

# Kundeninformation

## IT-Sicherheit bei PV-Anlagen, Batteriespeichern, Wärmepumpen und Wallboxen

**Eine moderne Energieanlage ist heute auch ein IT-System.** Wechselrichter, Batteriespeicher, Energiemanagementsysteme und Wallboxen werden zunehmend mit dem lokalen Netzwerk und dem Internet verbunden. Damit entstehen neben den elektrotechnischen Anforderungen auch Anforderungen an Netzwerksicherheit, Zugriffsschutz und Datenschutz.

Wichtig: Ein Gerät, das per LAN oder WLAN mit Ihrem Netzwerk verbunden wird, ist nicht einfach nur ein weiteres Elektrogerät. Es kann Daten übertragen, Cloud-Dienste nutzen, Fernzugriffe ermöglichen und – bei einer unsicheren Konfiguration – ein Risiko für weitere Geräte im Netzwerk darstellen.

### 1. Welche Komponenten sind vernetzt?

Je nach Anlage können Wechselrichter, Batteriespeicher, Smart Meter, Energiemanagementsysteme und Wallboxen über LAN, WLAN oder Mobilfunk kommunizieren. Häufig bestehen zusätzlich Verbindungen zu Hersteller-Clouds und Smartphone-Apps.

### 2. Warum die Einbindung ins Netzwerk wichtig ist

Wird beispielsweise ein Wechselrichter einfach in das vorhandene Heim- oder Firmennetz eingesteckt, befindet er sich möglicherweise im selben Netzwerk wie PCs, Server, NAS-Systeme, Drucker und andere Geräte. Aus IT-Sicht sollte eine solche Vertrauensstellung nicht ohne Prüfung entstehen.

### 3. Netzwerksegmentierung – Energiegeräte sollten getrennt werden

Eine sichere Lösung ist häufig ein separates Netzwerk bzw. VLAN für IoT- und Energiegeräte. Dadurch kann verhindert werden, dass ein kompromittiertes Gerät auf Büro-PCs, Server oder private Daten zugreifen kann. Die Firewall regelt anschließend, welche Verbindungen tatsächlich erforderlich sind.

### 4. Keine unnötigen Portfreigaben

Eine häufige Fehlkonfiguration ist die direkte Erreichbarkeit eines Wechselrichters oder einer Wallbox aus dem Internet über eine Portweiterleitung im Router. Solche Freigaben sollten nicht die Standardlösung für Fernwartung sein. Wenn ein Fernzugriff erforderlich ist, sollte er über einen kontrollierten und abgesicherten Zugang erfolgen, beispielsweise über eine geeignete VPN-/Remote-Access-Lösung.

### 5. WLAN ist nicht automatisch sicher

Auch bei WLAN sollte geprüft werden, in welchem Netzwerk das Energiegerät betrieben wird. Wenn möglich, sollten PV, Speicher und Wallbox nicht gemeinsam mit PCs, Smartphones und anderen vertrauenswürdigen Geräten im normalen WLAN betrieben werden. Ein separates IoT-/Energie-WLAN kann die Risiken deutlich reduzieren.

## 6. Welche Daten entstehen?

Moderne Energieanlagen können detaillierte Informationen über Erzeugung, Verbrauch, Lade- und Entladevorgänge sowie den Betrieb einer Wallbox erfassen. Daraus können – je nach Anlage und Datenumfang – Rückschlüsse auf Nutzungsmuster und Anwesenheitszeiten entstehen.

## 7. Hersteller-Cloud und Datenschutz

Viele Anlagen verwenden Cloud-Dienste für Monitoring, Apps, Fernwartung oder Firmware-Updates. Das kann sinnvoll sein, sollte aber bewusst erfolgen. Kunden sollten wissen: Welche Daten werden übertragen? An wen? Wo werden sie verarbeitet bzw. gespeichert? Wie lange? Welche Benutzer und Dienstleister haben Zugriff? Welche Funktionen sind lokal ohne Cloud möglich?

## 8. Benutzerkonten und Passwörter

Nach der Installation sollten Standardpasswörter geändert und individuelle Zugangsdaten verwendet werden. Installateur-, Service- und Benutzerkonten sollten nachvollziehbar dokumentiert werden. Nicht mehr benötigte Zugänge sollten deaktiviert werden. MFA/2FA sollte aktiviert werden, sofern verfügbar.

## 9. Firmware und Sicherheitsupdates

Wechselrichter, Speicher und Wallboxen enthalten Software und benötigen deshalb ebenfalls Updates. Sicherheits- und Firmwareupdates sollten regelmäßig geprüft und nach Möglichkeit zeitnah installiert werden. Außerdem sollte eindeutig festgelegt sein, wer für Aktualisierung und Sicherheitsmeldungen verantwortlich ist.

## 10. Fernwartung – Komfort und Risiko abwägen

Fernwartung kann praktisch sein, bedeutet aber zusätzlichen Zugriff. Dokumentiert werden sollte: Wer kann zugreifen? Über welchen Weg? Mit welchen Rechten? Wie lange? Wie wird der Zugang geschützt? Wann wird er deaktiviert?

## 11. Was sollte bei der Übergabe dokumentiert werden?

Zu einer professionellen Installation gehört aus IT-Sicht möglichst eine nachvollziehbare Dokumentation. Dazu gehören Geräte, Netzwerkanschlüsse, IP-/MAC-Adressen, VLANs, Cloud-Dienste, Fernzugänge, relevante Firewall-Regeln, Benutzerkonten und Firmwarestände.

## Was können Sie als Kunde erwarten?

| Grundsatz      | Was bedeutet das?                                                              |
|----------------|--------------------------------------------------------------------------------|
| Transparenz    | Welche Geräte sind mit Netzwerk und Internet verbunden?                        |
| Sicherheit     | Unnötige Portfreigaben und direkte Internetzugriffe vermeiden.                 |
| Trennung       | Energie-/IoT-Geräte soweit sinnvoll vom normalen Netz trennen.                 |
| Zugriffsschutz | Standardpasswörter, unnötige Konten und unkontrollierte Fernzugänge vermeiden. |
| Datenschutz    | Cloud-Nutzung und Datenübertragung nachvollziehbar machen.                     |
| Dokumentation  | Netzwerk, Geräte, Zugänge und Einstellungen dokumentieren.                     |

Wartung

Verantwortlichkeit für Updates und Sicherheitsprüfungen festlegen.

## Unser Tipp

**Lassen Sie bei der Installation einer netzwerkfähigen Energieanlage nicht nur den elektrischen Anschluss, sondern auch die IT-Einbindung prüfen.** Netzwerksegmentierung, sichere Zugangsdaten, kontrollierte Internetkommunikation und nachvollziehbare Dokumentation können verhindern, dass aus einer modernen Energieanlage ein Sicherheitsrisiko für das gesamte Netzwerk wird.

## Technischer Hintergrund

Die IT-Sicherheitsbetrachtung ergänzt die elektrotechnischen Anforderungen und beschäftigt sich insbesondere mit Netzwerksegmentierung, Zugriffsschutz, Fernzugriff, Cloud-Kommunikation, Updates und Datenschutz.

Hinweis: Diese Kundeninformation dient der allgemeinen technischen Information. Sie stellt keine Rechtsberatung dar und ersetzt weder die elektrotechnische Planung, Prüfung und Abnahme noch eine individuelle datenschutzrechtliche Beratung.