Technische Information

PUBLIC CYBER SECURITY

Richtlinien für eine sichere PV-Anlagenkommunikation

Inhaltsverzeichnis

1 Hinweise zu diesem Dokument

1.1 Gültigkeitsbereich

Dieses Dokument gilt für alle Produkte, die innerhalb eines Netzwerks zur PV-Anlagenkommunikation miteinander verbunden sind und direkt oder indirekt über Kommunikationsmedien mit dem Internet verbunden werden können.

Dieses Dokument ergänzt die Dokumente, die jedem Produkt beigefügt sind, und ersetzt keine der vor Ort gültigen Normen oder Richtlinien. Lesen und beachten Sie die Dokumente, die mit dem Produkt geliefert wurden.

1.2 Zielgruppe

Die Informationen in diesem Dokument sind für Installateure und Betreiber von PV-Anlagen mit SMA Wechselrichtern sowie für Planer von PV-Anlagen bestimmt.

1.3 Weiterführende Informationen

Für weiterführende Informationen besuchen Sie Websites von Sicherheitsorganisationen wie:

Sicherheitsorganisation	Dokument	Hyperlink
BSI (Bundesamt für Sicherheit in der Informationstechnik)	Sichere Passwörter 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)	Industrial Control System Security: Top 10 Bedrohungen und Gegenmaßnahmen v1.2	https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_005.pdf?__blob=publicationFile&v=4
NIST (Nationales Institut für Standards und Technologie, Bundesbehörde der USA)	10 Basic Cybersecurity Measures	https://ics-cert.us-cert.gov/sites/default/files/documents/10_Basic_Cybersecurity_Measures-WaterISAC_June2015_S508C.pdf

Links zu weiterführenden Informationen finden Sie unter www.SMA-Solar.com:

Dokumententitel	Dokumentenart
"Webconnect-Anlagen im Sunny Portal"	Bedienungsanleitung
"SMA SPEEDWIRE FELDBUS"	Technische Information
"Anlagenüberwachung - SMA Sicherheits- und Passwortkonzept bei passwortgeschützen PV-Anlagen mit Bluetooth® Wireless Technology"	Technische Beschreibung
"SMA Modbus®-Schnittstelle"	Technische Information
"SunSpec® Modbus®-Schnittstelle"	Technische Information

2 Einleitung

Die meisten Betriebstätigkeiten, wie die Überwachung und Steuerung von PV-Anlagen, können lokal durch den Anlagenbetreiber oder Service-Mitarbeiter durchgeführt werden, ohne dass dazu eine Datenkommunikation über die öffentliche Internet-Infrastruktur notwendig ist. Diese Betriebstätigkeiten, darunter die Datenkommunikation zwischen Anlagenbetreiber, Service-Mitarbeiter und PV-Wechselrichter, Datenlogger oder zusätzlichen Einrichtungen, können erfolgen, indem lokale Displays, Tastenfelder oder der lokale Zugang des Webservers eines Gerätes im lokalen Netzwerk (LAN) der PV-Anlage oder des Hauses verwendet werden.

In anderen Anwendungsfällen von PV-Anlagen sind diese auch Teil des globalen Kommunikationssystems, welches auf Internet-Infrastrukturen basiert.

Die Datenkommunikation über das Internet ist ein moderner, wirtschaftlich praktikabler und kundenfreundlicher Ansatz, um den einfachen Zugriff für beispielsweise folgende moderne Anwendungen zu ermöglichen:

- Cloud-Plattformen (z. B. Sunny Portal)
- Smartphones oder anderen mobilen Geräten (iOS- oder Android-Apps)
- SCADA-Systeme, die aus der Ferne verbunden sind
- Versorgerschnittstellen für Netzsystemdienstleistungen

Alternativ können ausgewählte, gesicherte Kommunikationsschnittstellen verwendet werden. Diese Lösungen entsprechen allerdings nicht mehr dem Stand der Technik und ihre Verwendung ist teuer (besondere Kommunikationsschnittstellen, separate Weitverkehrsnetze und anderes).

Bei Verwendung der Internet-Infrastruktur gelangen die mit dem Internet verbundenen Systeme in einen prinzipiell unsicheren Bereich. Potenzielle Angreifer suchen ständig nach angreifbaren Systemen. Sie verfolgen in der Regel kriminelle, terroristische oder betriebsstörende Ziele. Ein Datenkommunikationssystem sollte nicht mit dem Internet verbunden werden, ohne dass Maßnahmen zum Schutz von PV-Anlagen und anderen Systemen vor solchem Missbrauch getroffen wurden.

Um PV-Anlagen vor unerwünschten Angriffen durch Unbefugte (z. B. Kriminelle oder Geheimdienste) wirksam zu schützen, muss das lokale Netzwerk so sauber und geschlossen wie möglich gehalten werden. Wird eine PV-Anlage oder ein ähnliches System mit dem Internet verbunden, hat der Anlagenbetreiber oder Netzwerkadministrator folgende Verantwortung:

- Kenntnisse über alle Geräte, die im lokalen Netzwerk aktiv sind
- Kenntnisse über die Kommunikationsanforderungen und Funktionen aller Geräte
- Kenntnisse über mögliche Schwachstellen aller Geräte
- Kenntnisse über alle Accounts, die auf die Systeme zugreifen
- Kenntnisse über Möglichkeiten, den Zugang zum lokalen Netzwerk und zu den Geräten zu beschränken (z. B. durch sichere Passwörter)
- Alle notwendigen Schutzmaßnahmen in Bezug auf Cybersicherheit installieren und konfigurieren (Router, Firewall, Proxy-Server)
- Prüfung und gegebenenfalls Verbesserung der Schutzmaßnahmen hinsichtlich Aktualität und Eignung

Wenn diese Voraussetzungen erfüllt sind, kann davon ausgegangen werden, dass die PV-Anlage in einem System betrieben wird, das den Status „behind the fence" (BTF) hat. Ein direkter Zugriff von außen ist unmittelbar nicht möglich.

Die meisten industriellen Kommunikationssysteme verwenden größtenteils standardisierte Feldbus-Kommunikationsprotokolle. Aus diesem Grund ist eine BTF-Strategie unerlässlich, da die meisten Feldbus-Systeme keine integrierten Sicherheitsmechanismen besitzen und durch zusätzliche Maßnahmen geschützt werden müssen. Dies gilt auch für die beiden Feldbus-Kommunikationsprotokolle SMA Data2+ und Modbus TCP, die in Kommunikationslösungen von SMA Solar Technology AG zum Einsatz kommen. Beim Kommunikationsprotokoll Data2+ bietet ein Passwortschutz eine Sicherheitsfunktion für SMA Produkte. Eine Ausnahme bildet das WAN-Kommunikationsprotokoll Webconnect, das eine sichere Verbindung mit Ende-zu-Ende-Verschlüsselung bietet. Webconnect wird allerdings in lokalen Netzwerken nicht verwendet. Es ist für die sichere Internetkommunikation zwischen PV-Wechselrichtern oder Datenloggern und dem Sunny Portal oder den mobilen Lösungen konzipiert.

i Sicherheitsrisiko durch Modbus TCP

Modbus TCP ist in den meisten SMA Produkten als öffentliche Kundenschnittstelle vorhanden. Modbus TCP lässt sich nicht ohne Weiteres sicher über das Internet übertragen. Innerhalb einer PV-Anlage kann die fehlende Authentifizierung von Modbus TCP ein potentielles Sicherheitsrisiko darstellen. Aus diesem Grund ist Modbus TCP standardmäßig in SMA Produkten deaktiviert. Bei Bedarf muss Modbus TCP in der Benutzergruppe "Installateur" aktiviert werden. Diese Aktivierung sollte nicht leichtfertig erfolgen, sondern immer durch zusätzliche Maßnahmen zur Absicherung des Gesamtsystems begleitet werden.

3 Risiken

Mit dem Internet verbundene Systeme, die nicht speziell gesichert sind, können genutzt werden, um in das Netzwerk des Kunden einzudringen (hinter dem Internet-Router). Auf diese Weise kann es zu Angriffen auf beinahe alle Geräte kommen, die sich in dem Netzwerk befinden. Wenn die potenziellen Angreifer einmal die Möglichkeit erhalten haben, in das Netzwerk einzudringen, treten die folgenden Risiken in Erscheinung:

- Ausspionieren von Benutzernamen, Passwörtern und anderen vertraulichen Daten
- Eindringen in mit dem Netzwerk verbundene Geräte, um Botnet-Agenten zu installieren oder Cross-Site-Scripting-Angriffe vorzunehmen
- Eindringen in mit dem Netzwerk verbundene Geräte, um das Geräteverhalten zu manipulieren (z. B. durch Man-in-the-Middle- oder Replay-Angriffe)
- Eindringen in mit dem Netzwerk verbundene Geräte, um übermittelte Daten zu manipulieren, die falsche Reaktionen von übergeordneten Systemen auslösen sollen
- Eindringen in mit dem Netzwerk verbundene Geräte, um das Nutzerverhalten auszuwerten (z. B. zur Planung von Einbrüchen und Diebstählen)
- Eindringen in mit dem Netzwerk verbundene Geräte, um das Nutzerverhalten zur Verwendung von personalisierter Werbung auszuwerten

Mögliche Folgen können sein:

- Finanzielle Verluste durch:
  - Ausbleibende Erträge bei der Energieerzeugung
  - Falsch verwendete Netzeinspeisungs- oder Verbrauchstarife
  - Beschädigung von Geräten
- Identitätsdiebstahl
- Negative Auswirkungen auf die Stabilität des öffentlichen Stromnetzes (sofern die Anzahl und die Größe der kompromittierten Systeme dazu ausreicht)
  - Verlust der Erlaubnis zur Anbindung an das öffentliche Stromnetz
  - Rechtliche Folgen

4 Gegenmaßnahmen

Um die grundlegenden Anforderungen eines sicheren Systems zu erfüllen, empfiehlt SMA Solar Technology AG ein Mindestmaß an Sicherheitsvorkehrungen. In Kombination mit den Sicherheitsfunktionen der SMA Produkte ist dadurch ein angemessen sicherer Betrieb der PV-Anlage möglich. Beachten Sie folgende Regeln für den sicheren Betrieb einer PV-Anlage:

- Sicherstellen, dass Firewall und Proxy-Server sicher konfiguriert sind.
- Sicherstellen, dass Sie physikalisch getrennte Netzwerksegmente für die Netzwerkverbindungen der PV-Anlage verwenden (Trennung von Heim- oder Büronetzwerk).
- Sicherstellen, dass Unbefugte weder physischen noch virtuellen Zugang zu SMA Produkten und anderen mit dem Netzwerk verbundenen Geräte erhalten.
  - Verhindern Sie die physikalische Manipulation des Systems aus dem lokalen Netzwerk.
  - Verhindern Sie die Anwendung von Spionagegeräten am lokalen Netzwerk (z. B. fremde/unbekannte WLAN-Accesspoints).
  - Verhindern Sie das Ausspionieren des Registrierungsschlüssels (RID) für die Registrierung im Sunny Portal, der üblicherweise am Produkt aufgebracht ist. Der Registrierungsschlüssel ist ein gerätespezifischer, zufällig vergebener Schlüssel, der den physikalischen Zugriff auf das Produkt beweist.
  - Verwahren Sie das Wissen über Systemdetails (Gerätetypen, Passwörter, RID) nach dem Prinzip: „So viel wie nötig, so wenig wie möglich." Halten Sie diese Informationen so geheim wie möglich.
  - Halten Sie alle Passwörter, Webconnect RID und den SMA Grid Guard-Code geheim. Der Grid Guard-Code identifiziert autorisierte Installateure, wenn diese netzrelevante Systemparameter verändern.
  - Überprüfen Sie regelmäßig die System-Protokolldateien aller Geräte, die für die IT-Sicherheit relevant sind.
  - Verbinden Sie keine unbekannten Speichermedien (USB-Sticks, SD- oder CF-Speicherkarten) mit Ihren Geräten. Prüfen Sie solche Medien vor der Verwendung auf Schadsoftware.
  - Verwenden Sie keine unbekannten und unsicheren Geräte in Ihrem Netzwerk.
  - Erstellen Sie regelmäßige Backups der Systeme.
  - Schaffen Sie für relevante Systeme reduntante Lösungen und Verfahren. Eine einfache Lösung: Für jedes kritische Systemelement sollte es ein vorkonfiguriertes Ersatzteil als Backup geben.
- Sicherstellen, dass Sie keine Portweiterleitung oder Ähnliches zwischen WAN und lokalem Netzwerk verwenden.

  - Verbinden Sie sich für den externen Zugriff über VPN oder Webconnect. Jede Fernverbindung (Wartung, Support, Direktvermarktung, Netzsystemdienstleistungen) sollte ausschließlich über solche sicheren Kommunikationsmethoden erfolgen.
- Sicherstellen, dass in der Firewall alle nicht verwendeten IP-Ports geblockt sind. Nicht verwendete IP-Ports auf anderen Systemen sollten deaktiviert sein. Jeder offene IP-Port stellt ein potenzielles Risiko für das Eindringen in das System dar.
- Sicherstellen, dass sie SFTP-Server (gesicherte FTP-Server) und keine ungesicherten externen FTP-Server verwenden. FTP-Server übertragen Dateien unverschlüsselt. Bei der Verwendung von SFTP-Servern werden die Dateien während der Übertragung verschlüsselt.
- Sicherstellen, dass Sie sichere externe Mail-Server für E-Mails verwenden. Die meisten E-Mail-Anbieter erlauben heutzutage ohnehin nur noch TLS-Zugriff (oder Ähnliches).
- Sicherstellen, dass Produkte, die nicht von SMA Solar Technology AG stammen, sicher sind. Unsichere Produkte können Angreifern ungewollten Zugriff auf das lokale Netzwerk verschaffen.
  - Halten Sie die Antivirus- und Antischadsoftware und die Regeln für Router und Firewall immer aktuell.
  - Erlauben Sie nur die absolut notwendigen Ausnahmen von Schutzmechanismen.
  - Befolgen Sie die Empfehlungen für Sicherheitsupdates des Betriebssystems.
- Sicherstellen, dass die vergebenen Zugriffsrechte auf die PV-Anlage auf eine klare Weise (welcher Benutzer bekommt welche Zugriffsrechte) organisiert sind.
  - In den meisten Fällen ist die Benutzergruppe "Benutzer" für die Überwachung der PV-Anlage ausreichend. Die Benutzergruppe "Installateur" sollte ausschließlich bei der Inbetriebnahme und Parametrierung des Produkts eingesetzt werden.
- Sicherstellen, dass alle ab Werk eingestellten Passwörter spätestens bei der Inbetriebnahme in eigene Passwörter geändert werden. Ab Werk eingestellte Passwörter sind weitläufig bekannt.
- Sicherstellen, dass Sie ausschließlich sichere Passwörter nach den gängigen Richtlinien verwenden.
  - Das Passwort sollte aus mindestens acht Zeichen, darunter Buchstaben, Zahlen und gängige Sonderzeichen (!=?#+-:;*) bestehen.
  - Das Passwort sollte nicht einfach zu erraten sein (z. B. „1?deFa-7“).
- Sicherstellen, dass jedes Passwort nur für eine einzige PV-Anlage verwendet wird.
- Sicherstellen, dass Sie sich nach jedem Zugriff auf die PV-Anlage abmelden. Aktive Internetsitzungen könnten z. B. durch einen Man-in-the-Middle-Angriff übernommen werden.
- Sicherstellen, dass Sie für den WLAN-Zugriff aller Geräte mindestens die WPA-Verschlüsselung oder besser die WPA2-Verschlüsselung verwenden.
  - Verwenden Sie keine älteren Verschlüsselungsmethoden wie WEP.
  - Verzichten Sie niemals gänzlich auf Verschlüsselungsmethoden.
- Sicherstellen, dass alle Mitarbeiter in Bezug auf Cybersicherheit sensibilisiert sind.

  - Sorgen Sie für die Schulung von Mitarbeitern in Bezug auf Cybersicherheit.
- Sollten Sie den Verdacht haben oder feststellen, dass ein Angriff auf Ihr System stattgefunden hat, beauftragen Sie einen Spezialisten um den Schaden festzustellen und weitere Auswirkungen zu verhindern.
- Sollten Sie den Verdacht haben oder feststellen, dass ein Angriff auf SMA Produkte stattgefunden hat, informieren Sie bitte unverzüglich SMA Solar Technology AG. Dazu wenden Sie sich bitte an folgende E-Mail-Adresse:
  - Information-Security@SMA-Solar.com