Technolution B.V.
Burg. Jamessingel 1
P.O. Box 2013
2800 BD GOUDA
The Netherlands

T +31(0)182 59 40 00
E info@technolution.eu
I www.technolution.eu

MEMO RISICO REDUCTIE OVERZICHT

Dit rapport is tot stand gekomen in opdracht van RVO.nl op verzoek van de TKI Urban Energy.

Project:	Voorbeeldproject Transformatorhuisje		
Van:	Ontwerpteam Trafohuisje	Datum:	Dag-maand-jaar

Context

Naast het voorbeeld van een risico-analyse die binnen de handreiking al beschreven is (HEMS) is ter inspiratie ook een tweede voorbeeld opgenomen. Dit voorbeeld betreft een device dat in een transformatorhuisje hangt, waarmee de sensoren worden uitgelezen en de actuatoren worden aangestuurd. In het voorbeeld zijn niet alle mogelijke risico's verder uitgewerkt, maar er is voldoende uitgewerkt om te begrijpen hoe deze handreiking werkt.

Conclusies en aanbevelingen

Het device dat we gaan ontwikkelen, komt op een risicovolle plek te hangen. Het belangrijkste is dat middenspanningschakelaars op afstand bediend worden. Het op het verkeerde moment bedienen van de schakelaars kan een grote storing tot gevolg hebben. Als tweede heeft het device veel communicatie naar de buitenwereld. Dat betekent dus ook dat de buitenwereld bij ons device kan komen. De gevolgen hiervan zijn moeilijk in te schatten, maar zullen minimaal tot uitval leiden. Om deze reden zijn een aantal maatregelen getroffen. De kostenverhoging voor het project bedragen ongeveer € 70K. Hiermee besparen we een jaarlijks risicobedrag van ongeveer € 145K.
Het advies is dan ook om alle genoemde maatregelen te implementeren.

Geïdentificeerde risico's

De belangrijkste risico's bij het inzetten van het device zijn:

- onbetrouwbare leveranciers van het device;
- kwetsbaarheden door veroudering van de firmware van het device;
- fysieke en logische toegang tot het device;
- fysieke en logische toegang tot het communicatiekanaal.

Leveranciers kunnen 'geheime' achterdeurtjes in hun device aanbrengen. Deze achterdeurtjes kunnen vervolgens gebruikt worden om (een deel van) de energievoorziening plat te leggen. Gezien de kritische infrastructuur waarin deze devices zich bevinden, is het realistisch te denken dat andere naties geïnteresseerd zijn in toegang tot deze devices.

Verouderde firmware kan ervoor zorgen dat het device kwetsbaar is voor bijvoorbeeld ransomware.

Als een externe toegang krijgt tot het device of het communicatiekanaal kan dit leiden tot het ongeoorloofd schakelen van de MS-schakelaars of het falsificeren en injecteren van data (waardoor bijvoorbeeld de regelsystemen in de backoffice verkeerde outputwaarden genereren). Dit kan, naast de imagoschade van ons bedrijf, veel financiële schade opleveren.

Genomen maatregelen

De genomen maatregelen zorgen ervoor dat:

- het plaatsen van 'geheime' achterdeurtjes lastiger wordt;
- het verouderen van firmware wordt tegengegaan;
- de fysieke en logische toegang tot de systemen bemoeilijkt wordt;
- de gevolgen van een inbraak op één device beperkt blijven tot dat ene device.

Restrisico's

Omdat het wegnemen van alle risico's onbetaalbaar of zelfs onmogelijk is, zijn er nog een paar risico's die we op dit moment accepteren. Het doel is dat de overgebleven kwetsbaarheden alleen door zeer professionele hackers kunnen worden benut en het gevolg van zo'n aanval beperkt is.

Systeemoverzicht

Het device hangt in een transformatorhuisje en is via een modem verbonden met het OT-netwerk van de DSO. Het toegepaste netwerk wordt ingekocht bij een provider van 2G/3G/4G mobiele netwerken. De sensoren zijn via een lokaal ISM-net (wireless) verbonden met het device. De actuatoren zijn via een wired modbus verbonden.

Schakelen van de actuatoren moet op een voorgedefinieerde manier gebeuren. Het fout, te veel of niet schakelen kan ernstige schade toebrengen aan de infrastructuur.
De sensoren zijn minder belangrijk. Het uitvallen van de uitlezing is op korte termijn niet cruciaal. Indien er langere tijd geen uitlezingen zijn, kan dit tot problemen leiden.

Aanpak risicoanalyse

Het doel van een risicoanalyse is om te bepalen welke risico's er gelopen worden indien een te ontwikkelen systeem operationeel wordt. Een risico heeft altijd een waarschijnlijkheid van optreden en een impact als het risico optreedt. Bij het optreden kan dit het bedrijf schade opleveren (geld, imago). Door het nemen van maatregelen wordt de kans van optreden of de impact die het risico kent, verkleind. Ook een maatregel kost geld om deze te implementeren. En deze afweging moet worden gemaakt tijdens de analyse.

Voor het uitvoeren van de risicoanalyse worden de volgende stappen uitgevoerd:

1. identificatie van de bedrijfsmiddelen (systeemonderdelen, informatie, …) en de contacten naar de buitenwereld;
2. inventariseren van de risico's (uitgaande van een onbeveiligd systeem);
3. bepalen of risico's acceptabel zijn;
4. bepalen van de maatregelen die risico's reduceren (bestaande en nieuwe);
5. inventariseren van de restrisico's na het nemen van de maatregelen;
6. bepalen of de restrisico's acceptabel zijn (herhalen van stappen 4, 5 en 6 totdat alle restrisico's acceptabel zijn);
7. conclusie en bepalen van het advies.

De bovenstaande stappen zullen in een Risico Reductie Overzicht en in deze memo worden beschreven.

Risico Reductie Overzicht

Risico's

In dit hoofdstuk staan de initiële risico's van het systeem beschreven zonder dat er al tegenmaatregelen zijn genomen.

I1	Apparatuur van onbetrouwbare leveranciers
Omschrijving	De apparatuur die wordt gekocht, wordt vaak ontworpen en/of geproduceerd in landen die zich ook bezighouden met cyberaanvallen op kritische infrastructuur van Nederland. Het kan dan zijn dat in de apparatuur functionaliteit zit om deze landen toegang te laten krijgen tot het systeem en daarmee de energievoorziening kunnen beïnvloeden.
Kans	Kans: relatief klein, eens in de 10 à 20 jaar Impact: kan groot worden doordat energielevering stil kan komen te liggen
Financieel	Bij optreden kunnen de kosten tot € 1M oplopen. Jaarbedrag van dit risico is dan: € 75K
Maatregel	M1, M2, M3

I2	Veroudering van firmware
Omschrijving	Veroudering van firmware op de apparatuur zal leiden tot ongewenste kwetsbaarheden (bijvoorbeeld voor ransomware).
Kans	Kans: groot, eens in de 2 à 5 jaar Impact: middel
Financieel	Bij optreden: € 100K Jaarkosten: € 50K
Maatregel	M4, M5

I3	Toegang tot het interne netwerk van het transformatorhuisje
Omschrijving	Indien iemand fysiek of logisch toegang heeft tot het transformatorhuisje, kan hij via de bestaande netwerkaansluiting op het interne netwerk. Via deze aansluiting kan dan toegang worden verkregen tot alle andere devices en zelfs de backoffice. Het wissen van gegevens, het manipuleren van gegevens of het veranderen of starten van bepaalde functionaliteit behoort dan tot de mogelijkheden.
Kans	Kans: groot (2-5 jaar) Impact: groot
Financieel	Bij optreden: € 100K Jaarkosten: € 50K
Maatregel	M6

I4	Toegang tot communicatiekanaal
Omschrijving	Kwaadwillende personen kunnen fysiek of logisch toegang verkrijgen tot het communicatiekanaal tussen het transformatorhuisje en de backoffice. Het communicatiekanaal kunnen ze dan verstoren of als een *'man in the middle'* gaan meeluisteren en beïnvloeden.
Kans	Kans: middel (5 -10 jaar) Impact: groot
Financieel	Bij optreden: € 100K Jaarkosten: € 20K

I4	Toegang tot communicatiekanaal
Maatregel	M7, M8, M102, M103, M104

I5	Geen communicatie met de backoffice mogelijk
Omschrijving	Al dan niet door kwade opzet kan de communicatie tussen de backoffice en het transformatorhuisje wegvallen. Dit kan de energievoorziening in gevaar brengen.
Kans	Kans: groot (2 -5 jaar) Impact: groot
Financieel	Bij optreden: € 100K Jaarkosten: € 50K
Maatregel	M9

Maatregelen

In dit hoofdstuk staan de maatregelen beschreven die genomen worden naar aanleiding van de (initiële) set van risico's.

M1	Maak gebruik van open standaarden
Omschrijving	Door gebruik te maken van open standaarden creëer je keuzevrijheid van leverancier/producent van de apparatuur die ingekocht wordt. Deze vrijheid is nodig als apparatuur, waarvan achteraf is aangetoond dat deze 'geheime' achterdeurtjes bevat, uit te kunnen faseren.
Geadresseerd risico	I1
Financieel	Verwachting is dat dit geen extra kosten met zich meebrengt.
Restrisico	G1

M2	Audit ontwerp-, fabricage- en leveringsprocessen van de apparatuur
Omschrijving	Om te bepalen dat er geen ongewenste functionaliteit in de apparatuur zit, kunnen de ontwerp-, fabricage- en leveringsprocessen worden geaudit. Zo kan bijvoorbeeld de broncode van de firmware worden bekeken door een expert.
Geadresseerd risico	I2
Financieel	€ 20K (2 weken werk + inhuren specialist)
Restrisico	G1

M3	Uitvoeren penetratietest op de aangeschafte apparatuur
Omschrijving	Om te bepalen dat er geen ongewenste functionaliteit in de apparatuur zit, kunnen penetratietesten worden uitgevoerd. Hierbij gaan security-specialisten proberen het apparaat aan te vallen en rapporteren zij hun bevindingen.
Geadresseerd risico	I1
Financieel	€ 50K (5 weken werk + inhuren specialist)
Restrisico	G1

M4	Afspraken maken met leverancier over securitypatches

M4	Afspraken maken met leverancier over securitypatches
Omschrijving	Verouderde firmware bevat kwetsbaarheden en deze moeten gerepareerd (gepatched) worden, maar het is wel belangrijk dat deze patches ook beschikbaar zijn. Hiervoor zijn afspraken met de leverancier nodig.
Geadresseerd risico	I1
Financieel	Onduidelijk wat extra kosten zijn als dit als eis wordt meegenomen in de aanbesteding
Restrisico	G2

M5	Regelmatig firmware updaten
Omschrijving	Verouderde firmware moet gepatcht worden. Dit is een actie die op afstand kan worden uitgevoerd en regulier ingepland is.
Geadresseerd risico	I1
Financieel	Onduidelijk wat extra kosten zijn als dit als eis wordt meegenomen in de aanbesteding
Restrisico	G2

M6	Toegangsbeperkende maatregelen
Omschrijving	Door het aanbrengen van deugdelijk hang- en sluitwerk, toegangsdeuren, hekken et cetera wordt ongeoorloofde toegang tot het transformatorhuisje lastiger gemaakt. Daarnaast wordt een eventuele inbraak gemeld en kan daar direct op geacteerd worden.
Geadresseerd risico	I3
Financieel	€ 5K per transformatorhuisje
Restrisico	R1

M7	Gebruik een eigen APN
Omschrijving	Voor 2G/3G/4G wordt geen internet gebruikt, maar een eigen APN die is ingekocht bij de netwerkprovider. De netwerkprovider zorgt ervoor dat er geen berichten van en naar andere netwerken (bijvoorbeeld internet) loopt.
Geadresseerd risico	I4
Financieel	€ 50 per jaar extra ten opzichte van internet
Restrisico	R3

M8	Gebruik cryptografisch beschermde secure tunnel
Omschrijving	Gebruik een cryptografisch beschermde secure tunnel zoals TLS, IPSec of OpenVPN. Dit levert een extra laag van bescherming op, mocht de APN toch gecompromitteerd worden.
Geadresseerd risico	I4
Financieel	Geen extra kosten, omdat dit het configureren van bestaande functionaliteit is.
Restrisico	R3

M9	Zorg voor goedgedefinieerd en veilig ‘default gedrag’

M9	Zorg voor goedgedefinieerd en veilig 'default gedrag'
Omschrijving	Mocht de communicatie wegvallen, dan kan er niet gemeten worden en kan er ook niet op afstand worden geschakeld. Goedgedefinieerd 'default gedrag' van het device zorgt ervoor dat het transformatorhuisje goed en veilig blijft opereren.
Geadresseerd risico	I5
Financieel	Geen extra kosten
Restrisico	G4

AFGEWEZEN	Gebruik vaste communicatielijnen in plaats van draadloos
Omschrijving	Om te voorkomen dat er wordt ingebroken op de draadloze communicatie kunnen vaste lijnen gebruikt worden voor deze communicatie. Hierop is, mits goed aangelegd, veel lastiger in te breken.
Geadresseerd risico	I4
Financieel	
Reden afwijzing	Het is veel te kostbaar om dit uit te voeren. Daarnaast is het herstellen van een defecte kabel een zeer kostbare en tijdrovende inspanning.

Nieuwe risico's

In dit hoofdstuk staan de risico's beschreven die nog bestaan na het nemen van de (eerste) set van maatregelen.

R1	Langzame opvolging alarmering
Omschrijving	Ondanks alle toegangbeperkende maatregelen kan er nog steeds fysiek worden ingebroken in het transformatorhuisje. De tijd die het kost om de alarmering hiervan op te volgen kan door de aanvaller gebruikt worden om een aanval uit te voeren op het device.
Kans	Kans: middel (5-10 jaar) Impact: groot
Financieel	Bij optreden: € 100K Jaarkosten: € 50K
Maatregel	M101, M102, M103, M104

Maatregelen

In dit hoofdstuk staan de maatregelen beschreven om de nog niet geaccepteerde restrisico's te verminderen.

M101	Client isolation
Omschrijving	Het mobile communicatie netwerk (de APN) wordt zo ingericht dat een device alleen bij de backoffice kan en niet via de APN bij een andere device. De leverancier van de APN configureert dit in zijn firewall.
Geadresseerd risico	R1
Financieel	Geen extra kosten als de APN goed wordt aanbesteed
Restrisico	R2

M102	Client authenticatie

M102	Client authenticatie
Omschrijving	De backoffice accepteert alleen berichten van een device als deze voorzien zijn van een geldig echtheidskenmerk (digitale handtekening).
Geadresseerd risico	R1
Financieel	€ 50 per jaar per transformatorhuisje voor certificaten
Restrisico	R2

M103	Server authenticatie
Omschrijving	Een device accepteert alleen berichten (bijvoorbeeld schakelcommando's) van de backoffice als deze voorzien zijn van een geldig echtheidskenmerk (digitale handtekening).
Geadresseerd risico	R1
Financieel	€ 200 per jaar voor certificaten in backoffice
Restrisico	R2

M104	Timestamping
Omschrijving	De sensordata zullen worden voorzien van een timestamp zodat er geen oude berichten kunnen worden hergebruikt om foute data te injecteren.
Geadresseerd risico	R2
Financieel	€ 5K
Restrisico	R2

Nieuwe risico's

In dit hoofdstuk staan de risico's beschreven die nog bestaan na het nemen van de (eerste en tweede) set van maatregelen.

R2	Onveilig omgaan met cryptografische sleutels voor authenticatie
Omschrijving	Voor digitale handtekening zijn cryptografische sleutels nodig. Deze sleutels mogen niet in handen komen van kwaadwillenden.
Kans	Kans: middel (5-10 jaar) Impact: groot
Financieel	Bij optreden: € 100K Jaarkosten: € 50K
Maatregel	M201

R2	Onveilig omgaan met cryptografische sleutels voor de secure tunnel
Omschrijving	Voor de secure tunnel zijn cryptografische sleutels nodig. Deze sleutels mogen niet in handen komen van kwaadwillenden.
Kans	Kans: middel (5-10 jaar) Impact: groot
Financieel	Bij optreden: € 100K Jaarkosten: € 50K
Maatregel	M201

Maatregelen

In dit hoofdstuk staan de maatregelen beschreven om de nog niet geaccepteerde restrisico's te verminderen.

M201	Keymanagement implementeren
Omschrijving	Het creëren, distribueren, opslaan, gebruiken en verwijderen van sleutelmateriaal voor de backoffice en de devices wordt met behulp van zorgvuldig beschreven procedures uitgevoerd. Daarnaast is er een proces dat regelmatig het sleutelmateriaal ververst.
Geadresseerd risico	R1
Financieel	€ 50K voor het beschrijven van procedures en € 20K per jaar voor het uitvoeren hiervan.
Restrisico	G2/G3

Restrisico's

In dit hoofdstuk staan de uiteindelijk geaccepteerde risico's beschreven.

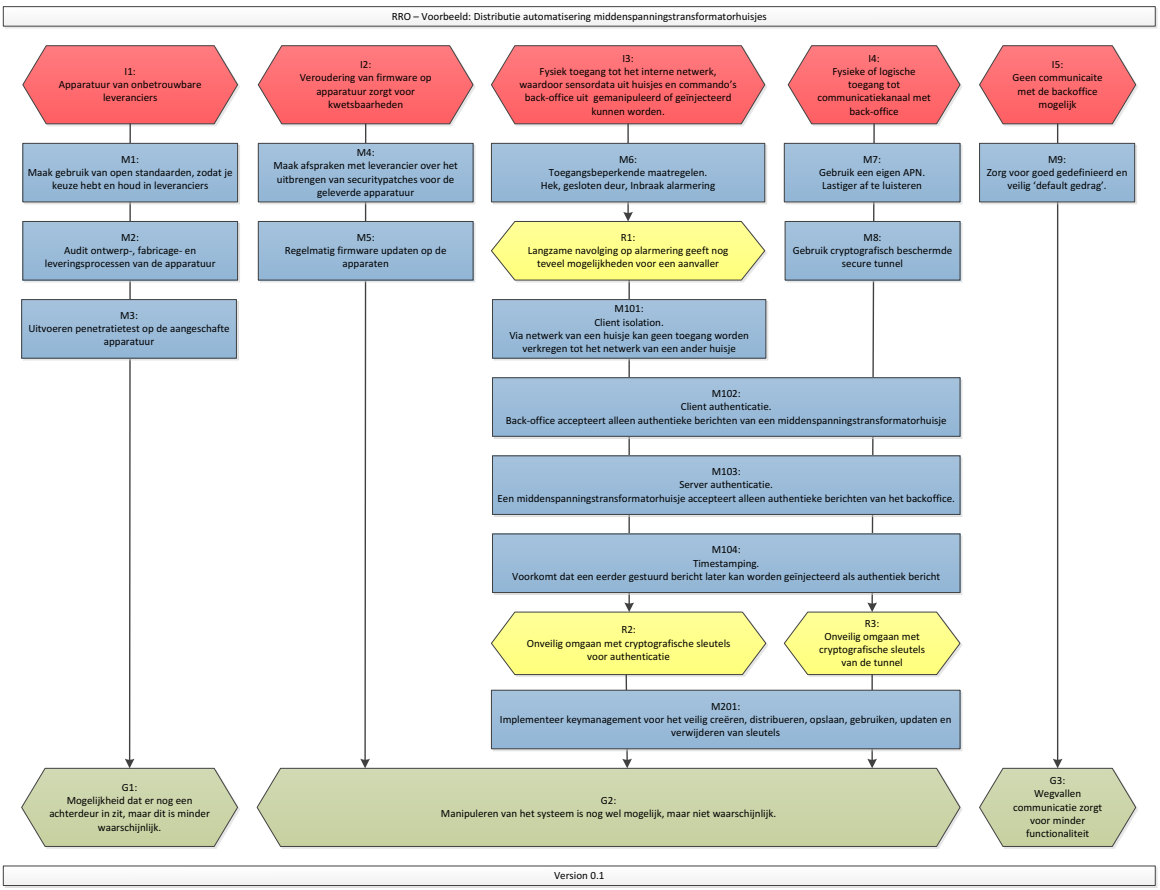
G1	Mogelijkheid dat er nog een 'achterdeur' in zit, maar dit is minder waarschijnlijk.
Omschrijving	Ondanks dat er van alles is geaudit en getest, kan er nog wel een 'achterdeur' in de code zitten. Door gebruik van open standaarden kan een alternatief worden gevonden.
Kans	Klein
Financieel	-

G2	Manipuleren van het systeem is nog wel mogelijk, maar niet waarschijnlijk
Omschrijving	Ondanks alle genomen maatregelen kan het systeem door zeer professionele hackers waarschijnlijk nog wel gekraakt worden.
Kans	Klein
Financieel	-

G3	Wegvallen communicatie zorgt voor minder functionaliteit
Omschrijving	Bij het wegvallen van de communicatie verliest de netbeheerder functionaliteit. Er kunnen geen meetdata worden verzameleden er kan niet op afstand worden geschakeld. Door de genomen maatregelen blijft de functie van het transformatorhuisje geborgd.
Kans	Klein
Financieel	-

RRO-diagram

In de onderstaande afbeelding is de grafische representatie van de risicoanalyse uit deze memo zichtbaar.


RRO – Voorbeeld: Distributie automatisering middenspanningstransformatorhuisjes
I1: Apparatuur van onbetrouwbare leveranciers
I2: Veroudering van firmware op apparatuur zorgt voor kwetsbaarheden
I3: Fysiek toegang tot het interne netwerk, waardoor sensordata uit huisjes en commando's back-office uit gemanipuleerd of geïnjecteerd kunnen worden.
I4: Fysieke of logische toegang tot communicatiekanaal met back-office
I5: Geen communicaite met de backoffice mogelijk
M1: Maak gebruik van open standaarden, zodat je keuze hebt en houd in leveranciers
M4: Maak afspraken met leverancier over het uitbrengen van securitypatches voor de geleverde apparatuur
M6: Toegangsbeperkende maatregelen. Hek, gesloten deur, Inbraak alarmering
M7: Gebruik een eigen APN. Lastiger af te luisteren
M9: Zorg voor goed gedefinieerd en veilig 'default gedrag'.
M2: Audit ontwerp-, fabricage- en leveringsprocessen van de apparatuur
M5: Regelmatig firmware updaten op de apparaten
R1: Langzame navolging op alarmering geeft nog teveel mogelijkheden voor een aanvaller
M8: Gebruik cryptografisch beschermde secure tunnel
M3: Uitvoeren penetratietest op de aangeschafte apparatuur
M101: Client isolation. Via netwerk van een huisje kan geen toegang worden verkregen tot het netwerk van een ander huisje
M102: Client authenticatie. Back-office accepteert alleen authentieke berichten van een middenspanningstransformatorhuisje
M103: Server authenticatie. Een middenspanningstransformatorhuisje accepteert alleen authentieke berichten van het backoffice.
M104: Timestamping. Voorkomt dat een eerder gestuurd bericht later kan worden geïnjecteerd als authentiek bericht
R2: Onveilig omgaan met cryptografische sleutels voor authenticatie
R3: Onveilig omgaan met cryptografische sleutels van de tunnel
M201: Implementeer keymanagement voor het veilig creëren, distribueren, opslaan, gebruiken, updaten en verwijderen van sleutels
G1: Mogelijkheid dat er nog een achterdeur in zit, maar dit is minder waarschijnlijk.
G2: Manipuleren van het systeem is nog wel mogelijk, maar niet waarschijnlijk.
G3: Wegvallen communicatie zorgt voor minder functionaliteit
Version 0.1