Technische informatie

PUBLIC CYBER SECURITY

Richtlijnen voor een veilige communicatie met PV-installaties

Inhoudsopgave

1 Toelichting bij dit document

1.1 Geldigheid

Dit document geldt voor alle producten, die binnen een netwerk voor PV-installatiecommunicatie op elkaar zijn aangesloten en direct of indirect via communicatiemedia met het Internet kunnen worden verbonden.

Dit document is een aanvulling op de documenten die met de afzonderlijke producten worden meegeleverd en vervangt geen enkele van de ter plaatse geldende normen of richtlijnen. Lees de met het product meegeleverde documenten aandachtig en neem deze in acht.

1.2 Doelgroep

De informatie in dit document is bedoeld voor installateurs en exploitanten van PV-installaties met SMA omvormers evenals voor planners van PV-installaties.

1.3 Aanvullende informatie

Wilt u meer informatie? Bezoek dan de websites van veiligheidsorganisaties zoals:

Veiligheidsorganisatie	Document	Hyperlink
BSI (Bundesamt für Sicherheit in der Informationstechnik) [Bonduits Federaal Bureau voor Informatiebeveiliging]	Sichere Passwörter in Embedded Devices [Veilige wachtwoorden in embedded devices]	https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_069.pdf?__blob=publicationFile
BSI (Bundesamt für Sicherheit in der Informationstechnik) [Bonduits Federaal Bureau voor Informatiebeveiliging]	Industrial Control System Security: Top 20 Bedrohungen und Gegenmaßnahmen v1.2 [Top 10 Bedreigingen en tegenmaatregelen v1.2]	https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_005.pdf?__blob=publicationFile&v=4
NIST (National Institute of Standards and Technology, USA) [NIST: Nationaal Instituut voor Normen en Technologie, federale overheid USA]	10 Basic Cybersecurity Measures [10 fundamentele cyberveiligheidsmaatregelen]	https://ics-cert.us-cert.gov/sites/default/files/documents/10_Basic_Cybersecurity_Measures-WaterISAC_June2015_S508C.pdf

Links naar pagina's met meer informatie vindt u op www.SMA-Solar.com:

Documenttitel	Documenttype
"Webconnect-installaties in Sunny Portal"	Gebruiksaanwijzing
"SMA SPEEDWIRE VELDBUS"	Technische informatie
"Installatiebewaking - SMA beveiligings- en wachtwoordconcept bij d.m.v. wachtwoord beveiligde PV-installaties met Bluetooth® Wireless Technology"	Technische beschrijving

Documenttitel	Documenttype
"SMA Modbus®-Schnittstelle" (SMA Modbus®-interface)	Technische informatie
"SunSpec® Modbus®-Schnittstelle" (SunSpec® Modbus®-interface)	Technische informatie

2 Inleiding

De exploitant of onderhoudsmedewerkers kunnen de meeste bedrijfshandelingen zoals het toezien op, en het aansturen van zonnestroominstallaties uitvoeren zonder dat datacommunicatie via de infrastructuur van het openbare internet vereist is. Deze bedrijfshandelingen – waartoe worden gerekend: de datacommunicatie tussen exploitanten van installaties, tussen onderhoudsmedewerkers en PV-omvormers, dataloggers en bijkomende voorzieningen – zijn mogelijk bij toepassing van lokale beeldschermen, toetsenborden of de lokale toegang van de webserver van een apparaat of toestel in het lokale netwerk (LAN) van de zonnestroominstallatie of vanuit het eigen huis.

In andere toepassingssituaties van zonnestroominstallaties maken dergelijke voorzieningen deel uit van het globale communicatiesysteem dat gebaseerd is op het gebruik van de infrastructuur van het internet.

Datacommunicatie via het internet is een moderne, goedkoop toe te passen en klantvriendelijke manier om eenvoudig toegang te krijgen tot bijvoorbeeld onderstaande moderne toepassingen:

- Cloud-platforms (bijv. Sunny Portal)
- Smartphones of andere mobiele apparatuur (iOS- of Android-apps)
- SCADA-systemen, waarmee van elders verbinding wordt gemaakt,
- interfaces voor netbeheer

Als alternatief kunnen ook bepaalde, beveiligde communicatie-interfaces worden toegepast. Dergelijke mogelijkheden komen overigens niet meer overeen met de huidige stand der techniek. Toepassing ervan is duur (door de bijzondere communicatie-interfaces, aparte (inter)nationale communicatienetwerken en dergelijke).

Bij toepassing van de infrastructuur van het internet komen de met dat internet verbonden systemen terecht in een principieel onveilige omgeving. Potentiële belagers zoeken doorlopend naar kwetsbare systemen. Zij hebben gebruikelijk criminele, terroristische of bedrijfsvoering verstorende doelen. Een datacommunicatiesysteem mag niet met het internet worden verbonden zonder dat maatregelen zijn getroffen om de zonnestroominstallaties en andere systemen te beschermen tegen dergelijk misbruik.

Om zonnestroominstallaties effectief te beschermen tegen ongewenste benadering door onbevoegden (zoals criminelen of geheime diensten) moet u het lokale netwerk zo 'schoon' en gesloten mogelijk houden. Maakt u verbinding tussen een zonnestroominstallatie of een soortgelijk systeem? Dan is de exploitant of hun netwerkbeheerder verantwoordelijk voor het onderstaande:

- kennis van alle toestellen die via het lokale netwerk onderling communiceren,
- kennis van de communicatie-eisen en -functies van alle toestellen,
- kennis van alle mogelijke zwakke punten van alle toestellen,
- kennis van alle accounts die zich toegang tot het systeem willen verschaffen,
- kennis van de mogelijkheden om de toegang tot het lokale netwerk en tot de toestellen in te perken (bijvoorbeeld door het gebruik van wachtwoordbeveiliging),
- het installeren en configureren van alle vereiste veiligheidmaatregelen betreffende cyber-veiligheid (routers, firewall, proxy-servers),
- het inspecteren en eventueel verbeteren van de veiligheidmaatregelen qua actualiteit en geschiktheid.

Wordt aan deze voorwaarden voldaan? Dan kunt u ervan uitgaan dat de zonnestroominstallatie zodanig in een systeem functioneert alsof die installatie "achter een muur" staat. Directe toegang van buitenaf is dan rechtstreeks niet mogelijk.

De meeste industriële communicatiesystemen maken in overwegende mate gebruik van gestandaardiseerde veldbuscommunicatieprotocollen. Om die reden is een "achter een muur"-strategie absoluut noodzakelijk omdat de meeste veldbussystemen geen ingebouwde veiligheidmechanismen hebben en dus door aanvullende maatregelen moeten worden beveiligd. Dat geldt ook voor de beide veldbuscommunicatieprotocllen SMA Data2+ en Modbus TCP welke in de communicatieapplicatie van SMA Solar Technology AG worden toegepast. In geval van het communicatieprotocol Data2+ voorziet een wachtwoordbeveiliging in bescherming van de producten van SMA. Een uitzondering daarop is het WAN-communicatieprotocol Webconnect dat een veilige verbinding biedt met versleuteling tussen de beide eindstations van die verbinding. Webconnect wordt echter niet toegepast in lokale netwerken. Webconnect is namelijk geconcipieerd voor een veilige communicatie via internet tussen PV-omvormers of dataloggers en Sunny Portal of mobiele applicaties.

i Veiligheidrisico door gebruik van Modbus TCP

Modbus TCP is in de meeste producten van SMA als openbare interface voor de klanten beschikbaar. Modbus TCP kan niet zonder meer veilig gegevens via het internet versturen. Binnen een zonnestroominstallatie kan het ontbreken van een mogelijkheid tot authenticeren in Modbus TCP aanleiding zijn voor een potentieel veiligheidrisico. Om die reden is de functie Modbus TCP standaard gedeactiveerd in de producten van SMA. Desgewenst kan Modbus TCP worden geactiveerd binnen de gebruikersgroep Installateurs. Activeer Modbus TCP echter niet lichtzinnig, maar omgeef die altijd met aanvullende maatregelen om het volledige systeem te beschermen.

3 Risico's

Via het internet onderling verbonden systemen, die niet speciaal worden beveiligd, kunnen worden misbruikt om in een netwerk van een klant binnen te dringen (dus tot achter de internetrouter). Op die manier kunnen bijna alle op het netwerk aangesloten toestellen worden aangevallen. Hebben potentiële belagers eenmaal de mogelijkheid te pakken om een netwerk binnen te dringen? Dan treden onderstaande bedreigingen op:

- het bespioneren op gebruikersnamen, wachtwoorden en andere vertrouwelijke gegevens;
- toegang krijgen op de in het netwerk opgenomen toestellen om botnet-agenten te installeren of om "Cross site scripting"-aanvallen uit te voeren;
- toegang krijgen op de in het netwerk opgenomen toestellen om het gedrag daarvan te manipuleren (bijvoorbeeld door middel van intermediaire aanvallers ("Man in the Middle") of 'Replay'-aanvallen);
- toegang krijgen op de in het netwerk opgenomen toestellen om doorgezonden gegevens te manipuleren en zo reacties van hogere orde-systemen uit te lokken;
- toegang krijgen op de in het netwerk opgenomen toestellen om het gebruikersgedrag te evalueren (bijvoorbeeld bij het voorbereiden van inbraak en diefstal);
- toegang krijgen op de in het netwerk opgenomen toestellen om het gebruikersgedrag te analyseren voor gepersonaliseerde reclame.

De mogelijke gevolgen daarvan zijn:

- financieel verlies door:
  - uitblijvende inkomsten uit energieopwekking,
  - onjuiste toepassing van tarieven voor teruglevering naar het elektriciteitnet of voor opgenomen energie voor eigen gebruik,
  - beschadiging van toestellen,
- diefstal van identiteit,
- negatieve effecten op de stabiliteit van het openbare stroomnet (mits het aantal en de omvang van de gecompromitteerde systemen daarvoor voldoende groot is),
  - verlies van de vergunning tot inkoppeling op het openbare stroomnet
  - juridische gevolgen

4 Oplossingen

Om aan de basiseisen voor een veilig systeem te voldoen, adviseert SMA Solar Technology AG een minimaal aantal veiligheidvoorzieningen. In combinatie met de veiligheidsfunctie in de producten van SMA is op die manier een passend veilig bedrijf van de zonnestroominstallatie mogelijk. Neem onderstaande regels voor een veilig bedrijf van een zonnestroominstallatie in acht:

- Verzeker uzelf ervan dat firewall en proxy-server correct zijn geconfigureerd.
- Verzeker uzelf ervan dat de fysiek gescheiden netwerksegmenten toepast voor de netwerkverbindingen tussen de onderdelen van de zonnestroominstallatie (scheiding tussen de netwerken thuis en op kantoor).
- Verzeker uzelf ervan dat onbevoegden fysiek noch virtueel toegang kunnen krijgen tot producten van SMA en van anderen via de met het netwerk verbonden toestellen.
  - Voorkom het fysiek manipuleren van het systeem vanuit het lokale netwerk.
  - Voorkom het gebruik van spionerende apparaten op het lokale netwerk (bijvoorbeeld door gebruik van vreemde of onbekende WLAN-toegangspunten).
  - Voorkom het aflezen van de registratiecode waarmee registratie in Sunny Portal mogelijk is. Die code is gebruikelijk op een product aangebracht. De registratiecode is een toestelspecifiek, willekeurig samengestelde sleutel die fysieke toegang tot een product bewijst.
  - Bewaar de vertrouwelijkheid van systeemdetails (zoals de soort of typeaanduiding van toestellen, wachtwoorden, registratiecodes) op basis van het principe: "Zoveel als nodig is maar zo min mogelijk". Houd deze informatie zo geheim mogelijk.
  - Houd alle wachtwoorden, de registratiecode van Webconnect en de SMA Grid Guard-code geheim. Geautoriseerde installateurs maken gebruik van de Grid Guard-code om zich te identificeren teneinde systeemparameters, die relevant zijn voor het elektriciteitnet, te kunnen wijzigen.
  - Inspecteer periodiek de systeemlogboeken die voor de IT-veiligheid relevant zijn.
  - Sluit geen onbekende geheugenmedia (zoals USB-geheugenpennen, SD- of CF-geheugenkaarten) op uw apparaten of toestellen aan. Inspecteer voorafgaand aan het gebruik dergelijke media op de aanwezigheid van eventuele schadelijke programma's.
  - Gebruik geen onbekende of onveilige apparaten of toestellen in uw netwerk.
  - Maak regelmatig – als operationele reserve – backupbestanden van uw systeem.
  - Creëer betrouwbare oplossingen en procedures voor de relevante systemen. Een eenvoudige oplossing: zorg dat voor elk kritisch systeemelement een op vooraf geconfigureerd vervangend onderdeel als reserve aanwezig is.
- Verzeker uzelf ervan dat u niet aan port forwarding doet of soortgelijke functie biedt tussen een WAN en uw lokale netwerk.

  - Wilt u toegang van buitenaf? Maak dan verbinding via een VPN of via Webconnect. Elke verbinding van elders (onderhoud, support, directe verkoop, netbeheer) moet uitsluitend via dergelijke veilige communicatiemethoden lopen.

- Verzeker uzelf ervan dat u in de firewall alle niet gebruikte IP-poorten blokkeert. Zorg dat niet gebruikte IP-poorten van andere systemen buiten werking zijn gesteld. Elke openstaande IP-poort vormt een potentieel risico dat iets of iemand uw systeem binnendringt.
- Verzeker uzelf ervan dat u gebruik maakt van een SFTP-server (beveiligde FTP-server) en dat u geen gebruik maakt van een onbeveiligde externe FTP-server. FTP-servers dragen in de regel bestanden onversleuteld over. Bij toepassing van SFTP-servers worden daarentegen alle bestanden versleuteld op het moment van overdracht.
- Verzeker uzelf ervan dat u veilige externe e-mailservers gebruikt voor uw e-mailverkeer. De meeste aanbieders van e-maildiensten staan tegenwoordig uitsluitend nog TLS-toegang (of een soortgelijke toegang) toe.
- Verzeker uzelf ervan dat producten die niet afkomstig zijn van SMA Solar Technology AG veilig zijn. Onveilige producten kunnen aanvallers een ongewenste toegang verschaffen tot uw lokale netwerk.
  - Houd uw antivirus- en antimalwaresoftware altijd actueel evenals de toegangsregels voor uw routers en firewall.
  - Sta uitsluitend de absoluut noodzakelijke uitzonderingen op de veiligheidmechanismen toe.
  - Volg de adviezen betreffende actualisering van de veiligheidfuncties van het toegepaste besturingsysteem op.
- Verzeker uzelf ervan dat verleende toegangsrechten tot de zonnestroominstallatie op een eenduidige en heldere manier zijn georganiseerd (dus: welke gebruiker krijgt welke toegangsrechten).
  - In de meeste gevallen volstaat de gebruikersgroep 'Gebruikers' voor het toezicht op de zonnestroominstallatie. Zet uitsluitend de gebruikersroep 'Installateurs' in voor het in bedrijf stellen en parameteriseren van het product.
- Verzeker uzelf ervan dat alle af fabriek ingestelde wachtwoorden uiterlijk op het moment van inbedrijfstelling zijn gewijzigd in zelfbedachte wachtwoorden. Af fabriek ingestelde wachtwoorden zijn alom bekend.
- Verzeker uzelf ervan dat u uitsluitend wachtwoorden toepast die in overeenstemming zijn met de algemeen geldende richtlijnen.
  - Een wachtwoord moet minstens acht karakters tellen en bestaan uit letters, cijfers en bijzondere tekens (!=?#+-:;*).

  - Het wachtwoord mag niet eenvoudig te raden zijn (bijvoorbeeld "1?deFa-7").
- Verzeker uzelf ervan dat u elk wachtwoord slechts voor een enkele zonnestroominstallatie wordt gebruikt.
- Verzeker uzelf ervan dat u zich na elke toegang tot een zonnestroominstallatie ook weer afmeldt. Actieve internetsessies kunnen bijvoorbeeld door een intermediaire aanvaller ("Man in the Middle") worden overgenomen.
- Verzeker uzelf ervan dat voor de WLAN-toegang alle toestellen minstens gebruik maakt van WPA-codering of beter nog: WPA2-codering.
  - Gebruik geen verouderde methoden voor codering, zoals WEP.
  - Zie nooit volledig af van het gebruik van enige versleutelmethode.
- Verzeker uzelf ervan dat alle medewerkers zich bewust zijn van het belang van cyber-veiligheid.
  - Zorg dat medewerkers worden geschoold in cyber-veiligheid.
- Denkt u of constateert u dat uw systeem is aangevallen? Raadpleeg dan een deskundige voor het vaststellen van de schade om gevolgschade te voorkomen.
- Denkt u of constateert u dat SMA-producten zijn aangevallen? Informeer dan a.u.b. dadelijk SMA Solar Technology AG. Stuur uw bericht a.u.b. aan het volgende e-mailadres:
  - Information-Security@SMA-Solar.com