Wie Sie Fernwartung und Monitoring sicherer machen können

Betreiber von Maschinen und Anlagen erwarten höchstmögliche Produktivität und Verfügbarkeit sowie eine schnelle Fehlerbeseitigung im Störungsfall. Die Prozessüberwachung, Remote Maintenance und Predictive Maintenance sind daher sehr effektive Instrumente für die Anlageneffizienz. Die erweiterten Services benötigen allerdings einen permanenten Onlinezugang. Dadurch steigen jedoch die Sicherheitsrisiken erheblich. Deshalb stellt sich die Frage, welche Standards bei der IT-Sicherheit heute für Fernwartungs- und Monitoringlösungen mindestens notwendig und wie sie in der Praxis umsetzbar sind.

SecurITy made in Germany

genua Ein Unternehmen der Bundesdruckerei

Inhalt

1. Fernwartungslösungen und Monitoringkonzepte sind im Umbruch

Mit der Einführung von Industrie 4.0 und „Smart Services“ sind neue digitale Monitoringkonzepte und Fernwartungslösungen verfügbar, die vollkommen neue Möglichkeiten eröffnen. Sie verändern sich von rein reaktiven Instrumenten zur Beseitigung von Störungen hin zu aktiven onlinebasierten Effizienzlösungen:

Cloud-Plattformen bieten Smart Data Analytics zur Analyse des Anlagenzustands mit Kennzahlen zur Gesamtanlageneffektivität (OEE = Overall Equipment Effectiveness). Sie sind der Ausgangspunkt für neue Services, um den Anlagenbetrieb weiter zu optimieren.

Mit einer vorausschauenden Wartung (Predictive Maintenance) können die Anlagendaten genutzt werden, um bereits erste Anzeichen einer Störung zu erkennen und Wartungen proaktiv durchzuführen.

Die aktiven Instrumente werden ergänzt mit Fernwartungslösungen (Remote Maintenance), um Fehler schnell zu beseitigen und die Anlagenverfügbarkeit sicherzustellen.

Bei der Einführung von Online-Plattformen und Fernwartungslösungen sind allerdings die zunehmenden Cyberrisiken zu berücksichtigen.

2. Monitoring- und Fernwartungszugänge sind akut gefährdet

Laut dem Lagebericht zur IT-Sicherheit vom Bundesamt für Sicherheit in der Informationstechnik (BSI) hat sich die Gefährdungslage weiter verschärft. Es gibt eine hohe Dynamik bei der Weiterentwicklung von Schadprogrammen und Angriffswegen.

Das Problem:
Dem gestiegenen Sicherheitsrisiko stehen vielfach unzureichende Sicherheitsmaßnahmen gegenüber.

So zeigen einfache Portscans regelmäßig Tausende offener Ports. Angreifer scannen das Internet aktiv nach solchen Zugängen, um darüber ihre Malware zu installieren.

Eine Kaspersky-Studie berichtet, dass die durchschnittlichen Kosten aufgrund eines Datenlecks bei kleinen und mittleren Unternehmen im Vergleich zum Vorjahr um 37 Prozent auf 120.000 US-Dollar gestiegen sind (Kaspersky-Studie, Folgekosten eines Cybersicherheitsvorfalls, 2018).

Knapp

70 %

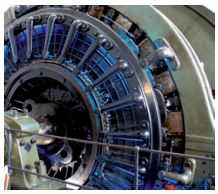
der Unternehmen und Institutionen in Deutschland sind nach dem BSI-Lagebericht 2018 Opfer von Cyber-Angriffen geworden.

„Jeder zweite erfolgreiche Angriff führte dabei zu Produktions- bzw. Betriebsausfällen.“

Aber auch zugelassene Fernwartungszugriffe können unerwünschte Folgen haben. So sind bei einer Fernwartungssession oft komplette Netzsegmente oder Produktionsstränge mit allen darin befindlichen Komponenten und Anlagen im Zugriff, einschließlich der Maschinen anderer Hersteller. In der Folge können sensible und schützenswerte Produktions- und Anlagendaten ungehindert abfließen.

Schließlich kann ein unkontrollierter Fernwartungszugang zur falschen Zeit auch laufende Betriebsprozesse empfindlich stören oder gar die Sicherheit von Mitarbeitern an der Maschine gefährden.

3. Anlagenbauer benötigen effiziente und sichere Fernwartungssysteme



Anlagenbauer nutzen Fernwartungszugänge, um aus der Ferne direkt auf ihre Anlagen zugreifen, Probleme erkennen und schnell lösen zu können. In der Gewährleistungsphase können darüber vertraglich zugesicherte Leistungen besonders effizient erbracht werden. Anschließend sind die Fernwartung und andere Teleservice-Leistungen ein zunehmend attraktives Service-Instrument.

Für erweiterte Services bis hin zu neuen Geschäftsmodellen ist in der Regel ein ständiger Zugriff auf die Anlagen erforderlich. Typische Stichworte sind hier Industrie 4.0 mit „Smart Services“ und die Plattform-Modelle. Hier sollen Daten über die laufenden Prozesse erfasst, gespeichert und ausgewertet werden.

So sagen 46 Prozent der Industrieunternehmen, dass sie auf Basis der Digitalisierung komplett neue Produkte und Dienstleistungen entwickeln oder diese planen, berichtet der Digitalverband Bitkom („Digitalisierung schafft neue Geschäftsmodelle in der Industrie“, Bitkom 2019).

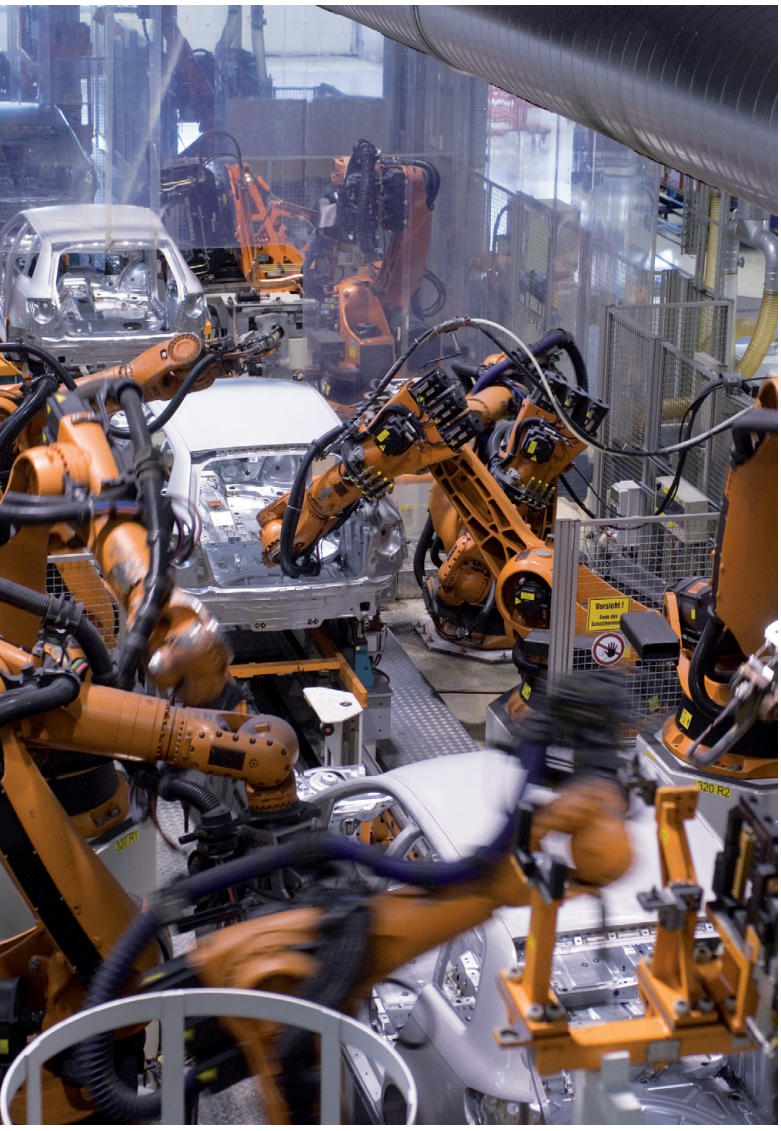
Für neue Wartungsmodelle wie Predictive Maintenance ist es für Anlagenbauer sehr wichtig, dass möglichst viele Anlagenbetreiber einem Online-Zugriff zustimmen. Denn erst mit einer ausreichend großen Datenbasis können verlässliche Vorhersagen über den Verschleiß oder die Störanfälligkeit von Maschinenkomponenten getroffen werden.

Anlagenbauer mit einer großen Zahl von Maschinen im Feld haben allerdings die Sorge, dass der Aufwand für die Konfiguration und die Verwaltung der Online-Zugänge durch unterschiedlichste kundenindividuelle Vorgaben und Regeln schnell sehr groß werden kann. Deshalb wünschen sie sich eine effizient nutzbare, umfassend und flexibel konfigurierbare Lösung für alle Fernwartungszugänge.

Letztendlich entscheidet aber das Sicherheitsniveau der Fernwartungslösung darüber, ob und in welchem Umfang solche Zugriffe in das Kundennetz erfolgen dürfen.

Häufig fehlt bei den Anlagenbetreibern die Akzeptanz, weil vom Fernwarter zwar ein hoher Sicherheitsstandard versprochen wird, das tatsächliche Sicherheitsniveau aber oft unklar bleibt.

4. Für Anlagenbetreiber ist die Sicherheit das wichtigste Kriterium



Anlagenbetreiber wissen,
dass den Vorteilen einer Prozessoptimierung und einer hohen Maschinenverfügbarkeit durch die Fernwartung zusätzliche Sicherheitsrisiken gegenüberstehen. Sie befürchten das Abfließen sensibler Produktionsdaten, eine (un)beabsichtigte Einschleusung von Malware und generell den Verlust an Kontrolle durch die Zugriffe in ihre sensiblen Netzwerke. Ein ständiger Onlinezugang z. B. zur Zustandsüberwachung wird daher sehr kritisch gesehen. Anlagenbetreiber sind sehr skeptisch, ob die Daten sicher ausgeleitet werden. Kleinen und mittelständischen Unternehmen fehlt zudem das Know-how, hier ihre eigenen Sicherheitspolicies zu entwickeln und gegenüber den Herstellern durchzusetzen.

Aus Sicht der Anlagenbetreiber
sollten bei der Sicherheit von Fernzugriffen deshalb Mindeststandards eingehalten werden. Ein zentraler Punkt ist dabei, dass die Anlagenbetreiber jederzeit die volle Kontrolle über externe Zugriffe behalten.

Anlagenbetreiber brauchen volle **Kontrolle** über Zugriffe

5. BSI fordert bestmögliche Absicherung der Fernwartung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) betont in seiner Analyse zur „Fernwartung im industriellen Umfeld“, dass die Einrichtung eines Fernwartungszuganges generell eine erhebliche Bedrohung darstellt. Die Fernwartungsschnittstelle sollte deshalb bestmöglichst abgesichert werden. „Die Produkteigenschaften einzelner Lösungen unterscheiden sich dabei teilweise signifikant.“

Das BSI hat deshalb generische Anforderungen für industrielle Fernwartung gemäß dem Stand der Technik formuliert (vgl. BSI-CS 054 und BSI-CS 108, Version 2.0 vom 11.07.2018). Die Anforderungen betreffen die Architektur, die sichere Kommunikation, die Authentisierungsmechanismen, die organisatorischen Anforderungen und weitere sinnvolle Regelungen.

DIE WICHTIGSTEN ANFORDERUNGEN:

Verbindungsaufbau nur von innen nach außen

Fernwartungszugriff auf ein Wartungsobjekt beschränken

Direkte Wartungszugriffe aus dem Internet ausschließen

Fernwartern nur unbedingt notwendige Rechte einräumen

Den Datentransfer verschlüsseln

Fernwartungszugriffe revisionssicher dokumentieren

Sichere Authentifizierung

6. Mit diesen Vorgaben wird eine sichere Fernwartung erreicht

Eine vertrauenswürdige Fernwartungslösung sorgt dafür, dass der Anlagenbetreiber über jeden Zugriff die Kontrolle behält. Das Ziel ist die größtmögliche Transparenz für Anlagenbetreiber und Dienstleister. Die folgenden Vorgaben von 6.1 bis 6.7 können das sicherstellen.

> Als Spezialist für IT-Sicherheit empfiehlt genua, die Anforderungen des BSI für die industrielle Fernwartung immer nur komplett umzusetzen, da sich die einzelnen Elemente untereinander ergänzen und ein fehlendes Glied in der Kette die Sicherheit des Gesamtsystems gefährdet.

6.1 Verbindungsaufbau nur von innen nach außen zulassen

Der Verbindungsaufbau für eine Fernwartungssession darf nur von innen nach außen erfolgen. Gegenüber dem Internet dürfen keine Ports dauerhaft geöffnet sein.

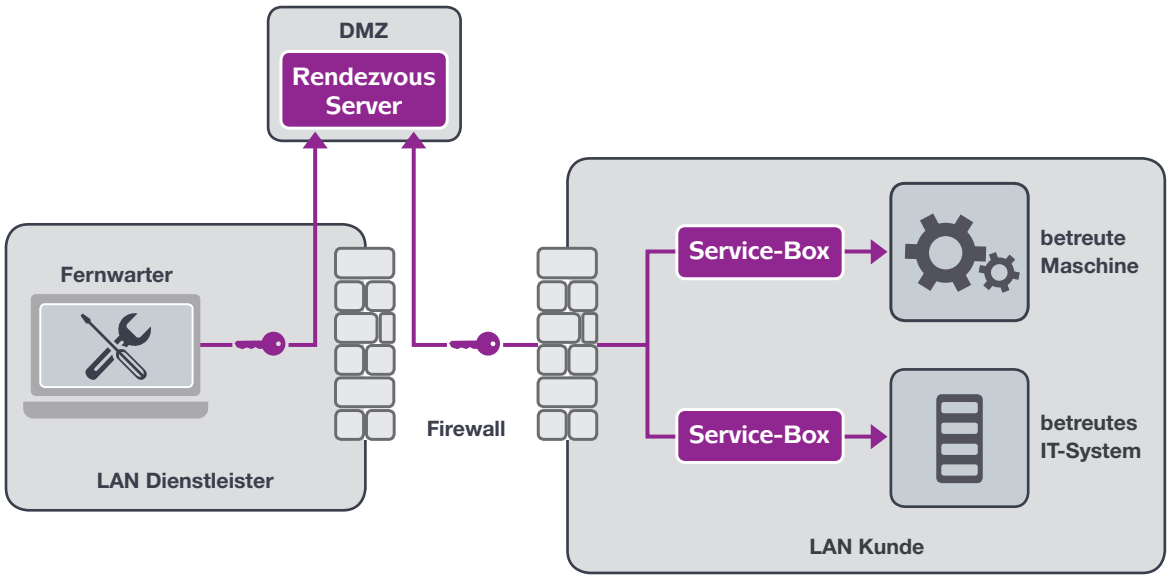
Externe Zugriffe per Schlüsselschalter kontrollieren

Kontrolle Schlüsselschalter:
Einseitige Fernwartungszugriffe externer Dienstleister sollten z. B. durch Hardware-Schlüsselschalter oder Software-Optionen ausgeschlossen werden. Dann ist ein Onlinezugriff erst möglich, wenn die Mitarbeiter des Anlagenbetreibers die Fernwartungssession von innen heraus aktiv einleiten.

6.2 Den direkten Fernwartungszugriff aus dem Internet ausschließen

Eine direkte Verbindung mit dem Internet sollte ausgeschlossen werden, indem eine neutrale Zwischenebene in einer demilitarisierten Zone (DMZ) eingefügt wird.

Das Rendezvous-Konzept:
Sichere Fernwartungslösungen setzen auf einen sogenannten Rendezvous-Server, der in der demilitarisierten Zone (DMZ) neben der Firewall installiert wird. Hierhin bauen sowohl der Wartungs-Service als auch der Maschinenbetreiber zum vereinbarten Zeitpunkt verschlüsselte Verbindungen auf. Erst mit deren Rendezvous auf dem zentralen Server entsteht die durchgängige Wartungsverbindung zur betreuten Maschine.



6.3 Den Datentransfer verschlüsseln

Um die Sicherheit und Vertraulichkeit von Maschinen und Anlagen zu gewährleisten, muss der Datentransfer sicher verschlüsselt werden.

Verschlüsselter Datentransfer:
Ein Mindeststandard für den externen Zugriff ist eine sichere VPN-Verbindung (Virtual Private Network) mit ausschließlich hochsicheren Verschlüsselungs-Algorithmen.

6.4 Sichere Authentifizierung umsetzen

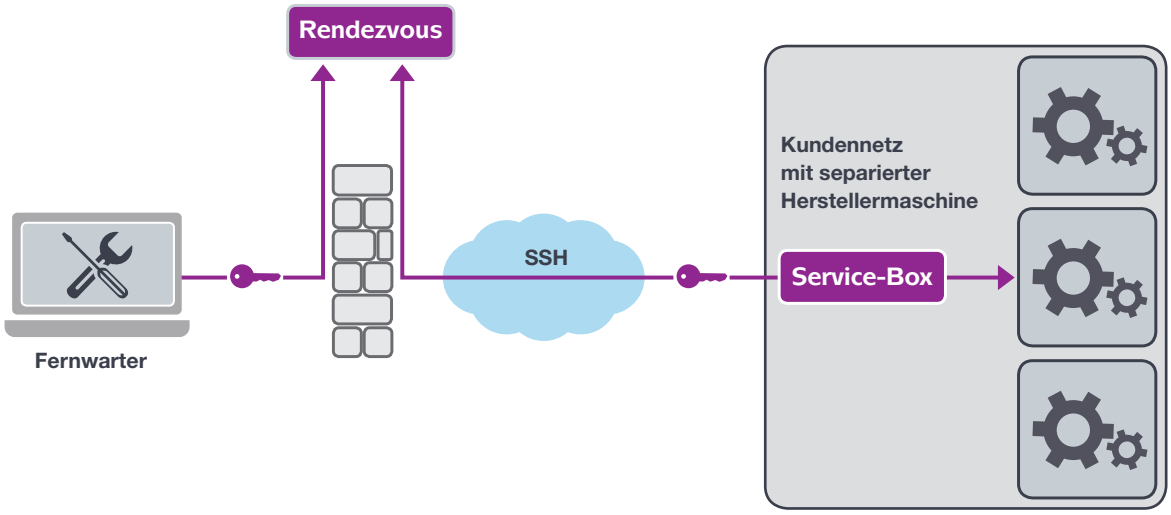
Für den Zugriff auf das Produktionsnetz sollte eine sichere 2-Faktor-Authentifizierung zwingend notwendig sein.

Beispielsweise durch die Eingabe eines Passworts (FAKTOR WISSEN) und das Einstecken einer Smartcard (FAKTOR BESITZ).

6.5 Den Onlinezugriff auf ein Objekt beschränken

Zusätzlich gilt es den unerwünschten Zugriff auf komplette Anlagen, besonders schützenswerte Anlagenkonfigurationen oder weitere Komponenten im Netzwerk auszuschließen.

Zugriffsbeschränkung auf ein Wartungsobjekt:
Um Fernwartungszugriffe feingranular auf ein einzelnes Fernwartungsobjekt zu beschränken, empfiehlt sich eine Datenverbindung per SSH (Secure Shell) anstelle von IPsec (Internet Protocol Security). SSH ist ein Netzwerkprotokoll, mit dem sich die verschlüsselte Verbindung über eine Firewall auf eine IP-Adresse und einen Port begrenzen lässt. Demgegenüber wird mit IPsec ein vollkommen transparenter und gerouteter Netzzugriff eingerichtet.



6.6 Fernwartern nur unbedingt notwendige Rechte einräumen

Für jeden Fernwarter sollten feingranulare Rechte definiert werden, die exakt nur die Optionen erlauben, die für die jeweilige Rolle unbedingt notwendig sind.

Granulares Rollen- und Rechtesystem: Die Zugriffsprofile sollten modular konfigurierbar sein, um u. a. auch Standorte, Zugriffszeiten oder Zugriffspunkte regeln zu können. Das Ziel sollte ein granulares Rollen- und Rechtesystem sein, dass in einer einzigen Managementoberfläche verwaltet wird.

6.7 Jeden Fernwartungszugriff revisionssicher dokumentieren

Jeder Fernwartungszugriff muss revisionssicher in Echtzeit protokolliert und dokumentiert werden, um Veränderungen im Netz und an den Anlagen jederzeit überwachen, kontrollieren und auswerten zu können. Damit können unerwünschte Eingriffe, Fehlbedienungen oder Verstöße gegen Vereinbarungen eindeutig nachvollzogen und identifiziert werden.

EXTERNE ZUGRIFFE KONTROLLIEREN:

- Nach Möglichkeit sollten bei einer Fernwartung Veränderungen an der Anlage durch eigene Mitarbeiter erfolgen und der externe Experte sollte dies aus der Ferne begleiteten. Wird der externe Experte selbst tätig, sollte der Maschinenbediener den Eingriff parallel über die Bedienoberfläche überwachen können.

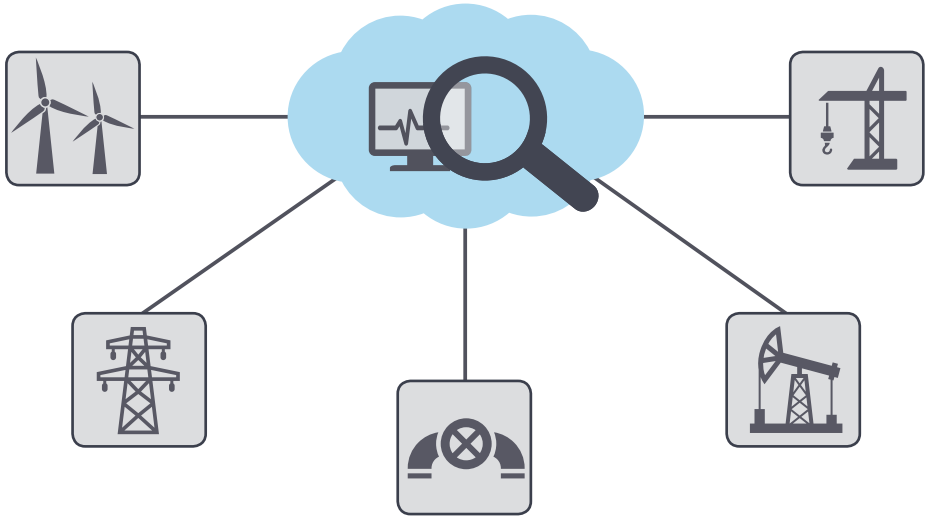
LOGGING UND VIDEOAUFZEICHNUNGEN:

- Logging-Funktionen mit Protokollierung aller erlaubten und abgewiesenen Verbindungen sind eine Grundvoraussetzung. Darüber hinaus sollten alle Vorgänge während des Fernwartungsvorgangs als Videoaufzeichnung für spätere Auswertungen dokumentiert werden.

7. Edge Computing ermöglicht sicheres Monitoring

Beim Anlagenmonitoring wird der Zustand von Komponenten und Anlagen kontinuierlich kontrolliert und überwacht. Kenndaten zeigen beispielsweise den aktuellen Status, die Verfügbarkeit und die Effizienz der Anlage. Dafür werden oft eine Vielzahl an Sensordaten erfasst, analysiert und bewertet.

Die Analyse dieser Datenmengen erfolgt immer häufiger in der Cloud, weil hier bereits fertige Analysekomponenten verfügbar sind oder eine größere Rechenpower genutzt werden kann. Hier erfüllt das Edge Computing eine wichtige Zwischenfunktion.



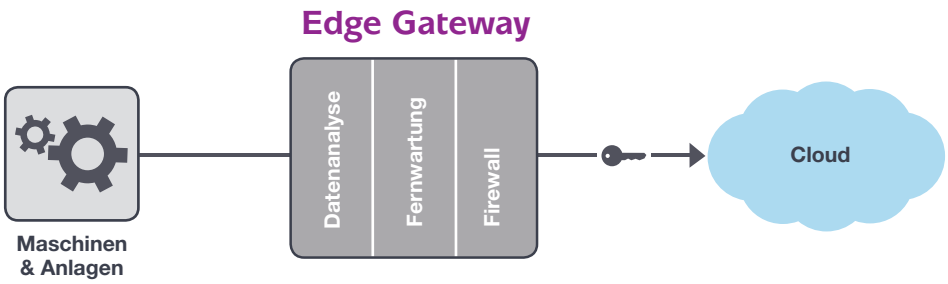
7.1 Edge Computing verringert die Komplexität

Beim Edge Computing werden die Daten dort vorverarbeitet, wo sie generiert werden, also in der Nähe der Maschine oder Anlage. Ein Edge Gateway ruft die Zustands- und Leistungsdaten von der Maschine ab und führt eine Vorverarbeitung der Daten durch. Dabei werden aus der gesamten Datenmenge die Informationen herausgefiltert, die für die Auswertungen gebraucht werden. Nur diese Daten müssen zur Auswertung beispielsweise in die Cloud übertragen werden.

Das ermöglicht eine größere Sicherheit, kürzere Latenzzeiten bei Realtime-Daten und eine geringere Komplexität. Auf diese Weise kann auch sichergestellt werden, dass sensible Produktionsdaten ausschließlich vor Ort verarbeitet werden.

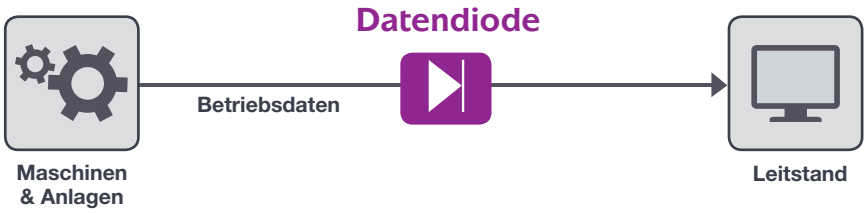
7.2 Sicherheitsgateway erweitert Edge Computing

Ein Edge Gateway sollte eine Firewall sowie eine Remote-Access-Komponente für sichere Fernwartungszugriffe beinhalten. Über die Firewall werden die gewonnenen Informationen sicher verschlüsselt zu den eigenen Servern oder zur Cloud weitergeleitet. Dabei schützt die Firewall den Edge Computer und die damit vernetzte Maschine vor Cyber-Attacken.



8. Hochsicheres Monitoring erfordert Datentransfers in nur einer Richtung

Bei erweiterten Services wie Predictive Maintenance oder einer Prozessüberwachung ist ein permanenter Onlinezugang zu Maschinen oder Anlagen notwendig. Das erfordert nochmals deutlich verschärfte Sicherheitsvorkehrungen. Das BSI empfiehlt bei rein passivem Monitoring beispielsweise für das Ablesen von Statusinformationen, Messwerten oder Systemzuständen andere Lösungen, wie reine Push-Verfahren (vgl. BSI-CS 108, Version 2.0 vom 11.07.2018). Eine solche Lösung ist ein Datentransfer, der nur in einer Richtung möglich ist.



8.1 Datendiode erlaubt nur Einbahn-Datentransfers

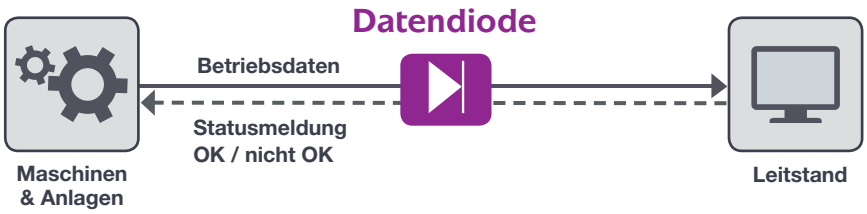
Eine Datendiode lässt ausschließlich einen Einbahn-Datentransfer zu. In der Gegenrichtung wird der Informationsfluss abgeblockt. Geschützt hinter dieser Datendiode können Maschinen, Anlagen und IT-Systeme somit Daten von der Anlage zum Leitstand oder über öffentliche Netze zum Servicecenter des Herstellers versenden, ohne dass ihre Integrität gefährdet wird.

Eine Datendiode eignet sich deshalb auch zur Vernetzung hochkritischer Systeme wie Gasturbinen oder chemische Anlagen, ohne die vernetzten Systeme der Gefahr von Attacken aus dem Internet auszusetzen.

8.2 Zuverlässiges Monitoring benötigt Feedback-Kanal

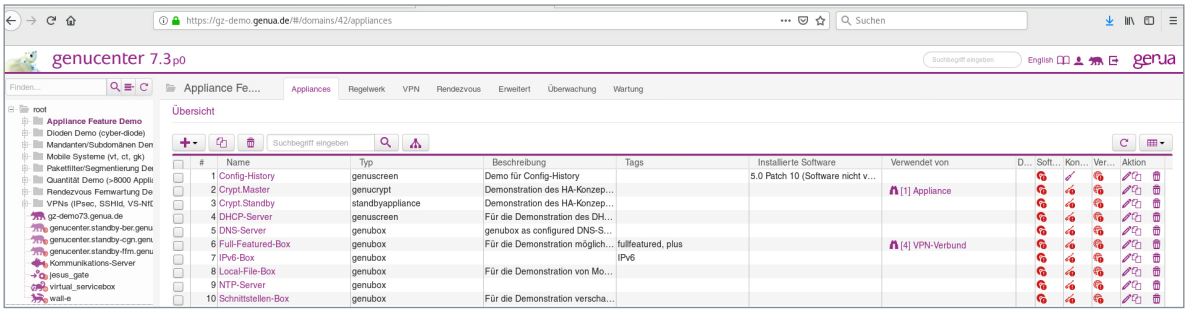
Das zuverlässige Monitoring von Anlagen benötigt allerdings die Gewissheit, dass die gesendeten Datenpakete auch angekommen sind. Hier sollte eine Datendiode eingesetzt werden, die über einen reinen Feedback-Kanal für Statusmeldungen verfügt. Darüber wird vom Empfänger an den Sender zurückgemeldet, ob alle Daten korrekt und komplett angekommen sind.

Das Feedback ist minimal:
Es besteht lediglich aus einem Status-Bit (OK / nicht OK) pro Verbindung. Durch die Beschränkung des Feedback-Kanals auf diese eine Information ist ein Missbrauch ausgeschlossen. Selbst bei einer fehlerhaften Administration entstehen keine Sicherheitslücken (Security by Design).



9. Zentrales Management ermöglicht komfortable Administration

Unverzichtbarer Bestandteil einer Fernwartungslösung ist ein zentrales Management für die Überwachung, Konfiguration und Verwaltung einer Vielzahl von Wartungsobjekten. Darüber können beispielsweise Sicherheits-Patches zentral auf alle Fernwartungskomponenten verteilt werden.



9.1 Fernwartungsprofile vereinfachen die Administration

Für jedes Wartungsobjekt müssen individuelle Parameter eingestellt und verwaltet werden. Das kann von den Nutzerberechtigungen, Protokoll- und Porteinstellungen, über Angaben zur Anlage bis hin zu Vorgaben über erlaubte Servicezeiten reichen. Diese Parameter sollten in individuellen Fernwartungsprofilen einstellbar und vom zentralen Management und ggf. in speziellen Fernwartungs-Apps administrierbar sein.

9.2 Administrationsaufgaben standardisieren und automatisieren

Die Administration einer großen Zahl an Wartungsobjekten bzw. Wartungs-Dienstleistern kann durch die Vielzahl der Einstellungen und Regelungen sehr aufwendig und fehleranfällig sein. Deshalb ist es von großem Vorteil, wenn wiederkehrende Aufgaben und bereits vorhandene Standard-Nutzerprofile nicht immer wieder neu erstellt werden müssen. Hier bietet die Management-Software vorkonfigurierte Abläufe, automatisch übertragbare Konfigurationen und Nutzerprofile.

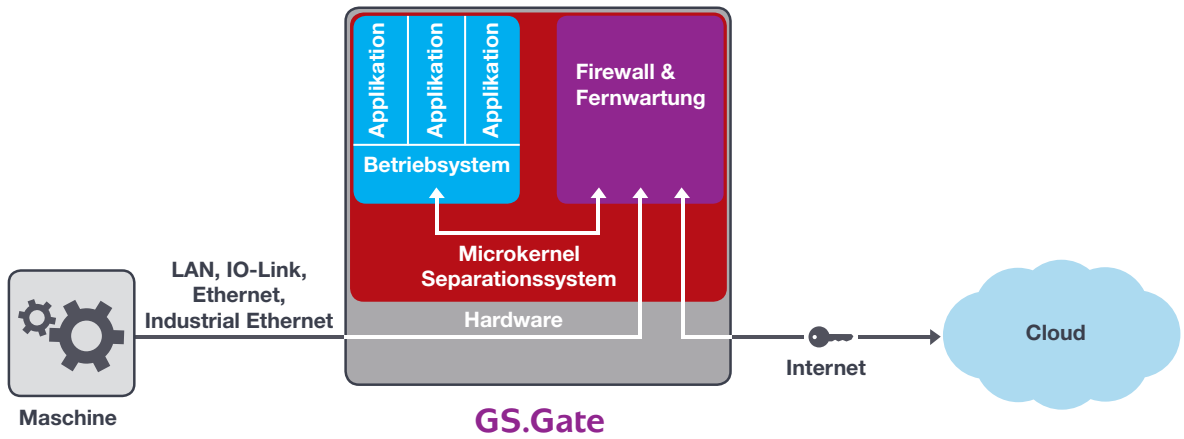
10. Security by Design gewährleistet hohe Sicherheit

Herkömmliche Produkte werden vorrangig für ausgewählte Funktionen entwickelt und meistens unter hohem Zeitdruck in den Markt gebracht. Die Sicherheit muss oftmals durch zusätzliche Anpassungen und Erweiterungen nachgebessert werden. Das macht die Lösungen nochmals komplexer und sicherheitstechnisch anfälliger. Im Gegensatz dazu steht das Prinzip „Security by Design“. Hier wird die Software und Hardware von Anfang an unter Sicherheitsanforderungen geplant und umgesetzt, um sie so unempfindlich wie möglich gegen Angriffe zu machen.

10.1 GS.Gate basiert auf Security by Design

Beim Cloud Edge Gateway GS.Gate von genua sind in einer industrietauglichen Hardware zwei getrennte Bereiche angelegt: Ein Edge Computer und ein Sicherheitsgateway. Der Edge Computer wird vom Sicherheitsgateway strikt abgeschottet. Auf der untersten Ebene des GS.Gate läuft ein auf das Wesentliche reduzierte Microkernel-Betriebssystem, das die getrennten Bereiche erzeugt. Die separierten Bereiche verfügen über jeweils eigene Betriebssysteme sowie fest zugewiesenen Hardware-Ressourcen.

Im Edge Computer können Maschinenhersteller oder -betreiber mittels der Container-Technologie Docker ihre individuelle Anwendungen zum Beispiel zur Fernwartung installieren. Im Sicherheitsgateway befinden sich eine Firewall sowie die Remote-Access-Komponente für sichere Fernwartungszugriffe. Nach außen in Richtung Netzwerk ist nur das speziell gehärtete Sicherheitsgateway sichtbar. Hinter diesem Schutzschirm kann der Anwendungsbereich des Edge Computers ohne ständige Eingriffe durch Updates und Patches betrieben werden.



10.2 cyber-diode basiert auf Security by Design

Bei der cyber-diode von genua ist die Dioden-Funktion sehr minimalistisch programmiert – lediglich wenige hundert Zeilen Code – und läuft auf einem Microkernel-Betriebssystem, das ebenfalls auf das Allernotwendigste reduziert ist. Durch die geringe Komplexität ist der Dioden-Prozess einfach zu analysieren, der komplette Code kann überprüft und formal verifiziert werden, um Fehler in dieser entscheidenden Komponente auszuschließen. Bei der vs-diode von genua wird die gleiche Technologie eingesetzt.

Die vs-diode ist vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zugelassen für den Einsatz bis zur hohen Geheimhaltungsstufe

GEHEIM.

11. Praxisbeispiele, wie Industrieunternehmen eine sichere Fernwartungslösung nutzen

11.1 Werkzeughersteller KOMET schützt vernetzte Produktion

Die Hersteller von über 90 Maschinen wollten sich bei der KOMET GROUP mit unterschiedlichsten Fernwartungslösungen in das Produktions-Netzwerk einwählen. Dem Vorteil einer hohen Maschinenverfügbarkeit standen Sicherheits-Risiken und ein immenser Verwaltungsaufwand entgegen. KOMET hat deshalb für alle Maschinenhersteller eine einheitliche, sichere und effiziente Fernwartungslösung eingeführt und dabei eine große Akzeptanz erreicht.

▶ **Anwenderbericht KOMET GROUP**

11.2 Verpackungsmaschinenhersteller Gerhard Schubert setzt auf hochsichere Vernetzung

Verpackungsmaschinenhersteller setzt auf sichere Anlagenvernetzung

Gateway schützt vor *Zugriff*

Fernwartung | Sollen Maschinen für Datenanalysen in der Cloud vernetzt werden, sind die Sicherheitsbedenken groß. Gerhard Schubert setzt daher auf eine sichere Fernwartungslösung von Genua.

Sollen Maschinen für Datenanalysen oder Fernwartungs-Services vernetzt werden, sind die Sicherheitsbedenken groß. Zu Recht, sagt der Verpackungsmaschinenhersteller Gerhard Schubert. Deshalb setzt der Hersteller bei der Vernetzung von Maschinen auf Edge Computing und eine Sicherheitstechnik, die höchste Schutzanforderungen erfüllt und auch in sensiblen staatlichen Bereichen eingesetzt wird.

▶ **Anwenderbericht Gerhard Schubert**

11.3 Maschinenhersteller INDEX-Werke nutzt sichere Cloud-Anbindung für Monitoring

Die INDEX Gruppe aus Esslingen bieten für Ihre CNC-Drehmaschinen Apps auf Basis einer Multicloud-as-a-Service-Plattform an, um den Status der Maschinen zu überwachen, Alarmmeldungen zu erhalten oder Kollisionen der Frässpindeln zu erkennen. Die Cloud-Anbindung folgt den BSI-Empfehlungen für eine besonders hohe Cybersicherheit im industriellen Umfeld.

▶ **Anwenderbericht INDEX Gruppe**

Weitere Informationen:

www.genua.de/automatisierung

Komfortable Fernwartung für die Industrie – mit Sicherheit!

Industrie 4.0: Sichere Anbindung an die SAP-Cloud

Über genua

Die genua GmbH ist ein deutscher Spezialist für IT-Sicherheit. Das Leistungsspektrum umfasst die Absicherung sensibler Schnittstellen und Netze im Behörden- und Industriebereich bis hin zur Anbindung hochkritischer Infrastrukturen, die zuverlässig verschlüsselte Datenkommunikation via Internet, Fernwartungs-Systeme sowie Remote Access-Lösungen für mobile Mitarbeiter und Home Offices. Alle Produkte werden von genua in Deutschland entwickelt und produziert.

Regelmäßige Zertifizierungen und Zulassungen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) belegen die Produktqualität. Zahlreiche Kunden aus der Industrie und dem öffentlichen Bereich setzen auf die Erfahrung und Lösungen des 1992 gegründeten Unternehmens, das am Hauptsitz in Kirchheim bei München sowie an den Standorten Berlin, Köln, Leipzig und Stuttgart über 250 Mitarbeiter beschäftigt. genua ist ein Unternehmen der Bundesdruckerei-Gruppe.

genua GmbH | Domagkstraße 7 | 85551 Kirchheim bei München
tel +49 89 991950-0 | info@genua.de | www.genua.de

Bilder: Titelmotiv Fotolia/zapp2photo, Seite 3 Fotolia/Gorodenkoff, Seite 5 Fotolia/Lucky Dragon, Seite 6 shutterstock/Betastock