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 HEMS		
Van:	Ontwerpteam HEMS	Datum:	dag-maand-jaar

Context

Binnen de handreiking wordt eveneens dit voorbeeld gebruikt ter illustratie.

Een HEMS is een sturingssysteem dat in huis wordt geplaatst, primair om het binnenklimaat en comfort te regelen door aansturing van installaties (bijvoorbeeld warmtepomp, ventilatie). In de toekomst wordt verwacht dat de functionaliteit van HEMS verder uitgebreid zal worden, en dat er naast optimalisatie van energiegebruik en comfort op gebouwniveau, ook interactie zal zijn met energiemarkten (bijvoorbeeld door het aanbieden van flexibiliteit voor balanshandhaving, vermijden van netcongestie of portfolio optimalisatie van de programma verantwoordelijke partij). Een HEMS is in dat geval niet alleen aangesloten op installaties in huis, maar ook op een backoffice van de HEMS-leverancier en/of een aggregator.

Het apparaat is aan de ene kant aangesloten op een backoffice van de HEMS-leverancier of van de aggregator, en aan de andere kant op sensoren en energie gebruikende installaties in huis.

Conclusies en aanbevelingen

Geïdentificeerde risico's

Om het HEMS goed in het veld te zetten, zal een bepaald niveau van harding moeten worden geïmplementeerd. Het gaat voornamelijk over het beschermen tegen hackers en het voorkomen dat het HEMS een toegangspunt voor hackers wordt om op een thuisnetwerk te komen.

Genomen maatregelen

De maatregelen die genomen moeten worden, zijn (standaard)manieren om te voorkomen dat iemand van buitenaf ongewenst op het HEMS komt. Daarnaast zullen een aantal aanbevelingen in de gebruikershandleiding komen te staan, die moeten voorkomen dat het HEMS verkeerd kan worden gebruikt, of die moeten voorkomen dat als het HEMS toch gehackt wordt, dit grote gevolgen heeft.

Restrisico's

Het blijft voor een deel de verantwoording van de installateur/gebruiker om het HEMS op een veilige en voor de buitenwereld afgeschermde plek te hangen. Hier zijn we afhankelijk van. Wel zal er een methode worden ingebouwd om de firmware (OS en functionaliteit) remote te updaten. Hiermee kunnen we dan eventuele problemen oplossen en updates automatisch uitrollen naar de HEMS'en.

Ons advies is wel om tweemaal per jaar de firmware van het HEMS te updaten. Hiervoor zullen we actief updates aanbieden aan de gebruiker. Op deze manier kunnen we proactief problemen voorkomen.

De kosten bij het optreden van een (rest)risico zijn beperkt, maar de imagoschade voor het bedrijf kan zo groot zijn dat we moeten kunnen aantonen dat wij alles hebben gedaan om het te voorkomen. Een slecht naam kan betekenen dat wij geen HEMS'en meer kunnen verkopen.

Systeemoverzicht

Een HEMS is bedoeld om de apparatuur binnen een huishouden zo te regelen dat het efficiëntste energieverbruik wordt gerealiseerd. Het HEMS bestuurt aan de ene kant alle installaties (zoals boiler, warmtepomp, ventilatie, en in de toekomst mogelijk ook EV-lader, warmteopslag , elektriciteitsopslag en is aan de nadere kant verbonden met een backoffice van de HEMS-leverancier en/of een aggregator.

Het HEMS is aan de apparatuur verbonden door middel van: ZigBee, RS485, IP (wifi), Dig I/O. De interface naar de gebruiker voor het besturen van het HEMS gaat via een webinterface. De interface naar de energieleverancier gaat via het standaardinternet over het thuisnetwerk van de gebruiker (wifi of wired).

Aanpak risicoanalyse

Het doel van een risicoanalyse is om te bepalen welke risico's er gelopen worden indien er een te ontwikkelen systeem operationeel wordt. Een risico heeft altijd een kans van optreden en een impact als het risico optreedt. Bij het optreden kan dit de leverancier (of gebruiker) 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 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	Afluisteren van privacygevoelige gegevens
Omschrijving	Het HEMS gaat allerlei informatie over het huishouden verzamelen. Deze informatie zal als gevoelige informatie worden bestempeld. Kwaadwillinden kunnen deze informatie afluisteren en er verkeerde dingen mee doen.
Kans	Middel: eens in de 5 à 10 jaar
Financieel	Bij optreden: • boete privacyautoriteit: € 200K • derving klanten door imagoschade: € 400K Jaarkosten: € 120K
Maatregel	M2

I2	Beïnvloeden van gedrag door manipulatie en injectie van berichten
Omschrijving	Het HEMS regelt verschillende huishoudelijke installaties. Indien een kwaadwillinde toegang krijgt tot het HEMS kan deze de apparatuur bedienen en verkeerde dingen laten doen. Dit kan gevolgen hebben voor de apparatuur zelf, maar ook zorgen voor een overbelasting van het energienetwerk (indien er meerdere HEMS'en tegelijkertijd worden overgenomen.
Kans	Groot (2-5 jaar)
Financieel	Bij optreden: € 300K Jaarkosten: € 150K
Maatregel	M2

I3	Inbreken op device zorgt voor functieverlies
Omschrijving	Het HEMS regelt verschillende huishoudelijke installaties. Indien een kwaadwillinde toegang krijgt tot het HEMS kan deze de gewenste functies aan/-uitschakelen.
Kans	Groot: 2-5 jaar
Financieel	Bij optreden: € 100K Jaarkosten: € 50K
Maatregel	M2, M3

I4	Inbreken op het HEMS en het gebruiken om andere systemen van gebruiker aan te vallen (bijvoorbeeld thuisbankieren)
Omschrijving	Het HEMS hangt in het thuisnetwerk van de gebruiker. Het is dus goed mogelijk dat via kwetsbaarheden in het OS (in ons geval Linux) andere devices in het netwerk kunnen worden bereikt.
Kans	Middel: 5-10 jaar
Financieel	Bij optreden: • schadeclaims: € 200K • derving klanten door imagoschade: € 400K Jaarkosten: € 120K
Maatregel	M1, M2, M3

I5	Verlies van functie door uitval van communicatie
Omschrijving	Het HEMS is afhankelijk van goede communicatie met een aggregator. Zonder deze communicatie kan het zijn dat de functionaliteit niet goed werkt of zelfs een averechts effect heeft op de gewenste functionaliteit.
Kans	Groot: 2-5 jaar

I5	Verlies van functie door uitval van communicatie
Financieel	Bij optreden: € 100K Jaarkosten: € 50K
Maatregel	M4

Maatregelen

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

M1	Het HEMS op een gescheiden netwerk aansluiten, bijvoorbeeld het gastennetwerk op een wifirouter
Omschrijving	Het is verstandig om alle apparatuur en het HEMS aan te sluiten op een gastennetwerk. Hiermee kunnen de apparatuur en het HEMS niet op het gewone netwerk van de gebruiker komen. Dit zal in de handleiding worden beschreven.
Geadresseerd risico	I4
Financieel	Geen: gastennetwerken zijn configureerbaar op wifirouter van klant.
Restrisico	R2

M2	TLS-tunnels gebruiken voor de IP-verbindingen tussen het HEMS en de backoffice
Omschrijving	Om te voorkomen dat kwaadwillinden niet de communicatie tussen de backoffice en het HEMS kunnen afluisteren of beïnvloeden, zal het IP-verkeer tussen de leverancier en het HEMS via secure TLS-tunnels worden geregeld. Deze maatregel reduceert het de mogelijkheden die een hacker heeft om het HEMS van buitenaf aan te vallen. Hiervoor zullen alle HEMS'en een eigen (geheime) sleutel krijgen en een publieke sleutel van de backoffice bezitten.
Geadresseerd risico	I1, I2, I3, I4
Financieel	€ 20K extra aan inrichtingskosten voor backoffice
Restrisico	R1, R2

M3	Hardening van het HEMS
Omschrijving	We zullen het HEMS zo veel mogelijk beschermen tegen aanvallen van buitenaf. We doen dit door: • niet-gebruikte netwerkpoorten uit te zetten; • gebruikerstoegang middels wachtwoorden; • niet-gebruikte functies op lokale poorten (bijvoorbeeld USB) dichtzetten.
Geadresseerd risico	I3, I4
Financieel	Geen: dit is een kwestie van het juist inrichten van beschikbare middelen.
Restrisico	R2

M4	Terugvallen op gedefinieerd standalone gedrag van het HEMS als communicatie uitvalt

M4	Terugvallen op gedefinieerd standalone gedrag van het HEMS als communicatie uitvalt
Omschrijving	Bij het wegvallen van de stuursignalen vanuit de aggregator zullen we als eerste terugvallen op oudere waarden (er wordt bij een update van de waarde niet alleen de huidige waarde, maar ook een aantal verwachte waarden in de toekomst meegestuurd). Als er geen waarden meer zijn om op te regelen, is er een standaard (standalone) gedrag ingebouwd. Het standalone gedrag is via de configuratie in te stellen.
Geadresseerd risico	I5
Financieel	Geen
Restrisico	G4

AFGEWEZEN	Geen gebruikmaken van de infrastructuur van de gebruiker
Omschrijving	Door helemaal los te communiceren van het netwerk van de gebruiker, los je veel potentiële bedreigingen op. We denken dan aan een eigen CUG-communicatiekanaal naar de aggregator (eigen simkaart). Deze oplossing is echter kostenverhogend en zorgt ook voor maandelijkse kosten. Hierdoor is het HEMS niet meer interessant voor de gebruiker.
Geadresseerd risico	I1, I2, I3, I4
Financieel	Niet van toepassing
Reden afwijzing	Kostenverhogend voor de gebruiker, waardoor het HEMS niet meer verkocht kan worden.

Nieuwe risico's

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

R1	Na verloop van tijd zijn de gebruikte cryptografische protocollen en sleutellengtes verouderd
Omschrijving	Cryptografische protocollen worden regelmatig geüpdatet en verbeterd. Cryptografische sleutels gebruikt bij encryptie verouderen. Dit zal uiteindelijk leiden tot een makkelijk kraakbare secure tunnel.
Kans	Middel: 5-10 jaar
Financieel	Bij optreden: € 600K Jaarkosten: € 120K
Maatregel	M5, M6

R2	Veroudering van firmware op het HEMS zorgt voor kwetsbaarheden
Omschrijving	In ieder stuk software zitten kwetsbaarheden. Zolang ze niet ontdekt zijn, is er niets aan de hand. Maar aangezien we een standaard-OS (Linux) gebruiken, zullen in de loop van de tijd kwetsbaarheden worden ontdekt. Hiermee kan dan dus toegang worden verkregen tot ons HEMS.
Kans	Groot: 2-5 jaar
Financieel	Bij optreden: € 600K Jaarkosten: € 120K
Maatregel	M5

Maatregelen

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

M5	Regelmatig updaten van firmware en sleutels in HEMS
Omschrijving	Om te voorkomen dat kwetsbaarheden in het OS en de secure tunnel gebruikt kunnen worden door kwaadwillinden, moet de software (en het OS) regelmatig kunnen worden geüpdatet. Er zal tweemaal per jaar automatisch een (security)update worden uitgerold naar alle HEMS'en. Van deze update wordt ook gebruikgemaakt om het sleutelmateriaal op het HEMS te verversen.
Geadresseerd risico	R1, R2
Financieel	Jaarkosten: € 40K voor maken en distribueren van updates
Restrisico	G1, G2, G3

M6	Regelmatig updaten van crypto-instellingen en sleutels van server in backoffice
Omschrijving	Om te voorkomen dat kwetsbaarheden in het OS en de secure tunnel gebruikt kunnen worden door kwaadwillinden, moet de software (en het OS) regelmatig kunnen worden geüpdatet. Er zal tweemaandelijks een (security)update worden uitgerold op de backoffice. Daarnaast wordt jaarlijks het sleutelmateriaal op de backoffice ververst.
Geadresseerd risico	R1
Financieel	Jaarkosten: € 20K voor updaten backoffice
Restrisico	G2, G3

Restrisico's

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

G1	Afluisteren en beïnvloeden is nog steeds mogelijk, maar wel met aanzienlijk meer inspanning.
Omschrijving	De verwachting is dat het afluisteren van de datacommunicatie zo moeilijk is, dat de standaardhacker dit niet lukt. Daarnaast is het, indien we ontdekken dat het HEMS afgeluisterd wordt, mogelijk om snel updates uit te voeren.
Kans	Klein
Financieel	Middel (vooral imagoschade)

G2	Inbreken op het HEMS is nog steeds mogelijk, maar wel met aanzienlijk meer inspanning.
Omschrijving	De verwachting is dat het inbreken in het HEMS zo moeilijk is dat de standaardhacker dit niet lukt. Daarnaast is het, indien we ontdekken dat er in het HEMS ingebroken kan worden, mogelijk om snel updates uit te voeren.
Kans	Klein
Financieel	Middel (vooral imagoschade)

G3	Hacken van andere systemen via het HEMS is nog steeds mogelijk door gebrek aan controle op de netwerkscheiding.
Omschrijving	We kunnen niet meer doen dan het in de gebruikshandleiding adviseren.
Kans	Niet van toepassing
Financieel	Niet van toepassing

G4	Bij uitval van communicatie kan het HEMS niet optimaal functioneren.
Omschrijving	We hebben een standalone stand gemaakt. Deze gaat automatisch in werking zodat het aansturen van de apparaten doorgaat. Details van deze regeling kunnen worden bijgesteld door de gebruiker. Op deze manier hebben we voldoende gedaan om deze situatie te dekken.
Kans	Middel
Financieel	Niet van toepassing

G5	Black-out uitlokken door bij meerdere huishoudens grootverbruikers aan/uit te schakelen
Omschrijving	Als het aantal aangesloten HEMS'en en het aantal te controleren apparaten groot wordt, zou een hacker door het controleren van veel HEMS'en tegelijkertijd kunnen zorgen voor een situatie waar alle (grote) verbruikers op hetzelfde moment aan of juist uit schakelen.
Kans	Klein
Financieel	Vooral imagoschade

RRO-diagram

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