Den Haag / Utrecht, 3 mei 2018

"Cyber security in het Urban Energy domein", 3 april 2018 – deelsessies

Inleiding
Op 3 april 2018 vond in Den Haag de bijeenkomst plaats "Cyber security in het Urban Energy domein".

Partijen, die voor de beveiliging van hun bedrijfsvoering cyber security hoog op de agenda hebben staan, en leveranciers van producten en diensten op het gebied van cyber security hebben met elkaar zeven presentaties verzorgd.

1. Maarten Hoeve	ENCS (European Network for Cyber Security)
2. Maria Garnaeva	Kaspersky
3. Jako Jellema	Agentschap Telecom
4. Marijn van Schoote	Havenbedrijf Rotterdam
5. Arie van Bellen	ECP - Platform voor de InformatieSamenleving
6. Bart Luijkx	Alliander
7. Wilbert Prinssen	Technolution

De bijeenkomst werd afgerond met drie deelsessies, waarbij werd teruggekeken op de presentaties en werd besproken hoe we verder (kunnen) gaan met cyber security. De deelsessies richtten zich op:
A. gebouwde omgeving;
B. energie-infrastructuur;
C. bedrijven en bedrijventerrein.

Hieronder volgt een verslag van ieder van de drie deelsessies.

Afkortingen:
- TSE Topsector Energie;
- UE TKI Urban Energy;
- RVO Rijksdienst voor Ondernemend Nederland.

A. Gebouwde omgeving
Moderator en verslag: Nicole Kerkhof en Olivier Ongkiehong (beiden RVO).

Olivier heet de aanwezigen welkom namens TSE, UE en RVO. TSE, UE en overheid willen de energietransitie faciliteren en zien dat cyber security daarbij steeds belangrijker wordt. Daarom hebben ze in 2017 een opdracht uitgezet bij Technolution hetgeen heeft geresulteerd in een handreiking "Cyber security for smart energy" met handvatten om met dit onderwerp al in de ontwerp fase van een nieuw product of nieuwe dienst aan de slag te gaan met een risico inventarisatie. Zie ook https://topsectorenergie.nl/tki-urban-energy/kennisdossiers/cybersecurity-smartenergy.

Vragen aan de deelnemers:
1. Kunnen jullie met deze handreiking aan de slag?
2. Zien jullie andere manieren, waarop TSE en UE jullie kunnen ondersteunen?

Reacties op vraag 1: kunnen jullie met de handreiking aan de slag?
De handreiking is door enkelen gelezen.

Reacties:

- Vandebron Energie geeft aan dat ze op zoek is naar slimme oplossingen en ziet daarbij zeker het belang van Cyber Security. Het onderwerp meenemen vanaf design gebeurt nog niet bewust en ze gaat zeker het kennisdossier en de handreiking lezen.
- Vanuit de ICT hoek, bouwer van ICT voor thermostaten, wordt aangegeven dat er in het werk van partijen een kruising ontstaat met specifieke energie stromen. Wil graag inzicht in welke risico's specifiek daarvoor zijn genoemd en welke rol een klein bedrijf hierin heeft ten opzichte van bijvoorbeeld een netbeheerder.
- In de handreiking worden twee casussen nader uitgewerkt: HEMS (home energy management systeem) en transformatorhuis. Inzicht krijgen in jouw product en jouw dienst en zo vroeg mogelijk in het ontwerp daarvan bedenken welke situaties en consequenties zich kunnen voordoen voorkomen later veel aanpassingen.
- Hoe kan cyber security ook decentraal worden opgepakt? Hoe ziet de netbeheerder dit? En mag je beperkingen aan huishoudens stellen? Met als doel dat ook echt iedereen over dit onderwerp gaat nadenken en zich er bewust van wordt.
- Daarnaast wordt opgemerkt dat risico's in de handreiking worden uitgedrukt in geld bedragen terwijl de daadwerkelijke gevolgen van risico's veel breder zijn. Denk bijvoorbeeld ook aan veiligheid voor patiënten in het ziekenhuis en voor de maatschappij. Het gaat dus bij beide casussen in de handreiking om een brede context waarvoor nu nog geen gestandaardiseerde aanpak is.
- Een netbeheerder geeft aan dat inzicht nodig is wat het hacken van een thermostaat voor gevolg heeft voor de elektriciteitsvoorziening. Ook inzicht in het motief van de hacker kan daarbij helpen. Het is zaak om van beide kanten (netbeheer enerzijds en woning of gebouw anderzijds) het risico in kaart te brengen, inzicht te krijgen en verantwoordelijkheid te nemen. We staan voor veel uitdagingen in een wereld die zich snel ontwikkelt.
- Kaspersky geeft aan dat bij 'slimme' devices weinig gewezen wordt op het feit dat de gebruiker het standaard wachtwoord moet wijzigen. Ook vanuit de leverancier moeten partijen daar meer op wijzen en aangeven wat de eigenschappen van een goed wachtwoord zijn.
- Onderzoek naar een andere techniek als oplossing voor een wachtwoord zou een vervolg kunnen zijn (zie bijvoorbeeld de OV chipkaart met één eigenaar en één verantwoordelijke, minder kans op fouten en inbraken).

Reacties op vraag 2: andere manieren, waarop TSE en UE kunnen ondersteunen?

- De deelnemers zien het programma van vanmiddag als nuttig en van belang voor de bewustwording.
- Als aandachtspunt wordt meegegeven dat je wat betreft security ook moet kijken naar de zorg over de betrouwbaarheid van de energievoorziening. Dit is met name van belang bij de bepaling van het 'rest' risico volgens de handreiking: het risico dat overblijft na het treffen van maatregelen. Denk daarbij na over bedrijven, die uit productie gaan als ze geen energie meer geleverd krijgen.
- Daarnaast wordt ook het APDO 2017 genoemd wat ingaat op de vraag hoe je moet omgaan met vertrouwelijke informatie en hoe die te beschermen. (Bron: https://www.defensie.nl/onderwerpen/militaire-inlichtingen-en-veiligheid/industrieveiligheid).
- De woorden "pragmatisch" en "proportioneel" uit de laatste presentatie van Technolution over de handreiking vragen om verduidelijking. Bijvoorbeeld toegespitst op de beide casussen in de handreiking: HEMS en transformatorhuis.
- CWI benadrukt dat cyber security ook vanuit het onderzoek moet worden bekeken, "bottom-up". Daarnaast geeft CWI aan dat er ook iets bestaat zoals "security by data absence".
- Afgesloten wordt met de wens van alle partijen dat we het thema cyber security gezamenlijk aanpakken en (mede) benaderen vanuit de decentrale toepassingen op energiegebied.

B. Energie-infrastructuur
Moderator en verslag: Tijs Wilbrink (TSE, digitalisering) en Yvonne Boerakker (UE).

Tijs heet de aanwezigen welkom en vraagt deelnemers wat de Topsector Energie en TKI Urban Energie samen met de sector zouden kunnen oppakken om te zorgen dat 'cyber security by design' het uitgangspunt wordt.

Cybersecurity by design
- Dat **cyber security by design** wenselijk is, wordt beaamd. Het later nog op orde zien te krijgen (rework) zal tot veel hogere kosten leiden. Ook de maatschappelijke kosten zullen hoog zijn door het uitvallen van bijvoorbeeld een netvlak. Het is dus wenselijk dat cyber security bij het ontwerp van producten/diensten/systemen wordt meegenomen, dus ook bij installaties die achter de meter geplaatst worden.
  - De kosten van 'rework' worden minder expliciet benoemd in de handleiding. Suggestie is om dit wel te doen in verband met bewustwording.
  - Tip voor de handreiking is de voorbeelden uit te breiden naar onderwerpen waarop veel jonge bedrijven actief zijn (bijvoorbeeld laadpalen).

Kennisdeling met andere industrieën en landen
- Is het **zinvol om kennis te delen** met andere industrieën (bijv. banking) of met andere landen. Niet in de vorm van een bijeenkomst (zoals vandaag), maar systematisch opgepakt.
- Er wordt gesproken wie er zou moeten **toezien** op het 'op orde zijn' van cyber security in de sector.
  - ACM wordt genoemd, de toezichthouder van de energiesector, maar specifiek voor het onderwerp cyber security is de mening van de deelnemers dat het Agentschap Telecom mogelijk een logischere partij is. Het toezicht mag best 'streng' zijn, want dit draagt er toe bij dat partijen hun security beter zullen organiseren.
  - Qua bewustwording is er ook nog wel wat te winnen bij de eindgebruikers – ook zij hebben een rol en verantwoordelijkheid.

Toenemende relatie tussen cybersecurity en IoT
- De cyber security bij laadpalen is nog niet 'op orde'. Wat zou helpen is dat gemeentes bij een aanbesteding cyber security als voorwaarde/criterium opnemen.
- Uitdagend is het als je alleen hardware leverancier bent. Na verkoop is er dan geen relatie meer met de klant. Wie is er dan verantwoordelijk voor updates? De producent? De leverancier?
- Voorstel is dat eisen gesteld worden aan apparaten die aan het energienet gekoppeld worden.

Benadering en programmering
- Er is ook behoefte aan analyses van de robuustheid op systeemniveau, dus rekening houdend met interacties in de keten.
- Hoe weeg je af wat de optimale balans is tussen enerzijds investeringen in het vermijden van aanvallen en anderzijds investeringen in resilience (het snel weer opkrabbelen).
- Laten we met zijn allen positief blijven, digitalisering brengt veel kansen, laat cyber crime niet het dominante thema worden.
- Een no regret maatregel is het zoneren van systemen. Hierdoor kun je bij een aanval de impact beperken.
- De discussie gaat nu erg over technische aspecten. Zouden we de discussie niet breder moeten voeren, bijvoorbeeld ook over de menselijke factor bij bedrijfsvoering en over opleidingen?

C. Bedrijven en bedrijventerreinen
Moderator en verslag: John Post (TSE, digitalisering) en Chris Vos (UE).

Slechts twee personen hadden de handreiking van Technolution gezien, dus is er niet ingegaan op de vraag of er nog iets ontbreekt in die handleiding. Drie conclusies uit de daaropvolgende discussie zijn als volgt.

1. **Digitalisering onvermijdelijk bij energietransitie**
   Alle sectoren zijn met elkaar verbonden, dit kan niet zonder digitalisering.

2. **Bewustzijn van dreigingen en de noodzaak van cyber security is een belangrijk verbeterpunt, zowel bij bedrijven als bij werknemers.**

   Bedrijven
   Er zijn nog altijd bedrijven die de noodzaak van cyber security niet inzien. Voorbeeld dat werd genoemd is de IOT infrastructuur die bij Havenbedrijf Rotterdam wordt opgezet. Deze moet zo snel mogelijk operationeel zijn zodat er geld kan worden verdiend, aan cyber security wordt pas achteraf aandacht besteed.

   Systemen moeten niet alleen de functie vervullen waarvoor ze worden ontworpen en aangeschaft, maar ook geschikt zijn voor onderhoud, beveiliging en updates.

   Werknemers
   Mensen in de organisatie zijn vaak de zwakste schakel in de beveiliging, met name voor bedrijven die hun cyber security goed op orde hebben. Te veel mensen zijn zich nog niet bewust van risico's, klikken bijvoorbeeld nog op links in phishing mails. Trainingen om awareness te verbeteren, bijvoorbeeld in de vorm van (rollen)spellen zijn naar verwachting een stuk effectiever dan een 10 pagina tellend instructieboek. Echter instructieboekjes zijn wel vaak volledi ger, belangrijk is om dit ook te waarborgen bij (rollen)spellen.

   Naast awareness is het ook belangrijk dat bedrijven en medewerkers weten hoe te handelen als er toch wat gebeurt: impact van "breaches" en aanvallen minimaliseren, wie moet de medewerker bellen als er wat raars binnenkomt?

3. **Door verder gaande IT/OT integratie kunnen zwakke schakels ontstaan. Verschillende leveranciers leveren eigen 'proprietary' IoT elementen.**
   De integratie van OT (operationele technologie) en IT (informatie technologie) creëert nieuwe mogelijkheden. Maar er zijn ook maatschappelijke, institutionele en ethische consequenties aan verbonden. De integratie is vaak een zwak punt, met name als deze integratie door verschillende organisaties heen loopt.

   Stel dat je per ongeluk een partij met slechte IT beveiliging koppelt aan de OT van jouw eigen fabriek. Dan loop je het risico, dat kernprocessen, productie en dienstverlening worden bedreigd in hun voortgang en/of hun kwaliteit.