NCP
SECURE COMMUNICATIONS

Sichere Fernwartung per VPN

Wie sich Fernwartung gefahrlos gestalten lässt

Trust Seal
www.teletrust.de/itsmig

SecurITy made in Germany

Inhalt

Sichere Fernwartung per VPN – Wie sich Fernwartung gefahrlos gestalten lässt 3

Warum der Fernzugriff auf die OT rapide zunimmt 4

Wie Unternehmen durch Predictive Maintenance Ausfälle minimieren 4

Warum Sicherheit bei der Fernwartung so entscheidend ist 5

- Weshalb sich kleine Betriebe nicht in Sicherheit wiegen sollten 6
- Welche Sicherheitslücken für die OT besonders gefährlich sind 6

Wie Unternehmen ihre OT vor Cyberangriffen schützen können 7

- Warum Unternehmen die Fernwartung sorgfältig planen und regeln sollten 8
- Wie Hersteller und Betreiber Fernwartungsschnittstellen sicher gestalten 9
- Weshalb das BSI VPN-Verbindungen empfiehlt 9

Wie Wartungsprozesse zuverlässig ablaufen 10

- Warum integrierte IT-Komponenten die Sicherheit gefährden können 10

Wie cloudbasierte Fernwartungskonzepte aufgebaut sind 10

- Wenn die Fernwartung mehrere Fertigungslinien umfasst 12

Worauf Anlagenhersteller bei ihrem Fernwartungskonzept achten sollten 12

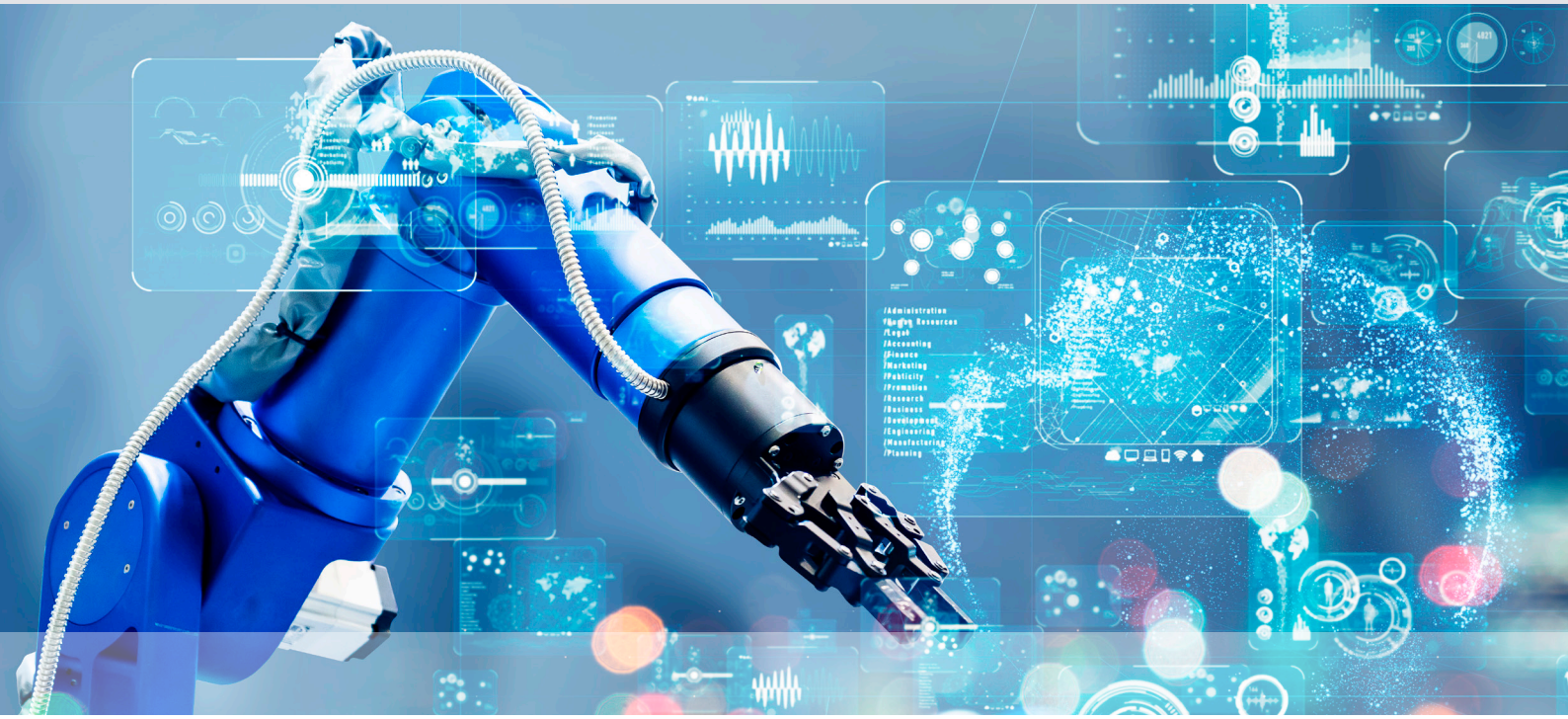
- Wo IT und OT zusammentreffen, sind beide Expertisen gefragt 12
- Wie sich das IIoT Gateway gut in die Umgebung einfügt 13

Was bei Fernwartung als Managed Service zu beachten ist 14

Wie Betreiber vorhandene Maschinen in die Fernwartung integrieren 15

Warum eine bereichsübergreifende VPN-Lösung die Sicherheit erhöht 16

Wie VPN verschiedenste Remote-Access-Szenarien absichert 16



Sichere Fernwartung per VPN

Wie sich Fernwartung gefahrlos gestalten lässt

Digitale Transformation und Industrie 4.0 sind bei vielen Fertigungsbetrieben seit Jahren zentrale Themen. Deren Umsetzung wurde durch die coronabedingten Lockdowns seit dem Frühjahr 2020 erheblich vorangetrieben. Damit die Produktion weiterlaufen konnte, haben etliche Firmen die Automatisierung schneller umsetzen müssen als geplant. Das galt auch für die Wartung von Maschinen und Anlagen, die auf Fernwartung umzustellen waren. Entsprechend viele Maschinen und Anlagen sind heute an das IT-Netz gekoppelt. Um hier die Risiken von Cyberangriffen zu minimieren, sollten Hersteller wie Anwender geeignete Sicherheitsvorkehrungen treffen. Der sichere Fernzugriff per Virtual Private Network (VPN) spielt dabei eine wesentliche Rolle.

Mit Industrie 4.0 und dem Industrial Internet of Things (IIoT) hält die IT bereits seit einigen Jahren Einzug in den Fertigungsbereich und die Gebäudeautomation. Dazu verbinden Unternehmen die in ihrem Betrieb vorherrschende operative Technologie (OT) mit einem Datennetz. So können Anwender ortsunabhängig über die Cloud Abläufe automatisieren sowie Maschinen, Anlagen und Prozesse überwachen und kontrollieren. Das soll Fertigungsschritte beschleunigen. Zudem kann ein Unternehmen die im OT-Bereich ermittelten Daten in der Cloud mithilfe unterschiedlicher Anwendungen analysieren, verarbeiten und nutzen.

Warum der Fernzugriff auf die OT rapide zunimmt

Der Fernzugriff auf Maschinen und Anlagen wird mit dem neuen Mobilfunkstandard 5G und IIoT weiter rapide zunehmen. Das gilt vor allem für Unternehmen mit verteilten Produktionsstandorten sowie in der Zulieferindustrie, um Fertigungsprozesse sicherzustellen. Mit digitalisierten Prozessen soll gewährleistet werden, dass die Arbeitsschritte klar definiert und wiederholbar sind und dementsprechend ablaufen. Anwender wie weiterverarbeitende Betriebe können die Produkte und deren Bestandteile jederzeit eindeutig identifizieren und nachvollziehen.

864 Mrd. $

=

8 %

Jahresumsatz jährlich

Maschinenstillstände bei Fortune-Global-500-Unternehmen

Der Senseye-Bericht 2021 ***The True Cost Of Downtime*** hat 72 international agierende Industrieunternehmen zu Maschinenstillständen befragt und kommt zu dem Schluss, dass Fortune-Global-500-Industrieunternehmen geschätzte 3,3 Millionen Stunden pro Jahr aufgrund ungeplanter Maschinenstillstände verlieren. Die finanziellen Kosten dieser Stillstände werden auf 864 Milliarden US-Dollar berechnet. Das entspricht acht Prozent ihrer jährlichen Umsätze. Die Kosten setzen sich zusammen aus durchschnittlichen Kosten für Umsatzausfälle, Geldstrafen, Stehzeiten der Mitarbeiter und Maschinen.

Darüber hinaus wird für produzierende Betriebe die Anlagenverfügbarkeit immer wichtiger. Bei Störungen können sie nicht warten, bis ein Servicetechniker anreist. Zu groß ist das Risiko, dass Lieferfristen nicht eingehalten werden können und womöglich die komplette Logistik auf den Kopf gestellt wird. Das ist selbst für sicherheitsbedachte Unternehmen ein Grund, hier einen Fernzugriff auf ihre Anlagen zuzulassen. Denn so können Servicetechniker schnell auf Alarmmeldungen reagieren und ortsunabhängig auf Anlagen zugreifen. Von noch größerem Vorteil ist der Fernzugriff, wenn Maschinen schwer zugänglich sind.

Wie Unternehmen durch Predictive Maintenance Ausfälle minimieren

Mit der Digitalisierung des Telefonnetzes sind zunehmend cloudbasierte, vorausschauende Wartungskonzepte in den Mittelpunkt gerückt. Damit lassen sich Störungen beseitigen, bevor

es zu Ausfällen kommt. Manche Fertigungsbetriebe nutzen diese Konzepte für ihre gesamte Produktionsumgebung und binden selbst ältere Anlagen und Maschinen ein, um das Qualitätsmanagement zu optimieren.

> Die durchschnittliche Nutzungsdauer von Fabrikausrüstung beträgt 20 Jahre. Die meisten Anlagen müssen so lange laufen, damit sie sich rentieren.
>
> ***Peter Früauf**, VDMA-Experte*

Bei der vorausschauenden Wartung (Predictive Maintenance) liefern Sensoren in Maschinen und Anlagen regelmäßig aktuelle Statusdaten wie Temperatur, Leistung, Umdrehungen, Feuchtigkeit oder Auslastung an eine zentrale Plattform in der Cloud. Bei Abweichungen von hinterlegten Sollwerten kann das Serviceteam proaktiv handeln und beispielsweise ein bestimmtes Bauteil austauschen oder die Wartungsarbeiten vorziehen, bevor größere Schäden entstehen. Das reduziert Ausfallzeiten und verlängert die Laufzeit der Anlage. Die Netzwerkschnittstelle kann zudem dazu genutzt werden, aktuelle Firmware-Updates auf die Maschinen zu laden. Dadurch sind diese technisch stets auf dem neuesten Stand und zudem automatisch mit den aktuellen Sicherheits-Patches ausgestattet.

Warum Sicherheit bei der Fernwartung so entscheidend ist

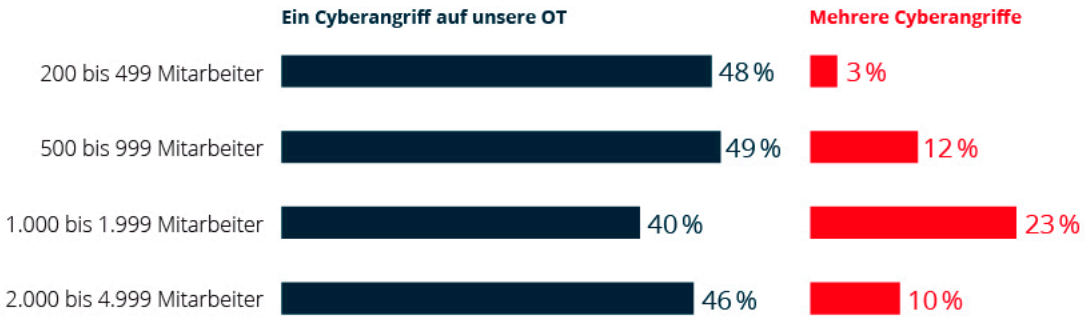
Bei all den Vorzügen sollten Hersteller und Betreiber von Anlagen mit Fernzugriff immer die Sicherheit im Auge behalten. Sobald Maschinen und Anlagen an das Internet gekoppelt sind, müssen sie in das unternehmensweite IT-Sicherheitskonzept eingebunden werden, damit sie nicht zum Einfallstor für Hackerangriffe werden. Denn diese können Kontrollsysteme außer Kraft setzen, Prozessabläufe empfindlich stören oder gar eine Anlage für Stunden stilllegen. Eine Absicherung nach dem Zero-Trust-Prinzip minimiert das Risiko solcher Ausfälle im OT-Bereich. Dabei greifen Anwender auf Maschinen und Anlagen ausschließlich über ein Virtual Private Network (VPN) zu.

Soll die cloudbasierte Fernwartung einer Maschine oder Anlage abgesichert werden, betrifft das nicht nur den Hersteller mit seinem Wartungspersonal beziehungsweise den mit der Wartung beauftragten Managed Service Provider. Gefordert ist auch der Endkunde, denn dieser muss die Netzwerkumgebung dafür auslegen.

Weshalb sich kleine Betriebe nicht in Sicherheit wiegen sollten

Die Marktforscher von Techconsult haben für ihre aktuelle Fokus-Point-Studie „Absicherung und Fernwartung in der Operational Technology“ [1] 213 produzierende Unternehmen in Deutschland mit 500 bis 5.000 Mitarbeitern zu OT-Sicherheitsvorfällen im Jahr 2020 befragt. Dabei stellte sich heraus, dass bei fast der Hälfte der befragten Unternehmen die OT mindestens einmal Ziel einer Cyberattacke gewesen war. Die Unternehmensgröße spielte dabei keine Rolle.

Cybersecurity-Vorfälle auf die Operational Technology nach Unternehmensgröße

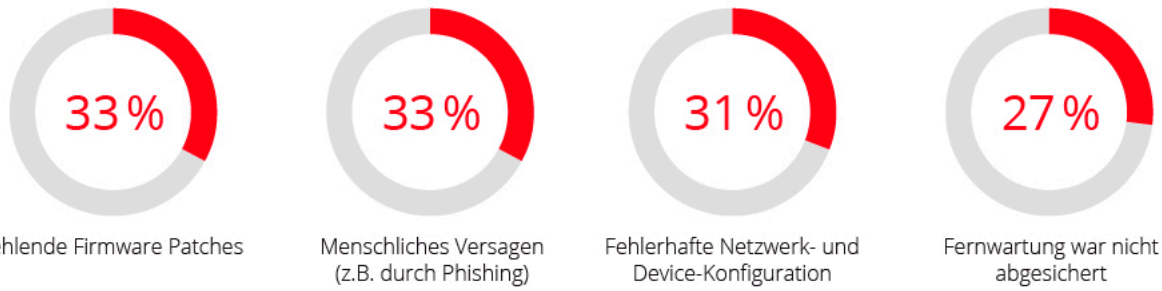


Basis: 213 Unternehmen

Welche Sicherheitslücken für die OT besonders gefährlich sind

Als Grund für die Sicherheitsvorfälle im OT-Bereich nannte ein Drittel der attackierten Unternehmen fehlende Firmware und Patches, ein weiteres Drittel menschliches Versagen, etwa bei Phishing-Angriffen. 31 Prozent gaben als Ursache fehlerhafte Netzwerk- und Gerätekonfigurationen an. Darüber hinaus führte bei 27 Prozent der Unternehmen eine nicht abgesicherte Fernwartung zu einem Cyberangriff.

Gründe für IT-Sicherheitsvorfälle in der OT



Basis: 123 Unternehmen

Mehrfachnennungen möglich

[1] Techconsult: Absicherung und Fernwartung in der Operational Technology. Kassel, Juni 2021

Als häufigste Reaktionen auf eine Attacke haben die Unternehmen die betroffenen Komponenten abgeschaltet (42 Prozent) oder sämtliche Verbindungen beziehungsweise die Kommunikation nach außen gekappt (39 Prozent). Ein Viertel der betroffenen Unternehmen hat sogar die gesamte Produktion sicherheitshalber gestoppt. Für alle bedeuteten die Angriffe erhebliche finanzielle Einbußen.

Reaktionen der Unternehmen auf Cyberangriffe in der Produktion

Basis: 123 Unternehmen

Mehrfachnennungen möglich
Filter: Ja, wir hatten in den letzten 12 Monaten einen Cybersecurity-Vorfall in der IT des Produktionsumfelds (OT).

Wie Unternehmen ihre OT vor Cyberangriffen schützen können

Um sich vor künftigen Angriffen besser zu schützen, installierte die Hälfte der betroffenen Unternehmen eine Security-Software im Produktionsumfeld, 47 Prozent haben den Fernzugriff sowie die Fernwartung besser abgesichert. 41 Prozent lassen jetzt im Rahmen des Fernwartungskonzepts Firmware-Updates remote auf die Maschinen und Anlagen laden, damit diese immer mit den neuesten Sicherheits-Updates ausgestattet sind.

Maßnahmen für die digitale Absicherung des Produktionsumfeldes

Basis: 213 Unternehmen

Mehrfachnennungen möglich

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat mit dem OPS.1.2.5 eine Richtlinie für die Fernwartung erarbeitet. Diese geht nicht nur auf die wichtigsten Gefährdungen ein, sondern beschreibt auch, welche Anforderungen eine Lösung sowie die beteiligten Schnittstellen erfüllen müssen, damit die Informationen, die bei der Fernwartung gespeichert, verarbeitet und übertragen werden, ausreichend geschützt sind.

Das gefährdet laut BSI eine sichere Fernwartung

- ✓ fehlende oder unzureichende Planung und Regelung der Fernwartung
- ✓ unzureichende Kenntnisse über Regelungen der Fernwartung
- ✓ ungeeignete Nutzung von Authentisierung bei der Fernwartung
- ✓ fehlerhafte Fernwartung
- ✓ Verwendung unsicherer Protokolle in der Fernwartung
- ✓ unsichere und unkontrollierte Fremdnutzung der Fernwartungszugänge
- ✓ Nutzung von Online-Diensten für die Fernwartung
- ✓ unbekannte Fernwartungskomponenten

Warum Unternehmen die Fernwartung sorgfältig planen und regeln sollten

Auf Anraten des BSI sollte die Fernwartung „sorgfältig geplant, aufgebaut und geregelt“ sein. Den Unternehmen empfiehlt das Bundesamt, eine eigene Richtlinie zur Fernwartung zu erstellen, die all denjenigen bekannt sein sollte, die an Konzeption, Aufbau und Betrieb der Fernwartung beteiligt sind. Es ist wichtig, dass der Betreiber der Anlage die dort festgelegten Berechtigungen in sein Identitäts- und Berechtigungsmanagement für die Unternehmens-IT einbindet.

Entsprechend ist im Vorfeld zum Beispiel abzuklären, welche Maschinen, Anlagen und Steuerungen tatsächlich externen Zugriff benötigen. Auch bei der Erteilung von Zugriffsberechtigungen gilt das Minimalprinzip: Nur die betroffene authentifizierte Maschine darf in einem definierten Zeitfenster eine aktive verschlüsselte Verbindung zu einem autorisierten Servicetechniker aufbauen. Dieser ist in diesem Fertigungsnetz ausschließlich und immer auf dieses Zielsystem beschränkt.

Diese Richtlinien geben dem Administrator vor, wie er die Fernwartungslösung konfigurieren soll. Ist nichts vorgegeben, nutzt der Administrator womöglich kein für die Konfiguration notwendiges, sicheres und zertifikatsbasiertes Verfahren, sondern belässt es bei der Werkseinstellung mit unsicherem Passwort.

Das Fernwartungskonzept muss vollständig dokumentiert sein. Wichtig ist dabei zum Beispiel, welche Fernwartungszugänge existieren und welche davon aktiv von welchem Personenkreis genutzt werden. Übernimmt ein Hersteller oder ein Managed Service Provider die Fernwartung einer Anlage, muss ein Vertrag die Zuständigkeiten und Berechtigungen umfassend regeln, damit das Wartungspersonal die ihm zugeschriebenen rollenbasierten Berechtigungen strikt einhält und seine Fernwartungszugänge vollständig dokumentiert. Falls der Dienstleister oder Hersteller Anlagen mehrerer Kunden fernwartet, ist zu gewährleisten, dass zwischen den Netzen seiner Kunden keinerlei Verbindung besteht.

Wie Hersteller und Betreiber Fernwartungsschnittstellen sicher gestalten

Eine unzureichend gesicherte Fernwartungsschnittstelle gefährdet nicht nur das eigene Netz, sondern gegebenenfalls sogar ein darüber angebundenes Netz eines Dritten. Deshalb gilt es, die möglichen Zugänge und Kommunikationsverbindungen für die Fernwartung auf das notwendige Maß zu beschränken. Nach dem Fernzugriff ist die Verbindung wieder zu trennen. Zudem sollte die Fernwartungssoftware ausschließlich auf Maschinen und Anlagen installiert sein, die diese benötigen.

Unsichere Kommunikationsprotokolle, Verschlüsselungsalgorithmen oder Authentisierungsmechanismen gefährden Produktionsanlagen. Veraltete Versionen von IPsec, SSH oder SSL/TLS etwa bieten nur unzureichenden Schutz vor unbefugtem Zugriff. Das gilt ebenso für Protokolle, die Informationen in Klartext übertragen. Selbst die als sicher eingestuften Kommunikationsprotokolle sollten mit einem starken kryptografischen Verfahren verschlüsselt werden. Der für die Fernwartung verantwortliche Administrator muss die Stärke des verwendeten Algorithmus sowie der Schlüssel regelmäßig prüfen und bei Bedarf anpassen. Zudem wird eine Mehr-Faktor-Authentisierung empfohlen.

Weshalb das BSI VPN-Verbindungen empfiehlt

Wartet ein Hersteller seine Maschinen und Anlagen über eine Cloud-Plattform, rät das BSI zu einer Ende-zu-Ende-Verschlüsselung der Kommunikation. Ansonsten ist es dem Plattformanbieter möglich, mitzulesen. Außerdem könnten Hacker über die offene Kommunikation unbemerkt auf die angeschlossenen Maschinen und Anlagen zugreifen. Das BSI empfiehlt generell für Fernwartungszugänge, die über ein öffentliches Datennetz laufen, ein abgesichertes Virtual Private Network (VPN).

Wie Wartungsprozesse zuverlässig ablaufen

Eine sorgfältig geplante Fernwartung basiert auf regelmäßigen Prozessen und Software-Updates. Laufen die Fernwartungsprozesse nicht korrekt ab, kann dies zu Fehlfunktionen der gewarteten Maschine oder Fertigungsanlage führen. Verspätete oder fehlerhafte Wartungen führen zu Störungen und sind bei veralteter Firmware zudem eine Sicherheitslücke. Automatische Terminerinnerungen und Workflows wie Online-Updates können hier Abhilfe schaffen. Außerdem ist eine umfassende, stets aktuelle Dokumentation unverzichtbar.

Warum integrierte IT-Komponenten die Sicherheit gefährden können

Enthält die Anlage zugekaufte IT-Komponenten, sollte geprüft werden, ob diese mit Fernwartungsfunktionen ausgestattet sind, von denen der Anlagenhersteller und der Betreiber bisher nichts wussten. Diese Funktionen seien laut BSI oft schlecht dokumentiert und hätten durchaus Zugriff auf andere IT-Komponenten der Anlage. Deshalb ist es wichtig, diese Fernwartungsfunktionen abzuschalten oder in das Überwachungskonzept zu integrieren. Zuvor sollte ein IT-Administrator die Funktion unbedingt auf Security-Schwachstellen prüfen.

Wie cloudbasierte Fernwartungskonzepte aufgebaut sind

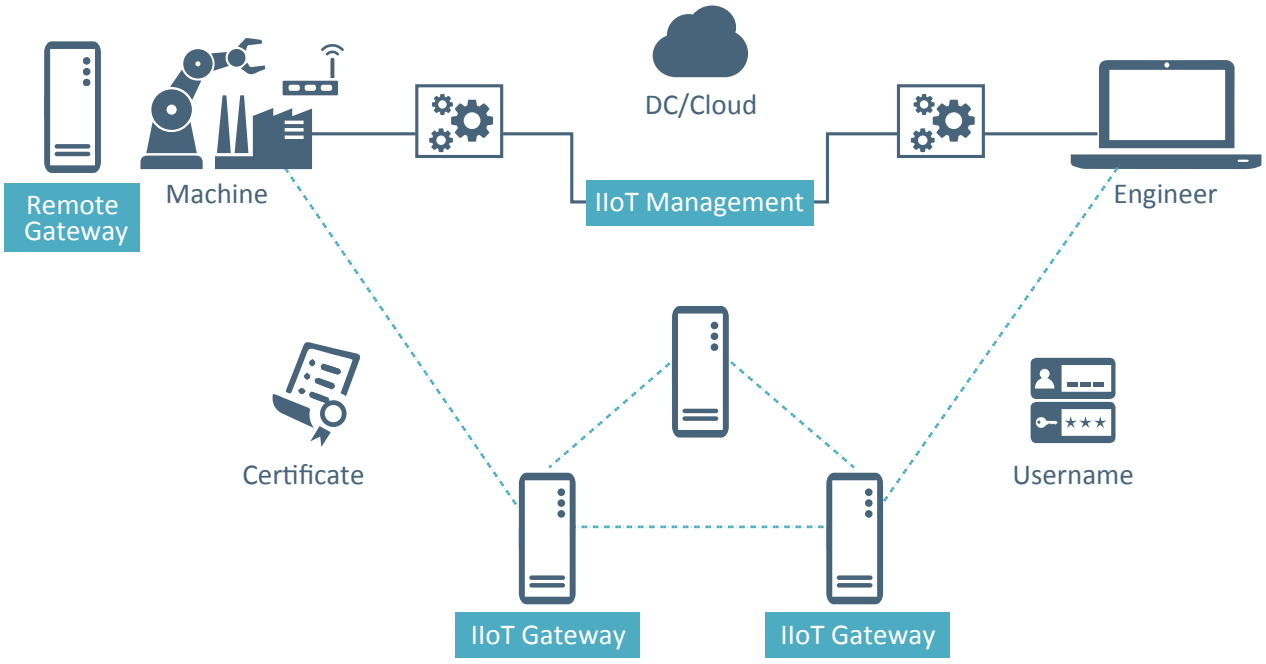
Fernwartungslösungen im Fertigungsumfeld arbeiten heute meist über eine zentrale Administration in der Cloud. Somit verwaltet und überwacht ein Administrator die Fernwartung per App. Diese empfängt und sendet Serviceaufträge und Störungsmeldungen aus, prüft die Berechtigungen, speichert und dokumentiert sämtliche Meldungen, Prozesse und Zugriffe.

Da die Cloud IP-basiert arbeitet, ist ein zertifikatbasiertes, Ende-zu-Ende-verschlüsseltes VPN-Netz ratsam. Oft sollen dabei eine Reihe von Maschinen remote gewartet werden. Dazu muss im Rechenzentrum des Betreibers oder eines Managed Sercvice Providers ein zentrales, softwarebasiertes IIoT Gateway installiert sein. Es sollte sich dort in einem sicheren Bereich befinden, etwa in einer demilitarisierten Zone. Es stellt von dort aus sichere VPN-Verbindungen zu mehreren ebenfalls softwarebasierten Remote Gateways direkt an den Maschinen her. Die Remote Gateways sind oft auf kleinen Industrie-PCs installiert.

Die Kommunikation zwischen innen (VPN) und außen regelt das zentrale IIoT Gateway. Daher ist es mit Schutzmechanismen wie einer Firewall ausgestattet. Es überträgt die Daten aus dem

Automatisierungsnetz über VPN-Tunnel ins IT-Netz, umgekehrt leitet es die Informationen aus dem VPN-Netz in das OT-Netz der Anlage weiter. Servicetechniker und Administrator sowie die Fernwartungs-App selbst sind ebenfalls über das Gateway an das VPN-Netz angeschlossen. Der SNMP-Verkehr (Simple Network Management Protocol) fließt direkt in die Management-App, die entsprechende Meldungen an den zuständigen Servicetechniker oder den Administrator ausgibt.

Der sichere Fernwartungszugriff per NCP Smart Maintenance



Will ein Techniker eine bestimmte Maschine fernwarten, verbindet er sich zum Beispiel bei der NCP-Fernwartungslösung per NCP-Softwareclient (App) mit dem zentralen Gateway im Rechenzentrum. Um wirklich alle möglichen Angriffspunkte bei der Fernwartung abzusichern, hat NCP in diesen Client eine Endpoint-Protection integriert: Sind zum Beispiel auf dem verwendeten Endgerät nicht die aktuellen Windows-Patches und Viren-Pattern installiert, lässt sich der NCP-Client nicht mit dem zentralen IIoT Gateway verbinden.

Steht die Verbindung zum zentralen Gateway, muss die VPN-Verbindung freigeschaltet werden. Das kann über vorab definierte Berechtigungen automatisch erfolgen, oder ein Mitarbeiter des Maschinenbetreibers schaltet die Verbindung über die Management-Oberfläche der VPN-Lösung manuell frei. Erst dann kann der Servicetechniker über den VPN-Tunnel die Wartungssoftware starten und betreiben. Darüber prüft er Maschineneinstellungen, die SNMP-Meldungen der Ma-

schine und misst zum Beispiel Laufleistung und die Umdrehungsgeschwindigkeit einer Maschine. So kann er aus der Ferne feststellen, ob die Maschine reibungslos läuft oder wo eine konkrete Störung auftritt und entsprechende Gegenmaßnahmen einleiten.

Wenn die Fernwartung mehrere Fertigungslinien umfasst

Auch für Fertigungslinien bieten sich Strukturen mit einem zentralen IIoT Gateway und dahinter liegenden Remote Gateways an. Das ermöglicht eine Inselsegmentierung für die angeschlossenen Linien. Bei der NCP-Lösung sind sogar identisch konfigurierte Segmente möglich, was bei manchen Fernwartungslösungen zu Problemen bei der Identifizierung von Zielsystemen führt. Abhilfe schafft eine gezielte Ansprache mit eindeutigen, temporären IP-Adressen und Authentisierungsmerkmalen von Gateways wie Clients. Die Remote Gateways können direkt auf Anlagen und Maschinen oder auf vorgeschalteten Hardwarekomponenten installiert werden. Mit ihnen lassen sich auch verschlüsselte oder unverschlüsselte Daten von anderen Geräten wie Sensoren oder Kameras aggregieren und verschlüsselt weitergeben. Das zentrale IIoT Gateway nimmt die auf diese Weise verschlüsselten OT-Daten vom Remote Gateway entgegen und übermittelt sie an die Management-App der Fernwartung oder andere weiterverarbeitende Systeme wie Edge-Devices.

Worauf Anlagenhersteller bei ihrem Fernwartungskonzept achten sollten

Für Maschinen- und Anlagenbauer, die ihre Systeme mit einer IT-gestützten Fernwartung ausstatten wollen, ist es sinnvoll, das Wartungskonzept so auszulegen, dass immer die Maschine den Verbindungsaufbau initiiert (asynchrone Kommunikation). Falls dies bei einer vorliegenden Störung einmal nicht möglich ist, sollte das Servicepersonal ausschließlich per Administratorzugang von außen auf die Anlage zugreifen können, was auf jeden Fall zu dokumentieren ist.

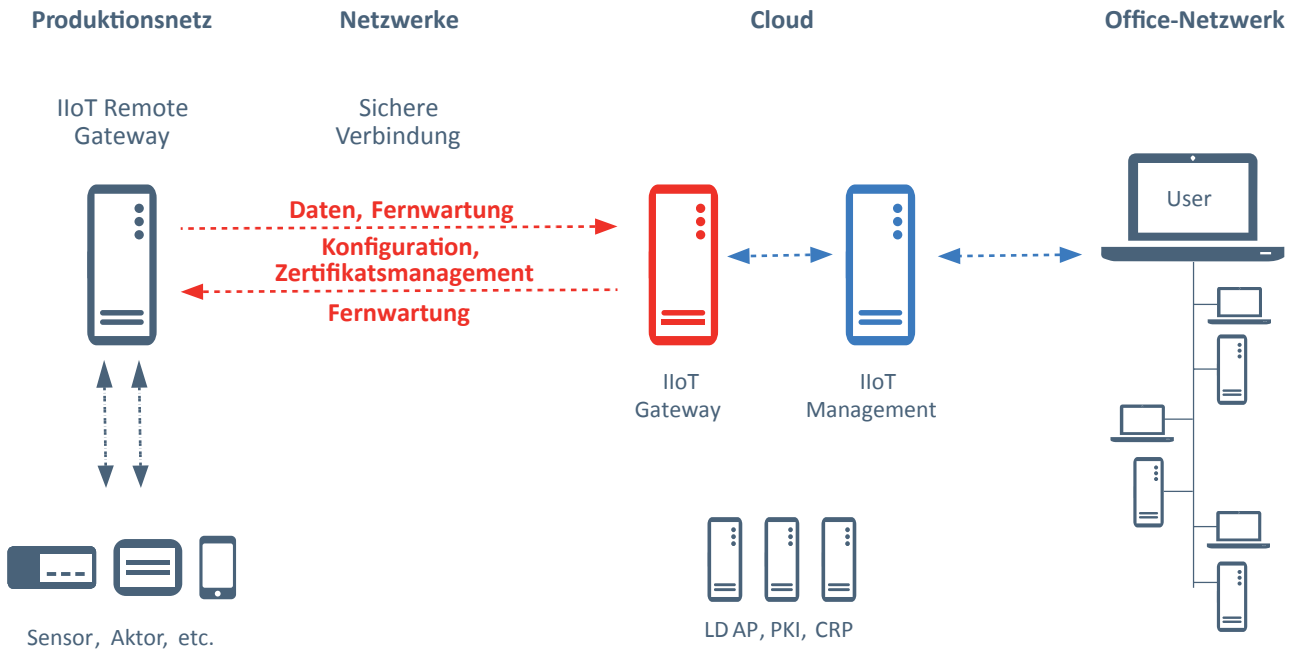
Wo IT und OT zusammentreffen, sind beide Expertisen gefragt

Darüber hinaus benötigt der Hersteller für die Fernwartung in seiner Maschine oder Anlage eine Schnittstelle zwischen OT und IT, um eine Verbindung für die Software aufbauen zu können. Folgende Fragen sind zu klären:

- Wo endet der Bereich der Automatisierung mit den zugehörigen seriellen Protokollen?
- An welcher Stelle soll die Kommunikation ins IT-Netz übergehen?

Diese Schnittstelle definieren OT-Experten aus der Fertigung am besten gemeinsam mit dem IT-Team, das die Fernwartungssoftware aufsetzt. So kann der Hersteller gleichermaßen die Wartungs- und IT-Sicherheitsanforderungen abdecken. Es ist generell ratsam, das IT-Team mit seinem Security-Know-how immer dann einzubeziehen, wenn im Fertigungsumfeld IIoT ins Spiel kommt.

Sichere Verbindungen zwischen den Netzen sind essenziell



Wie sich das IIoT Gateway gut in die Umgebung einfügt

Die Einsatzszenarien von Maschinen und Anlagen sind vielfältig. Meist wird eine Maschine in ein vorhandenes Fertigungsumfeld integriert. Damit sich Maschine und Gateway in möglichst viele Umgebungen integrieren lassen, sollte das zugehörige IIoT Gateway viele Schnittstellen und Treiber bereitstellen. Ist eine spezifische Konfiguration notwendig, fungiert in manchen Fällen auch ein Industrie-PC, der eine Maschine steuert, als Gateway.

Es gibt Steuerungen, die IPsec-Tunneling bis in die Maschine mit einem eigenen VPN-Client anbieten. Diese Verbindungen kann der Anlagenbauer eins zu eins und ohne zusätzliche Schnittstelle an das Gateway anschließen, das die Verbindungen einfach durchroutet. Das ist zum

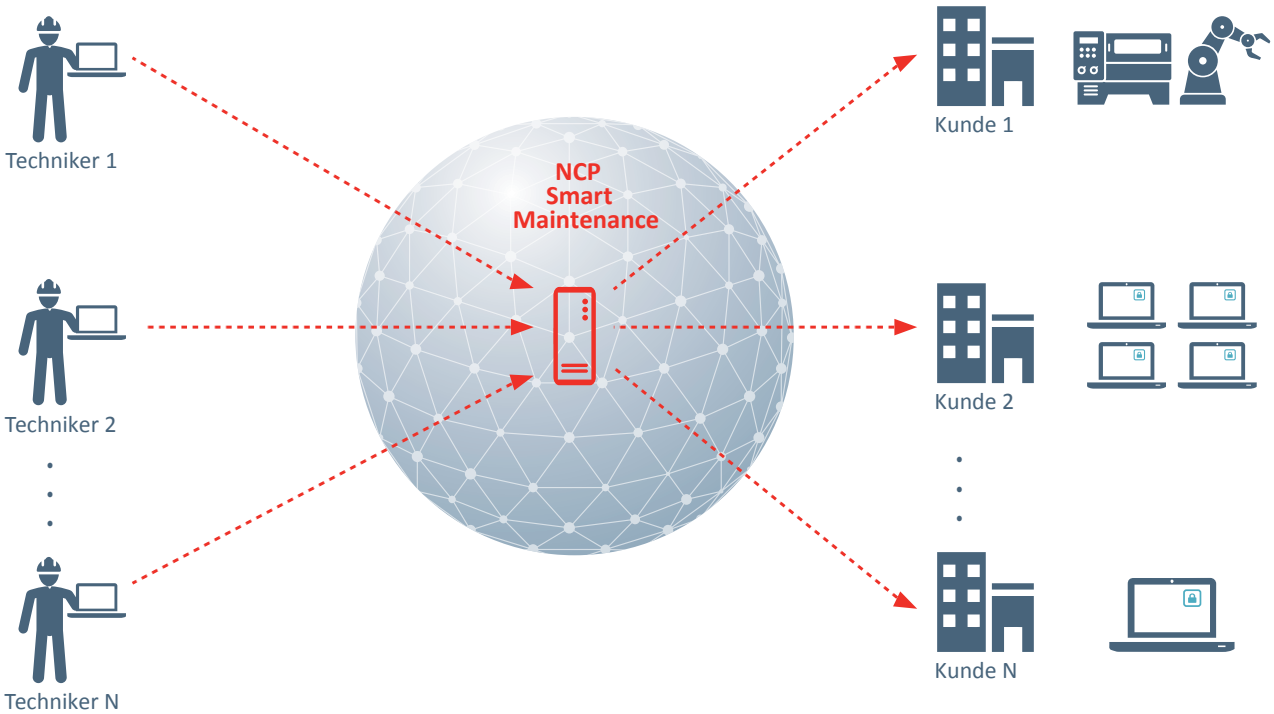
Beispiel für die mobilfunkbasierte Kommunikation mit Anlagen an entlegenen Orten sinnvoll. Entsprechend müssen Anlage und Steuerung für IP-basierte Kommunikation ausgelegt, abgesichert und kompatibel zu den integrierten Techniken sein.

Was bei Fernwartung als Managed Service zu beachten ist

Übernimmt die Fernwartung ein Managed Service Provider, sollte dieser mit dem Betreiber die Rahmenbedingungen vertraglich genau festhalten: Welche Angestellten des Dienstleistungsbetriebs dürfen auf welche Maschinen und Anlagen in welcher Funktion zugreifen – und das zu welchen Zeiten sowie in welchen Zeitfenstern?

Manche VPN-Lösungen für die Fernwartung wie NCP Smart Maintenance sind sogar mandantenfähig. In diesem Fall kann der Dienstleister über das zentrale Management in der Cloud für jeden Kunden die Zugriffsrechte sehr granular zuteilen. Es muss sichergestellt sein, dass keine Verbindungen zwischen den verschiedenen Kundennetzen entstehen.

Individuell zugeschnittene und sichere Fernwartung für Managed Service Provider



Wie Betreiber vorhandene Maschinen in die Fernwartung integrieren

Nachdem ein Betreiber festgelegt hat, welche Maschinen einen Fernzugriff benötigen, müssen die dafür notwendigen Schnittstellen zwischen IT und OT hergestellt werden. Gerade alte Maschinen in bestehenden Installationen erfordern oft eine Speziallösung. Denn ihre Software ist veraltet und die Schnittstellen sind proprietär oder nicht mehr aktuell. Ist keine IPsec-Verbindung möglich, bieten sich Verbindungen an, die auf einer TCP-Encapsulation von IPsec mit SSL-Header über den alternativen Port 443 laufen. So arbeitet zum Beispiel der NCP Path Finder[2]. Wenn der Markt kein passendes IIoT Gateway bietet, kann ein Industrie-PC mit den nötigen Schnittstellen, Treibern und der dafür notwendigen Software ausgestattet werden.

Das sollte ein VPN für eine sichere Fernwartung bieten

- ✓ geeignet für Cloud-Umgebungen oder andere Industrie-4.0-Strukturen
- ✓ hochverfügbar und voll virtualisierbar
- ✓ zentrales Management zur Verwaltung und Steuerung aller Anwender und angeschlossenen Geräte, Maschinen und Anlagen
- ✓ granulare Zuteilung von Zugriffsrechten
- ✓ Multi-Faktor-Authentifizierung (z. B. mit zusätzlichen kurzfristigen Einmalpasswörtern)
- ✓ Authentifizierung mit digitalen Zertifikaten in einer PKI (Public Key Infrastructure)
- ✓ starke Verschlüsselungsalgorithmen (z. B. IPsec IKEv2 mit ECC)
- ✓ Verbindungsaufbau von dedizierter Maschine zu einem bestimmten Techniker
- ✓ unterstützt aktuell sichere Protokolle wie IPv4/IPv6 oder SNMP v3
- ✓ erkennt Verstöße gegen vorgegebene Richtlinien und verweigert gegebenenfalls Zugriff
- ✓ Network Access Control bei VPN-Verbindungen
- ✓ erlaubt mandantenfähige, sicher getrennte Verwaltung vieler Kunden und Standorte

[2] NCP engineering: VPN Path Finder Technology – Hochsicheres Mobile Computing auch in „IPsec-feindlichen“ Remote Access-Umgebungen.

Warum eine bereichsübergreifende VPN-Lösung die Sicherheit erhöht

Selbst wenn die Wartung über das Firmennetz oder eine private Cloud erfolgt, sollten die Zugriffsrechte genauso granular zugeteilt werden, wie das bei externem Wartungspersonal der Fall ist. Sonst besteht die Gefahr, dass ein nicht autorisierter Mitarbeiter auf die Anlagensteuerung zugreift.

Bei der Auswahl der VPN-Lösung für die Fernwartung ist zu überprüfen, ob das Unternehmen bereits eine VPN-Lösung für den Zugriff von Remote-Mitarbeitern verwendet. Denn dann ist es sinnvoll, diese auch für die Fernwartung zu nutzen. So kann die IT-Abteilung beides über eine Managementoberfläche verwalten. Nutzt ein Unternehmen zum Beispiel die Fernwartungslösung Smart Maintenance von NCP, lassen sich über die zugehörige VPN-Managementoberfläche NCP Secure Enterprise Management (SEM) alle Fernzugriffsszenarien zentral managen, egal ob für mobile Mitarbeiter oder Anlagen und Maschinen. Das stellt sicher, dass die Sicherheitsrichtlinien unternehmensweit durchgängig eingehalten werden.

Wie VPN verschiedenste Remote-Access-Szenarien absichert

Unternehmen können mit einer VPN-Lösung vielfältige Zugriffsszenarien absichern. Techniker haben damit die Möglichkeit, schnell auf abgelegene Anlagen wie Kleinkraftwerke oder Solarparks zuzugreifen. Auch schwer zugängliche Maschinen und Anlagen wie in gesundheitsgefährdenden Umgebungen, in Reinräumen, Kliniken oder beispielsweise Selfservice-Standorten von Banken können per VPN auf sichere Weise remote gewartet werden. So unterschiedlich die Anwendungsszenarien auch sind: Mit Smart Maintenance und der zentralen Managementsoftware SEM kann ein IT-Team alle Szenarien aus einer Hand administrieren. Die Infrastruktur eignet sich für Kunden mit vielfältigen Szenarien wie auch für Managed Service Provider, die ihren Kunden individuell zugeschnittene Lösungen anbieten wollen.

Sichere Kommunikation vom Technologiemarktführer

Die NCP engineering GmbH mit Sitz in Nürnberg verfügt über eine mehr als 35-jährige Geschichte und hat damit mehr Erfahrung und ist länger im Markt tätig als so mancher Tech-Gigant. Arbeiten nach Kundenwunsch und Ziele wie Benutzerfreundlichkeit, Kompatibilität sowie Wirtschaftlichkeit stehen bei NCP ganz klar im Fokus. Dies belegen zahlreiche Referenzen von Kunden sowie OEM-Partnerschaften mit Firmen wie Juniper Networks, der Deutschen Telekom, Lancom Systems, WatchGuard, Sophos und Phoenix Contact.

NCP
SECURE COMMUNICATIONS

Sie haben Fragen oder möchten einen Termin für eine Produktdemonstration vereinbaren? Dann kontaktieren Sie uns!

NCP engineering GmbH
Dombühler Straße 2
90449 Nürnberg

Tel.: +49 911 9968-0
vertrieb@ncp-e.com
www.ncp-e.com

Wir freuen uns auf das Gespräch!