Technische Information

PUBLIC CYBER SECURITY

Richtlinien für eine sichere Anlagenkommunikation

Inhaltsverzeichnis

1 Hinweise zu diesem Dokument

1.1 Gültigkeitsbereich

Dieses Dokument gilt für alle Produkte (z. B. Wechselrichter, Batterien, Kommunikationsprodukte) einer PV-Anlage. Diese Produkte können direkt oder indirekt über Kommunikationsmedien mit dem Internet verbunden sein. Dies schließt sowohl Produkte von SMA als auch von anderen Herstellern ein.

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 den Produkten geliefert wurden.

1.2 Zielgruppe

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

1.3 Inhalt und Struktur des Dokuments

Dieses Dokument beschreibt technische und organisatorische Maßnahmen, die von Installateuren und Betreibern von SMA Produkten für den sicheren Betrieb von PV-Anlagen umgesetzt werden müssen. SMA als Hersteller ist sich seiner Verantwortung bewusst und implementiert ein hohes Maß an Cybersicherheit in seinen Geräten auf Basis des SMA Secure Development Life Cycle. Ein Secure Development Live Cycle umfasst alle Sicherheitsmaßnahmen über den gesamten Lebenszyklus eines Produktes vom Design bis hin zur Außerbetriebnahme. Der SMA Secure Development Life Cycle ist an der IEC 62443-4-1 ausgerichtet.

Um Risiken so weit wie möglich zu reduzieren, bedarf es jedoch der Unterstützung aller Beteiligten. SMA empfiehlt Installateuren, Betreibern und Planern von PV-Anlagen daher dringend, die in diesem Dokument aufgeführten Anforderungen zu beachten und umzusetzen.

2 Einleitung

2.1 Ziele von Cybersicherheit

Cybersicherheit ist entscheidend für den Schutz von Daten, Privatsphäre und Aufrechterhaltung des Geschäftsbetriebs. Folgende Ziele verfolgt SMA bei Cybersicherheit:

- **Schutz sensibler Daten**: Daten, die von SMA Produkten gesammelt oder auf diesen Produkten gespeichert werden, können von Cyber-Kriminellen nicht missbraucht werden.
- **Vermeidung finanzieller Verluste**: Finanzielle Verluste durch Cyber-Angriffe können zu keinen finanziellen Verlusten, sowohl für Einzelpersonen als auch für Unternehmen führen.
- **Einhaltung von Compliance- und gesetzlichen Verpflichtungen**: Unternehmen halten bei Verwendung von SMA Produkten Cybersicherheitsstandards und -vorschriften ein. Dadurch werden rechtliche Konsequenzen vermieden und das Vertrauen der Stakeholder gewahrt.
- **Sicherstellung der Aufrechterhaltung des Geschäftsbetriebs**: Effektive Cybersicherheitsmaßnahmen verhindern Unterbrechungen, die durch Cybervorfälle verursacht werden und sorgen so für einen reibungslosen Betrieb. Für Energiesysteme stellen sie die kontinuierliche Energieversorgung sicher.

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.

2.2 Anwendungen von PV-Anlagen im globalen Kommunikationssystem

Die meisten Betriebstätigkeiten, wie die Überwachung und Steuerung von PV-Anlagen, können lokal durch den Anlagenbetreiber oder Service durchgeführt werden, ohne dass dazu eine Datenkommunikation über die öffentliche Internet-Infrastruktur notwendig ist. Diese Betriebstätigkeiten umfassen die Datenkommunikation zwischen Anlagenbetreibern, dem Service und PV-Wechselrichtern, Datenloggern oder zusätzlichen Einrichtungen. Sie können über lokale Displays, Tastenfelder oder den lokalen Zugang zum Webserver eines Geräts im lokalen Netzwerk (LAN) der PV-Anlage oder des Hauses erfolgen.

In einigen Anwendungsfällen von PV-Anlagen ist die PV-Anlage 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 andere mobile Endgeräte (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. Das gilt z. B. für dezidierte Kommunikationsschnittstellen oder separate Weitverkehrsnetze (WAN).

Sehen Sie dazu auch:

- Hardening ⇒ Seite 7

3 Szenarien für Cyber-Angriffe

Die Bewertung von Cybersicherheitsrisiken umfasst die Bewertung der Wahrscheinlichkeit und der Auswirkungen von Angriffen auf bestimmte Geräte oder Systeme. Um den Überblick zu behalten, ist es entscheidend, alle potenziellen Angriffsszenarien zu bewerten. Dies wird erreicht, indem mögliche Angriffsszenarien für ein Gerät oder System skizziert werden. Dabei müssen Verwendungszweck und Umgebungsbedingungen des Geräts oder Systems beachtet werden.

Im Folgenden finden Sie eine nicht abschließende Liste wichtiger Angriffsszenarien, möglicher Folgen für Geräte und Systeme sowie deren Betreiber und einige Gegenmaßnahmen. Beachten Sie, dass tatsächliche Angriffe in der Regel eine Kombination verschiedener Szenarien umfassen.

Angriffsszenario	Mögliche Ziele des Angreifers	Mögliche Folgen für Betreiber	Gegenmaßahmen
Spear-Phishing: Der Angreifer kontaktiert das Opfer direkt per E-Mail oder Telefon um z. B. Anmeldeinformationen für ein Gerät zu erhalten.	• Manipulation des Geräts oder der Anlage • Zufügen von Schaden	• Verlust der Kontrolle über die Anlage • Finanzielle Verluste • Vorgaben des Netzbetreibers und normative Vorgaben werden nicht mehr eingehalten	• Keine Anmeldeinformationen weitergeben. • Anmeldeinformationen sicher und für Dritte unzugänglich aufbewahren.
Fernzugriff mit Standard-Zugangsdaten: Der Angreifer sucht nach Geräten, die mit dem Internet verbunden sind, z. B. weil die Portweiterleitung im Router aktiviert ist. Inbetriebnahme der Geräte wurde nicht korrekt durchgeführt.	• Manipulation der Energieversorgung einer ganzen Region • Zufügen von Schaden	• Verlust der Kontrolle über mehrere Anlagen in einer Region oder Anlagen mit Produkten eines Herstellers • Finanzielle Verluste • Netzausfälle	• Nie die Portweiterleitung im Router der Anlage aktivieren. • Inbetriebnahme wie in den Anleitungen der Geräte oder des Systems beschrieben durchführen.
Advanced Persistent Threats (APT): Der Angreifer installiert eine technisch ausgefeilte Schadsoftware auf dem Zielgerät oder -system. Die Schadsoftware wird nicht erkannt. Der Angreifer löst den Angriff zu einem späteren passenden Zeitpunkt aus.	• Manipulation der Energieversorgung einer ganzen Region • Zufügen von Schaden	• Verlust der Kontrolle über mehrere Anlagen in einer Region oder Anlagen mit Produkten eines Herstellers • Zerstörung des Zielgeräts oder -systems • Finanzielle Verluste • Netzausfälle	• Hardening der Geräte und Anlagen durchführen (siehe Kapitel 5.1, Seite 7). • Netzwerk segmentieren. • Erweiterte Zugangsbeschränkungen für Anlagen festlegen. • Angriffserkennungssysteme (Intrusion Detection Systems, IDS) verwenden.

4 Beispiel für einen Cyber-Angriff: Downgrade-Angriff

Reale Angriffe bestehen aus mehreren Angriffsschritten, alle zusammen werden als "Angriffsvektor" bezeichnet. Im Folgenden wird ein möglicher konkreter Angriffsvektor für einen Angriff auf eine PV-Anlage beschrieben. In diesem Beispiel wird ein Downgrade Angriff beschrieben. Damit sind Angriffe gemeint, die eine Firmware auf einen veralteten Stand zurück setzen, so dass durch neue Versionen bereits geschlossene Sicherheitslücken wieder geöffnet werden.

Dies ist keine Beschreibung eines echten Angriffs oder eines realen Systems oder Geräts, sondern ein theoretisches Beispiel.

Ziel des Angreifers: Ein Angreifer möchte sich Zugang zu einem Wechselrichter verschaffen, um ihn abzuschalten. In einer früheren Firmware-Version gab es eine öffentlich bekannte Schwachstelle, die eine Anmeldung ohne Passwort ermöglicht. Zusätzlich ermöglicht die Benutzeroberfläche des Geräts Updates ohne Authentifizierung.

Vorgehen des Angreifers:

1. Der Angreifer verwendet eine spezialisierte internationale Suchmaschine, um einen Ziel-Wechselrichter zu identifizieren, der per Portweiterleitung mit dem Internet verbunden ist. Der Angreifer baut eine Verbindung zum Zielgerät auf.
2. Der Angreifer verwendet öffentliche und gerätespezifische Informationen, um auszuwerten, welche Firmware-Version auf dem Gerät verwendet wird. Bei der verwendeten Software handelt es sich um eine neuere Version, bei der die Sicherheitslücke bereits behoben ist.
3. Der Angreifer sucht nach einer alten Firmware-Version, die die Sicherheitslücke aufweist. Der Angreifer sucht diese Version in verschiedenen Internet-Ressourcen, schließlich erhält er sie in einem speziellen Diskussionsforum.
4. Der Angreifer verwendet die alte Firmware-Version und versucht, diese Firmware über die Benutzeroberfläche hochzuladen. Dies ist möglich, da das Gerät ein Update ohne Authentifizierung zulässt.
5. Nun muss der Angreifer warten, bis das Gerät neu gestartet wird. Das Ziel-Gerät führt Updates nur nachts durch.
6. Das Gerät installiert die alte Firmware inklusive der Schwachstelle. Da das Gerät die Version eines Updates nicht überprüft, ist das Downgrade möglich. Dies ist die Hauptursache, warum dieser Angriff möglich ist.
7. Der Angreifer verschafft sich über die Schwachstelle in der alten Firmware-Version Zugriff auf den Wechselrichter und manipuliert Parameter so, dass der Wechselrichter nicht mehr einspeist.

5 Maßnahmen für Cybersicherheit

5.1 Hardening

Angesichts der Weiterentwicklung von Cyber-Bedrohungen ist Cybersicherheit für Einzelpersonen, Organisationen und Regierungen weltweit von entscheidender Bedeutung. Hardening ist ein wirksames Mittel, um das Risiko von Cyberangriffen deutlich zu reduzieren. Hardening bezeichnet eine Technik, die Angriffsfläche eines Systems auf ein Minimum zu reduzieren, indem Einstiegspunkte für Angriffe auf ein Gerät verringert werden. So kann z. B. die Sicherheit eines Systems erhöht werden, indem nur Software eingesetzt wird, die für den Betrieb des Systems notwendig ist und deren sicherer Ablauf garantiert werden kann.

Die Empfehlungen müssen in allen Anlagen befolgt werden.

5.2 Verantwortung des Anlagenbetreibers für Cybersicherheit

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 (Asset Management)
- Kenntnisse über die Kommunikationsanforderungen und Funktionen aller Geräte (Secure Communication, Hardening)
- Kenntnisse über mögliche Schwachstellen aller Geräte (z. B. automatische Updates)
- Kenntnisse über alle Accounts, die auf die Systeme zugreifen (Identity and Access Management)
- 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, Netzwerksegmentation))
- Prüfung und gegebenenfalls Verbesserung der Schutzmaßnahmen hinsichtlich Aktualität und Eignung

Sehen Sie dazu auch:

- Asset Management ⇒ Seite 8
- Hardening ⇒ Seite 7

5.3 Behind the fence-Strategie (BTF)

Wenn der Anlagenbetrieber seiner Verantwortung bezüglich Cybersicherheit (siehe Kapitel 5.2, Seite 7) gerecht wird, 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.

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.

5.4 Defense in Depth-Konzept

Für die maximale Sicherheit Ihrer PV-Anlage empfiehlt SMA einen Defense in Depth-Konzept ("Verteidigung in der Tiefe").

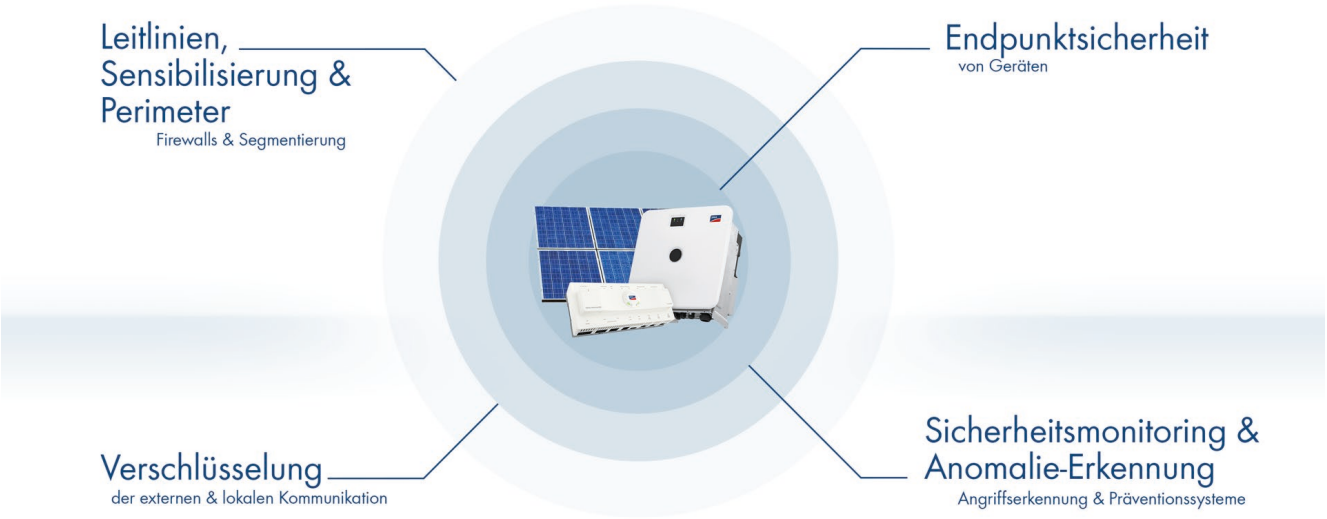

Abbildung 1: Veranschaulichung des Defense in Depth-Konzepts

Ein ganzheitliches Sicherheitskonzept sollte nach IEC 62443 aufgebaut werden. Diese Norm richtet sich an alle Systembeteiligten, einschließlich Betreiber, Planer und Hersteller, und zielt darauf ab, ein Gesamtkonzept auf Basis spezifischer Sicherheitsstufen für verschiedene Zonen und deren Verbindungen aufzubauen.

5.5 Asset Management

5.5.1 Asset Management

Asset Management bezeichnet das Management aller Komponenten, die sich in der Anlage und im Netzwerk befinden. Ein zeitgemäßes Asset Management ist entscheidend für den Schutz der digitalen Infrastruktur eines Unternehmens. Es ist notwendig für:

- **Erkennung von Schwachstellen**: Effektives Asset Management hilft bei der Erkennung von Schwachstellen in Hardware, Software, Daten und Netzwerkressourcen. Durch das Verständnis des Assets und seines Werts, des Standorts und der Schwachstelle können Unternehmen Sicherheitsmaßnahmen entwickeln und priorisieren.
- **Minimierung von Risiken**: Asset Management gewährleistet die Funktionalität, Verfügbarkeit und Vertraulichkeit der Assets. Es minimiert das Risiko von unbefugtem Zugriff, Sicherheitsproblemen und Datenlecks.
- **Transparenz und Kontrolle**: Das Asset Management bietet Einblicke in digitale Assets und ermöglicht Unternehmen, sie während ihres gesamten Lebenszyklus zu überwachen und zu schützen. Ohne ein angemessenes Management mangelt es Unternehmen möglicherweise an Wissen über wichtige Assets.

In Heim-Systemen reicht es in den meisten Fällen aus, ein Dokument mit einer Liste der in das Heimnetzwerk integrierten Komponenten zu führen. In großen Systemen ist ein professionelles, toolbasiertes Asset Management wichtig, um Risiken zu identifizieren, kritische Anlagenteile zu schützen und die erforderlichen Ressourcen für das Management des Energiesystems zu planen. In vielen Regionen der Welt ist ein solches Asset Management für bestimmte Arten von Anlagen gesetzlich vorgeschrieben.

5.5.2 Asset Management Checkliste

Die folgende Liste kann verwendet werden, um die Konfiguration Ihrer PV-Anlage nach der Erstinbetriebnahme zu prüfen. Die Prüfung sollte zusätzlich regelmäßig wiederholt werden, um sicherzustellen, dass Ihre Anlage über den gesamten Lebenszyklus vor Cyber-Kriminalität geschützt ist.

- ☐ Eine aktuelle Liste der Geräte mit den erforderlichen Informationen (IP-Adresse, Gerätetyp, Name des Geräts usw.) muss vorhanden sein. Diese Liste kann manuell oder automatisch (empfohlen) gepflegt werden.
- ☐ Ein Asset Management Service, der alle erforderlichen Informationen sammelt und bei Änderungen informiert, sollte in Ihr Netzwerk eingebunden sein.
- ☐ Ein Prozess, um die Berichte des Asset Management Service regelmäßig zu prüfen, sollte implementiert sein.

5.6 Identitäts- und Zugriffsmanagement

5.6.1 Identitäts- und Zugriffsmanagement

Jeder Zutritt zu elektronischen Geräten oder sensiblen Räumlichkeiten sollte durch geeignete Authentifizierungsmechanismen und die Vergabe von Nutzungsrechten in Abhängigkeit von der Rolle des Nutzers (Berechtigung) abgesichert werden. Dies gilt für jede Art von Energiesystem oder PV-Anlage (Home, Commercial & Industrial, Large Scale).

Bei komplexeren Systemen im Bereich Industrial oder Large Scale besteht der Bedarf an zusätzlichen Maßnahmen, um ein angemessenes Sicherheitsniveau in Bezug auf Authentifizierung und Autorisierung zu erreichen. In solchen Fällen sollten Tools für das Identitäts- und Zugriffsmanagement implementiert werden. Diese sind ein wichtiger Bestandteil einer ganzheitlichen Cybersicherheits-Strategie. Dadurch werde unbefugte Zugriffe verhindert, eine zentralisierte Automatisierung und Überwachung ermöglicht und bei Vorfällen wird ein Alarm aktiviert.

5.6.2 Checkliste für Identitäts- und Zugriffsmanagement

Die folgende Liste kann verwendet werden, um die Konfiguration Ihrer PV-Anlage nach der Erstinbetriebnahme zu prüfen. Die Prüfung sollte zusätzlich regelmäßig wiederholt werden, um sicherzustellen, dass Ihre Anlage über den gesamten Lebenszyklus vor Cyber-Kriminalität geschützt ist.

- ☐ Alle Geräte Ihres Energiesystems müssen über ein angemessenes Identitäts-Management verfügen, z. B. durch Erzwingen eines Logins auf allen Anwendungen und Vergabe entsprechender Rechte (Role Based Access Control).
- ☐ Eine Anbindung an ein an ein zentrales Benutzerverwaltungssystem, z.B. über LDAPS an ein Active Directory (AD)-System sollte vorhanden sein.
- ☐ Nutzerkonten sollten nicht geteilt werden.
- ☐ Wenn die gemeinsame Nutzung von Konten nicht vermieden werden kann, muss eine Liste der Konten und einzelnen Benutzer, die diese Konten verwenden dürfen, vorhanden sein. Es müssen verbindliche Richtlinien für die Verwendung der Konten und Prozesse zur Überwachung der Nutzung vorhanden sein.

5.7 Segmentierung

5.7.1 Segmentierung

Die Netzwerksegmentierung ist eine Cybersicherheitstechnik, die verwendet wird, um ein Netzwerk in kleinere, isolierte Bereiche zu unterteilen. Auf diese Weise wird das Risiko verringert, dass sich Schad-Software oder böswillige Angriffe über das gesamte Netzwerk ausbreiten. Darüber hinaus trägt die Netzwerksegmentierung dazu bei, sensible Daten und Anwendungen von weniger sicheren Komponenten zu trennen. Es ist eine wesentliche Komponente der Netzwerksicherheitsarchitektur und verbessert die Kontrolle und Widerstandsfähigkeit gegen Cyber-Bedrohungen.

Einge Best Practices sind:

- **Kontinuierliche Überwachung und Prüfung von Netzwerken:** Regelmäßige Bewertung der Netzwerksegmente, um Schwachstellen zu identifizieren und die ordnungsgemäße Konfiguration sicherzustellen
- **Vermeidung von Über- oder Untersegmentierung:** Anstreben eines Gleichgewichts; Zu viele Segmente können komplex sein, während zu wenige die Sicherheit beeinträchtigen können
- **Begrenzung der Zugriffspunkte von Drittanbietern:** Kontrolle des externen Zugriffs auf bestimmte Segmente, um unbefugten Zugriff zu verhindern
- **Identifizieren und Kennzeichnen von Assets:** Klarheit über die Bedeutung von Assets in jedem Segment, um den Schutz zu priorisieren (risikobasierter Ansatz)
- Kombination von ähnlichen Netzwerkressourcen: Konsolidierung von verwandten Ressourcen, um das Management zu vereinfachen und die Komplexität zu reduzieren

5.7.2 Checkliste für Segmentierung

Die folgende Liste kann verwendet werden, um die Konfiguration Ihrer PV-Anlage nach der Erstinbetriebnahme zu prüfen. Die Prüfung sollte zusätzlich regelmäßig wiederholt werden, um sicherzustellen, dass Ihre Anlage über den gesamten Lebenszyklus vor Cyber-Kriminalität geschützt ist.

☐ Erstellen Sie ein Netzwerkdiagramm, das alle relevanten Geräte in Ihrem Netzwerk enthält.

☐ Fügen Sie Grenzlinien um Gruppen von Geräten ("Segmenten") hinzu, die dieselbe Sicherheitsstufe haben sollen, z. B. das Heimnetzwerk oder das Unternehmens-IT-Netzwerk und das Energiesystemnetzwerk.

☐ Implementieren Sie die Netzwerktrennung für alle Segmente, die im obigen Diagramm definiert sind. Dies wird als "Segmentierung" bezeichnet.

☐ Überprüfen Sie die Wirksamkeit der Segmentierung.

5.8 Sichere Kommunikation

5.8.1 Sichere Kommunikation

SMA implementiert in seinen Geräten unterschiedliche Kommunikationsmöglichkeiten (sogenannte "Protokolle"), abhängig von den Anforderungen an den Verwendungszweck des jeweiligen Geräts. Gemäß der Regel "Security by Design" ist es das Ziel von SMA, genau solche Protokolle bereitzustellen, die über aktuelle Sicherheitsmechanismen verfügen, um die Sicherheitsziele Vertraulichkeit, Integrität und Authentifizierung zu erreichen. Gängige Beispiele für solche sicheren Kommunikationsprotokolle sind HTTPS (für Websites und Webanwendungen) und FTPS/SFTP (für den Dateiaustausch). In einigen Fällen kann dieses Ziel aus Gründen der Interoperabilität oder der Verfügbarkeit geeigneter Alternativen nicht erreicht werden.

Die Empfehlungen für sichere Kommunkation müssen in allen Anlagen befolgt werden.

5.8.2 Liste der unsicheren Protokolle und Abhilfemaßnahmen

Im Folgenden geben wir einige Informationen und Empfehlungen für diejenigen Protokolle, die nicht über angemessene Sicherheitsmechanismen verfügen. Bitte beachten Sie, dass möglicherweise nicht alle der hier aufgeführten Protokolle in Ihrem spezifischen Produkt verfügbar sind. Liste der unsicheren Protokolle und Abhilfemaßnahmen:

Protokoll	Zweck	Risiken	Maßnahmen zur Risikominderung
Modbus	Datenaustausch zwischen verschiedenen Geräten	• **Keine Authentifizierung**: Es ist unklar, wer Modbus-Befehle sendet, möglicherweise ist es ein Angreifer. • **Keine Verschlüsselung**: Eine Offenlegung von Informationen ist möglich, ein Angreifer kann die Kommunikation abhören.	• Modbus ist in SMA-Geräten standardmäßig deaktiviert. • Aktivieren Sie Modbus nur bei Bedarf und wenn die Kommunikation innerhalb Ihres lokalen Netzwerks durch eine ordnungsgemäß konfigurierte Firewall geschützt ist. • Eine Netzsegmentierung sollte für Ihr PV-Anlagennetz vorhanden sein. • Konfigurieren Sie niemals eine Portweiterleitung in Ihr lokales Netzwerk oder das Netzwerksegment Ihrer PV-Anlage.
FTP-Push (File Transfer Protocol)	Dateiaustausch zwischen verschiedenen Systemen. Für FTP-Push wird kein Dienst auf dem Gerät bereitgestellt, sondern nur eine Verbindungsmöglichkeit zu FTP-Servern von Drittanbietern.	• **Keine Verschlüsselung**: Der Angreifer kann die FTP-Kommunikation abhören und die Anmeldedaten (ID, Passwort) abfangen. In einem nächsten Schritt kann er diese Zugangsdaten für die Anmeldung auf dem FTP-Server verwenden und damit beginnen, Dateien zu manipulieren oder zu zerstören oder bösartige Dateien hochzuladen.	• Richten Sie Verbindungen zu FTP-Servern von Drittanbietern ein, die sichere Versionen von FTP wie SFTP oder FTPS bereitstellen. • Wenn ein Server eines Drittanbieters keine sichere FTP-Version zur Verfügung stellt, nur nicht klassifizierte Daten übertragen, insbesondere keine geheimen Daten oder Passwörter.

5.8.3 Checkliste für sichere Kommunikation

Die folgende Liste kann verwendet werden, um die Konfiguration Ihrer PV-Anlage nach der Erstinbetriebnahme zu prüfen. Die Prüfung sollte zusätzlich regelmäßig wiederholt werden, um sicherzustellen, dass Ihre Anlage über den gesamten Lebenszyklus vor Cyber-Kriminalität geschützt ist.

☐ Stellen Sie sicher, dass alle Protokolle, die für den bestimmungsgemäßen Gebrauch eines Geräts nicht erforderlich sind, deaktiviert sind.

- ☐ Verhindern Sie die Verwendung unverschlüsselter Protokolle. Wenn sie unbedingt erforderlich sind, sollte eine Netzwerktrennung als Abhilfemaßnahme implementiert werden.
- ☐ Stellen Sie sicher, dass alle physischen Anschlüsse (z. B. USB) deaktiviert sind, wenn sie nicht benötigt werden und eine Deaktivierung möglich ist.
- ☐ Werden USB-Anschlüsse bereitgestellt, die nicht benötigt werden und die nicht per Software deaktiviert werden können, können Sie sogenannte "Port-Blocker" verwenden.

5.9 Updates

Die meisten Cybersicherheitsrisiken gehen von Software oder Softwarekomponenten ("Bibliotheken") aus, die Schwachstellen aufweisen. Diese Risiken können behoben werden, indem ein Gerät aktualisiert wird, sobald eine Softwareversion vorhanden ist, welche die Schwachstelle nicht mehr enthält. Daher ist es zunächst wichtig, sicherzustellen, dass alle Ihre Geräte aktualisiert werden können. Dies ist bei allen SMA Produkten der Fall.

Im nächsten Schritt ist es entscheidend, alle Ihre Geräte und insbesondere alle SMA Produkte auf dem neuesten Stand zu halten. Mit Updates werden Sicherheitslücken geschlossen, um zu verhindern, dass Angreifer Schwachstellen im Produkt ausnutzen. Dies schützt auch Ihre Daten und beugt Verletzungen des Datenschutzes vor. Aktuell werden immer mehr IoT-Geräte ("Internet of Things"-Geräte) von Angreifern missbraucht, um Angriffe wie DDoS-Attacken ("Distributed Denial of Service"-Attacken) durchzuführen. Hierbei handelt es sich um einen Angriff, der von vielen IP-Adressen gleichzeitig durchgeführt wird, um den angegriffenen Dienst so stark auszulasten, dass er für legitime Nutzer nicht mehr nutzbar ist.

IoT-Geräte werden auch genutzt, um andere Systeme im Internet anzugreifen. Wenn Sie Ihre Produkte auf dem neuesten Stand halten, schützen Sie sich nicht nur selbst, sondern tragen auch zu einem sichereren Internet für alle bei.

SMA empfiehlt automatische Updates, wo es möglich ist. Alle SMA Geräte können automatisch aktualisiert werden. Wenn Sie sich gegen automatisierte Updates entscheiden, müssen Sie eine Update-Strategie und einen Update-Prozess implementieren, der Personen und Verantwortlichkeiten sowie einen Zeitplan für die manuellen Updates definiert.

Die Empfehlungen für Updates müssen in allen Anlagen befolgt werden.

5.10 Protokollierung und Überwachung

5.10.1 Protokollierung und Überwachung

Selbst wenn man alle Empfehlungen aus diesem Dokument befolgt, kann es Situationen geben, in denen eine Verletzung der Sicherheit oder ein Angriff nicht verhindert werden kann. Für solche Fälle sollten zusätzliche Maßnahmen vorgesehen werden, die zumindest die Aufdeckung von Angriffen ermöglichen. Die Protokollierung und Überwachung ist die Hauptvoraussetzung für eine schnelle und effektive Reaktion auf jede Art von Vorfall. Im Falle eines Vorfalls entscheiden die Reaktionsgeschwindigkeit und die Wirksamkeit der Maßnahmen über die Schwere der Auswirkungen eines solchen Angriffs.

5.10.2 Checkliste für Protokollierung und Überwachung

Die folgende Liste kann verwendet werden, um die Konfiguration Ihrer PV-Anlage nach der Erstinbetriebnahme zu prüfen. Die Prüfung sollte zusätzlich regelmäßig wiederholt werden, um sicherzustellen, dass Ihre Anlage über den gesamten Lebenszyklus vor Cyber-Kriminalität geschützt ist.

- ☐ Überprüfen Sie bei Heimsystemen, ob Ihr Router eine Art von Protokollierung und Überwachung bietet. Wenn ja, aktivieren Sie diese und überprüfen Sie die Protokolle mindestens einmal im Monat.
- ☐ Implementieren Sie ein Intrusion Detection System (IDS).
- ☐ Testen Sie regelmäßig die Monitoring-Tools und -Maßnahmen einschließlich eines IDS.
- ☐ Implementieren Sie einen Prozess zur Definition von Verantwortlichkeiten und zur regelmäßigen Überprüfung der Wirksamkeit Ihrer Überwachungsmaßnahmen

5.11 Geräte- und Nutzergeheimnisse

5.11.1 Geräte- und Nutzergeheimnisse

Um Ihre Assets vor unbefugtem Zugriff zu schützen, ist es wichtig, Ihre Geräte- und Nutzergeheimnisse wie Passwörter oder den WiFi PSK (Pre Shared Key) zu sichern. Dazu gehört nicht nur der Schutz dieser Geheimnisse vor unbefugtem Zugriff, sondern auch die Verwendung starker Passwörter, die es einem Angreifer erschweren, das Passwort zu erraten oder durch einen Brute-Force-Angriff, dem Ausprobieren aller möglichen Passwörter, zu bestimmen.

Die Empfehlungen müssen in allen Anlagen befolgt werden.

5.11.2 Checkliste für Geräte- und Nutzergeheimnisse

Die folgende Liste kann verwendet werden, um die Konfiguration Ihrer PV-Anlage nach der Erstinbetriebnahme zu prüfen. Die Prüfung sollte zusätzlich regelmäßig wiederholt werden, um sicherzustellen, dass Ihre Anlage über den gesamten Lebenszyklus vor Cyber-Kriminalität geschützt ist.

- ☐ Geheimnisse nicht auf Papier schreiben.
- ☐ Wenn Passwörter auf Papier gedruckt sind, bewahren Sie das Papier an einem sicheren Ort (z. B. einem Safe) auf.
- ☐ Verwenden Sie einen Passwort-Manager (spezielle Software zum Speichern von Passwörtern in einer verschlüsselten Datenbank oder Datei).
- ☐ Geben Sie niemals Passwörter an Dritte oder anderes Systeme weiter.
- ☐ Ändern Sie alle Standardpasswörter in individuelle Passwörter.
- ☐ Verwenden Sie keine einfachen Passwörter (wie z. B. 1234).
- ☐ Erstellen Sie komplexe Passwörter, bestehend aus mindestens 8 Zeichen, Buchstaben, Zahlen und Sonderzeichen.
- ☐ Verwenden Sie eine Passphrase, um Ihr Passwort zu erstellen.
- ☐ Verwenden Sie nicht dasselbe Passwort für verschiedene Konten.
- ☐ Verwenden Sie einen Passwort-Manager , um zufällige Passwörter zu generieren und sicher zu speichern.

5.12 Checkliste für weitere Maßnahmen

Die folgende Liste kann verwendet werden, um die Konfiguration Ihrer PV-Anlage nach der Erstinbetriebnahme zu prüfen. Die Prüfung sollte zusätzlich regelmäßig wiederholt werden, um sicherzustellen, dass Ihre Anlage über den gesamten Lebenszyklus vor Cyber-Kriminalität geschützt ist.

Segmentierung:

- ☐ Stellen Sie sicher, dass die Firewall und der Proxyserver ordnungsgemäß konfiguriert sind.
- ☐ Für die Netzanschlüsse der PV-Anlage physisch (oder zumindest logisch) getrennte Netzsegmente verwenden (z. B. Trennung von Heim- oder Büronetz).

Netzwerkeinstellungen und Protokolle:

- ☐ Keine Portweiterleitung oder Ähnliches zwischen WAN und LAN verwenden.
- ☐ Deaktivieren Sie alle Protokolle in allen Geräten, die für die Kommunikation innerhalb Ihrer Anlage nicht notwendig sind.
  - Deaktivieren Sie Modbus, wenn möglich (dieses Protokoll unterstützt keine Verschlüsselung oder Authentifizierung).
  - Speedwire: Wenn alle Geräte die verschlüsselte Kommunikation von Speedwire unterstützen, stellen Sie sicher, dass Sie die verschlüsselte Version im Systemmanager aktivieren.
  - WiFi Access Point: Deaktivieren Sie den WiFi Access Point nach der Ersteinrichtung.
- ☐ Verwenden Sie keine unsicheren externen FTP-Server. Verwenden Sie stattdessen SFTP (Secure FTP), um Daten mit Verschlüsselung zu übertragen.

☐ Verwenden Sie für WLAN-Verbindungen die WPA- oder WPA2-Verschlüsselung. Ältere Verschlüsselungsmethoden (z.B. WEP) sind kompromittiert.

Anmeldedaten:

☐ Alle Standardpasswörter ändern.

☐ Ihre gerätespezifischen Anmeldeinformationen privat halten.

- RID (Registration ID - für die Registrierung des Gerätes im Sunny Portal)
- PIC (Product Identification Code - für die Registrierung des Gerätes im Sunny Portal)
- Product Key (benutzergeneriert - für das Zurücksetzen des Passworts)
- Device Key (zum Zurücksetzen des Passworts des Admin-Kontos)
- WiFi PSK (für den WiFi Access Point des Geräts)

☐ WiFi PSK ändern. Falls vom Gerät unterstützt, ändern Sie den PSK nach der Ersteinrichtung.

☐ Stellen Sie sicher, dass Sie die erforderlichen Zugriffsrechte den richtigen Personen zuweisen.

Sonstiges:

☐ Automatische Updates aktivieren.

☐ Deaktivieren Sie den Servicezugriff. Aktivieren Sie den Servicezugriff nur, wenn Sie Unterstützung durch den SMA Service benötigen und der Service Zugriff auf Ihr System benötigt.

☐ Schützen Sie Ihr Gerät vor physischem Zugriff, um böswillige Manipulationen zu verhindern.

☐ Überprüfen Sie regelmäßig Protokolldateien auf verdächtige Aktivitäten.

☐ Schließen Sie keine unbekannten Speichergeräte (USB-Sticks, SD- oder CF-Speicherkarten) an Ihre Geräte an. Überprüfen Sie solche Speichergeräte auf Malware, bevor Sie sie verwenden.

☐ Überprüfen Sie regelmäßig, ob sich in Ihrem Netzwerk unbekannte Geräte befinden.

☐ Erstellen Sie regelmäßige Backups.

☐ Halten Sie Ihre Fernzugriffsausrüstung immer auf dem neuesten Stand. Spielen Sie regelmäßig Sicherheitspatches ein und verwenden Sie einen aktuellen Virenscanner.

☐ Stellen Sie sicher, dass Sie sich nach jedem Zugriff aus Ihrer PV-Anlage abmelden. Aktive Internetsitzungen könnten von einer Man-in-the-Middle-Attacke übernommen werden.

☐ Stellen Sie sicher, dass alle Mitarbeiter Cybersicherheitsschulungen erhalten.

Stilllegung:

☐ Setzen Sie Ihr Gerät auf die Werkseinstellungen zurück, um alle persönlichen Daten und Zugangsdaten (z. B. Ihr WLAN-Passwort) zu löschen.

☐ Entfernen Sie Ihr Gerät aus dem Sunny Portal.

5.13 Wichtige Hinweise

Sollten Sie den Verdacht haben oder feststellen, dass ein Angriff auf Ihr System stattgefunden hat, lassen Sie den Schaden von einem Spezialisten beurteilen, um weitere Auswirkungen zu verhindern.

Sollten Sie den Verdacht haben oder feststellen, dass ein Angriff auf SMA Produkte stattgefunden hat, informieren Sie uns umgehend. Verwenden Sie hierfür folgende E-Mail-Adresse: Information-Security@sma.de

ENERGY
THAT
CHANGES

SMA

www.SMA-Solar.com