanval. Ook het gebruiken van fysieke scheiding tussen werkplekken die verbonden zijn met internet en computers die de installatie aansturen zou de aanval mogelijk hebben voorkomen of ieder geval veel moeilijker hebben gemaakt.

4.2 Cyberaanval op Iraanse uraniumverrijking (Stuxnet)

4.2.1 De malware is zeer complex en specifiek gemaakt om het Uranium-verrijkingsproces te vertragen

In juni 2010 is de Stuxnet malware ontdekt. De ontdekte malware had twee opvallende eigenschappen: Het maakte gebruik van een toen nog onbekend softwarelek in Windows en het was specifiek gericht op specifieke (merk en type) industriële controlesystemen die in fabrieken en installaties worden gebruikt. Het doel van de malware was het verstoren en vertragen van het Uranium verrijkingsproces.

Stuxnet is complexe malware: Het bevatte meerdere *0-day exploits* (nog onbekende softwarelekken). Het vinden en exploiteren van deze nieuwe lekken is duur (deze moeten worden gekocht of gezocht hetgeen veel tijd vergt). Verder had Stuxnet verschillende lagen van versleuteling, hetgeen het lastig maakt om de software te analyseren. Als laatste werd er ook gebruik gemaakt van twee software-certificaten (digitale handtekeningen) van derde partijen om legitiem te lijken. Deze certificaten zijn vermoedelijk op frauduleuze wijze verkregen.

Ook bevat Stuxnet een aantal specifieke functionaliteiten dat de malware geschikt maakt voor dit soort aanvallen:

- Verspreiding (en aanpassingen van de functionaliteit) van Stuxnet is mogelijk via USB-sticks en LAN-verbindingen. Er is dus geen directe internetverbinding benodigd voor de aanval
- Het maakt gebruik van technieken om detectie te voorkomen, zoals het aanpassen van de meetwaarden waardoor de medewerkers niet konden zien dat er iets niet correct was

4.2.2 Ook met gepatchte systemen, monitoring en geen externe verbindingen blijft deze aanval mogelijk

Nu Stuxnet geanalyseerd is, is het relatief eenvoudig om deze te voorkomen door gebruik te maken van de patches die Microsoft heeft uitgebracht. De *0-day exploits* die gebruikt zijn (en die met veel moeite of geld verkregen zijn) zijn nu niet meer bruikbaar. Ook het detecteren van dit virus kan worden gedaan door de meeste antivirus-pakketten. De belangrijkere vraag

is hoe het mogelijk is om te beschermen tegen vergelijkbare geavanceerde aanvallen die nog niet geanalyseerd zijn.

Goede monitoring, een gelaagd netwerk, beperkte gebruikersrechten etc., maken de kans op een geslaagde aanval kleiner, maar hadden Stuxnet niet kunnen voorkomen. Heel strikte maatregelen rondom fysieke toegang, gebruik van mobiele apparaten etc. kunnen de kans verder verkleinen, maar zijn niet altijd mogelijk vanuit een kostenperspectief.

4.3 Insideraanval op het rioolsysteem van Maroochyshire in Australië

4.3.1 Aanval wordt uitgevoerd door ontevreden ex-medewerker met detailkennis van de systemen

De aanval in 2000 op het rioolsysteem van Maroochyshire is niet uitgevoerd via internet, maar wel door iemand die niet (meer) bij het bedrijf werkte en daarom via externe kanalen (in dit geval via een versleutelde radioverbinding) zorgde voor een verstoring waarbij ongeveer 1 miljoen liter ongezuiverd rioolwater in de rivier, lokale parken en woonwijken terecht is gekomen.

Deze aanval is uitgevoerd door een ontslagen medewerker, die detailkennis had van de SCADA-systemen van het rioolsysteem. Door bewust verkeerde signalen via zijn twee-weg radio te versturen (vanuit zijn auto, waardoor hij dus wel in de buurt van de rioolzuiveringsinstallatie moest zijn) kon hij het systeem langere tijd manipuleren.

De aanval laat zien dat door detailkennis van de omgeving het mogelijk is om met beperkte middelen grote schade te veroorzaken.

4.3.2 Door gebruik te maken van versleutelde communicatie en SCADA-autorisatie had de aanval voorkomen kunnen worden

Voor deze aanval was het niet nodig om gebruik te maken van geavanceerde hack technieken, omdat de verbindingen niet versleuteld waren en er onvoldoende gebruik gemaakt werd van autorisatiemechanismen. Ook het goed monitoren van de communicatie zou sneller duidelijkheid hebben gegeven over de bron van de verkeerde instructies, waardoor de impact beperkt zou zijn gebleven.

4.4 Slammer worm incident bij de Ohio Davis-Besse kerncentrale

4.4.1 Worm krijgt toegang tot veiligheidssystemen kerncentrale via laptop aannemer

Behalve bewuste verstoring van vitale infrastructuur kan de verstoring ook een onverwacht bijverschijnsel zijn. Dit was het geval in 2003 toen de Slammer worm niet allen veel generieke Windows servers onbruikbaar maakte, maar dat deze ook ervoor zorgde dat een deel van de veiligheidssystemen vijf uur lang niet meer gebruikt konden worden. De centrale was op dat moment niet operationeel, dus er was geen directe impact op de elektriciteitsvoorziening of op de omgeving.

De worm nestelde zich eerst in de computer van een David-Besse-aannemer. Deze medewerker koppelde zijn laptop aan het bedrijfsnetwerk en passeerde zo de bedrijfsfirewall. Eenmaal in het bedrijfsnetwerk vond de worm zijn weg naar de verwerkingscontrolesystemen van de reactor omdat het verwerkingscontrolesysteem was

gekoppeld aan het bedrijfsnetwerk. De worm zorgde ervoor dat de medewerkers geen toegang meer hadden tot het veiligheidsparameterschermsysteem dat 'cruciale veiligheidsindicatoren' leverde, zoals koelsystemen, externe stralingssensoren etc.

4.4.2 Impact blijft beperkt door analoge fallback mechanismen

De impact van de worm is beperkt gebleven, omdat er behalve de geautomatiseerde veiligheidssystemen ook een fallback mogelijk aanwezig was, waarbij de medewerkers via analoge systemen de veiligheid alsnog kunnen bewaken. Uiteraard is dit systeem veel arbeidsintensiever en vergt het vooral tijdelijk noodzakelijke inzet van (meer) medewerkers. Wel toont het aan dat een buitenstaander toegang kon krijgen tot de netwerken waar de IACS-systemen op draaien. Het is niet aangetoond of het ook mogelijk was om de veiligheidssystemen te manipuleren (d.w.z. aangeven dat het veilig is, terwijl er bewust een veiligheidssysteem uitgeschakeld is). Door de grote hoeveelheid netwerkverkeer zorgde de worm ervoor dat de noodzakelijke data niet beschikbaar was voor de veiligheidssystemen.

4.5 Maatregelen genomen na incidenten

4.5.1 Maatregelen naar aanleiding van incident met elektriciteitsnetwerk van Oekraïne

Het is niet altijd mogelijk om een incident te koppelen aan nieuw beleid of striktere uitvoering van bestaand beleid. Wel kan geconstateerd worden dat een incident niet altijd LEIDT tot afdoende beveiliging. Het elektriciteitsnetwerk in Oekraïne is ook in december 2016 aangevallen, en ook die aanval heeft ertoe geleid dat een grote groep mensen voor een langere tijd geen elektriciteit had.

Wel heeft deze aanval ertoe geleid dat in de VS de FERC (Federal Energy Regulatory Commission) naar aanleiding van het incident in Oekraïne acties heeft ondernomen om het veiligheidsniveau beter te garanderen. De FERC heeft de NERC (North American Electric Reliability Corporation) opgedragen om te komen met een vernieuwde betrouwbaarheidsstandaard. In deze standaard staat een aantal minimumcriteria waaraan voldaan moet worden:

- Garanderen van software integriteit;
- Veilige toegang op afstand door de leverancier;
- Noodzakelijke risicomanagement procedures, en
- Inkoopmaatregelen om toekomstige veiligheid te garanderen.

4.5.2 Maatregelen naar aanleiding van incident met rioolwater in Australië

Het *Australian Department of Communication, Information Technology and the Arts* (DCITA) heeft acties ondernomen om bedrijven die werken met IACS-systemen beter te informeren over de risico’s. Dit is gedaan door het organiseren van workshops voor het management van die organisaties die IACS-systemen inzetten en hun operators. Verder heeft de Australische overheid recent een initiatief geïnitieerd met de naam *Trusted Information Sharing Network for Critical Infrastructure Protection*, hetgeen onder andere ook gericht is op IACS-systemen. Hierin worden genoemd als strategische aandachtsgebieden:

- Betere communicatie tussen overheid en bedrijfsleven en tussen bedrijven over incidenten;
- Zorgen voor een goed begrip van de strategische issues door samenwerking met internationale partners, universiteiten, onderzoeksinstellingen en andere overheidsorganen, en
- Zorgdragen voor goed risicomanagement.

4.5.3 Maatregelen naar aanleiding van Stuxnet en Slammer aanval

Omdat zowel Stuxnet alsook Slammer niet specifiek gericht zijn op vitale infrastructuur in de onderzochte landen, is de link naar nieuw beleid wat meer indirect. Het is zeker niet uit te sluiten dat deze incidenten ook bijgedragen hebben aan de aanleiding voor EU Richtlijn 2016/1148 (die in Nederland is ingevoerd middels de Wet beveiliging netwerk- en informatiesystemen).

Alle geïnterviewde beheerders van vitale infrastructuur geven aan de aanvallen die relevant zijn voor hun sector uitgebreid geanalyseerd te hebben. Op basis hiervan zijn waar nodig maatregelen aangescherpt of toegevoegd. Dit geeft ook aan dat het heel belangrijk is dat de incidenten gemeld worden.[1] Wel wordt aangegeven dat de communicatie met de inlichtingendiensten niet altijd eenvoudig is, omdat sommige aanvallen alleen gedeeld mogen worden met mensen die het juiste screeningsniveau hebben. Niet alle organisaties hebben mensen in dienst met een daartoe benodigd screeningsniveau.

4.6 Conclusie

De incidenten bij Maroochyshire en de Ohio Davis-Besse kerncentrale laten zien dat geavanceerde software zoals Stuxnet niet noodzakelijk is voor het uitvoeren van een geslaagde aanval. Uit de IACS-CERT-monitor blijkt dat veel IACS-systemen toegankelijk zijn via het Internet. Ook zoekmachines zoals shodan.io[2] maken het eenvoudiger om IACS-systemen te vinden die aangesloten zijn op het Internet. Ook al gaat dit vooral over niet vitale infrastructuur, het maakt wel extra duidelijk dat het belangrijk is om de basisbeveiliging op orde te hebben.

Ook de menselijke factor blijft belangrijk: Als een ex-medewerk(st)er nog steeds toegang heeft tot de IACS-systemen, kan hij of zij mogelijk op afstand alsnog incidenten veroorzaken. Verder laten de voorbeelden (met uitzondering van Stuxnet) ook zien dat met relatief goedkope en eenvoudige oplossingen (gebruik maken van 2-factor autorisatie, goede monitoring, gebruik maken van antivirus-software) vrijwel alle (tot nu toe gesignaleerde) incidenten of voorkomen konden worden, danwel de impact beperkt kon worden. En als er een succesvolle aanval is geweest, zorgt het snel communiceren over deze aanval dat er maatregelen genomen kunnen worden zodat de impact bij andere organisaties beperkt blijft.

Maatregelen om zeer geavanceerde aanvallen zoals Stuxnet af te slaan, zijn wel duur. Daarvoor blijft een goede risico-inventarisatie nodig: In sommige gevallen kan het nodig zijn om een kortdurende verstoring te accepteren. Het inrichten van incident response is dan wel extra belangrijk.

[1] Het melden van incidenten is verplicht. Dit staat beschreven in de Wet beveiliging netwerk- en informatiesystemen (Wbni).

[2] https://www.us-cert.gov/sites/default/files/Annual_Reports/FY2016_Industrial_Control_Systems_Assessment_Summary_Report_S508C.pdf

5 Invloed van en op het buitenland n.a.v. problemen met IACS in vitale infrastructuur

In dit hoofdstuk wordt ingegaan op mogelijke effecten van verstoringen in het buitenland op de vitale infrastructuur in Nederland en andersom. Wat merkt Nederland van verstoringen in de vitale infrastructuur van onze buurlanden (waarbij ook het Verenigd Koninkrijk en Noorwegen worden meegenomen i.v.m. de verwevenheid van de vitale infrastructuur)? Wat merken de buurlanden bij een verstoring in de Nederlandse vitale infrastructuur?

5.1 Maatregelen elektriciteitsdistributie (Europees)

Zoals al in de vorige hoofdstuk aangegeven, zijn er geen voorbeelden van incidenten als gevolg van een cyberaanval op IACS-systemen in West Europa bekend. Daarom is het onderstaande voorbeeld gebruikt als illustratie van de mogelijke gevolgen van een grensoverschrijdende cyberaanval, ook al was de oorzaak van het beschreven incident niet binnen IACS-systemen.

Europese eigenaren van elektriciteitsdistributienetwerken werken samen in het *European Network of Transmission System Operators for Electricity* (ENTSO-E). Dit samenwerkingsverband heeft o.a. vaste afspraken gemaakt over de wijze van communicatie betreffende maatregelen die grensoverschrijdend effect (kunnen) hebben op elektriciteitsdistributie. Deze afspraken worden regelmatig in de praktijk toegepast – bijvoorbeeld bij bijzondere transporten. De kern van de afspraak is dat de eigenaar van het distributienetwerk zelf 15 minuten heeft om maatregelen te treffen. Blijken deze niet afdoende, dan neemt de betreffende eigenaar contact op met de eigenaren van de aangrenzende netwerken. Deze afspraken gelden ongeacht wat de oorzaak van de maatregelen is – een bijzonder transport of een maatregel die een eigenaar van een distributienetwerk neemt als gevolg van een cyberaanval op zijn IACS-systemen.

Een voorbeeld van het belang van tijdige communicatie over aanpassingen in gevraagde distributiecapaciteit is een transport dat in 2006 plaatsvond over de rivier Eems in Duitsland. Het transport was van tevoren gemeld en bij de eigenaar van het distributienetwerk ter plaatse, E.ON, was ook alles ingepland. Voor het bijzondere transport was een onderbreking in een van de belangrijke noord-zuid hoogspanningsverbindingen gepland. Dit betekende dat E.ON van tevoren plannen had ingediend hoe het elektrisch vermogen (onder normale omstandigheden bijna 10.000 MW) dat in Noord-Europa werd opgewekt tijdelijk zou worden verminderd en via andere routes naar de gebruikers in West- en Zuid-Europa zou worden omgeleid. In het schema werd dus van tevoren een vermindering van gevraagd vermogen voorzien gedurende een bepaalde tijd. Bij de uitvoering werden echter veel wijzigingen op korte termijn doorgevoerd, die niet in de actualisatie van het schema waren doorgevoerd waardoor de andere netbeheerders niet tijdig werden geïnformeerd. Hierdoor konden de andere netbeheerders en producenten hun energieproductie- en netcapaciteit niet meer tijdig aanpassen. De gebrekkige onderlinge communicatie had gevolgen in heel Europa, van stroomuitval tot afschakelen van elektriciteitscentrales (teveel productie) en afnemers (teveel vraag) tot aan veranderingen van de netfrequentie van het hoogspanningsnet.

5.2 Maatregelen water

In Nederland zijn de normen voor bescherming tegen hoogwater in de Waterwet vastgelegd. Ook het doorlopende proces van toetsen, verbeteren en beheren is in de wet beschreven, evenals de taken en verantwoordelijkheden van betrokken overheden (Rijk, waterschappen en provincies). De wet schrijft voor dat de beheerder de dijken toetst op veiligheid. De minister van Infrastructuur en Waterstaat stelt voor elke toetsronde opnieuw de randvoorwaarden en de regels voor de toetsing in het Wettelijk Toets Instrumentarium (WTI) vast. Deze kunnen veranderen als de zeespiegel is gestegen, de rivier of de zeebodem

anders is komen te liggen of hogere afvoeren zijn opgetreden. De resultaten van de toetsing worden gerapporteerd aan de minister van Infrastructuur en Waterstaat.[1] Dit betekent dat de minister van Infrastructuur en Waterstaat toetsing van IACS-systemen in de (vitale) waterkeringen en sluizen onderdeel kan uit laten maken van het WTI.

Daar waar nodig werkt RWS direct samen met Duitse autoriteiten m.b.t. het sturen en afstemmen van hoogwaterbescherming, calamiteitenzorg en rampenbestrijding.

Specifiek op het gebied van stormvloedkeringen werkt RWS samen in een nationaal en internationaal netwerk I-STORM waarbinnen onderling kennis wordt gedeeld. Alhoewel veiligheid een van de thema's is waarop binnen het netwerk informatie gedeeld wordt, is pas recent de behoefte ontstaan om ook informatie over cybersecurity binnen dit netwerk te delen[2]. Doordat ook landen buiten de EU en NAVO aan dit netwerk deelnemen is het niet mogelijk om alle vertrouwelijke kennis te delen binnen dit netwerk.

Volgens geïnterviewden is het voor Nederland als deltagebied van belang om in het kader van voorzorgsmaatregelen landoverstijgende oefeningen te houden – mogelijk met TIBER-EU als voorbeeld[3] – met partnerorganisaties uit het hele stroomgebied. Voor de Rijn zou dit dan samen met Duitse, Franse en Zwitserse zusterorganisaties zijn. Voor de Maas en Schelde samen met Vlaamse, Waalse en Franse zusterorganisaties.

5.3 Maatregelen nucleair

De maatregelen in de nucleaire sector vallen in twee type maatregelen uiteen: Maatregelen indien enkel de levering van elektriciteit wegvalt en maatregelen ingeval van een incident dat mogelijk ook invloed heeft op de omgeving en mensen. Maatregelen die enkel de levering van elektriciteit aan het elektriciteitsnet betreffen zijn identiek als die voor elke andere producent en beschreven in paragraaf 5.1.

Bij incidenten van de nucleaire installatie treedt een ander protocol in werking, ongeacht wat de oorzaak is. Het niveau van maatregelen – ook in de omgeving van de installatie - is afhankelijk van de inschaling van het incident op de internationale INES-schaal[4] (*International Nuclear and Radiological Event Scale*). Alle vergunninghouders (wereldwijd) dienen ongewone gebeurtenissen bij hun toezichthouder te melden. In Nederland is de toezichthouder de Autoriteit Nucleaire Veiligheid en Stralingsbescherming (ANVS), in België het Federaal Agentschap voor Nucleaire Controle (FANC) en in Duitsland het betreffende deelstaat en het *Bundesamt für kenrtechnische Entsorgungssicherheit (BfE)*. Onderlinge communicatie en coördinatie ingeval van een incident vindt plaats tussen deze instanties.

Als voorbeeld en in aanvulling op de beschrijvingen in hoofdstuk 4: Het ongeval met de kernreactor in Three-Mile-Island (Harrisburg, Verenigde Staten, 1979) is een gebeurtenis op niveau 5 van de INES-schaal; de ongevallen in Tsjernobyl en Fukushima zijn gebeurtenissen op niveau 7 van de INES-schaal (het hoogste). Een gebeurtenis zoals die vorig jaar gemeld door de kerncentrale in Emsland (Duitsland) heeft op de INES-schaal niveau 0, omdat deze buiten het kerngedeelte plaatsvond en er geen radioactief materiaal (water) kon ontsnappen. Deze gebeurtenis moest wel conform internationaal geldende afspraken gemeld worden aan de toezichthouder.

---

[1] Bron: Eindrapport Veiligheid Nederland in kaart

[2] Bron: A cybersecurity information sharing process for Storm Surge Barriers (Thesis for the completion of the executive master in Cybersecurity), Ing. Jeroen A. M. Gaiser CISSP, december 2018

[3] Zie paragraaf 6.2

[4] Bronnen: https://www.autoriteitnvs.nl/onderwerpen/ines en https://www.iaea.org/topics/emergency-preparedness-and-response-epr/international-nuclear-radiological-event-scale-ines

5.4 Conclusie

Omdat water, gas- en elektriciteitsnetwerken internationaal met elkaar verbonden zijn en de impact van een nucleair incident groot kan zijn (zoals in hoofdstukken 3 en 4 beschreven), is het organiseren van regelmatige internationale oefeningen volgens een vast (sectoraal) raamwerk zeer nuttig. De bestaande internationale samenwerking kan worden uitgebreid met expliciet aandacht voor cyberveiligheid van IACS-systemen en het ontwikkelen van internationale sectorale raamwerken (naar voorbeeld van TIBER-EU). Intersectorale communicatie wordt op Europees niveau getest middels ISIDOOR.

Specifiek voor water (dijken, keringen en sluizen) geeft de Waterwet de Minister van Infrastructuur en Waterstaat de mogelijkheid om de beveiliging van IACS-systemen expliciet in het WTI-kader op te nemen, omdat deze voor elke toetsronde opnieuw wordt vastgesteld. Opgemerkt dient te worden dat het WTI een Nederlands kader is, verankerd in Nederlandse wetgeving.

6 Internationale ontwikkelingen op het gebied van IACS

In dit hoofdstuk wordt ingegaan op internationale ontwikkelingen op het gebied van IACS. Dit betreft landoverstijgende ontwikkelingen waardoor deze abstracter zijn dan de maatregelen beschreven in hoofdstuk 7. De vragen waar dit hoofdstuk op ingaat zijn: Wat zijn de bestaande IACS-toepassingen? Welke van de oplossingen zijn al volwassen, welke nog niet en op welke gebieden wordt nog onderzoek verricht? Welke ontwikkelingen binnen EU en NAVO zijn relevant (o.a. TIBER-EU) voor cybersecurity van IACS-systemen?

6.1 EU Richtlijn 2016/1148

Op 6 juli 2016 werd door de Raad en het Europees Parlement de Richtlijn (EU) 2016/1148 aangenomen (hierna: NIS-richtlijn). In Nederland is de Wet beveiliging netwerk- en informatiesystemen (WBNI) de wet die de regels ter transpositie van richtlijn (EU) 2016/1148 bevat.

Het doel van de NIS-richtlijn bestaat erin een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Europese Unie tot stand te brengen. Dit betekent dat de beveiliging van het internet en de particuliere netwerken en informatiesystemen die de werking van onze samenleving en economie ondersteunen, moet worden verbeterd. Het eerste belangrijke element in dit verband is de paraatheid van de lidstaten, die moet worden gewaarborgd door middel van nationale cyberbeveiligingsstrategieën, zoals omschreven in de richtlijn, de werkzaamheden van de CSIRT's en de bevoegde nationale autoriteiten.

De richtlijn geeft de lidstaten tevens de mogelijkheid om de werkingssfeer van de CSIRT’s uit te breiden naar andere sectoren en diensten waar de richtlijn niet van toepassing is. Dit is vooral bedoeld zodat de CSIRT’s operationele ondersteuning bieden in geval van cyberincidenten in ondernemingen en organisaties waarop de richtlijn niet van toepassing is, maar die ook belangrijk zijn voor de samenleving en de economie.

De NIS-richtlijn schrijft een aantal minimum security requirements voor aan aanbieders van essentiële diensten (waaronder energie, transport en water). Deze minimumeisen gelden daarmee na de transpositie naar nationale wetgeving in heel EU en bieden daarmee, samen met het IEC 62433 standaard een houvast voor evt. sectorale EU-raamwerken (naar voorbeeld van TIBER-EU voor het financiële sector of het C2M2 in de VS).

Tot slot biedt de NIS-richtlijn lidstaten de mogelijkheid om via het programma *Connecting Europe Facility* (CEF) voor digitale diensteninfrastructuur op het gebied van cyberbeveiliging EU-financiering aan te vragen en te ontvangen om de CSIRT’s van de lidstaten bij te staan met het oog op verbeterde vermogens en onderlinge samenwerking in het kader van een samenwerkingsmechanisme voor informatie-uitwisseling. Deze samenwerking is echter op vrijwillige basis.

De praktische vertaling van de NIS-richtlijn in wet- en regelgeving van enkele Europese landen wordt in hoofdstuk 7 besproken. Aangezien de richtlijn nog niet lang in werking is, is de ervaring met het in praktijk toepassen van alle (voorgenomen) beleidsmaatregelen in de genoemde landen op dit moment echter beperkt.

6.2 TIBER-EU

European framework for Threat Intelligence-based Ethical Red Teaming (kort: TIBER-EU) is een Europees raamwerk die Europese en nationale autoriteiten in staat stelt om met financiële instellingen samen te werken aan een programma waarmee de weerbaarheid

tegen cyberaanvallen wordt getest en verbeterd[1]. Volgens meerdere geïnterviewden is het wenselijk om soortgelijke sectorale raamwerken te ontwikkelen om een vaste basis te bieden voor gerichte gemeenschappelijke keten c.q. grensoverschrijdende oefeningen.

TIBER-EU is een gemeenschappelijk raamwerk voor een gecontroleerde, maatwerk, intelligence-led red team test van de kritieke live productiesystemen van de financiële instituties. Een intelligence-led red team bootst de tactieken, technieken en procedures (TTPs) na van echte actoren waar dreiging van uitgaat en die, op basis van een dreigingsanalyse, gezien worden als echte bedreiging voor de financiële instituties. Een intelligence-led red team test behelst het gebruik van een variëteit aan technieken om een aanval op de kritieke functies en de onderliggende systemen (d.w.z. mensen, processen en technologieën) van een financiële instelling te simuleren. Het help de institutie om haar beveiliging, detectie en response capabilities te beoordelen.

TIBER-EU is een voorbeeld van een Europees sectoraal raamwerk die gebruikt kan worden om zowel nationale als internationale cyberoefeningen te houden. Verder stelt dit nationale toezichthouders in staat stelt om gebruik te maken van onderzoeken van andere toezichthouders om zo voldoende zekerheid te krijgen over grensoverschrijdende risico's.

Nu is het TIBER-EU raamwerk nog gericht op de financiële sector, maar omdat ook binnen de vitale sectoren er een noodzaak is voor grensoverschrijdende, sector-specifieke tests, kunnen de structuren en methoden die binnen TIBER-EU zijn ontwikkeld mogelijk ook gebruikt worden binnen de verschillende vitale sectoren.

TIBER-EU kent de volgende kerndoelen:

- Het verhogen van de cyber-weerbaarheid van de financiële instellingen en van de financiële sector in het algemeen;
- Het Standaardiseren en harmoniserenvan de manier waarop financiële instellingen binnen de EU hun intelligence-led red tests uitvoeren, terwijl het ook ruimte overlaat voor elke jurisdictie om het raamwerk aan te passen aan specifieke behoeften;
- Het begeleiden van autoriteiten over hoe zij deze vorm van testen op nationaal of Europees niveau kunnen vaststellen, implementeren en beheren;
- Het ondersteunen van grensoverschrijdende en jurisdictie-overschrijdende intelligence-led red team testing voor multinationale financiële instellingen;
- Het faciliteren van discussies over toezichts-equivalentie daar waar autoriteiten op elkaars beoordeling middels TIBER-EU willen vertrouwen om daarmee ook regeldruk op de financiële instellingen verminderen en de onderlinge erkenning van de testen binnen de EU bevorderen, en
- Het creëren van een protocol voor grensoverschrijdende samenwerking tussen de autoriteiten, delen van resultaten en analyses.

Alhoewel TIBER-EU zich niet op IACS richt, hebben meerdere geïnterviewde organisaties aangegeven dat deze – of soortgelijke - systematiek ook toegepast kan worden op IACS binnen de vitale sectoren, omdat het organisaties helpt om hun cyberweerbaarheid te vergroten. Enkele geïnterviewde organisaties gaven aan ook behoefte te hebben aan hulp aangezien in hun sector het zinvol is om soortgelijke oefeningen in internationaal verband uit te voeren, waarbij betrokkenheid van toezichthouders / overheden (ofwel bilateraal oftewel op Europees niveau) nuttig kan zijn.

6.3 ENISA

Het EU-agentschap voor netwerk en informatiebeveiliging (ENISA) heeft tot doel het opschalen van de Europese vermogen in het verbeteren van response bij cyberaanvallen,

[1] Bron: ECB Tiber-EU Framework

het verbeteren van cyber resilience en het verhogen van vertrouwen in de digitale markt binnen de EU. ENISA is verantwoordelijk voor de ontwikkeling van een EU-cybersecurity certificatieraamwerk voor online diensten en consumentenapparaten. Het certificeringsraamwerk zal (voorlopig) niet verplicht zijn[1].

ENISA heeft sinds december 2018 een permanente status en een nieuw mandaat gekregen. Het meerjarenplan van ENISA voor 2019-2021[2] bevat een aantal prioriteiten die rechtstreeks gerelateerd zijn aan de invoering en praktische uitwerking van de (gevolgen van) de NIS richtlijn, waaronder:

- Het verbeteren van NIS-gerelateerde expertise, inclusief IACS- en SCADA systemen, met focus op aanbieders van vitale diensten;
- Het uitvoeren van een jaarlijkse NIS dreigingsanalyse;
- Het ondersteunen van relevant onderzoek en innovatie door lidstaten binnen de context van de European Cyber Security Organisation (ECSO);
- Het ondersteunen van (verdere) ontwikkeling van EU-beleid, mede gebaseerd op inventarisatie van bestaande initiatieven van individuele lidstaten;
- Het ondersteunen van de implementatie van beleid t.g.v. de NIS-richtlijn door de lidstaten, gericht op het delen van ervaringen en nationale standpunten;
- Het ontwikkelen en organiseren van Cyber Europe 2020 oefening(en).

Eind januari heeft ENISA een online risk-assessment tool voor IoT industrie en Smart Infrastructure operators beschikbaar gemaakt.

De huidige strategie van ENISA richt zich vooral op het bevorderen van samenwerking tussen de lidstaten – zowel de nationale CSIRTs als met sectoren, maar niet bv. het ontwikkelen van een gezamenlijke Europese contracteisen cq. clausules voor het contracteren van IACS-systemen, -producten en of -diensten. Voor zover zulke initiatieven bestaan, zijn ze vooralsnog beperkt tot enkele van de onderzochte landen (zie hoofdstuk 7).

Verder organiseert ENISA eens per twee jaar een oefening, Cyber Europe. Planners van Cyber Europe 2018 ontwikkelden een draaiboek rond luchtvaart, waaronder burgerluchtvaartautoriteiten, verleners van luchtvaartnavigatiediensten (ANSP's), luchthavenbedrijven, luchtvervoerders, met mogelijke gevolgen in andere sectoren. (Ook al is de luchtvaart niet geclassificeerd als een Categorie A vitale sector, de Defensie Pijplijn Organisatie is dat wel). Het scenario bevat door de praktijk geïnspireerde technische incidenten, forensische en malware-analyse, etc.

6.4 Europees energiesector heeft meerdere sectorale organisaties met aandacht voor cybersecurity

Het Europese energiesector kent drie organisaties op het gebied van cybersecurity. Lidmaatschap van deze organisaties kent een wisselende samenstelling – van netbeheerders tot breder lidmaatschap waarbij ook leveranciers en onderzoeksinstellingen zijn aangesloten:

- **European Energy - Information Sharing & Analysis Centre (EE-ISAC)**
  Het European Energy - Information Sharing & Analysis Centre (EE-ISAC) is een initiatief van enkele Europese energiemaatschappijen samen met leveranciers, universiteiten, NCSC, NATO CDC COE, ENISA om informatie over cybersecurity en -

[1] Bron: State of the union 2017, Cybersecurity EU agency and certification framework

[2] ENISA programming document 2019-2021, december 2018

resilience te delen. EE-ISAC neemt regelmatig deel aan sectorale conferenties met cybersecurity als focus.

- **European Network of Transmission System Operators for Electricity (ENTSO-E)**
  Het European Network of Transmission System Operators for Electricity (ENTSO-E) is een Europees netwerk van 43 netbeheerders uit 36 landen. Sinds 2009 heeft het een EU-mandaat ten aanzien van het intern energiemarkt. Cybersecurity is een van de aandachtsgebieden. Volgend op de adoptie van de NIS-richtlijn in alle EU-landen organiseerde ENTSO-E in januari 2019 de eerste cybersecurity conferentie “Energy Intrusion Detection 2019”. Beveiliging van ISAC was de focus van de conferentie.
- **European Network for Cyber Security (ENCS)**
  ENCS is een organisatie waarin Europese netbeheerders, energieproducenten en andere beheerders van kritieke energie-gerelateerde infrastructuur (o.a. Gasunie is lid). De organisatie werkt samen met haar leden aan toegepast onderzoek en ontwikkelt technische veiligheidsnormen en tests en verzorgt ook training. De organisatie heeft een testlab die de leden helpt te onderzoeken of hun beveiligingsmaatregelen correct zijn geïmplementeerd - voor individuele componenten of voor systemen (o.b.v. scenario’s).

6.5 Telecombedrijven geven aandacht aan netwerkbeveiliging

De wereldwijde organisatie van de mobiele telecomaanbieders, de GSMA, heeft concrete richtlijnen voor IoT beveiliging[1]. De GSMA is bezig met het opzetten van een Europese ‘task force’ met als doel het maken van Europese afspraken met beleidsmakers (EU) over netwerkbeveiliging en beoordeling van de netwerken op hun beveiliging. De taskforce richt zich op het beoordelen en waar nodig verbeteren van de bestaande testprocedures voor netwerkapparatuur. De GSMA geeft wel aan behoefte te hebben aan duidelijk beleid t.a.v. de vereiste beveiligingseisen.[2]

6.6 Conclusie

Binnen Europa zijn meerdere ontwikkeling n.a.v. NIS richtlijn gaande, zowel in individuele landen als in verschillende sectoren. Aangezien de richtlijn nog niet lang in werking is, is de ervaring met het in praktijk toepassen van alle (voorgenomen) beleidsmaatregelen in de verschillende landen op dit moment nog beperkt. Zoals reeds in eerdere hoofdstukken aangegeven, hebben diverse Nederlandse organisaties behoefte aan begeleiding cq. beleid o.a. bij het organiseren van landoverstijgende (sectorale) oefeningen en ontwikkeling van raamwerken die zowel nationaal bruikbaar zijn maar ook goed aansluiten op raamwerken van andere Europese landen. Betere samenwerking binnen de EU is dus belangrijk. Binnen Europa is deze rol belegd bij ENISA.

[1] Bron: https://www.gsma.com/iot/iot-security/iot-security-guidelines/

[2] Bron: https://www.gsma.com/newsroom/statement/gsma-calls-on-europe-to-safeguard-network-security/

7 Best practices uit andere landen/sectoren

In dit hoofdstuk worden de ontwikkelingen in een aantal landen besproken. Dit zijn zowel directe buurlanden van Nederland als landen die – vanwege hun geografische ligging of vanwege omvang van bepaalde vitale sectoren (o.a. nucleair) al verder zijn met het ontwikkelen van ook voor Nederland relevante nationale *best practices*. Hierbij wordt ingegaan op de volgende onderzoeksdeelvragen: Hoe is de bovenstaande IACS-problematiek in andere landen en of sectoren in andere landen aangepakt? Wat zijn de ervaringen? Wat zijn de *good practices* uit verschillende sectoren?

7.1 Duitsland

7.1.1 Definitie van vitale infrastructuur is vergelijkbaar en gebaseerd op sector-specifieke limieten

Duitsland heeft de vitale infrastructuur in 2015 geïdentificeerd als gevolg van de toen aangenomen ICT-beveiligingswet (voluit: *Gesetz zür Erhögung der Sicherheit informationstechnischer Systeme (ICT-Sicherheidsgesetz*)). De aanwijzing van de kritieke infrastructuursectoren is in Duitsland middels een AMvB (verordnung) gebeurd – voluit "*Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV*).

De in Duitsland geïdentificeerde vitale infrastructuur is vergelijkbaar met die in Nederland: Energie, water, voedsel(productie), informatie- en communicatietechnologie, verkeer en transport, gezondheidszorg en financieel sector (banken en verzekeraars). Er zijn echter ook verschillen: In tegenstelling tot Nederland rekent Duitsland echter ook voedsel(productie) tot de vitale infrastructuur. Vitale infrastructuur in de zin van de Duitse wet betreft faciliteiten, locaties en apparatuur (of delen daarvan) die:

1. Binnen een van de aangewezen, hierboven genoemde sectoren vallen en
2. '*Van hoog belang zijn voor het functioneren van de maatschappij omdat het falen of aantasting van (hun diensten) zou leiden tot materiele tekorten of gevaar voor openbare veiligheid.*'[1]

De organisaties die als aanbieders van vitale diensten in de zin van de Duitse wet beschouwd worden, zijn net als in Nederland verder aangewezen. In Duitsland zijn hiervoor in de wet specifieke limieten per sector opgenomen (bv. voor elektriciteitsproductie geldt een minimale capaciteit van de centrale en voor voedselproductie minimale hoeveelheid die een fabriek produceert).

De NIS-richtlijn is in Duitsland al in juni 2017 bij wet vastgelegd. Tegelijkertijd is de Duitse telecommunicatiewet aangepast om de wettelijk toegestane mogelijkheden voor het herkennen en blokkeren van cyberaanvallen te verbreden c.q. te verbeteren. De wet geeft meer bevoegdheden aan het *Bundesamt für Sicherheit in der Informationstechnik* (BSI), zowel ten aanzien van de aanbieders van kritieke infrastructuurdiensten als voor samenwerking met de deelstaten. Tegelijkertijd is de BSI-Kritisverordnung aangepast met de eisen aan de eigenaren van de vitale infrastructuur, die uit de NIS-richtlijn voortvloeien.

[1] Bron: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/BSI/BSI_Act_BSIG.pdf?__blob=publicationFile&v=4

De BSI heeft in Duitsland de rol van de centrale landelijke CERT voor vitale infrastructuur en werkt in deze hoedanigheid samen met de CERTs van de bondslanden en andere internationale CERTs.

7.1.2 Rol van de BSI ten aanzien van de kritieke infrastructuur in Duitsland

De rol van BSI ten aanzien van de vitale sectoren is al in de IT-Sicherheidsgesetz uit 2015 gedefinieerd. De Duitse wet die de NIS-richtlijn transponeert definieert daarnaast ook de verantwoordelijkheden van organisaties in de vitale infrastructuur.

Ten aanzien van vitale infrastructuur en ICT(inclusief IACS)-beveiliging vervult BSI de volgende rollen en bevoegdheden:

- Voor de eigenaren van vitale infrastructuur is BSI het centrale meldpunt voor alle aangelegenheden t.a.v. ICT-beveiliging;
- BSI heeft het recht om ICT-producten en systemen die of op de markt verkrijgbaar zijn, of zullen zijn, te onderzoeken. Voor het onderzoek mag het derde partijen inzetten zolang er geen belangenconflict is met de leverancier van het product of de dienst die onderzocht wordt. BSI heeft hiervoor twee speciale afdelingen: Een afdeling is verantwoordelijk voor certificering van hardware gerelateerde producten en een tweede voor software en COTS;
- De BSI heeft een certificeringsprogramma voor ICT-auditors (dit betreft individuele personen). BSI kent een afdeling die verantwoordelijk is voor het toetsen en certificeren van ICT-beveiligingsdiensten, en
- BSI mag eisen stellen aan security audit raamwerken, procedures en mag, in samenspraak met organisaties in de vitale sectoren, technische en organisatie-eisen stellen aan organisaties die bevoegd zijn om een ICT-security audit uit te voeren. De eisen die aan de organisaties gesteld worden zijn gebaseerd op de ISO / IEC 17025 standaard[1]. De tot nu toe door de BSI gepubliceerde standaarden[2] zijn echter niet sector-specifiek.

7.1.3 Eigenaren van vitale infrastructuur in Duitsland moeten binnen twee jaar aantonen dat zij aan de wettelijke ICT-security eisen voldoen

De BSI-Kritisverordnung bevat eisen die Duitsland stelt aan de eigenaren van de vitale infrastructuur, die uit de NIS-richtlijn voortvloeien[3]:

- Binnen twee jaar na de inwerkingtreding van de NIS-wet moeten de eigenaren van de vitale infrastructuur afdoende organisatorische en technische maatregelen hebben genomen om verstoringen in beschikbaarheid, integriteit, authenticiteit en confidentialiteit van hun informatiesystemen, componenten of processen die van belang zijn voor het functioneren van de vitale infrastructuur in hun bezit. Hiervoor dienen zij voldoende maatregelen te treffen. Hierbij wordt proportionaliteitsbeginsel

[1] Bron: https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Stellen/Stellen_node.html, Verfahrensbeschreibung zur Anerkennung von Prüfstellen und Zertifizierung von IT-Sicherheitsdienstleistern, Version 3.4 Stand 11.03.2019

[2] Bron: https://www.bsi.bund.de/EN/Publications/BSIStandards/BSIStandards_node.html

[3] Bron: https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl117s1903.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s1903.pdf%27%5D__1549558845499

gehanteerd: voorzorgsmaatregelen worden als afdoende beschouwd tenzij de inspanning disproportioneel is ten aanzien van de consequenties van de verstoring of falen van de vitale infrastructuur in kwestie;
- Eigenaren van vitale infrastructuur en hun industrie-organisaties mogen suggesties doen aan de BSI v.w.b. industrie-specifieke security standaarden. BSI beoordeelt dan de voorgestelde standaarden en geeft aan of deze geschikt zijn om aan de gestelde eisen te voldoen;
- De eigenaren van vitale infrastructuur moeten compliance met de gestelde eisen kunnen aantonen. Dit moet minstens elke twee jaar gebeuren middels een security audit, review of certificering. De resultaten, inclusief mogelijk geconstateerde gebreken, moeten aan de BSI worden voorgelegd, en
- BSI mag zelf de compliance van een eigenaar van vitale infrastructuur toetsen. Hiervoor mogen gekwalificeerde derde partijen worden ingezet.

7.2 België

Net als Nederland heeft België de vitale infrastructuursectoren geïdentificeerd als: Energie, vervoer, telecom/digitale infrastructuur, financiële sector, drinkwater, gezondheidszorg, overheid.[1]

In België is de NIS-richtlijn vertaald tot “Wet tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid”. Om twijfels weg te nemen over de toepassing, bevat de wet een definitie en een duidelijk uitleg van wat onder de begrippen “netwerk- en informatiesysteem” en het begrip “apparaat dat digitale gegevens verwerkt” wordt verstaan, zijn SCADA-systemen (“alsook permanent of tijdelijk gekoppelde apparaten”) in de toelichtingsparagraaf van de wet expliciet genoemd.

Het federale *Computer Emergency Response Team*, kortweg CERT.be is de operationele dienst van het Centrum voor Cybersecurity België (CCB). CERT.be heeft als opdracht het opsporen, het observeren en het analyseren van online veiligheidsproblemen en het permanent informeren daarover.

CERT.be levert reactieve diensten, proactieve diensten en diensten met betrekking tot het beheer van de veiligheidskwaliteit in het domein van cybersecurity aan de aanbieders van essentiële openbare diensten, essentiële diensten en vitale infrastructuren. Ook bedrijven die geen essentiële diensten verlenen, kunnen een beroep doen op een beperkt aantal diensten van CERT.be.

Belgische kerncentrales vallen onder het toezicht van FANC. Het toezicht wordt uitgevoerd door deskundigen van de FANC filiaat Bel-V. Bel-V voert zowel aangekondigde als onaangekondigde inspecties en richt zich op alle vlakken van beveiliging – zowel fysiek als ICT- en IACS. De minimale eisen voor software zijn in 2013 door Bel-V vastgelegd[2]. De Nationale Veiligheidsoverheid (een organisatie die samengesteld is uit vertegenwoordigers van verschillende federale overheden, waaronder het FANC) nemen veiligheidsmachtigingen en veiligheidsattesten af van personen t.b.v. toegang tot veiligheidszones van een nucleaire inrichting, vervoer, kernmateriaal of nucleaire documenten.

[1] Bron: https://www.ccb.belgium.be/nl/vitale-sectoren

[2] Bron: Safety guideline “Assessment of Pre-existing and Commercial-Off-The-Shelf Software For Use in Functions Important to Safety”, Bel-V, 22-07-2013

7.3 Verenigde staten

7.3.1 Rollen, verantwoordelijkheden en vitale sectoren zijn benoemd

De vitale infrastructuur, rollen en verantwoordelijkheden zijn benoemd in de *Presidential Policy Directive 21- Critical Infrastructure Security and Resilience*[1]:

- PPD-21 benoemt o.a. de rollen en verantwoordelijkheden van de federale regering, staten, lokale en stambesturen en sector-specifieke agentschappen (in geval van VS gaat dit in meeste gevallen om het verantwoordelijke ministerie en in één geval om de *Environmental Protection Agency*);
- Tevens geeft het een aantal strategische acties (*strategic imperatives*) waarvan één gericht is op het vormen van een integrerende (over alle sectoren heen) analytische functie gericht op het voorbereiden van planning en operationele besluiten t.a.v. de vitale infrastructuur;
- 16 sectoren zijn aangewezen als 'vitaal' (chemie, commerciële faciliteiten, communicatie, kritieke productie, dammen, defensie, energie, financiële sector, voedsel en landbouw, overheid, gezondheidssector, IT, nucleair, transport en water en waterzuivering), en
- National Cybersecurity and Communications Integration Center – voor het delen van kritieke informatie tussen publieke en private sectoren.

7.3.2 Afdwingbare standaarden

De VS kennen afdwingbare cybersecurity standaarden voor de elektriciteitsproducenten en distributeurs[2]. Een aantal van deze standaarden geldt voor zgn. "Critical Infrastructure" (vitale infrastructuur) en betreft verschillende aspecten van cybersecurity. Daarnaast heeft het Department of Homeland Security een aantal *recommended practices* gepubliceerd voor gebruik bij inkoop van IACS-systemen[3] en voor energieleverigssystemen[4].

7.3.3 Sectorale security briefings en andere methodieken beschikbaar

EPA heeft, in samenwerking met de Association of State Drinking Water Administrators' (ADSWA) Security Committee een security briefing ontwikkeld voor drinkwaterbedrijven en afvalwaterreinigingsbedrijven. ADSWA heeft tevens een self-assesment ontwikkeld dat door de vele kleine drink- en afvalwaterbedrijven in de VS gebruikt kan worden. De self-assessment omvat ook, naast fysieke beveiliging, enkele vragen over de beveiliging van de ICT-systemen en personeel.

---

[1] Bron: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[2] Bron: https://www.nerc.com/pa/stand/Pages/ReliabilityStandardsUnitedStates.aspx?jurisdiction=United%20States

[3] Bron: Department of Homeland Security: Cyber Security Procurement Language for Control Systems

[4] Bron: Cybersecurity Procurement Language for Energy Delivery Systems

De elektriciteitssector heeft in 2014 een *cybersecurity capability maturity model* (ES-C2M2)[1] ontwikkeld. Het model dient als een standaard template voor of een self-assessment of een audit door een derde partij.

7.3.4 Mitigerende maatregelen en strategieën worden door ICS-CERT bijgewerkt n.a.v. incidenten

De VS kende oorspronkelijk een specifieke CERT voor IACS: het Industrial Control Systems Cyber Emergency Response Team (kortweg: ICS-CERT), onderdeel van het departement van Homeland Security. Sinds 2018 is de ICS-CERT samen met de US_CERT samengevoegd tot een organisatie, de Cybersecurity and Infrastructure Security Agency (CISA)[2]. . De CISA (en voorheen ICS-CERT) publiceert regelmatig diverse documenten met *recommended practices*[3]. Deze zijn zowel algemeen van aard als gevolg van analyses n.a.v. concrete aanvallen de VS of elders in de wereld. Daarnaast publiceert het regelmatig *white papers* over uiteenlopende onderwerpen, van risicoanalyse voor *smart cities* tot algemene *good practices* voor IACS cybersecurity tot industrie-specifieke beveiligingsmaatregelen.

Een van de algemene *good practice* documenten uit 2016 is getiteld '*Seven Steps to Effectively Defend Industrial Control Systems*'[4] en bevat concrete aanbevelingen die alle eigenaren van IACS-systemen kunnen treffen om de eigen cybersecurity te verbeteren. Deze *good practices* zijn gebaseerd op een analyse van in 2014 en 2015 gedetecteerde aanvallen op IACS-systemen. Conclusie van dit rapport is dat 98% van de aanvallen voorkomen had kunnen worden met implementatie van alle zeven genoemde *good practices*:

1. Applicatie *whitelisting;*
2. Het uitvoeren van gepaste configuratie en patch management;
3. Verkleinen van 'aanvalsoppervlak' (*attack surface area*);
4. Het bouwen van een verdedigbare omgeving;
5. Beheer van authenticaties;
6. Monitoring en response, en
7. Implementatie van beveiligd remote toegang.

Zoals al eerder gemeld in paragraaf 4.5, heeft n.a.v. het incident in Ukraine het ICS-CERT een 'alert' uitgevaardigd en de FERC heeft een update van de CIP Reliability Standards gepubliceerd die de *good practice* mitigerende maatregelen bevatten:

- Inkoop en licensiering van *trusted* hardware en software systemen;
- weten wie en wat zich op het netwerk bevindt;
- tijdige patching van systemen en strategisch lifecycle management / technologie verversing[5].

[1] `Bron: ELECTRICITY SUBSECTOR CYBERSECURITY CAPABILITY MATURITY MODEL (ES-C2M2), version 1.1, Februari 2014

[2] https://www.us-cert.gov/about-us

[3] https://ics-cert.us-cert.gov/Recommended-Practices

[4] https://ics-cert.us-cert.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf

[5] https://www.gpo.gov/fdsys/pkg/FR-2016-07-28/pdf/2016-17854.pdf

7.4 Finland

7.4.1 Cybersecurity strategie onderdeel van bredere maatschappelijke veiligheidsstrategie

Finland heeft al lang een nationale veiligheidsstrategie. De laatste nationale cybersecurity strategie stamt uit 2013. Factoren zoals geschiedenis, de nabijheid van Rusland, klimaat en geografie spelen een belangrijke rol in de Finse veiligheidsstrategie en maatschappelijke 'business continuity management' (BCM). De veiligheidsstrategie gaat veel verder dan defensie, binnenlandse veiligheid en vitale infrastructuur; het noemt zelfs de veiligheid van bevoorrading en psychologische weerbaarheid als functies die vitaal zijn voor het functioneren van de maatschappij[1]. Tot de vitale sectoren rekent Finland 'kritieke infrastructuur': elektriciteitsopwekking en -distributie, transport en logistieke dienstverlening, ICT (letterlijk: digitale datadiensten), communicatienetwerken en -diensten, betaal- en security transactiesystemen, beveiligde tijd- en plaatsbepalingssystemen en (drink)watervoorziening, aanleg en beheer van infrastructuur- en rioolbeheersystemen[2]. Daarnaast onderkent Finland zgn. 'kritieke productie en diensten', waaronder: voedselproductie, gezondheidszorg, industrie en productie en diensten t.b.v. militaire defensie.

7.4.2 Actueel implementatieprogramma met concrete doelen

Het meest recente implementatieprogramma voor de Finse cybersecurity strategie is voor de periode 2017-2020. Naast verscheidene zaken op ICT-vlak worden in de strategie de opwekking en distributie van elektriciteit en de veiligheid van bevoorrading (dit zijn: energie, transport, opslag en distributiesystemen, technische systemen, gezondheidszorg en maak- en herstelindustrie voor defensie) expliciet genoemd. De veiligheid van bevoorrading valt onder de verantwoordelijkheid van de National Emergency Supply Agency[3]. Ook hier zien we een verschil in de definitie van de vitale infrastructuur ten opzichte van Nederland: Opslag en distributie van voedsel behoort in Finland tot de vitale diensten met daarin een belangrijke rol voor de overheid.

De publiek beschikbare informatie bevat geen concrete maatregelen die binnen een supply chain geëist moeten of kunnen worden. De informatie is toegankelijk via het extranetportaal van de NESA.

7.5 Zweden

7.5.1 Gericht actieplan om in 2020 systematische beveiliging van vitale infrastructuur te bereiken

Zweden heeft een actieplan voor de bescherming van vitale maatschappelijke functies en vitale infrastructuur. Het actieplan wordt uitgevoerd onder de verantwoordelijkheid van de Swedish Contingencies Agency (MSB). Basis voor het actieplan is de samenwerking en informatie-uitwisseling met het bedrijfsleven.

---

[1] https://turvallisuuskomitea.fi/en/security-strategy-for-society/vital-functions/

[2] https://www.nesa.fi/finlands-new-security-of-supply-goals-focus-energy-supplies-digitalisation-logistics-and-cyber-security/

[3] https://www.nesa.fi/

De doelstelling van het actieplan is om in 2020 systematische beveiliging van de vitale infrastructuur te bereiken. Het actieplan is tweedelig: Maatregelen ter kennisverbetering en activiteiten voor implementatie van systematische beveiliging. (Measures for Knowledge Enhancement and Activities for the Implementation of Systematic Safety.)[1]

Het gedeelte 'Activiteiten voor implementatie van systematische beveiliging' is erop gericht dat het MSB, samen met andere relevante entiteiten, de voorwaarden en ondersteuning creëert zodat eigenaren en exploitanten van vitale maatschappelijke functies en vitale infrastructuur de doelstelling in 2020 hebben bereikt.

7.5.2 Voor vastlegging van verantwoordelijkheden van leveranciers worden oplossingen in opstellen van contracten voorgesteld

Een van de onderdelen van het actieplan is de zgn. robuuste contracten. De MSB dient suggesties te doen hoe robuuste contracten te ontwerpen zodat ook de verantwoordelijkheden van de (toe)leveranciers van vitale infrastructuur duidelijk zijn vastgelegd.

Eigenaren van vitale infrastructuur die tevens in de publieke sector vallen hebben de verplichting om te rapporteren over kritieke afhankelijkheden (let op: de formulering is dermate generiek dat het niet valt op te maken in welke mate de afhankelijkheden van (toe)leveranciers onder deze verplichting vallen).

7.6 Verenigd Koninkrijk

7.6.1 Vergelijkbare definities van vitale sectoren en vitale infrastructuur

De definitie van vitale infrastructuur in het Verenigd Koninkrijk is vergelijkbaar met Nederland: chemie, civiel nucleair, communicatie, defensie, veiligheidsdiensten, energie, financieel, voedsel, overheid, gezondheidszorg, ruimte, transport en water.[2] Ook in het VK zien we, net als in Duitsland, een verschil met Nederland. Ook het VK rekent voedsel(productie) tot de vitale infrastructuur.

Definitie van 'Critical National Infrastructure' is ook vergelijkbaar met de Nederlandse:

Critical National Infrastructure (CNI) is:
'Those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:
a) Major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or
b) Significant impact on national security, national defence, or the functioning of the state.'

7.6.2 NIS-richtlijn omgezet in een Cyber Assessment Framework

Cybersecurity binnen het VK is de verantwoordelijkheid van het *National Cybersecurity Center* (hierna: UK-NCSC, om onderscheid te maken met het Nederlandse NCSC). De UK-NCSC wordt hierin bijgestaan door het *Centre for the Protection of National Infrastructure* (CPNI). De NIS-richtlijn is in het VK geïmplementeerd in de vorm van een Cyber Assessment Framework (CAF). Hierbij geldt in het VK dat het civiele nucleaire sector (nog)

[1] Protection of Vital Societal Functions & Critical Infrastructure fact sheet; MSB 2015

[2] https://www.cpni.gov.uk/critical-national-infrastructure-0

niet onder de reikwijdte van de NIS-richtlijn valt. Het CAF is sector-agnostisch, maar kent in opzet de mogelijkheid om sector-specifieke toevoegingen zoals:

- CAF-profielen,
- Sector-specifieke interpretaties van 'bijdragende resultaten' (*contributing outcomes*)/indicatoren van *good practice*, en
- Sector-specifieke interpretaties van additionele 'bijdragende resultaten'/ indicatoren van *good practice* voor die gevallen waarin sector-specifieke cybersecurity eisen niet afdoende gedekt kunnen worden door een interpretatie van een generieke indicator.

Het CAF heeft vier doelstellingen, deze doelen zijn dermate generiek geformuleerd dat ze zowel op ICT als op IACS van toepassing zijn. Voor elk van de doelstellingen bevat het CAF-indicatoren waarmee een organisatie kan verifiëren of zij aan alle *good practices* voldoen.

- A: Governance, risicomanagement, asset management en supply chain,
- B: Security policies en procedures, Identity and Access Control, Data Security, System security, Netwerken en Personeelstraining,
- C: Monitoring en proactive discovery, en
- D: Response en recovery en Lessons Learned.

7.6.3 Aanbieders vitale infrastructuur zijn verantwoordelijk voor hun supply chain en moeten hun eisen contractueel vastleggen

Supply Chain valt in het CAF onder doelstelling A en stelt de aanbieder van vitale infrastructuur verantwoordelijk voor de beveiliging van de diensten die zij aanbieden – ongeacht het outsourcing model dat de aanbieder heeft gekozen.[1]

Principle

The organisation understands and manages security risks to networks and information systems supporting the delivery of essential services that arise as a result of dependencies on external suppliers. This includes ensuring that appropriate measures are employed where third party services are used. Regardless of your outsourcing model the OES remains responsible for the security of the service and therefore all the requirements that come from the NIS Directive.

Het UK-NCSC is tevens verantwoordelijk voor het delen van informatie over bedreigingen en actoren met de private sector. Hiertoe heeft het de Cybersecurity Information Sharing Partnership (CiSP) ingericht - een vertrouwelijk forum waarin intelligence real-time wordt gedeeld.[2] De invoering van de NIS-richtlijn in het VK kent tijdslijnen per sector. De tijdslijnen worden door het ministerie dat voor die sector verantwoordelijk is bepaald. Zo heeft het *Department for Business, Energy and Industrial Strategy* (kortweg: BEIS), ministerie verantwoordelijk voor de energiesector, duidelijke tijdslijnen uitgestippeld voor de aanbieders van vitale infrastructuur[3]:

- Tussen mei 2018 – november 2018 moesten aanbieders bepalen of zij onder de regels voor 'aanbieders vitale infrastructuur' (in het Engels: *Operators of Essential Services*, kortweg OES) vallen, zich melden bij de toezichthouder (*Competent*

[1] https://www.ncsc.gov.uk/guidance/caf-objective-a

[2] https://www.ncsc.gov.uk/threats

[3] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/721357/FINAL_NIS_Policy_Document_to_the_Energy_Sector_.pdf

Authority, kortweg: CA) voor hun sector en beginnen met het uitvoeren van een self-assessment conform de CAF. De aanbieders moeten het CAF self-assessment gebruiken om verbeterpunten te identificeren en verbeterplannen ontwikkelen.
In november 2018 moest de identificatie van de vitale aanbieders (OES) in het VK zijn afgerond;

- November 2018 – Q1 2019 heeft de industrie samen met de CA's, BEIS en NSCS gewerkt aan sector-specifieke beveiligingsrichtlijnen en beoordelingstools, en
- Uiterlijk in Q2 2019 moeten de sectorale CA's de self-assessments reviewen en een continu programma van inspecties en of audits door derde partijen ontwikkelen.

In 2017 heeft het Joint Committee on National Security Strategy een rapport opgesteld getiteld "Cybersecurity of the UK's Critical National Infrastructure"[1]. Het rapport is het resultaat van een parlementair onderzoek naar de staat van de cybersecurity maatregelen voor de vitale infrastructuur in het VK. Voor haar onderzoek heeft de parlementaire commissie gesproken met een scala aan experts uit verschillende sectoren en een aantal mogelijke (strategische) maatregelen en aanbevelingen opgehaald:

- Contractuele en niet-contractuele maatregelen die de aanbieders van vitale diensten kunnen nemen, waaronder:
  - Toegang die de (toe)leveranciers hebben tot de eigen IACS-systemen en de implicaties daarvan voor beveiliging;
  - Eis dat de (toe)leveranciers regelmatig een self-assessment uitvoeren;
  - Eis dat de (toe)leveranciers voldoen aan een minimum cybersecurity standaard zoals ISO27001 of de Cyber Essentials en Cyber Essentials Plus schemes;
- De regels die in het VK uit de NIS-richtlijn voortvloeien dwingen de dienstaanbieders in de (in de VK) vitale sectoren om 'passende maatregelen' te nemen daar waar zij diensten van derde partijen gebruiken, onder andere geldt dit voor:
  - Contracten.
    Bijvoorbeeld, de utilities gebruiken vaak contracten waarin een voorkeursleverancier en een back-up leverancier is vastgelegd. Door het stellen van beveiligingseisen al tijdens inkoop vallen (toe)leveranciers – niet enkel van IACS – die niet aan de eisen voldoen, van tevoren af.
  - Gespecificeerde "security eigenschappen" (*security properties*) voor producten en diensten die de dienstaanbieders inzetten voor de vitale dienstverlening.
  - De overheid in het VK heeft ervoor gekozen om de minimum security standaarden waar de directe leveranciers aan moeten voldoen in de contracten op te nemen en een security-equivalent van een 'credit rating' voor leveranciers op te stellen. Volgens meerdere geïnterviewde experts ligt echter de uitdaging in het beheersen van vaak lange en complexe leveringsketens niet bij de directe leveranciers, maar bij hun toeleveranciers. Sommige organisaties opteren er daarom voor om de primaire leverancier contractueel verantwoordelijk te maken voor het beheren van risico's in de eigen toeleveringsketen. National Grid (de TenneT van VK) is in dat opzicht zeer prescriptief en eist dat alle bedrijven in de gehele supply chain dezelfde certificering hebben als haar directe leveranciers.

7.7 Frankrijk

Frankrijk heeft de vitale sectoren en belangrijke organisaties binnen die sectoren reeds in 1998 geïdentificeerd t.b.v. het nationale beveiligingsraamwerk. Deze twaalf vitale sectoren ("*secteurs d'activités d'importance vitale*", afgekort SAIV) zijn voedsel, watermanagement, gezondheidszorg, de civiele, juridische en militaire activiteiten van de staat, energie, financiën, transport, elektronische communicatie van informatie en audiovisuele media,

[1] Bron: https://publications.parliament.uk/pa/jt201719/jtselect/jtnatsec/1708/170802.htm

delen van de industrie en tot slot lucht- en ruimtevaar en onderzoek. Ook hier zien we dus een verschil met de Nederlandse definitie van de vitale sectoren: Voedsel is, net als in Duitsland en het VK, een van de vitale sectoren. Verdeeld over deze twaalf sectoren zijn 200 kritieke organisaties uitgeroepen tot *"opérateurs d'importance vitale" (OIV).*

In 2013 heeft Frankrijk het nationale beveiligingsraamwerk en de lijst van vitale sectoren verankerd in het raamwerk Bescherming Vitale Informatie Infrastructuur ("protection des infrastructures d'information vitale", kortweg SIIV). Dit raamwerk wordt in de Engelstalige vertalingen van de relevante bronnen vaak aangeduid als de CIIP-wet.

Toezichthouder is de Franse Nationale Cybersecurity Agency (voluit: *Agence Nationale de la sécurité des systèmes d'information,* kortweg: ANSSI).

De veiligheidsregels betreffen preventieve maatregelen met als doel het verminderen van het risico van een succesvol cyberaanval. De regels worden gedefinieerd door de organisaties in samenwerking met ANSII en zijn gebaseerd zowel op internationale standaarden als op eigen operationele ervaring van ANSII en de verschillende organisaties.

Veruit de meeste regels zijn cros-sectoraal en betreffen wat ANSSI omschrijft als 'cyber hygiëne' en vallen in 20 categorieën[1]:

- Information assurance policies,
- Security accreditatie,
- Netwerk mapping,
- Security onderhoud,
- Logging,
- Logs correlatie en analyse,
- Detectie,
- Afhandeling van security incidenten,
- Afhandeling van security alerts,
- Crisismanagement,
- Identificatie,
- Authenticatie,
- Access control en privilege management,
- Beheer van toegangscontrole,
- Systeembeheer,
- Segmentatie in systemen en netwerken,
- Monitoring en filtering van netwerkverkeer,
- Remote toegang,
- Systems set up, en
- Indicatoren.

ANSSI heeft een evaluatieproces voor leveranciers van cybersecurity diensten en producten in het leven geroepen. Leveranciers kunnen zich op deze wijze (laten) certificeren voor het leveren van de volgende diensten aan de aanbieders van vitale infrastructuur diensten: Security audits, detectie, incident response. Het certificeren van leveranciers voor integratie en architectuur is gepland. De lijst bevat niet alleen de namen van de gecertificeerde leveranciers, maar ook het niveau van certificatie en de looptijd daarvan.

7.7.1 Nucleair sector is verplicht om veel informatie bij te houden

De Franse secretaris-generaal van defensie en nationale veiligheid heeft op 17 maart 2017 *arrêt* PRMD1703203A gepubliceerd waarin beschreven is hoe de nucleaire sector in Frankrijk de bestaande wetten op het gebied van cybersecurity moet uitvoeren. Deze aanpak omvat de elementen die als minimale industriestandaard beschouwd kunnen

[1] Bron: https://www.ssi.gouv.fr/en/cybersecurity-in-france/ciip-in-france/faq/#2-4

worden. Zo moet elke OIV een "*politique de sécurité des systèmes d'information*", wat vrij vertaald een security beleids- of strategiedocument ten behoeve van de beveiliging van informatiesystemen (inclusief IACS) is. Hierin moeten minimaal beschreven staan:

- De verantwoordelijkheden en governancestructuur van de ICT- en informatiebeveiligingsorganisatie,
- Een plan voor het creëren van bewustzijn onder de medewerkers, en
- Algemene beveiligingsmaatregelen, met name op het gebied van personeelscontrole, fysieke veiligheid, informatiesysteembeveiliging en beveiliging van werkomgevingen.

Verder schrijft het voor dat elke drie jaar een audit uitgevoerd moet worden (volgens *chapitre III du décret no 2015-350 du 27 mars 2015 précité*). Daarnaast is voorgeschreven dat elke OIV altijd een overzicht van de netwerk- en applicatiearchitectuur, inclusief koppelpunten en rechtenbeheer moet bijhouden en logbestanden van infrastructuuronderdelen moet bijhouden en kunnen analyseren om verdachte activiteit te kunnen detecteren.

7.8 Conclusie

Alle onderzochte landen hebben vitale sectoren geïdentificeerd en binnen de sectoren de aanbieders van vitale diensten. De systematiek voor de aanwijzing van de vitale sectoren en van de dienstaanbieders verschilt echter per land. Zo scharen o.a. Duitsland en Frankrijk voedselproductie ook onder noemer ‘vitaal’.

Alle Europese landen hebben ervoor gekozen om één gecombineerde CSIRT te hebben – d.w.z. een CSIRT met verantwoordelijkheid voor zowel ICT als IACS. Alleen de VS kent een specifieke IACS-CSIRT.

Een aantal landen (o.a. het VK) kent zgn. Cybersecurity Information Sharing Partnership (CiSP) - een vertrouwelijk forum waarin intelligence real-time wordt gedeeld. Dit kan betekenen dat er eisen gesteld (zullen) moeten worden aan het niveau van screening voor de CISOs van de deelnemende organisaties.

Een aantal van de onderzochte landen heeft bij de transpositie van de NIS-richtlijn in de nationale wetgeving expliciet SCADA en of industriële automatiseringssystemen in de reikwijdte van de wet opgenomen. Op deze wijze wordt duidelijk dat zowel ‘gewone’ ICT als IACS onder de reikwijdte van de wet vallen.

Aangezien de richtlijn nog niet lang in werking is, is de ervaring met het in praktijk toepassen van alle (voorgenomen) beleidsmaatregelen – zoals bv. het ontwikkelen van contractclausules voor het leveren van IACS-systemen, producten en diensten en de doorwerking van deze eisen in de (toe)leveringsketen - in de genoemde landen op dit moment echter beperkt.

8 Beschikbare strategische maatregelen en oplossingen

In dit hoofdstuk worden de mogelijke maatregelen uit vorige hoofdstukken geanalyseerd op toepasbaarheid voor de Nederlandse vitale sectoren. Voordat nieuwe maatregelen onderzocht worden, is het belangrijk om te analyseren welke maatregelen er al zijn.

Op dit moment zijn er al veel mogelijkheden om de digitale weerbaarheid van de Nederlandse vitale infrastructuur te borgen of te verbeteren. Zo is sinds 9 november 2018 de Wet Beveiliging Netwerk en Informatiesystemen (WBNI) van kracht geworden, die aangeeft dat alle aanbieders van essentiële diensten (AED's) de taak hebben om de digitale weerbaarheid te vergroten en de gevolgen van een cyberincidenten te beperken en zo maatschappelijke ontwrichting te voorkomen. De WBNI is gebaseerd op het Europese NIS-richtlijn. Alle andere EU-lidstaten hebben vergelijkbare wetten die een nationale transpositie van de NIS-richtlijn zijn.

8.1 Al ingezette maatregelen door beheerders vitale infrastructuur

Vitale infrastructuren worden vaak gebouwd voor een levensduur die veel langer is dan de (ondersteunde) termijn die een leverancier van servers en software geeft. Dit betekent dat (afhankelijk van contractuele afspraken) op den duur het risico bestaat dat bekende veiligheidsissues niet meer opgelost zullen worden.

Een ander issue is dat het aanbrengen van security patches ervoor kan zorgen dat een systeem niet meer functioneert, waardoor een beheerder (of de partij die het systeem geïmplementeerd heeft) het risico van aanpassen te groot vindt.

Uit de interviews met de beveiligingsverantwoordelijken binnen de vitale infrastructuur blijkt dat bovenstaande vaak voorkomende problemen bekend zijn. Wel geven zij aan dat binnen de vitale infrastructuur deze problemen in kaart gebracht zijn (waar het voorkomt) en dat er o.a. deze mitigerende maatregelen genomen zijn:

1. **Standaardisatie**: Er wordt alleen gewerkt met standaard onderdelen. Als deze niet meer ondersteund worden door de leverancier worden deze vervangen. De installatie wordt daarna opnieuw getest.
2. **Isolatie**: Het onderdeel wordt achter een firewall geplaatst. De toegang tot dit netwerk wordt gemonitord met een Security Incident en Event Management oplossing die specifiek ingericht is voor IACS. Als de veiligheidseisen heel hoog zijn, wordt er gebruik gemaakt van een data diode (een hardware oplossing die niet op afstand geconfigureerd kan worden).
3. **Contractuele afspraken**: Er wordt contractueel vastgelegd dat als er een veiligheidsissue bekend is de leverancier de patch certificeert en test zodat deze veilig geïnstalleerd kan worden.
4. **Monitoring van werkzaamheden door derden**: Als er noodzaak is dat een leverancier op afstand bij een installatie moet komen (bijvoorbeeld als de installatie niet goed functioneert) dan kan de beheerder fysiek een netwerkcomponent tijdelijk inschakelen zodat een leverancier het probleem kan oplossen. Hierbij wordt ook monitoring uitgevoerd door een specifiek IACS Security Operating Center (SOC).

Alle geïnterviewde organisaties geven aan dat er voldoende aandacht en budget is om deze bekende problemen op te lossen. Omdat het doel van het onderzoek gericht is op

strategische maatregelen, zijn deze opmerkingen niet gecontroleerd door middel van een audit.

8.2 Reeds bestaande wettelijke maatregelen (WBNI)

De Wet Beveiliging Netwerk- en Informatiesystemen (wbni) is per 9 november 2018 in werking getreden. Deze wet regelt een meldplicht van incidenten en een zorgplicht (treffen van beveiligingsmaatregelen). Vanaf 1 januari 2019 kunnen digitale dienstverleners incidenten melden bij het CSIRT (Computer Security Incident Response Team).

Bedrijven in de vitale sectoren moeten passende technische en organisatorische maatregelen nemen om de ICT en IACS te beveiligen. Verder moeten zij passende maatregelen treffen om incidenten te voorkomen en, als zich toch incidenten voordoen, de gevolgen daarvan zo veel mogelijk te beperken. In Nederland houdt Agentschap Telecom toezicht op de aanbieders van essentiële diensten (AED's) die onder het ministerie van Economische Zaken en Klimaat vallen en de op de aangewezen Digitale dienstverleners[1]. De Inspectie voor de Leefomgeving en Transport is toezichthouder voor de onder Ministerie van Infrastructuur en Water vallende AED's[2].

Bij organisaties in de vitale sectoren vinden regelmatig inspecties plaats, ook als er nog geen sprake is van een incident. Hierbij wordt onderzoek gedaan naar het complete risicomanagementproces en de passende maatregelen die een organisatie heeft getroffen. Agentschap Telecom geeft hierbij aan dat vooraf het gesprek aangegaan wordt met deze partijen, zodat organisaties weten waar ze zich aan moeten houden en dat uit volle overtuiging en uit zichzelf doen.

De toezichthouder heeft hierbij een aantal wettelijke bevoegdheden: Zo kan de toezichthouder een beveiligingsaudit uitvoeren bij een aanbieder van essentiële diensten of deze organisatie verplichten om zo'n audit zelf te laten uitvoeren. Als de toezichthouder constateert dat een organisatie zich niet aan wet- of regelgeving houdt dan biedt de wet verschillende mogelijkheden om handhavend op te treden, waaronder het opleggen van een bindende aanwijzing. Dat kan betekenen dat een organisatie een bepaalde maatregel moet treffen. Ook heeft de toezichthouder de bevoegdheid om boetes uit te delen.[3]

8.3 Toepasbaarheid maatregelen uit het buitenland en andere sectoren

Op basis van de gehouden interviews en literatuurstudie zijn onderstaande mogelijke maatregelen opgesteld die kunnen bijdragen aan de verbetering van de digitale weerbaarheid.

[1] https://www.agentschaptelecom.nl/actueel/nieuws/2018/november/9/wet-beveiliging-netwerk--en-informatiesystemen-van-kracht

[2] https://zoek.officielebekendmakingen.nl/stcrt-2018-61446.html

[3] https://www.agentschaptelecom.nl/documenten/publicaties/2018/09/26/brochure-algemene-informatie-wet-beveiliging-netwerken-informatiesystemen-wbni

8.3.1 Beheerder toont aan dat risico's vitale infrastructuur voldoende afgedekt zijn

Maatregel: In Duitsland bestaat de regel dat de beheerders van vitale infrastructuur elke twee jaar moeten aantonen dat zij voldoen aan de maatregelen die vastgesteld zijn per sector en dus dat de risico's voldoende zijn afgedekt. Deze bewijzen kunnen bestaan uit security audits, certificeringen of reviews. Eventuele issues die uit deze onderzoeken naar voren zijn gekomen moeten ook gerapporteerd worden. Wettelijk hebben de beheerders een zorgplicht voor de veiligheid van de vitale infrastructuur.

Input stakeholders: Zowel de beheerders van de vitale infrastructuur[1] alsook de toezichthouder zijn geen voorstander van een verplichte audit. Een self-assessment waarbij rekening gehouden kan worden met de specifieke zaken van de industrie wordt wel als nuttig ervaren. Door de sector zelf te laten bepalen hoe dit aangetoond wordt, blijft de hoeveelheid extra werk beperkter.

Conclusie: Door de beheerders zelf te laten kiezen voor de methode van het aantonen van IACS veiligheid, blijft de extra inspanning voor deze organisaties beperkt (ook naar de eigen directie wordt er gerapporteerd over de risico's). Verder kan er op deze manier maximaal gebruik gemaakt worden van de specifieke kennis die bij deze organisaties beschikbaar is m.b.t. de eigen specifieke manier van werken en beveiligen. Deze methode vereist wel een hoog kennisniveau bij de toezichthouder (vooral met betrekking tot volledigheidschecks).

Aanbeveling: Volg het Duitse model waarbij de beheerders zelf bepalen hoe zij aantonen dat de risico's voldoende afgedekt zijn. Als er onduidelijkheden zijn heeft de toezichthouder nu al het recht om te vragen naar een of meerdere aanvullende rapportage(s) of het uitvoeren van een audit.

8.3.2 Toezichthouder stelt samen met industrie een sector-specifiek controle raamwerk op

Maatregel: In het VK hebben de sectorale toezichthouders samen met de industrie een sector-specifiek raamwerk opgesteld met beveiligingsrichtlijnen en beoordelingstools.

Input stakeholders: Voor een aantal sectoren is dit controle raamwerk al gemaakt (Nucleair, Watervoorziening).

Conclusie: Het gezamenlijk opstellen (toezichthouder en industrie) van een raamwerk zorgt voor meer draagvlak en houdt rekening met de specifieke manier van werken en beveiligen binnen de sector. Verder geeft het alle bedrijven in de sector ook duidelijkheid waarop gecontroleerd gaat worden. Het nadeel van deze methode is wel dat het generiek moet zijn voor een hele sector, dus mogelijk een aantal specifieke zaken voor een individueel bedrijf mist. Dit kan ervoor zorgen dat het raamwerk als een "afvinklijst" wordt gebruikt, waarbij er minder wordt nagedacht over de specifieke risico's van een individueel bedrijf.

Een sector-specifiek raamwerk kan de minder volwassen bedrijven echter helpen bij het beter inrichten van de beveiliging. Als het model verplicht gemaakt wordt, kan dit ervoor zorgen dat de bedrijven zich gaan beperkten tot dit model. Dit kan het gevolg hebben dat er minder wordt nagedacht over de specifieke risico's van het bedrijf. Verder kan de toezichthouder dit model gebruiken bij het controleren van het self assessment van de meer volwassen bedrijven.

[1] Aanbieders van Essentiele diensten (AED's)

Aanbeveling: Zoek samenwerking met de sector om een sector-specifiek raamwerk op te stellen, maar maak dit raamwerk niet verplicht.

8.3.3 Handhaaf het gecombineerde CSIRT voor ICT en IACS; ga verder met het stimuleren van ISAC's

Maatregel: Een mogelijke maatregel om de focus op IACS-systemen te verhogen is het inrichten van een specifiek CSIRT voor ICAS, zoals de VS dit ook heeft. (https://ics-cert.us-cert.gov/). Alle andere onderzochte landen hebben echter een generiek CSIRT (Computer Security Incident Response Team).

Input stakeholders: Geen van de geïnterviewde stakeholders geeft aan een specifiek CSIRT voor IACS belangrijk te vinden. Een CSIRT voor een specifiek voor IACS-systemen zorgt mogelijk juist voor versnippering.

Conclusie: Ondanks dat nu zowel ICT alsook IACS incidenten op een centrale plaats verzameld worden, leidt dit niet tot "ondergesneeuwde" IACS incidenten. De IACS incidenten worden ook gemarkeerd. Andersom kan het splitsen in een ICIRT voor ICT en IACS wel leiden tot versnippering: informatie moet dan opgehaald worden bij verschillende onderdelen. Wel kan het nuttig zijn om met andere bedrijven in de sector de digitale weerbaarheid van de organisatie te verhogen door het starten van een Information Sharing and Analysis Centre (ISAC)[1].

Aanbeveling: Blijf bij de huidige methode van een generiek CSIRT, waarbij ICT en IACS gecombineerd zijn. Het is wel nuttig om de huidige aanpak van het stimuleren van ISAC's te continueren.

8.3.4 Maak standaard contractclausules die organisaties kunnen gebruiken bij aanbestedingen om de (IACS) beveiliging te waarborgen

Maatregel: In Zweden worden voor vastlegging van verantwoordelijkheden van leveranciers oplossingen in voorbeeldcontracten c.q. voorbeeldclausules voorgesteld.

Input stakeholders: Een aantal bedrijven neemt hiervoor al contractvoorwaarden op, maar dit is nog niet gestandaardiseerd. Een aantal geïnterviewde stakeholders geeft aan beleid t.a.v. eisen aan leveranciers wenselijk te vinden (vooral binnen overheid en i.r.t. aanbestedingswetgeving). Zij geven aan dat het NCSC hierin zou kunnen ondersteunen door (net als in Zweden) te komen met aanbevolen contractclausules.

Aanbeveling: Zorg voor standaard clausules voor IACS beveiliging in contracten. De rol van het NCSC is hierbij vooral gericht op het aandragen van IACS Security requirements. Andere organisaties (zoals bijvoorbeeld Centrum Informatiebeveiliging en Privacybescherming en Autoriteit Consument en Markt) kunnen de juridische ondersteuning coördineren.
Deze clausules geven organisaties een goede manier om op een gestandaardiseerde wijze de verantwoordelijkheden met betrekking tot het veilig houden van de vitale infrastructuur in contracten vast te leggen met (een keten van) leveranciers.

[1] https://www.ncsc.nl/aan-de-slag/samenwerken/doorontwikkelen-samenwerking

Op CISO niveau is er al veel overleg tussen de organisaties in de vitale sectoren. Door te stimuleren dat inkooporganisaties IACS- leveranciers scores delen, kan er gezamenlijk gezorgd worden voor een betere IACS beveiliging in toekomstige systemen en betere leverancierspresteaties.

8.3.5 Zorg voor gestandaardiseerde, sector-specifieke aanvalsscenario's

Maatregel: Zorg voor gestandaardiseerde, sector-specifieke aanvalsscenario's die de beheerders van vitale infrastructuur kunnen gebruiken om de robuustheid van deze infrastructuur te testen (zoals EU-TIBER in de financiële sector).

Input stakeholders: De geïnterviewde stakeholders geven aan het nuttig te vinden om sector-specifieke scenario's te kunnen testen. Het Initiatief ISIDOOR wordt door diverse stakeholders als nuttig ervaren, maar hierbij wordt wel aangegeven dat het als breed en ondiep wordt ervaren. Deels komt dit doordat deze organisaties ervoor kiezen om mee te doen op niveau brons (geen inbreng voor specifieke scenario's), deels doordat er veel zaken getest worden die als minder belangrijk worden ervaren.

Conclusie: ISIDOOR is nuttig, maar er is daarnaast behoefte aan sector specifieke tests. Verder kan waar relevant ook samenwerking worden gezocht met internationale partners. Bijvoorbeeld: Water is een keten; hack in Oostenrijk of Zwitserland kan ook gevolgen hebben in Nederland.

Aanbeveling: Het testen van sector-specifieke aanvalsscenario's heeft als doelstelling dat onvoldoende (en bij de organisatie nog onbekende) afgedekte risico's zichtbaar worden. Door het scenario c.q. de oefening sector-specifiek te maken, zullen organisaties eerder meedoen. Een advies van NCSC om dit te doen kan helpen om hier budget voor vrij te maken. Op deze manier kan het NCSC bijdragen (samen met ENISA) om de juiste voorwaarden te scheppen om binnen de NIS-richtlijn nationaal en internationaal per sector te oefenen. Verder kan het inrichten van een "Idaho Lab[1]" ervoor zorgen dat het testen van bepaalde scenario's mogelijk gemaakt wordt zonder dat er kans bestaat dat dit verstoringen oplevert in de bestaande infrastructuur.

8.4 Knelpunten en voorgestelde oplossingen op basis van de interviews

8.4.1 Garandeer dat adviezen van de minister meegenomen kunnen worden in aanbestedingen

Knelpunt: Als de minister van Justitie en Veiligheid een advies[2] geeft om een bepaalde leverancier niet meer te contracteren, is het niet altijd mogelijk om deze partij buiten de aanbesteding te houden. Door het verplichtende karakter van de aanbestedingswet kan het dus voorkomen dat deze partij gecontracteerd wordt ondanks het negatieve advies.

[1]Een test lab met daarin vergelijkbare hardware / software / configuratie als de bestaande vitale infrastructuur, https://www.apnews.com/80749f2dd5a84bb49b7aceb1a4c43b8e

[2] https://www.rijksoverheid.nl/documenten/kamerstukken/2018/05/14/voorzorgsmaatregel-ten-aanzien-van-gebruik-kaspersky-antivirussoftware

Aanbeveling: Bespreek met de ACM hoe ervoor gezorgd kan worden dat de adviezen van de minister voor aanbestedingen binnen de vitale sectoren in alle gevallen meegenomen mogen worden bij het bepalen van de afwegingscriteria. Op dit moment geldt er voor bijvoorbeeld defensie een uitzondering dat om redenen van staatsveiligheid een uitzondering gemaakt mag worden. Onderzoek of dit ook mogelijk is voor bedrijven in de vitale sectoren.

8.4.2 Meldpunt leveranciers die ondanks contractuele verplichting, onvoldoende meewerken aan veilig houden van infrastructuur

Knelpunt: Het contracteren van maatregelen om toekomstige issues op te lossen (bijvoorbeeld security patches, of certificering op nieuwe OS-versies als de oorspronkelijke niet meer ondersteund wordt) is nuttig, maar niet altijd afdoende. Als de leverancier groot is en de hoeveelheid afgenomen apparatuur beperkt, dan kan de leverancier ervoor kiezen om de (beperkte) privaatrechtelijke boete te betalen zoals vastgelegd in het contract bij de aankoop.

Aanbeveling: Richt een meldpunt in (bv. bij het Agentschap Telecom) voor bedrijven die ondanks contractuele voorwaarden niet willen voldoen aan het tijdig oplossen van veiligheidsproblemen in hun hardware of software. De inkoopafdeling of de securityorganisatie kan hier melden als leveranciers of systeem integrators niet willen of kunnen voldoen aan de noodzakelijke IACS-beveiligingsmaatregelen.
Zo kan dan gecontroleerd worden of dit ook bij andere bedrijven in andere landen optreedt en kan gezamenlijk druk uitgeoefend worden of zelfs boetes worden uitgedeeld. Omdat de beperkte privaatrechtelijke boete mogelijk niet voldoende is om de leverancier tot aktie te dwingen, is het goed om te onderzoeken wat de bestuursrechtelijke mogelijkheden zijn (zoals plaatsing op een landelijke zwarte lijst van leveranciers die niet meer mogen leveren aan bedrijven in de vitale sector)

8.4.3 Zorg voor security clearance bij bedrijven in de vitale sectoren om uitwisseling van AIVD-informatie mogelijk te maken

Knelpunt: In een aantal gevallen is er vanuit de AIVD of NCTV wel informatie beschikbaar over mogelijke aanvallen, maar kan die niet gedeeld worden vanwege het vertrouwelijke karakter van de betreffende informatie. Bij de beheerders van de vitale infrastructuur zijn er niet altijd mensen beschikbaar met de juiste security clearance.

Aanbeveling: Adviseer organisaties (net als ook in het VK) in de vitale sectoren om ervoor te zorgen dat een beperkt aantal personen (bijvoorbeeld de CISO en een teamlid) het noodzakelijke clearance niveau heeft zodat de AIVD in bepaalde gevallen informatie kan delen. Deze personen kunnen dan controleren of de organisatie voldoende voorbereid is voor de mogelijke aanval en waar nodig hier extra maatregelen voor inzetten.

8.5 Kostenefficiënte maatregelen: Methoden uit andere sectoren

Maatregelen om systemen 100% veilig te houden zijn onmogelijk, en maatregelen die dit zo dicht mogelijk benaderen hebben een zeer hoog kostenniveau. Voorkomen hoeft dan ook niet altijd beter te zijn dan genezen. In sommige gevallen kan het kostenefficiënter zijn om te

focussen op snel herstel in plaats van het voorkomen van een mogelijke verstoring. Uiteraard moet hier wel een goede risico-inventarisatie aan ten grondslag liggen: Bij een kerncentrale kunnen de gevolgen van een kortdurende verstoring nog steeds heel groot en langdurig zijn. De gevolgen van de uitval van gas voor een paar minuten zijn nog steeds kostbaar, maar als het voorkomen hiervan tientallen miljoenen euro's kost, is het goed om te overwegen deze maatregel niet uit te voeren. In dit geval zou het kunnen zijn dat het beter is om de uitval te oefenen en te zorgen voor mogelijkheden voor snel herstel van de dienstverlening.

Juist omdat diverse organisaties een winstoogmerk hebben (of de prijzen niet zomaar kunnen verhogen zonder goede onderbouwing richting de toezichthouder) is het belangrijk dat de veiligheidsmaatregelen in lijn zijn met de risico's. In de wet WBNI staat dan ook dat er "passende en evenredige technische en organisatorische maatregelen [genomen moeten worden] om de risico's voor de beveiliging van hun netwerk- en informatiesystemen te beheersen."

Een van de mogelijkheden om hier op een praktische manier mee om te gaan, is aangeven of wat het niveau van een mogelijke aanval is waartegen de maatregel dient te beschermen. Het NCSC[1] maakt hiervoor gebruik van onderstaande niveaus:

1. Cybervandalen en scriptkiddies,
2. Hacktivisten,
3. Interne actoren,
4. Beroepscriminelen,
5. Terroristen, en
6. Statelijke actoren.

Het uitgangspunt van deze lijst is dat er veel aanvallen zijn van het laagste niveau en een beperkt aantal van het hoogste niveau.

De ervaring uit andere sectoren met een hoog beveiligingsniveau (o.a. financiële instellingen zoals banken en verzekeraars) is dat de grote hoeveelheid aanvallen het beste bestreden kan worden met preventieve maatregelen. Voor aanvallen die niet vaak voorkomen (en technisch geavanceerder zijn) is het beter te focussen op detectie en snelle reactie zodat het een klein incident blijft. Zeer geavanceerde aanvallen (met nieuwe, onbekende aanvalspatronen) zijn vrijwel kostenefficiënt te voorkomen of te detecteren en zal er dus een (groter) incident optreden. De uitdaging bij deze incidenten is om te zorgen voor een korte hersteltijd.

Niveau aanval	Focus van maatregel
1. Cybervandalen en scriptkiddies **2. Hacktivisten,** **3. Interne actoren**	**Focus op preventie** **Mogelijke maatregelen:** Self assessments, audits, patch management, netwerkscheidingsmogelijkheden, snel delen van aanvalspatronen via CSIRT, (Computer Security Incident Response Team).

[1] https://www.nctv.nl/binaries/CSBN2017_tcm31-267075.pdf

Niveau aanval	Focus van maatregel
4. Beroepscriminelen **5. terroristen**	**Focus op vroege detectie en snelle reactie** **Mogelijke maatregelen:** 24/7 monitoring via SIEM/SOC, bij gedetecteerde aanval preventief externe netwerkverbindingen uitschakelen. Zorgen voor een extra beveiligd netwerk/toegangskanaal (met meer encryptie en vaker wisselende sleutels, speciale extra hardened laptops.
6. Statelijke actoren	**Focus op herstelmogelijkheden** **Mogelijke maatregelen:** Zorg voor mogelijkheden tot handbediening en snel herstel. Train om handbediening mogelijk te houden, en in contracten ervoor zorgen dat er altijd een “manual override” mogelijk blijft. Waar focus op hertel te grote risico’s inhoudt, kan er in uitzonderlijke gevallen gekozen worden voor extra fysieke beveiliging en analoge bediening/regel/veiligheidssystemen.

Tabel 2: Overzicht aanvalsniveaus en focus van maatregelen

Door ervoor te kiezen om niet alle risico’s te mitigeren met preventieve maatregelen kunnen de kosten beperkt gehouden worden, zonder dat het risiconiveau significant omhoog gaat.

Bijvoorbeeld: Het niveau van preventieve maatregelen om een Stuxnet stijl aanval (statelijke actor) te kunnen afslaan is heel duur. Door ook “snel herstellen” als maatregel op te nemen (en dit te oefenen) kan ook als er een aanval gemist wordt (ook al is die op zich van laag technisch niveau) toch snel weer verder gegaan worden met de normale operatie.

8.6 Conclusie

Ondanks dat de vitale sectoren in Nederland al heel veel goed doen (landelijke langdurige uitval van gas, elektra of water is nog niet voorgekomen) is het zeker mogelijk om te leren van andere landen en sectoren. De geïnterviewde organisaties geven aan dat zij het belangrijk vinden om ook richting de maatschappij aan te tonen dat ze veilig zijn. Ook een extra steun vanuit de overheid om scenario’s te testen (sector-specifiek) zou door alle organisaties als nuttig ervaren worden. Organisaties die met grens-overstijgende netwerken te maken hebben (elektriciteit, gas en water) geven tevens aan het nuttig te vinden steun te hebben bij het opzetten van internationale scenario’s en tests.
Aanvallen door statelijke actoren met een vrijwel onbeperkt budget zijn niet of zeer moeilijk tegen te houden. Hierbij kan het nuttig zijn als de toezichthouder aangeeft dat tot niveau 4 (terroristen) er preventieve of reactieve maatregelen moeten zijn, maar dat bij niveau 5 (statelijke actoren) voor een aantal sectoren het voldoende is te focussen op snel herstel.

Uiteraard is dit niet het geval als een verstoring direct al grote consequenties heeft (falende veiligheidssystemen bij een kerncentrale), maar (heel incidenteel) een korte verstoring van elektriciteit zou geaccepteerd kunnen worden als de maatregelen ter voorkoming hiervan te duur worden.

Bijlagen

Bijlage A. Uitgenodigde organisaties/platforms

Vitale processen	Te contacten organisatie
Landelijk transport en distributie elektriciteit	Verantwoordelijke/IACS expert van Tennet
Regionale distributie elektriciteit	Verantwoordelijke/IACS expert van Stedin
Gasproductie, landelijk transport en distributie gas	Gasunie
Olievoorziening	Verantwoordelijke/IACS expert van Central European Pipeline System (CEPS) (onderdeel van NATO)
Drinkwatervoorziening	Verantwoordelijke/IACS expert van Vereniging van Waterbedrijven in Nederland
Keren en beheren waterkwantiteit	Verantwoordelijke/IACS expert van Rijkswaterstaat
Grootschalige productie/verwerking en/of opslag (petro)chemische stoffen	Verantwoordelijke/IACS expert van Shell
België: Waterkering	Verantwoordelijke/IACS expert van Mobiliteit en Openbare Werken
Leverancier SCADA systemen	Verantwoordelijke/IACS expert van Siemens
Industrieel Platform Cybersecurity - NEN	Contactpersoon Industrieel Platform Cybersecurity
Industrial Automation and Control System Security Committee	Contactpersoon ISA 62443 (ISA 62443 is de naam van de Industrial Automation and Control System Security Committee of the ISA
TIBER-EU	Contactpersoon CBEST / TIBER (The Framework for Threat Intelligence-based Ethical Red Teaming (TIBER-EU)

Bijlage B. Knelpunten en maatregelen overzicht

Maatregel	Input Stakeholders	Aanbeveling Gartner onderzoekers
Beheerder toont aan dat risico's vitale infrastructuur voldoende afgedekt zijn: **In Duitsland bestaat de regel dat de beheerders van vitale infrastructuur elke twee jaar moeten aantonen dat zij voldoen aan de maatregelen die vastgesteld zijn per sector en dus dat de risico's voldoende zijn afgedekt. Deze bewijzen kunnen bestaan uit security audits, certificeringen of reviews. Eventuele issues die uit deze onderzoeken naar voren zijn gekomen moeten ook gerapporteerd worden.**	Zowel de beheerders van de vitale infrastructuur alsook de toezichthouder zijn geen voorstander van een verplichte audit. Een self-assessment waarbij rekening gehouden kan worden met de specifieke zaken van de industrie wordt wel als nuttig ervaren. Door de sector zelf te laten bepalen hoe dit aangetoond wordt, blijft de hoeveelheid extra werk beperkter.	Volg het Duitse model waarbij de beheerders zelf bepalen hoe zij aantonen dat de risico's voldoende afgedekt zijn. Als er onduidelijkheden zijn heeft de toezichthouder nu al het recht om te vragen naar een of meerdere aanvullende rapportage(s).
Toezichthouder stelt samen met industrie een sector-specifiek controle raamwerk op: **In het VK heeft de sectorale toezichthouder samen met de industrie een sector-specifiek raamwerk opgesteld met beveiligingsrichtlijnen en beoordelingstools.**	Voor een aantal sectoren is dit controle raamwerk al gemaakt (Nucleair, Watervoorziening).	Zoek samenwerking met de sector om een sector-specifiek raamwerk op te stellen, maar maak dit raamwerk niet verplicht
Handhaaf het gecombineerde CSIRT voor ICT en IACS; ga verder met het stimuleren van ISAC's: **Een mogelijke maatregel om de focus op IACS te verhogen is het inrichten van een specifiek CSIRT voor ICAS, zoals de VS dit ook heeft. (https://ics-cert.us-cert.gov/). Alle andere onderzochte landen hebben echter een generiek CSIRT (Computer Security Incident Response Team).**	Geen van de geïnterviewde stakeholders geeft aan een specifiek CSIRT voor ICS belangrijk te vinden. Een CSIRT voor een specifiek voor IACS zorgt mogelijk juist voor versnippering.	Blijf bij de huidige methode van een generiek CSIRT, waarbij ICT en IACS gecombineerd zijn. Het is wel nuttig om de huidige aanpak van het stimuleren van ISAC's te continueren.

Maatregel	Input Stakeholders	Aanbeveling Gartner onderzoekers
Maak standaard contractclausules die organisaties kunnen gebruiken bij aanbestedingen om de (IACS) beveiliging te waarborgen: **In Zweden worden voor vastlegging van verantwoordelijkheden van leveranciers oplossingen in opstellen van contracten voorgesteld.**	Een aantal bedrijven neemt hiervoor al contractvoorwaarden op, maar dit is nog niet gestandaardiseerd. Een aantal geïnterviewde stakeholders geeft aan beleid t.a.v. eisen aan leveranciers wenselijk te vinden (vooral binnen overheid en i.r.t. aanbestedingswetgeving). Zij geven aan dat het NCSC hierin zou kunnen ondersteunen door (net als in Zweden) te komen met aanbevolen contractclausules.	Zorg voor standaard clausules voor IACS-beveiliging in contracten. De rol van het NCSC is hierbij vooral gericht op het aandragen van IACS Security requirements. Andere organisaties (zoals bijvoorbeeld Centrum Informatiebeveiliging en Privacybescherming en Autoriteit Consument en Markt) kunnen de juridische ondersteuning coördineren. Deze clausules geven organisaties een goede manier om op een gestandaardiseerde wijze de verantwoordelijkheden met betrekking tot het veilig houden van de vitale infrastructuur in contracten vast te leggen met (een keten van) leveranciers. Op CISO-niveau is er al veel overleg tussen de organisaties in de vitale sectoren. Door te stimuleren dat inkooporganisaties IACS-leveranciers scores delen, kan er gezamenlijk gezorgd worden voor een betere IACS-beveiliging in toekomstige systemen en betere leverancierssprestaties.

Maatregel	Input Stakeholders	Aanbeveling Gartner onderzoekers
Zorg voor gestandaardiseerde, sector-specifieke aanvalsscenario's: Zorg voor gestandaardiseerde, sector-specifieke aanvalsscenario's die de beheerders van vitale infrastructuur kunnen gebruiken om de robuustheid van deze infrastructuur te testen (zoals EU-TIBER in de financiële sector).	De geïnterviewde stakeholders geven aan het nuttig te vinden om sector-specifieke scenario's te kunnen testen. Het Initiatief ISIDOOR wordt door diverse stakeholders als nuttig ervaren, maar hierbij wordt wel aangegeven dat het als breed en ondiep wordt ervaren. Deels komt dit doordat deze organisaties ervoor kiezen om mee te doen op niveau brons (geen inbreng voor specifieke scenario's), deels doordat er veel zaken getest worden die als minder belangrijk worden ervaren.	Het testen van sector-specifieke aanvalsscenario's heeft als doelstelling dat onvoldoende (en bij de organisatie nog onbekende) afgedekte risico's zichtbaar worden. Door het scenario c.q. de oefening sector-specifiek te maken, zullen organisaties eerder meedoen. Een advies van NCSC om dit te doen kan helpen om hier budget voor vrij te maken. Op deze manier kan het NCSC bijdragen (samen met ENISA) om de juiste voorwaarden te scheppen om binnen de NIS-richtlijn nationaal en internationaal per sector te oefenen. Verder kan het inrichten van een "Idaho Lab " ervoor zorgen dat het testen van bepaalde scenario's mogelijk gemaakt wordt zonder dat er kans bestaat dat dit verstoringen oplevert in de bestaande infrastructuur

Knelpunt	Aanbeveling Gartner onderzoekers
Garandeer dat advies van minister van JenV meegenomen kan worden in aanbestedingen: Als de minister een advies geeft om een bepaalde leverancier niet meer te contracteren, is het niet altijd mogelijk om deze partij buiten de aanbesteding te houden. Door het verplichtende karakter van de aanbestedingswet kan het dus voorkomen dat deze partij gecontracteerd wordt ondanks het negatieve advies.	Bespreek met de ACM hoe ervoor gezorgd kan worden dat de adviezen van de minister voor aanbestedingen binnen de vitale sectoren in alle gevallen meegenomen mogen worden bij het bepalen van de afwegingscriteria. Op dit moment geldt er voor bijvoorbeeld defensie een uitzondering dat bij redenen van staatsveiligheid een uitzondering gemaakt mag worden. Onderzoek of dit ook mogelijk is voor bedrijven in de vitale sectoren
Meldpunt leveranciers die ondanks contractuele verplichting, onvoldoende meewerken aan veilig houden van infrastructuur: Het contracteren van maatregelen om toekomstige issues op te lossen (bijvoorbeeld security patches, of certificering op nieuwe OS-versies als de oorspronkelijke niet meer ondersteund wordt) is nuttig, maar niet altijd afdoende. Als de leverancier groot is en de hoeveelheid afgenomen apparatuur beperkt, dan kan de leverancier ervoor kiezen om de (beperkte) boete te betalen.	Richt een meldpunt in (bv. bij het Agentschap Telecom) voor bedrijven die ondanks contractuele voorwaarden niet willen voldoen aan het tijdig oplossen van veiligheidsproblemen in hun hardware of software. De inkoopafdeling of de securityorganisatie kan hier melden als leveranciers of systeem integrators niet willen of kunnen voldoen aan de noodzakelijke IACS-beveiligingsmaatregelen. Zo kan dan gecontroleerd worden of dit ook bij andere bedrijven in andere landen optreedt en kan gezamenlijk druk uitgeoefend worden of zelfs boetes worden uitgedeeld.
Zorg voor security clearance bij bedrijven in de vitale sectoren om uitwisseling van AIVD-informatie mogelijk te maken: In een aantal gevallen is er vanuit de AIVD wel informatie beschikbaar over mogelijke aanvallen, maar kan die niet gedeeld worden vanwege het vertrouwelijke karakter van de betreffende informatie. Bij de beheerders van de vitale infrastructuur zijn er niet altijd mensen beschikbaar met de juiste security clearance.	Adviseer organisaties in de vitale sectoren om ervoor te zorgen dat een beperkt aantal personen (bijvoorbeeld de CISO en een teamlid) het noodzakelijke clearance niveau heeft zodat AIVD-informatie gedeeld kan worden. Deze personen kunnen dan controleren of de organisatie voldoende voorbereid is voor de mogelijke aanval en waar nodig hier extra maatregelen voor inzetten.

Bijlage C. Geraadpleegde literatuur

Alle website bronnen zijn gecontroleerd en geraadpleegd op 16 juli 2019

Kristian Steenstrup, *2018 Strategic Roadmap for IT/OT Alignment*, Gartner Research 2018

Wam Voster, *Secure Your OT With Basic Security Hygiene*, Gartner Research 2018

Earl Perkins et al, *Market Guide for Operational Technology Security*, Gartner Research 2017

Kristian Steenstrup, et al. *Hype Cycle for Managing Operational Technology 2017* , Gartner Research 2017

Langner, *To Kill a Centrifuge, A Technical Analysis of What Stuxnet's Creators Tried to Achieve* from: https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf

FERC Notice of Inquiry to address several urgent cybersecurity issues affecting the bulk electric system. (https://www.gpo.gov/fdsys/pkg/FR-2016-07-28/pdf/2016-17854.pdf)

FERC Takes Action on Cybersecurity in Response to Ukrainian Cyber (Attacks

https://www.alstonprivacy.com/ferc-takes-action-cybersecurity-response-ukrainian-cyber-attacks/

Homeland Security, Seven Strategies to Defend IACSs

https://www.us-cert.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf

NCTV, Cybersecuritybeeld Nederland CSBN 2019

https://www.ncsc.nl/documenten/publicaties/2019/juni/12/cybersecuritybeeld-nederland-2019

E-ISAC, *Analysis of the Cyber Attack on the Ukrainian Power Grid*, from: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

Industrial Internet Consortium, I*ndustrial Internet of Things Volume G4: Security Framework* from: https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf

CyberX Labs, *Global IACS & IIoT Risk Report* from: https://cdn2.hubspot.net/hubfs/2479124/Report%20-%20Global%20IACS%20&%20IIoT%20Risk%20Report.pdf

Checklist Beveiliging van CS/SCADA from: https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2019/mei/01/checklist-beveiliging-ics-scada/FS2012-02-Checklist-beveiliging-van-ICS-SCADA-systemen.pdf

NCTV Magazine Nationale Veiligheid en crisisbeheersing nr.3 2015 - NCTV

From: https://www.nctv.nl/binaries/magazine-nationale-veiligheid-en-crisisbeheersing-2015-3_tcm31-29649.pdf

Wet beveiliging netwerk- en informatiesystemen (WBNI) https://zoek.officielebekendmakingen.nl/stb-2018-387.pdf

ISIDOOR II Vevin beschrijving

http://www.vewin.nl/Waterspiegelartikelen/14-ISIDOOR%20II%20-%20Operationele%20cyberoefening%20publieke%20en%20private%20sector%2005-2017.pdf

Critical Infrastructure Protection, H6 LESSONS LEARNED FROM THE MAROOCHY WATER BREACH, Jill Slay and Michael Miller
https://www.researchgate.net/publication/221654716_Lessons_Learned_from_the_Maroochy_Water_Breach

Australian Trusted Information Sharing Network for Critical Infrastructure Protection
https://www.tisn.gov.au/Documents/CriticalInfrastructureResilienceStrategyPlan.PDF

Websites:

https://www.nctv.nl/organisatie/nationale_veiligheid/vitale_infrastructuur/index.aspx

https://tweakers.net/nieuws/80611/minister-schultz-scada-systemen-rijksoverheid-zijn-veilig.html

https://www.tweedekamer.nl/kamerstukken/plenaire_verslagen/kamer_in_het_kort/cda-vraagt-naar-digitale-beveiliging-sluizen

Alle vragen betreffende dit rapport kunnen geadresseerd worden aan:

Peter Kivits
Managing Partner Nederlandse overheid
Gartner Nederland BV
1101 BH Amsterdam Zuidoost
Email: peter.kivits@gartner.com

Dit rapport is bestemd voor:
Ministerie van Justitie en Veiligheid

Elly van den Heuvel
Ministerie van Justitie en Veiligheid
Turfmarkt 147 den Haag
Email: e.c.van.den.heuvel@nctv.minvenj.nl

Gartner®