BEHEBUNGSMASSNAHMEN IN BEZUG AUF DIE FOLGEN DES VORFALLS MIT DEN VON SOLAR-OT EINGESETZTEN CHIYU-SENSOREN

Einsatz der neuesten Firmware & Ausbau/Verbesserung der SOLAR-OT-Überwachungsplattform

Autorin	Bestätigt durch
Deirdre STARSKY, Technische Projektleiterin	Elena PIZARI, Generaldirektorin Industrie

ZIEL

Das vorliegende Dokument beschreibt die 2 Abhilfemaßnahmen nach dem Vorfall in den von SOLAR-OT eingesetzten Zugangskontrollsystemen:

1. Dringende Bereitstellung der Firmware-Updates auf allen Systemen
2. Die Optimierung der Konfiguration der Überwachungsplattform

1. DRINGENDE BEREITSTELLUNG DES FIRMWARE-UPDATES

Der Hersteller CHIYU hat ein Firmware-Update für die „SEMAC"-Zugangskontrollsysteme entwickelt, das die Sicherheitslücke behebt => Es muss von SOLAR-OT dringend an allen Standorten installiert werden
Hier ist die Versionsnummer der Firmware, die auf den SEMAC S2 (67 % der Solarparks) eingesetzt werden soll: 670VYJLN
Hier ist die Versionsnummer der Firmware, die auf den SEMAC S3V3 (33 % der Solarparks) eingesetzt werden soll: 628AUYSD

2. OPTIMIERUNG DER KONFIGURATION DER ÜBERWACHUNGSPLATTFORM

KONFIGURATION

Das Ziel sollte darin bestehen, die Anzahl der technischen Elemente, die zur Durchführung eines Angriffs missbraucht werden können, einzuschränken, indem nur die unbedingt notwendigen Dienste und Geräte installiert werden.
Die Erhöhung des Sicherheitsniveaus erfolgt durch eine gezielte Umsetzung verschärfter Maßnahmen, einschließlich:

- der Begrenzung der Funktionen der Plattform
- des rationalen Managements der materiellen Elemente der Plattform

A. Änderung der Standardkonfiguration

Jede Komponente ist gemäß einem spezifischen Standard konfiguriert, einschließlich:

- technischer Konten sowie der zugehörigen Authentifizierungselemente
- der verwendeten Netzwerkanschlüsse
- der Installations- und Arbeitsverzeichnisse
- der Zugriffsrechte auf Verzeichnisse und Dateien
- des zur Ausführung eines Dienstes oder eines Prozesses verwendeten Kontos und der mit diesem Konto verbundenen Rechte
- der Konfigurationsdateien für Sicherheitselemente, insbesondere in Bezug auf die Rückverfolgbarkeit.

B. Einschränkung der zugänglichen Funktionen

Nur die Module, die für den Betrieb und die Sicherheit der Plattform unbedingt erforderlich sind, werden aufrechterhalten, auf angemessene Weise konfiguriert sowie regelmäßig gewartet und überwacht.

Zu diesem Zweck analysiert der Betreiber die technische Funktionsweise der Plattform, um daraufhin installierte, aber nicht genutzte Dienste oder Funktionen einzustellen.
Von jeder Hardware- oder Softwarekonfiguration erfolgt eine Bestandsaufnahme in Form einer Referenzkonfiguration.

C. Bestandsaufnahme der angeschlossenen Elemente

Der Betreiber führt eine vollständige technische Bestandsaufnahme der Elemente durch, aus denen sich die Plattform zusammensetzt und erstellt umfassende Mappings. Das Bestandsverzeichnis umfasst alle Gerätschaften, die dauerhaft oder vorübergehend, physisch oder aus der Ferne mit der Plattform verbunden sein können (Arbeitsplatzrechner, Server, Peripheriegeräte etc.).

Falls sich Dritte mit der Plattform verbinden, vermerkt der Betreiber dies in seinem Mapping und bezieht dies in seine Risikoanalyse mit ein.

D. Verwendung von Elementen, die sich unter der Kontrolle des Betreibers befinden

Der Betreiber verwaltet direkt folgende Elemente:

- Bereitstellung von Updates
- Kontrolle aller Elemente
- Die Fernkonfiguration

ABSCHOTTUNG

Die Plattform folgt einer Segmentierungslogik, indem sie jedes Subsystem auf seine eigenen Aktionen beschränkt, um:

- die Angriffsfläche zu begrenzen
- einen möglichen Angriff einzudämmen
- die Auswirkungen einer Kompromittierung zu begrenzen
- die Anpassung des Sicherheitsniveaus eines jeden Subsystems zu ermöglichen

Die Abschottung gilt sowohl für physische als auch Logikmittel.

A. Segmentierung in Subsysteme

Die Segmentierung in Subsysteme wird nach folgenden Kriterien vorgenommen:

- Funktionen
- Datenschutzniveau
- Ausmaß der Exposition
- Sicherheitsstufe

Jede Verbindung zwischen den Subsystemen muss durch ein funktionales Erfordernis gerechtfertigt werden können.

B. Physische Abschottung

Ein Server ist den kritischsten Anwendungen gewidmet.

C. Logische Abschottung

Alle auf dem Server gespeicherten Daten werden im Vorfeld verschlüsselt. Jedes Subsystem folgt einem eigenen Verschlüsselungsschema.

Jegliche Kommunikation zwischen den Subsystemen läuft über das verschlüsselte und authentifizierte VPN.

FERNZUGRIFF

A. Öffentlicher Zugang

Der öffentliche Zugang folgt dem HTTPS-Protokoll und die Plattform wird durch die Vorlage eines Serverzertifikats authentifiziert.

Für die Nutzer der Plattform wird die Zwei-Faktor-Authentifizierung eingeführt.

B. Mobiler Zugang

Mobile Geräte werden dahingehend konfiguriert, dass die Kommunikation mit der Plattform über einen authentifizierten und verschlüsselten Tunnel erfolgt. Hierbei darf der Tunnel nicht deaktivierbar sein und der Zugang zum Internet oder zu einem lokalen Netzwerk ist nicht möglich. Die Systempartition und die Datenpartition sind vollständig verschlüsselt.

Die Zwei-Faktor-Authentifizierung ist auf dem Arbeitsplatzrechner eingerichtet.

NETZWERKFILTER

Zusätzlich zur Abschottung werden Filtermechanismen eingesetzt.

A. Filterpunkte

Die Verbindungen zwischen den Subsystemen sind die Hauptfilterpunkte, bei denen Perimeterfilter und lokale Filter angewendet werden.

B. Filterregeln

Die globale Fließmatrix schließt die geltenden Filterregeln mit ein. Sie wird jährlich aktualisiert.

C. Umsetzung

Die Filterung erfolgt durch dedizierte Firewalls, die auf dem Prinzip der Genehmigungslisten basieren.