Remote Monitoring
Mit dieser **Checkliste** zu **mehr Sicherheit für Ihre Daten**!

SEKAS

SEKAS.DE

Remote Monitoring? Aber sicher!

Die Digitalisierung mit Schlagworten wie Industrie 4.0 und Smart Factory bietet Unternehmen zahlreiche Chancen. Gleichzeitig gewinnt das Thema IT-Sicherheit wegen der zunehmenden Vernetzung massiv an Bedeutung. Wer die Potenziale nutzen will, ohne die Sicherheit zu vernachlässigen, braucht entsprechende Konzepte und Lösungen.

Fast täglich kursieren in den Medien neue Meldungen zu Datenpannen oder Hacker-Attacken. Das nachfolgende Paper zeigt am Beispiel von Remote Monitoring, wie bestehende Risiken vermieden werden können.

Inhalt

Fernwartung vs. Remote Monitoring

Zunächst gilt es, die Begriffe Fernwartung und Fernüberwachung (Remote Monitoring) auseinanderzuhalten.

Während es beim **Remote Monitoring** um ein **reines Beobachten** geht, ermöglicht die **Fernwartung** das **Eingreifen in die Anlage**. Wird ein Fernwirken von außen technisch ermöglicht, besteht aber die Gefahr, dass Angreifer das missbrauchen.

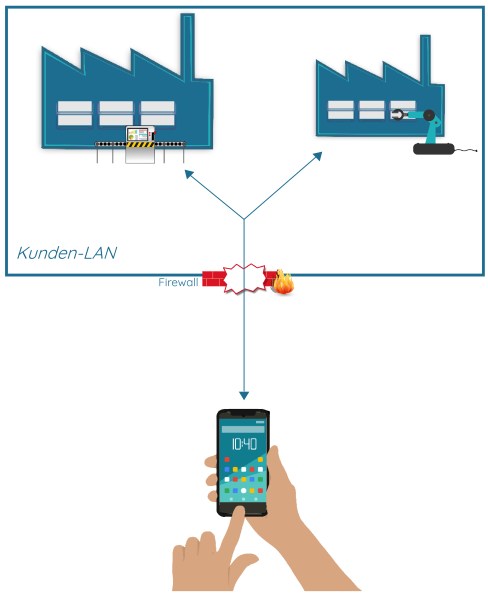
Um dieses Risiko zu vermeiden, ist es in vielen Fällen ratsam, dauerhaft nur eine Monitoring-Lösung zu betreiben und einen Zugriff von außen zunächst gar nicht zu ermöglichen. Kommt es zu einer Störung, bei der ein Fernwirken erforderlich ist, kann temporär und streng kontrolliert das Netzwerk etwas geöffnet und die Nutzung einer Fernwartungslösung ermöglicht werden.

Zugriff auf das Netzwerk beschränken, Daten eingeschränkt teilen

Grundsätzlich gibt es **zwei Varianten**, ein Remote Monitoring aufzubauen: Entweder ermöglicht man den externen Zugriff auf das Anlagennetzwerk oder die Daten werden aus dem geschützten Netzwerk nach außen übertragen.

Für den externen Zugriff gibt es Lösungen, die gesicherte Verbindungen (z. B. via VPN) in ein Netzwerk ermöglichen. Hierfür muss das Netzwerk aber für einen externen Zugriff geöffnet werden, was die bereits erwähnten Risiken birgt. Zudem stellt sich die Frage, wie der Zugriff von außen zuverlässig auf das erforderliche Maß beschränkt wird.

Besser ist eine Lösung, die dieses Risiko vermeidet, indem die benötigten Daten grundsätzlich nur aus dem Anlagennetzwerk heraus übertragen werden und jeglicher Rückkanal als potenzielles Sicherheitsrisiko ausgeschlossen wird.

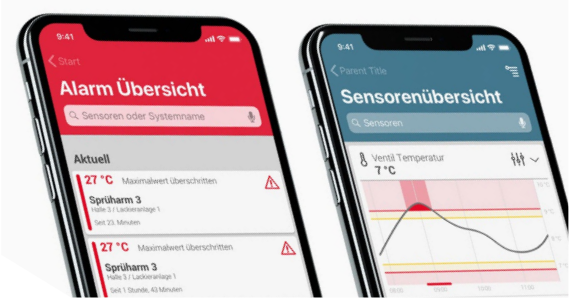


Für Remote Monitoring stehen prinzipiell zwei Lösungsansätze zur Verfügung: entweder lässt man einen Zugriff von außen zu oder man überträgt Daten aus dem Netzwerk nach außen.

„Daten sind das neue Gold“ - Datenhoheit behalten

Aus der Vernetzung und der Datenflut auf Anlagenebene ergibt sich ein neuer Aspekt. Die gesammelten Daten können die Grundlage für neue und lukrative Geschäftsmodelle sein, die unter Umständen sogar erst künftig entstehen. Nicht umsonst heißt es häufig „Daten sind das neue Gold“.

Somit gilt es, die Hoheit über seine eigenen Daten zu behalten und diese nicht unbedacht einem anderen Unternehmen, z. B. einem Anlagenhersteller oder Cloud-Anbieter, zu überlassen.



Remote Monitoring soll es Betreibern ermöglichen, schnell und übersichtlich über bestehende Störungen informiert zu werden.

Hier ist zunächst das Prinzip der Datensparsamkeit zu betrachten, denn es sind nicht alle Detail-Daten zum Zustand einer Anlage für ein Remote Monitoring erforderlich. Ziel einer Monitoring-Lösung ist es, Störungen schnell zu erkennen und relevante grundlegende Informationen zu der Störung zu einem Remote-Anwender zu transportieren.

Dazu sind nur wenige, zentrale, ggf. auch schon vorverarbeitete Informationen relevant. Für Anwendungsfälle mit größerem Informationsbedarf ist eher ein zweistufiges Tooling empfehlenswert. Soll zum Beispiel **Predictive Maintenance** genutzt werden, so basiert dies auf einer großen Sammlung historischer Anlagendaten und einer intelligenter Datenanalyse. Die Datensammlung und Analyse kann innerhalb des geschützten Netzwerkes des Anlagenbetreibers erfolgen. Wichtige Erkenntnisse aus dem Predictive Maintenance zum Anlagenzustand könnten dann aber von der Condition-Monitoring-Lösung an das Remote Monitoring gemeldet und so nach außen kommuniziert werden.

Beim Aufbau einer vernetzen Monitoring Lösung gilt es also zu definieren, welche Daten für ein voll umfassendes Monitoring aber ggf. nur intern benötigt werden und welche Daten auch außerhalb des Anlagennetzwerkes, z. B. für ein Remote Monitoring, relevant sind.

Der Betreiber der Anlage sollte hierbei selbst entscheiden können, welche Daten und Status-Information seiner Anlage überhaupt für eine Remote Überwachung relevant sind und nach außen übermittelt werden.

Im nächsten Schritt gilt es, diese Daten, die nach außen verfügbar gemacht werden sollen, entsprechend zu schützen.

Aus unserer Sicht können schon die nachfolgend diskutierten Aspekte maßgeblich zum Schutz der Vertraulichkeit der Daten beitragen, finden aber in der Praxis oftmals keine oder nicht ausreichend Anwendung.

Vertrauen ist gut - „Trust No One“ ist besser

Seine vertraulichen Daten vor einer Übertragung zu verschlüsseln sollte heutzutage selbstverständlich sein. Daten sollten bevorzugt **Ende-zu-Ende verschlüsselt** werden. Sie werden dabei vor der Übertragung verschlüsselt und erst am anderen Ende, z. B. in der entsprechenden App, entschlüsselt.

Wesentliche Frage dabei ist, wer Zugriff auf die Schlüsselmittel hat, die es ermöglichen, die Daten zu entschlüsseln. In den meisten Systemen werden für die Ende-zu-Ende-Verschlüsselung zwar individuelle, private Schlüssel angelegt, diese dann aber über die Hersteller-Lösung ausgetauscht oder dort gespeichert. Damit ist folglich auch der Lösungsanbieter technisch in der Lage, die Daten zu entschlüsseln und man muss darauf vertrauen, dass dies nicht missbraucht wird.

Im Gegensatz hierzu steht der im Bereich der Cybersecurity **Trust No One (TNO) Ansatz**. Hierbei dürfen prinzipiell nur diejenigen Parteien Zugriff auf die Schlüsselmittel haben, die die Daten auch erhalten und entschlüsseln sollen.

Bei einer nach diesem Prinzip aufgebauten Cloud-Lösung werden sämtliche Daten entsprechend verschlüsselt übertragen und **verschlüsselt in der Cloud gespeichert**. Die **Schlüssel werden beim Anwender erzeugt und bleiben ausschließlich in dessen Hand**. Damit bietet die Lösung eine echte Ende-zu-Ende-Verschlüsselung, denn z. B. auch der Cloud-Anbieter hat keinen Schlüsselzugriff.

Pseudonymisierung – Daten-Gold entwerten

Bei einer sicheren Monitoring Lösung sollten also z. B. Sensordaten und Zustandsinformation, wie oben beschrieben, durch Verschlüsselung geschützt werden. Daneben ist aber auch die Information zum Datenursprung und jegliche Metainformation zum Sensor als vertraulich einzustufen. Eine Verschlüsselung dieser Informationen ist nicht immer vollständig möglich, da über sie z. B. auch die Verteilung der Sensordaten an die Endgeräte und Anwender gesteuert wird.

Die Vertraulichkeit in diesem Kontext kann aber über eine **Pseudonymisierung** der Daten erreicht werden. Hierbei definiert der Anlagenbetreiber beispielsweise selbst die Sensoren seiner Anlagen und erzeugt dabei eine weltweit eindeutige anonyme Kennung (als Pseudonym) für jeden Sensor. Die Abbildungstabelle zwischen den Pseudonymen und den tatsächlichen Sensoren bleibt gemäß Trust No One Prinzip ebenfalls alleine für den Anlagenbetreiber zugreifbar.

An die Cloud werden ausschließlich das Pseudonym eines Sensors sowie ein **verschlüsselter Datenstrom** mit Sensordaten übermittelt. Die dort gespeicherten Daten sind somit völlig anonym und enthalten keinen Bezug zu einem konkreten Sensor, zu einer Maschine oder zum Anlagenbetreiber.

Aufgrund der fehlenden Metainformation, die eine Interpretation der gespeicherten Daten möglich machen würde, ist das ursprüngliche Daten-Gold für Dritte wertlos.

Checkliste für Ihre Remote Monitoring Lösung

Beim Aufbau einer Remote-Monitoring-Lösung empfehlen wir, intensiv auf die folgenden – oftmals vernachlässigten – Punkte zu achten:

- ☐ Vermeiden Sie eine Öffnung Ihres Netzwerkes nach außen. Liefern Sie bevorzugt **Daten nach außen, ohne einen Rückkanal** zu ermöglichen.
- ☐ Prüfen Sie, welche Information nach außen übermittelt werden muss. Beachten Sie beim Remote Monitoring das Prinzip der **Datensparsamkeit**.
- ☐ Stellen Sie sicher, dass Daten **ausschließlich über gesicherte Verbindungen** und **nur verschlüsselt** übertragen werden. Achten Sie hier auf moderne und sichere Verfahren.
- ☐ Achten Sie auf eine „echte" **Ende-zu-Ende Verschlüsselung** der Daten, d. h. hinterfragen Sie, wer Zugriff auf die Schlüsselmittel zur Ver- und Entschlüsselung hat. Setzen Sie möglichst auf einen **Trust No One Ansatz**.
- ☐ Hinterfragen Sie, welche Daten in der Lösung nicht verschlüsselt werden und prüfen Sie, ob hier eine Vertraulichkeit anderweitig, z. B. durch Pseudonymisierung unterstützt wird.

Ausblick: Datenverarbeitung trotz Verschlüsselung

Da auf dem Cloud-Server bei einem Trust No One Konzept keine Entschlüsselung der Daten erfolgen kann, ist deren dortige Verarbeitung zunächst unmöglich. Allerdings ist die serverseitige Verarbeitung die Basis für zahlreiche interessante Funktionen, die anders nicht sinnvoll umsetzbar sind.

Im Bereich Forschung und Entwicklung wird intensiv an neuartigen Verschlüsselungsverfahren gearbeitet, die dieses Dilemma auflösen sollen. Sie ermöglichen die Ausführung von Rechen- und Vergleichsoperationen auf verschlüsselten Daten. Damit können z. B. Toleranzbereiche serverseitig überprüft oder moderne Verfahren zur Zustandsschätzung, Datenfusion und -filterung umgesetzt werden.

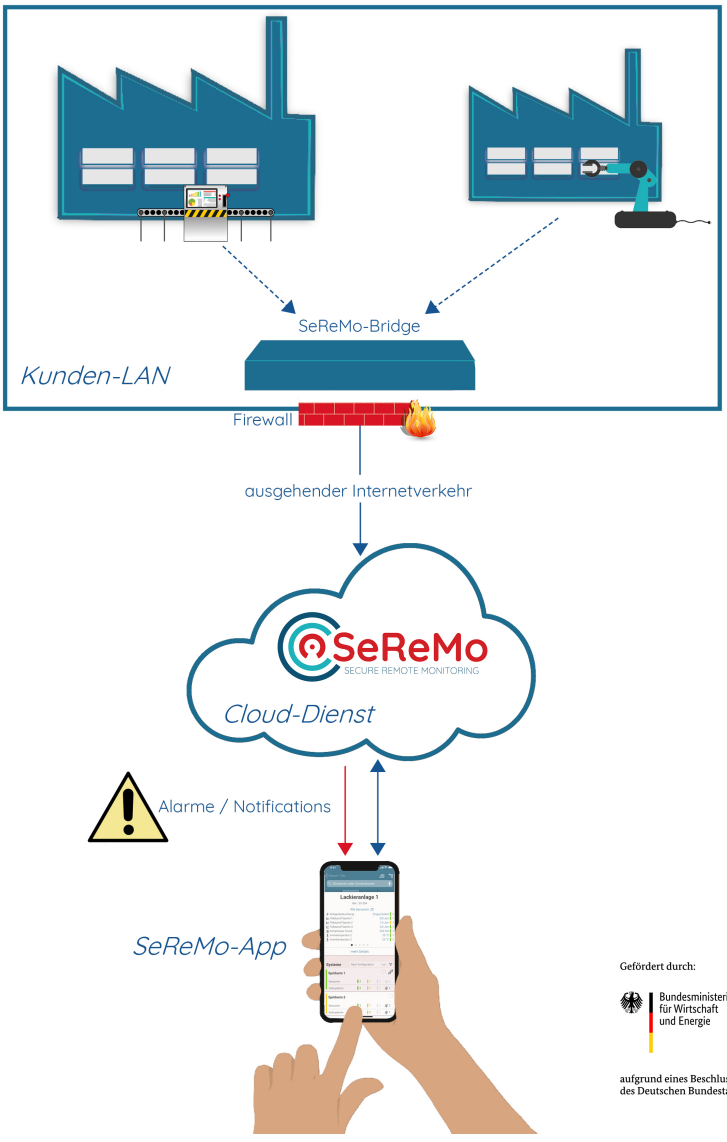
Für Anwender, denen es beim Remote Monitoring auf ein hohes Maß an Sicherheit ankommt, zeigt z. B. das Projekt **SeReMo** eine innovative und einzigartige Lösungsmöglichkeit auf. Hier wird u. a. auch an verschiedenen innovativen Verschlüsselungsverfahren geforscht.

Über SeReMo

SeReMo basiert auf einer **Cloud-Infrastruktur**, stellt dabei aber die Themen **Security und Vertraulichkeit der Daten** in den Mittelpunkt. SeReMo verzichtet vollständig auf einen Zugriff von außen auf das Netz der zu überwachenden Anlage. So kann ein unberechtigtes Fernwirken ausgeschlossen werden.

SeReMo erlaubt es, nur die für die Remote-Überwachung relevanten Daten bereitzustellen. Die Daten werden bei der Übermittlung durch ein ausgeklügeltes Trust No One Konzept geschützt und Ende-zu-Ende verschlüsselt. Sensible Daten des Kunden sind damit weder durch den Betreiber des Dienstes noch durch Dritte einsehbar.

Durch optional nutzbare spezielle Verschlüsselungsverfahren ist aber dennoch eine serverseitige Datenverarbeitung möglich, um hier z. B. eine Schwellwertüberwachung vorzunehmen, obwohl die Daten nicht entschlüsselt werden können.



Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Security und Sicherheit der Daten stehen bei SeReMo im Mittelpunkt. Die innovative Remote Monitoring Lösung eignet sich besonders für sensible Anwendungsbereiche.

Über die SEKAS GmbH

Die SEKAS GmbH ist ein mittelständisches Unternehmen für Software- und Systemengineering mit Sitz in München. Seit 35 Jahren haben wir uns als Entwicklungspartner namhafter, internationaler Kunden aus der Industrie sowie für öffentliche Auftraggeber etabliert. Mit einem hochqualifizierten und interdisziplinär besetzten Entwicklungsteam übernimmt SEKAS bevorzugt Kundenprojekte zur Entwicklung innovativer und anspruchsvoller IT-Systeme im technisch-wissenschaftlichen Umfeld. Die Tätigkeitsgebiete erstrecken sich von der Einbindung von Geräten und Sensoren, über die klassische Applikations- bis zur modernen Webentwicklung. Typische Anwendungsgebiete liegen im Bereich Messtechnik, Kommunikation, Funküberwachung und in der Energietechnik.

IHR PERSÖNLICHER ANSPRECHPARTNER:

SEKAS GmbH
Thomas Krenzke
T. +49 (0) 89 74 81 34 0
F. +49 (0) 89 74 81 34 99
E. thomas.krenzke@sekas.de
LinkedIn. /thomas-krenzke