

Cyber Security bei Solar-Log™

Whitepaper

In unserer Infrastruktur kommen immer mehr digitale und vernetzte Lösungen zum Einsatz, damit steigt das Risiko für Störungen und unerwünschte Einwirkungen von außen. Da wir mit unseren Produkten Teil dieser sensiblen Infrastruktur sind, steht das Thema Cyber Security bei uns ganz oben. Wir arbeiten aktiv daran, immer den höchsten Standard zu bieten, sind aber auch auf die Mitarbeit unserer Kunden und Partner angewiesen.

Dazu gibt es drei Punkte, die besondere Aufmerksamkeit verdienen und wir Ihnen hier erläutern wollen:

Aktuelle Firmware

Ein Baustein im Bereich der Cyber Security ist, die aktuelle Firmware auf unseren Solar-Log™ Geräten aufzuspielen. Neben neuen Implementierungen ist ein Schwerpunkt unserer Firmwareupdates das Thema Sicherheit und Stabilität.

Nur mit der aktuellen Firmware sind auch alle neusten Sicherheitsupdates gewährleistet und das Gerät entsprechend geschützt.

Dazu haben wir auf unserer Homepage [Solar-Log™ Firmware Download](#) immer die aktuelle Firmware für Sie bereitgestellt. Dort und auf unserem Firmware-Update-Server ist die neue Version der Solar-Log™ Base Firmware 6.3.0_172 verfügbar. Details zu den Kompatibilität sowie einen Überblick der Verbesserungen stehen in den [Release-Notes zur Firmware](#).

ISO/IEC 27001 Zertifikat

Eigentlich jeder Aspekt unseres täglichen Lebens ist immer stärker von der Digitalisierung betroffen und kann hierbei zu einem lohnenden Ziel werden. Gerade der immer stärkere Ausbau der dezentralen Energieerzeugungsanlagen kann nur durch den Einsatz von digitalen Lösungen gelingen. Hierzu bedarf es auch ausgeklügelter Schutzmechanismen und einer regelmäßigen Überprüfung der eingesetzten Mechanismen auf deren Wirksamkeit. Solar-Log™ hat sich verpflichtet, seinen Partnern im Markt bei der Bewältigung dieser ständigen Aufgabe zur Seite zu stehen.

Gerade durch das starke Wachstum in unserem Anlagenportfolio auf heute über 19,5 GWp installierter Anlagenleistung, sind wir uns unserer Verantwortung als Teil der Energieinfrastruktur bewusst. Um diesem auch nach außen entsprechend Rechnung zu tragen, haben wir unsere Prozesse und Abläufe in Bezug auf die Themen in der IT-Sicherheit einer Überprüfung durch die Zertifizierung gemäß der ISO/IEC 27001 unterzogen und erfolgreich zum Abschluss geführt.

Unsere Partner können in ihrer Infrastruktur sicher sein und auch gegenüber weiteren Prüfstellen nachweisen, dass ihre Partner, welche in der Infrastruktur zum Einsatz kommen, das Thema IT-Sicherheit ernst nehmen und sich hier regelmäßig neu hinterfragen.

Gerne stellen wir Ihnen das [ISO/IEC 27001 Zertifikat hier zur Verfügung](#).

Passwortschutz

Die Anforderungen an den Schutz personenbezogener Daten sind sehr hoch.

Sicherheitsmechanismen schränken vermeintlich den Komfort für den Nutzer ein, das ist meist jedoch nur oberflächlich betrachtet. Der Schaden, der bei einem Datenleck entsteht, ist mehrheitlich immens größer und erfordert aufwendige Maßnahmen, um ihn einzudämmen.

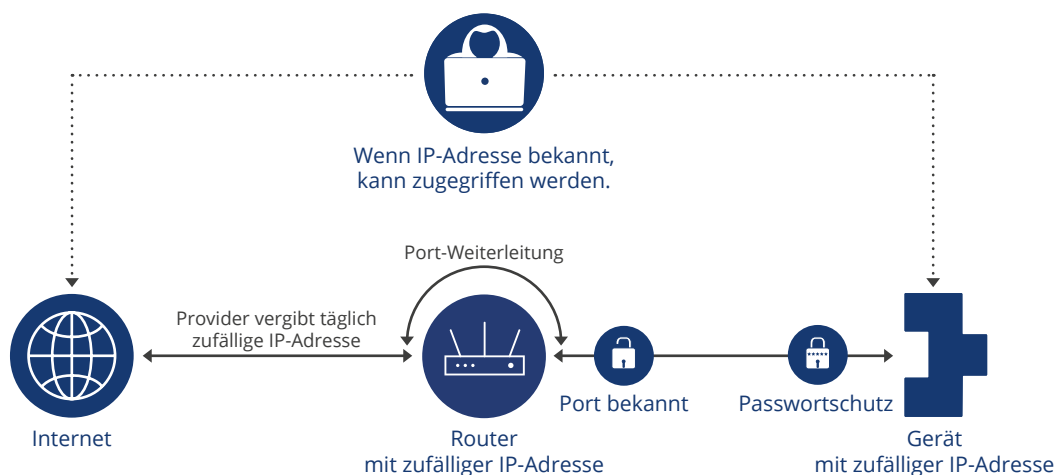
Geräte, die in Netzwerkinfrastrukturen eingesetzt werden, müssen eine Vielzahl an Sicherheitsmechanismen zur Verfügung stellen. Die Konfiguration dieser Geräte sollte immer aus Gesichtspunkten der Sicherheit erfolgen. Hierbei lassen sich zwei Bereiche definieren.

Zuerst müssen vorhandene Passwortfunktionen auf Geräten für den Zugriffsschutz gesetzt werden.

Solar-Log™ bietet diese Möglichkeit für seine Geräte und erläutert die Handhabung dieser Funktion auf dem Gerät und in der produktbegleitenden Dokumentation.

Für größtmöglichen Schutz vor unbefugten Zugriffen auf das Gerät sollte das Passwort bei der Erstinstallation gesetzt werden und die heute gängigen Anforderungen an Passwörter erfüllen:

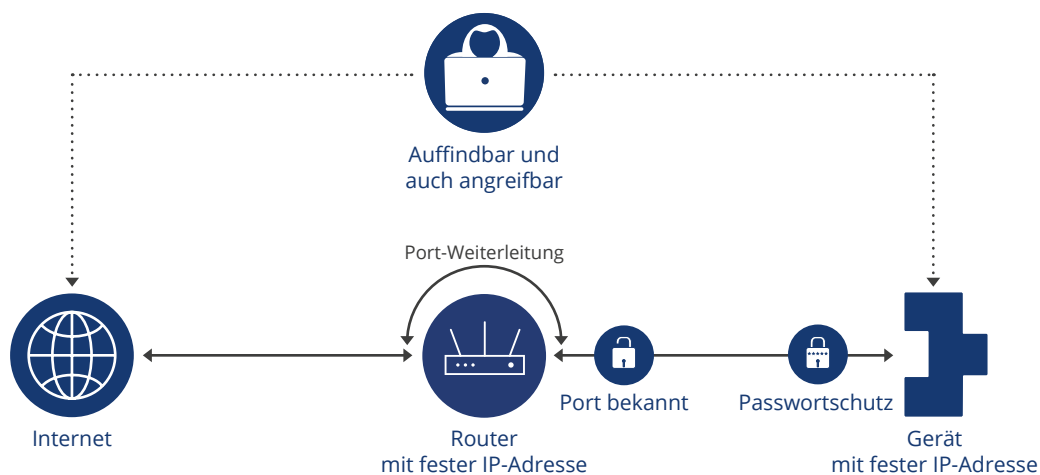
- Keine einzelnen Wörter oder Wortphrasen
- Mind. 9 Zeichen
- Kombination aus Großbuchstaben / Kleinbuchstaben / Ziffern und Sonderzeichen
- Das Passwort sollte nicht offen am Gerät angebracht werden und nur den berechtigten Personen bekannt sein.
- Für jedes Gerät ein eigenes Passwort nutzen.



Internetprovider vergeben nach einem Zufallsmechanismus die IP-Adressen der Router in Ihrem Netzwerk, welche täglich geändert werden. Diese IP-Adressen sind mit Hausnummern oder Hausadressen zu verglei-

chen. Ist der Standort eines Hauses bekannt, wird ein unerlaubter Zutritt nur noch durch verschlossene Türen verhindert. Im Netzwerk übernimmt der Router die Sicherheitsfunktion der Tür. Durch Port-Freigaben kann diese Tür jedoch offenstehen. Kennt man nun die IP-Adresse und den offenen Port, kann ohne Probleme auf das dem Port zugeordneten Gerät zugegriffen werden. Manche Services benötigen einen solchen Zugang in das Netzwerk, man sollte hier jedoch auf einen minimalen Umfang an geöffneten Ports (Türen) achten und die Dienste und Geräte, die dahinter liegen, mittels zusätzlicher Passwörter oder weiterer Mechanismen sichern.

Legt man die IP-Adresse vom Router dauerhaft fest, öffnet einen Port und definiert eine feste IP-Adresse für das Gerät im Netzwerk, welche dann über diesen Port erreichbar ist, so ist das Gerät über das Internet auffindbar und angreifbar. Somit sind alle vom Gerät bereitgestellten Anlagendaten oder persönlichen Daten für einen Angreifer potenziell verfügbar oder sicherheitsrelevanten Einstellungen, z. B. Netzeinstellungen für die Wirk- und Blindleistungssteuerung können verändert werden, was unter Umständen zu verheerenden Auswirkungen auf die Infrastruktur führen kann.



Daher sollten Sie als Nutzer die beiden erläuterten Punkte sehr ernst nehmen und auf die notwendige Konfiguration achten.

Solar-Log™ Geräte besitzen umfangreiche Mechanismen, um das Gerät im Netzwerk vor unbefugten Zugriffen zu sichern. Da wir das Thema IT-Sicherheit und Datenschutz immer im Fokus haben, entwickeln wir unsere Sicherheitsmechanismen ständig weiter. Für den bestimmungsgemäßen Betrieb des Solar-Log™ mit angebundenem Portal sind keine Netzwerkzugriffe aus dem Internet in das lokale Netzwerk notwendig. Dadurch ist bei einem bestimmungsgemäßen Gebrauch der Solar-Log™ Geräte sichergestellt, dass diese nicht im Internet sichtbar sind.

Wird ein Zugriff über das Internet auf den Solar-Log™ notwendig, empfehlen wir ausdrücklich, dass dieser Zugriff unbedingt durch einen IT-Spezialisten eingerichtet wird. Dieser ist in der Lage, zum Beispiel durch die Verwendung von VPN-Mechanismen den Zugang vor ungebetenen Zugriffen komplett abzusichern.