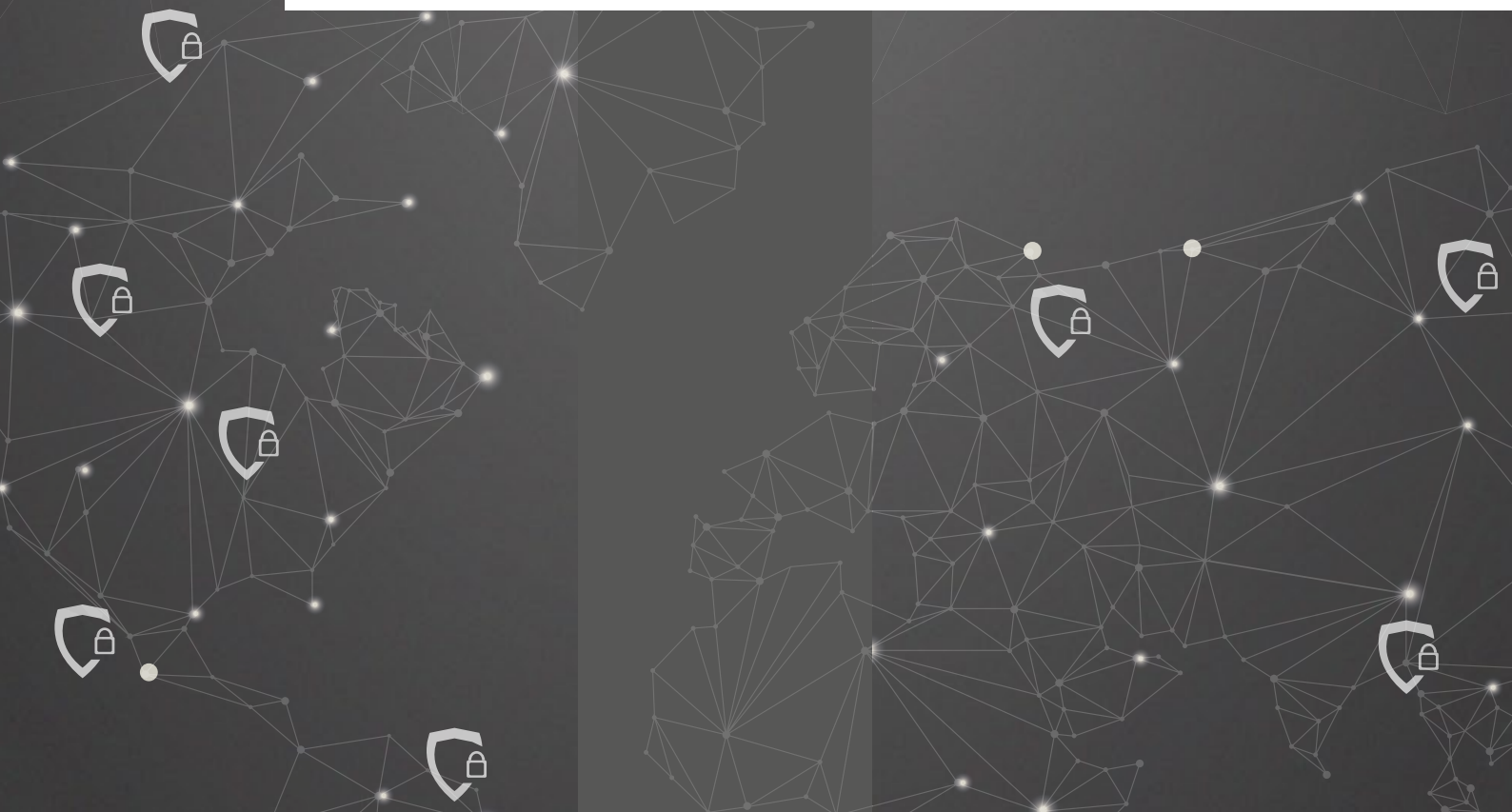
MB CONNECT LINE

WHITEPAPER

IT-SICHERHEIT

bei der industriellen Fernwartung



INHALTSVERZEICHNIS

EINLEITUNG

Viele Maschinen und Anlagen in der industriellen Fertigung sind heutzutage miteinander vernetzt. Diese Vernetzung zwischen Steuerungen, Bediengeräten und auch Antriebssystemen und dem damit verbundenen Zugang zum Internet ist die Voraussetzung für die Fernwartung.

„IT-SICHERHEITSKONZEPTE SIND FUNDAMENTAL, UM DIE IT-SICHERHEIT IN EINEM UNTERNEHMEN ZU GEWÄHRLEISTEN.“

Bei einer Fernwartung verbindet sich ein Benutzer ortsunabhängig über das Internet mit einer Maschinensteuerung (SPS, CNC) oder einem Bediengerät, beispielsweise einem HMI (Human Machine Interface). So kann er sich Prozessdaten anzeigen lassen oder in das Steuerungsprogramm eingreifen.

Maschinensteuerungen sind nicht auf das Thema IT-Sicherheit hin konzipiert. Ist ein Benutzer einmal mit einer ungeschützten Steuerung verbunden, kann er relativ leicht auch aufs gesamte Firmennetzwerk zugreifen. Solche Eingriffe sind aber unerwünscht. Deshalb sollten Maschinensteuerungen oder andere Endgeräte von Anlagen und Systemen durch geeignete Maßnahmen zur IT-Sicherheit geschützt sein, bevor sie mit dem Internet verbunden werden. Wirkungsvolle IT-Sicherheitssysteme für die Fernwartung wirken auf zwei Ebenen. Zum einen verwalten sie die Zugriffsrechte auf die Maschinen bzw. die entsprechenden Fernwartungsendpunkte. Damit erhalten nur autorisierte Benutzer einen Zugriff auf die Maschinen. Zum anderen müssen die Maßnahmen der IT-Sicherheit auch vor weitergehenden Cyberangriffen von außen schützen. Dies erfordert entsprechende bauliche und strukturelle Maßnahmen sowohl bei der Hard- als auch bei der Software. IT-Sicherheitskonzepte sind fundamental, um die IT-Sicherheit in einem Unternehmen zu gewährleisten. Je eher das Thema bereits in die Konzeptionierung und Planung einer Maschine oder Anlage einfließt, desto besser ist hinterher der Schutz, den das Konzept gewähren kann.

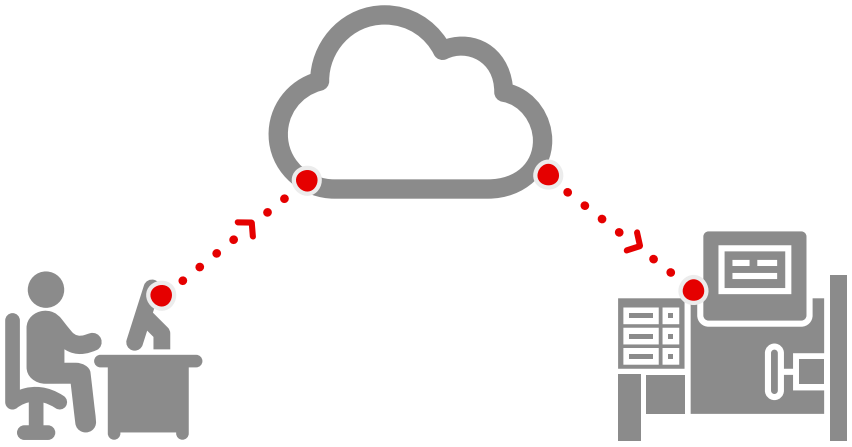
Im Rahmen dieses Whitepapers werden zunächst das Prinzip und die Funktionsweise des Fernwartungssystems von MB connect line beschrieben. Anschließend werden die relevanten Komponenten ausführlich hinsichtlich der Sicherheitsaspekte dargestellt und die Lösungsumsetzung mit höchsten IT-Sicherheitstandards erläutert.

MB CONNECT LINE

FUNKTIONSPRINZIP EINER FERNWARTUNG

FUNKTIONSPRINZIP EINER FERNWARTUNG

Bei einer Fernwartung verbindet sich ein autorisierter Benutzer, beispielsweise ein Servicetechniker, von einem beliebigen Ort aus über das Internet mit einer SPS-Steuerung oder einem HMI[1] als Bediengerät.
Was hier so einfach klingt, ist in der Umsetzung viel komplexer.
Der Fernzugriff des Benutzers erfolgt nicht direkt von seinem Rechner über das Internet auf die Maschine, sondern es ist noch eine Cloud dazwischengeschaltet. Der Benutzer verbindet sich über das Internet mit der Cloud und erhält dann über die Cloud den Zugriff auf die Maschine, für die er Berechtigungen besitzt.



Schematischer Aufbau eines Fernzugriffs. Der Benutzer wählt sich über eine Cloud ein und erhält Zugriff zur Maschine.

Drei Komponenten der Fernwartung

Ein industrielles Fernwartungssystem besteht folglich aus drei Komponenten: Im Zentrum befindet sich als erste Komponente die Cloud. Sie nimmt die Anfrage des Benutzers auf und stellt die Verbindung zum Endgerät her. Der sichere Benutzerzugriff ist die zweite Komponente beim Fernzugriff: Nur autorisierte Benutzer erhalten Zugriff auf die Cloud. Der dritte Part ist die Verbindung zwischen der Cloud und der Maschinensteuerung oder einem anderen Endgerät. Hierfür ist der Maschine oder dem Endgerät ein Router vorgeschaltet, der das Internet vom Firmennetz sicher trennt und nur autorisierte Zugriffe durchlässt.

Das Öko-System von MB connect line ist ein industrielles Fernwartungssystem mit Cloudanbindung und industriellem Router. Es besitzt sämtliche sicherheitsrelevante Faktoren und Eigenschaften. Bei MB connect line ist die Cloud gleichbedeutend mit dem Remote Service Portal mbCONNECT24. Dort sind die Zugriffsrechte sowie die Konfigurationen der Router hinterlegt. Außerdem schafft es die Verbindung zwischen dem Benutzer und der Maschine.

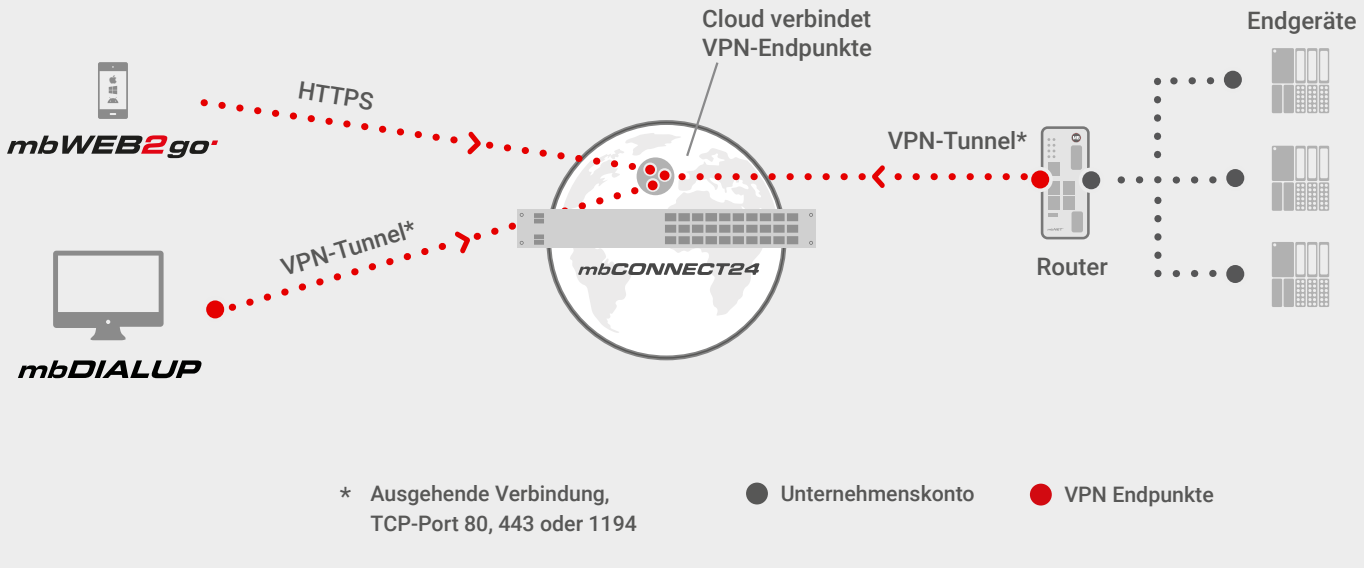
[1]) HMI: Human Machine Interface – Mensch-Maschine-Schnittstelle

FUNKTIONSPRINZIP EINER FERNWARTUNG

Der Verbindungsaufbau erfolgt mithilfe eines Virtuellen Privaten Netzwerkes, kurz VPN. Über dieses Netz werden ein VPN-Tunnel zwischen dem Rechner und der Cloud sowie ein VPN-Tunnel zwischen der Cloud und der Maschine aufgebaut. Dafür werden von Benutzer- und Maschinenseite jeweils ausgehende Verbindungen genutzt. Die Cloud verbindet diese beiden VPN-Tunnel miteinander. So entsteht eine gesicherte Verbindung zwischen dem Rechner und dem Router. Der Datenaustausch zwischen Benutzer und Endgerät erfolgt über diesen gesicherten VPN-Tunnel.

Der Benutzerzugriff kann sowohl webbasiert von jedem beliebigen Browser mithilfe von mbWEB2go oder auch per VPN-Client-Verbindung mit mbDIALUP erfolgen. Die industriellen Router mbNET besitzen Schnittstellen für die gängigen Steuerungssysteme sowie Endgeräte und können individuelle Zugriffsrechte auf die Endpunkte gewähren. Die in den Router integrierte Firewall schützt zudem vor unbefugtem Zugriff Dritter.

DAS ÖKOSYSTEM



Öko-System mit webbasiertem Benutzerzugang oder Client-Verbindung zum Remote Service Portal mbCONNECT24 sowie Router mbNET mit integrierter Firewall.

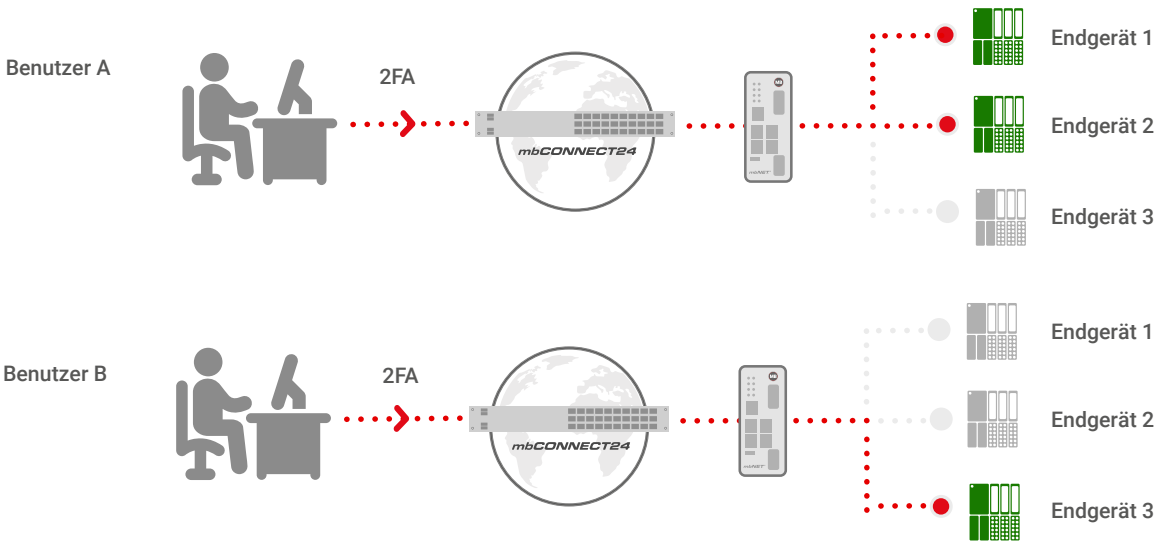
MB CONNECT LINE

UNSERE SCHUTZKONZEPTE

SCHUTZKONZEPTE

Zugriffsschutz

Der autorisierte Benutzer wählt sich über eine ausgehende Verbindung in das Remote Service Portal ein und legitimiert sich beispielsweise per 2-Faktor-Authentisierung (2FA): Neben einem individuellen Benutzernamen und einem Passwort erhält der Benutzer zeitnah zum Loginvorgang per SMS, Anruf, E-Mail oder über den TOTP (z.B. Google Authenticator) einen zusätzlichen PIN-Code, den er bei der Anmeldung eingeben muss. Erst dann erhält er Zugang zum System. Dort sind die ihm freigegebenen Endgeräte innerhalb der Maschine oder Anlage angezeigt und verfügbar.



Benutzer A erhält Zugriff auf Endgerät 1 und 2. / Benutzer B erhält Zugriff auf Endgerät 3.

Datenschutz

In der Cloud sind alle Daten hinterlegt, die im Zusammenhang mit dem Fernzugriff stehen. Dazu gehören die Benutzerdaten wie Name, E-Mail-Adresse oder Passwörter, aber auch die jeweiligen Zugriffsrechte auf die verschiedenen Komponenten auf der Maschinenseite. Jede Verbindung zwischen einem Benutzer und einem Endgerät an einer Maschine oder Anlage erfolgt nur und ausschließlich über die Cloud. Denn nur die Cloud kann den Benutzer anhand der hinterlegten Daten identifizieren und ihm über den Router die entsprechenden Rechte auf die Endgeräte zuweisen. Der sichere Datentransfer zwischen zwei VPN-Endpunkten ist über die eingerichteten VPN-Tunnel und die eingesetzten höchsten Verschlüsselungsstandards der Übertragungs-protokolle gewährleistet.

Maschinen- und Anlagenschutz

Maschinen und Anlagen sind durch den Router geschützt. Er trennt das Maschinennetzwerk (OT-Netzwerk) vom Firmennetzwerk (IT-Netzwerk). Ein Benutzer kann nur auf ihm freigegebene Maschinen- und Anlagen-komponenten zugreifen. Jeder Zugriff wird bezüglich Benutzername, Zeitpunkt und Dauer protokolliert.

MB CONNECT LINE

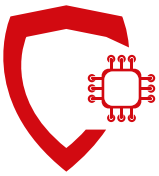
IT-SICHERHEITS-MERKMALE DES ÖKO-SYSTEMS

IT-SICHERHEITSMERKMALE DES ÖKO-SYSTEMS

Ein umfassendes und ganzheitliches Sicherheitskonzept berücksichtigt jeden Bereich innerhalb des Systems vom Benutzerzugriff über die Datenverwaltung in der Cloud bis zum Zugriff auf die Maschinen- und Anlagenkomponenten über den Router. Das Öko-System von MB connect line zeichnet sich hier durch folgende Merkmale aus:

Verschlüsselung

VPN-Verbindung mit AES-256-bit-Verschlüsselung über das Sicherheitsprotokoll TLS1.2/SSL. Dieser hohe Verschlüsselungsstandard erlaubt auch den sicheren Einsatz im Rahmen geschäftskritischer Anwendungen.



Verbindungen

Es wird nur mit ausgehenden Verbindungen gearbeitet. Somit ist eine nahtlose Integration in die vorhandene IT-Umgebung gewährleistet. Die vorhandenen IT-Sicherheitsstrategien bleiben unberührt. Zusätzlich wird die Übertragung von Gerät- und Komponentendaten zwischen Router und Portal mit einer separaten PKI gesichert.

Authentifizierung

Benutzername und Passwort mit zertifikatbasierter und optionaler 2-Faktor-Authentifizierung (2FA) mit SMS, Anruf, E-Mail oder TOTP (z.B. Google Authenticator) stellt die Authentizität des Benutzers sicher.

Tests

Regelmäßige toolgestützte und manuelle Penetrationstests gewährleisten die Serversicherheit.

MB CONNECT LINE

ZENTRALE VERMITTLUNGSSTELLE:

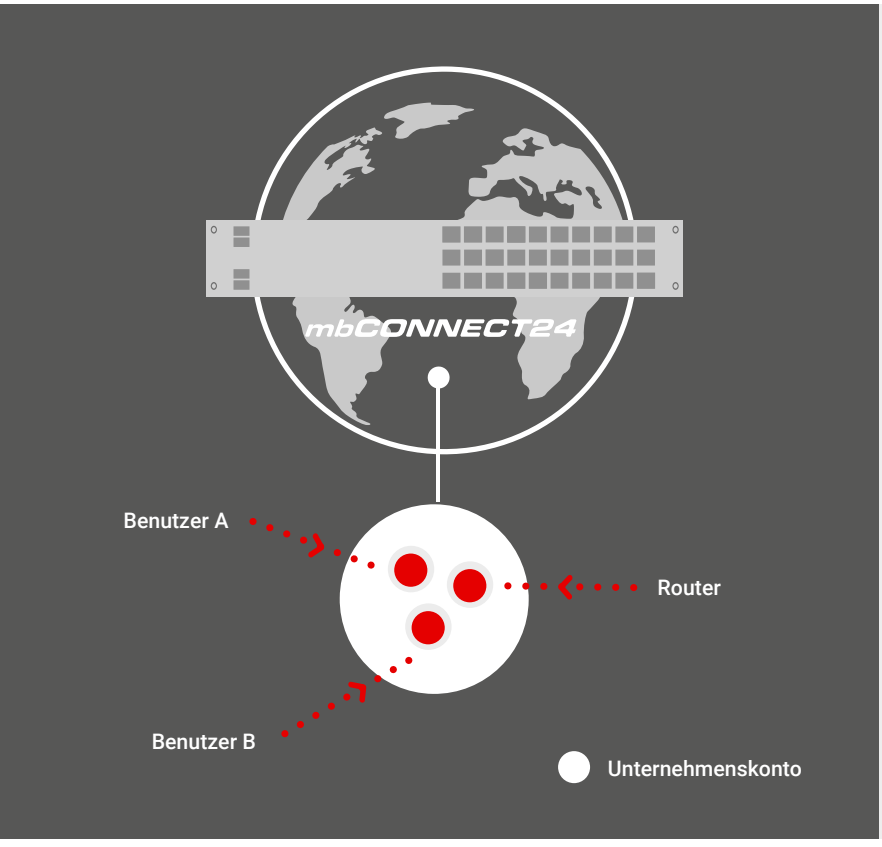
DAS REMOTE SERVICE PORTAL

ZENTRALE VERMITTLUNGSSTELLE: DAS REMOTE SERVICE PORTAL

Kernstück und zentrale Vermittlungsstelle des Fernwartungssystems ist das Remote Service Portal mbCONNECT24, auch als Cloud bezeichnet.

In diesem Portal findet die Verwaltung sämtlicher Projekte, Benutzer und Endgeräte statt. Mitarbeiter mit Administrationsrechten legen die Benutzerrechte sowohl interner als auch externer Mitarbeiter fest. Damit können nur eindeutig authentifizierte Benutzer auf einen abgeschlossenen Netzwerkbereich zugreifen. Auch die Zugriffsrechte auf die Router und die dahinterliegenden Endgeräte in Form von Maschinen- und Anlagenkomponenten sind durch die Festlegungen der Administratoren streng reglementiert und definiert.

Jede Verbindung zwischen einem PC oder mobilen Endgerät eines Benutzers auf der einen Seite und der Maschinenschnittstelle auf der anderen Seite erfolgt ausschließlich über die Cloud. Damit kann es keine anderen Zugriffe auf das Maschinennetzwerk geben als über dieses Portal. Der Zugriff auf die Cloud erfolgt sowohl maschinen- als auch benutzerseitig ausschließlich über ausgehende Verbindungen. Mit ausgehenden Verbindungen bleiben in der Unternehmensfirewall die Ports von außen nach innen gesperrt, was die IT-Sicherheit erheblich verbessert.

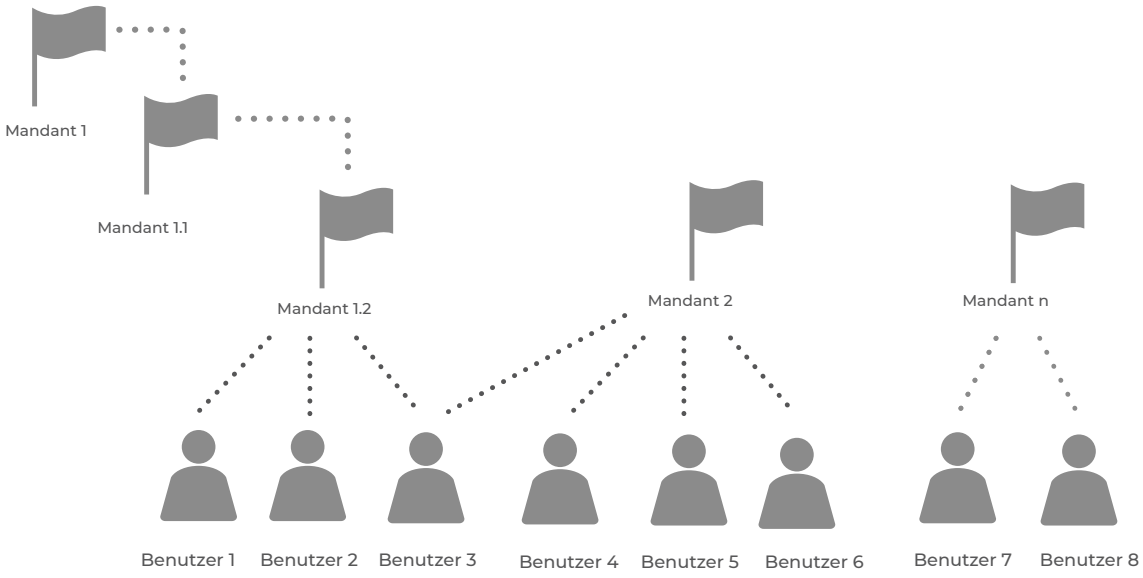


Das Remote Service Portal ist ein in sich geschlossenes System. Jedes Unternehmen erhält innerhalb dieser Cloud ein eigenes Konto (= Unternehmenskonto, Account).

Hierbei handelt es sich um einen abgeschlossenen Bereich innerhalb der gesamten Server- oder Cloudstruktur mit einem eigenen abgeschlossenen VLAN (virtuelles Netzwerk) und einer eigenen Datenbank. Damit ist jedes Konto absolut eigenständig.

Individuelle Zugriffsrechte

Die Rechtezuordnung fordert klare Definitionen sowie Zuordnungen und kann sowohl individuell gestaltet oder zu Mandanten zusammengefasst sein. Dabei können für jeden Benutzer die einzelnen Rechte von Komponente zu Komponente variieren: Für manche Routerinformationen kann der Benutzer umfangreiche Zugriffsrechte erhalten, für andere nur einfache Leserechte oder auch gar keinen Zugriff. Diese feingliedrige Definition der Rechte ist Aufgabe des Administrators. Die Hoheit über die Zugriffe ist also stets klar definiert. Um die Benutzer-/Zugriffsverwaltung noch differenzierter zu gliedern, können Zugriffsrechte auf Projekte und Geräte über das Mandantensystem noch feiner und exakter untergliedert werden. Die Rechteverwaltung und Sicherstellung erfolgt über die Cloud. Jeder Zugriff wird bezüglich Benutzernamen, Zeitpunkt und Dauer des Zugriffs protokolliert und kann somit jederzeit nachvollzogen werden.

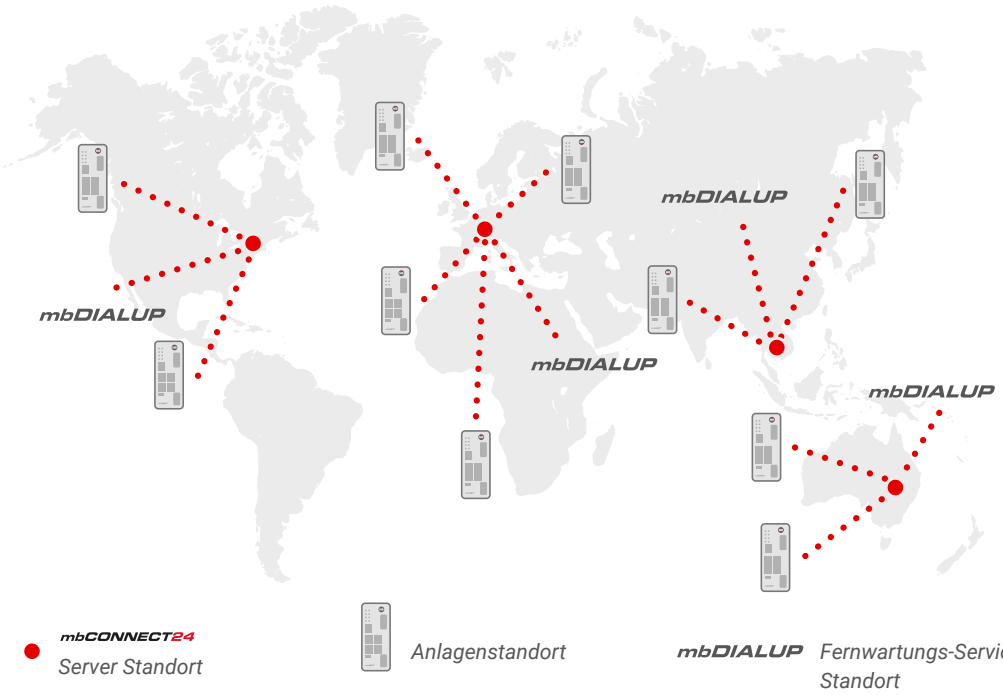


Beispielgrafik einer Benutzerverwaltung

Server

Physikalisch ist die Cloud oder das Remote Service Portal mbCONNECT24 eine Rechnerarchitektur in einem Rechenzentrum. Dieses Portal bietet die Administrationsoberfläche, um die Fernwartung einfach und intuitiv durchführen zu können.

Ein weltweites Angebot dieses Services sowie geringe Zugriffszeiten sind nur mit mehreren Serverstandorten erreichbar. MB connect line verfügt über insgesamt vier Serverstandorte in den USA, in Europa, in Asien und in Australien.



Jeder Serverstandort ist autark und befindet sich in einem abgeschlossenen Bereich innerhalb eines Sicherheitsdatenzentrums. Die einzelnen Standorte sind nicht miteinander vernetzt. Wird ein Unternehmenskonto angelegt, entscheidet sich das Unternehmen einmalig für einen festen Standort. Dort sind dann die Daten lokal sicher und definiert gespeichert. Jeder Standort hat eine einzige IP-Adresse. Damit gibt es auch nur einen einzigen Zugriff auf diesen Serverstandort. Das vereinfacht die Integration der Komponenten in Anlagen und Maschinen, da bei der Integration des Fernwartungssystems jeweils nur eine einzige Schnittstelle und damit eine einzige IP-Adresse eingetragen werden muss.

Neben den gehosteten Servern bietet MB connect line noch eine private Variante an. Diese sogenannte On-Premises-Lösung mymbCONNECT24.virtual kann in verschiedenste IT-Umgebungen integriert werden – sowohl im eigenen Haus als auch in ausgewählten Hostingzentren des Unternehmens. Damit hat das Unternehmen alleinigen und vollen Zugriff auf sämtliche Daten und Funktionen des Systems. Zusätzlich bietet die On-Premises-Variante auch weitere Funktionen wie Active-Directory-Anbindung (LDAP) der Benutzer und eine White-Label Möglichkeit.

Datensicherheit und Datenschutzgrundverordnung (DSGVO)

Datensicherheit ist der Schutz von Daten vor dem unbefugten Zugriff Dritter. Hierbei liegt besonderes Augenmerk auf dem Schutz persönlicher Daten. Dieser ist in Europa in der Datenschutzgrundverordnung (DSGVO) geregelt. Jederzeit muss klar definiert und nachvollziehbar sein, wo sich welche persönlichen Daten befinden. Da jeder Serverstandort auch Datenstandort ist, unterliegen die jeweiligen Daten sicher den dort herrschenden gesetzlichen Regelungen.

Sicherheitsmerkmale des Remote Service Portals

Die Sicherheitsmerkmale des Remote Service Portals von MB connect line entsprechen stets den hohen Standards und erfüllen regionale Anforderungen bezüglich Datenschutz und Datensicherheit. Besondere Merkmale des Remote Service Portals sind:

- Die Server werden durchgehend 24/7 überwacht.
- Es werden regelmäßige Backups erstellt.
- Für jeden Server existiert nur eine einzige IP-Adresse als Zugangspunkt.
- Für den Verbindungsaufbau ist nur ein ausgehender TCP-Port 80, 443 oder 1194 erforderlich.
- Sämtliche Hoster der Sicherheitsdatencenter sind zertifiziert nach ISO 27001/27707.
- Es existieren Ausfallpläne für schnelles Wiederherstellen im Störungsfall.
- Regelmäßige und automatisierte Sicherheitsupdates.
- Der Wartungs- und Diagnosezugang der Server ist beschränkt auf eine eindeutige Benutzergruppe von MB connect line.
- Der Firmenstandort Dinkelsbühl wurde vom TÜV Nord nach der IEC 62443-4-1 zertifiziert. Damit ist MB connect line in der Lage, Hard- und Software nach einem zertifizierten Prozess zu entwickeln, um ein Höchstmaß an Cyber-Sicherheit bereits in der Produktentwicklung zu bieten.


TÜVNORD

CERTIFICATE

Cybersecurity-related processes as per
IEC 62443-4-1 : 2018 (ML 2)

IEC 62443

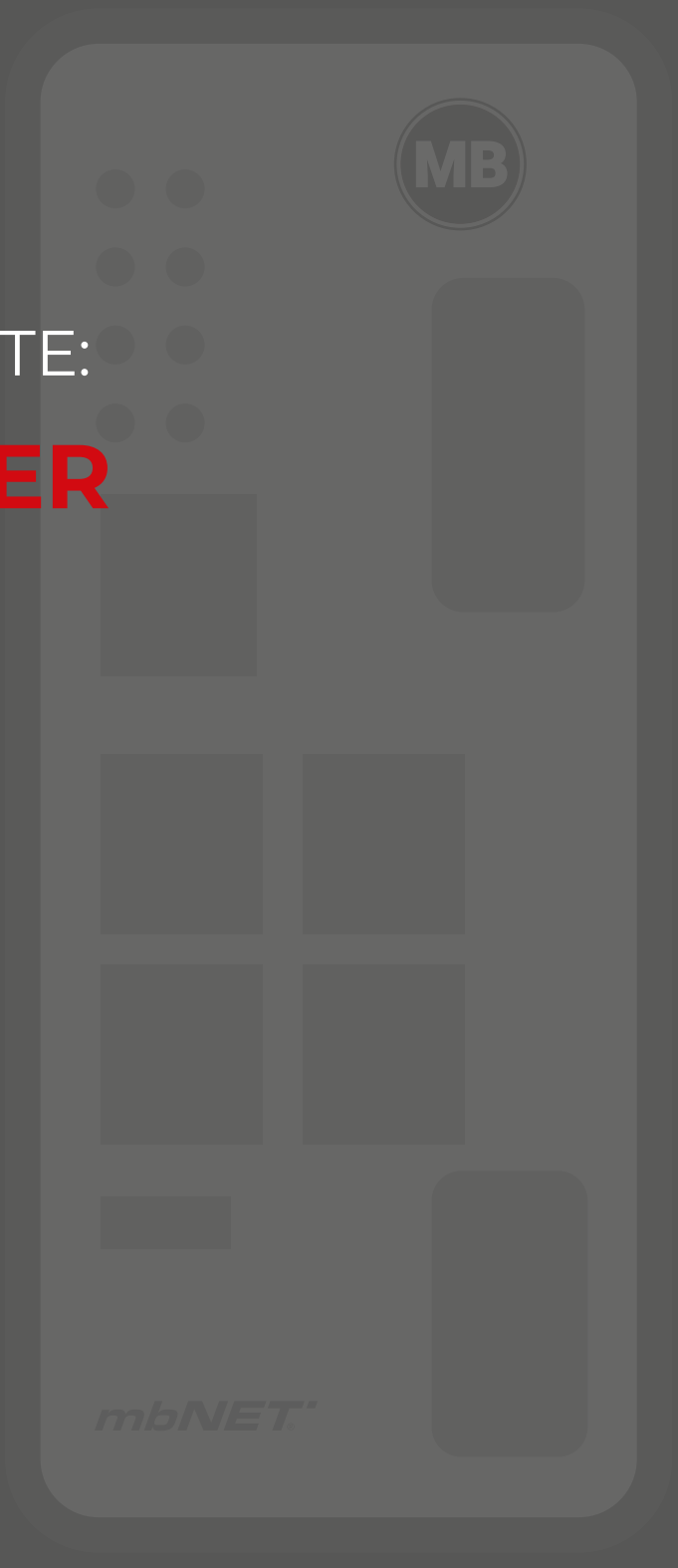
MB connect line GmbH
Winnettener Straße 6
91550 Dinkelsbühl
Germany

Product development life-cycle requirements related to cyber security of access products intended for use in IACS environments

MB CONNECTLINE

MASCHINENSEITE:

DER ROUTER

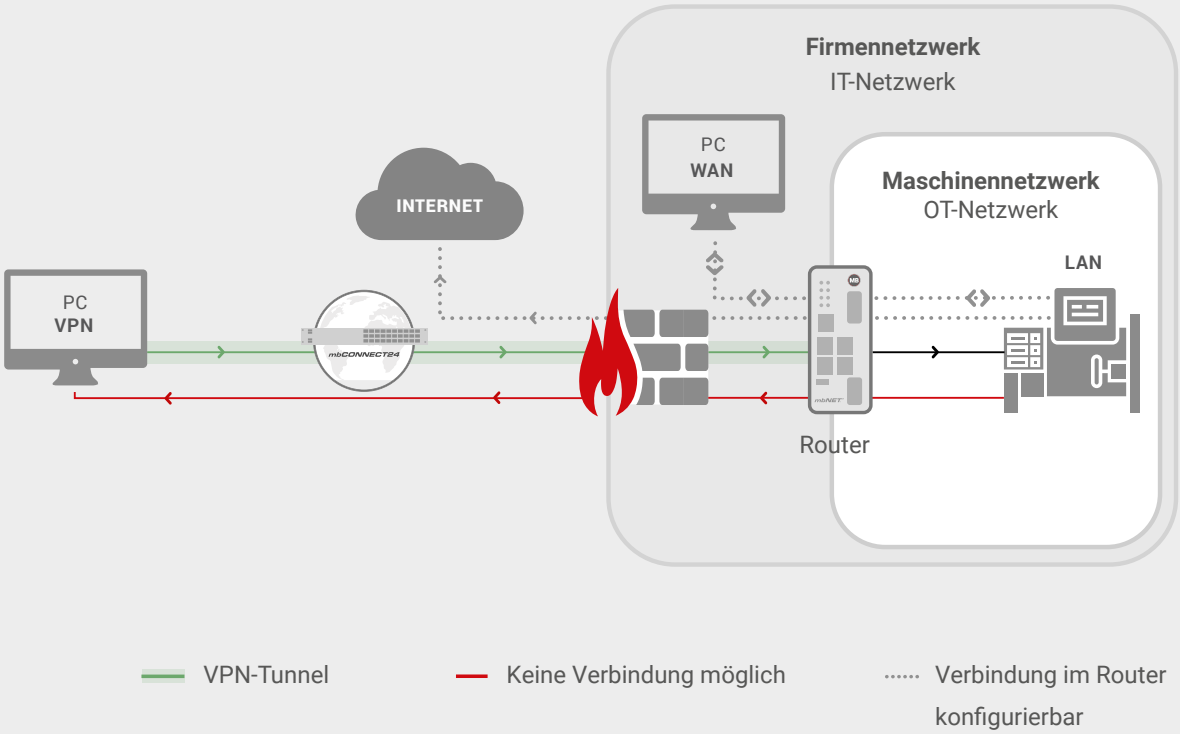


MASCHINENSEITE: DER ROUTER

Der Router verbindet die Maschine oder Anlage mit dem Internet. Er wird zwischen das Firmennetzwerk und das Maschinennetzwerk des Unternehmens geschaltet

Einbindung des Routers ins Firmennetz

Ein Netzwerk in einem Unternehmen ist normalerweise aufgeteilt in ein Firmennetzwerk oder IT-Netzwerk und ein Maschinennetzwerk, das OT-Netzwerk. Das Firmennetzwerk ist durch eine firmeneigene Firewall vom Internet getrennt. Der Router trennt das Maschinennetzwerk (LAN) vom Firmennetzwerk (WAN). Ein Fernwarter an PC „VPN“ gelangt über den VPN-Tunnel zum Router und kann von dort auf die ihm freigegebenen Endgeräte im LAN zugreifen. Ein Zugriff über diese Verbindung aufs WAN ist nicht möglich. Der Router regelt auch Zugriffe zwischen WAN und LAN. Ein interner Mitarbeiter kann mit seinem PC „WAN“ aus dem IT-Netzwerk aufs OT-Netzwerk zugreifen, was bei entsprechender Freigabe im Router auch umgekehrt möglich ist. Eine Verbindung vom LAN zum PC „VPN“ ist grundsätzlich nicht möglich und auch nicht konfigurierbar.



Einbindung des Routers in das Firmennetzwerk

MASCHINENSEITE: DER ROUTER

Technische Merkmale der Router

Da der Router ausgehende Verbindungen zur Cloud nutzt, müssen in der Unternehmensfirewall keine eingehenden Ports geöffnet werden und das Netzwerk ist vor direkten Zugriffen von außen geschützt. Hat der Router über diesen Weg einen VPN-Tunnel zur Cloud aufgebaut, können die Daten zwischen der Cloud und dem Router bzw. zwischen dem Benutzer und dem Endgerät ausgetauscht werden. Der Router soll höchstmögliche IT-Sicherheit sowohl in der Bedienung als auch in der Hardware bieten. Beide Ansätze verfolgt MB connect line unter den Bezeichnungen Security by Default und Security by Design parallel.

Security by Default

Security by Default bezieht sich auf die Konfiguration des Routers. In seinem Auslieferungszustand sind sämtliche Sicherheitsmerkmale des Routers aktiviert. Die Firewall von IT nach OT ist gesperrt und von OT nach IT ist nur das Notwendigste für den Betrieb zugelassen. Damit ist das höchste Maß an IT-Sicherheit gegeben. Sollen Sicherheitsmerkmale deaktiviert werden, muss dies durch eine Konfigurationsänderung erfolgen. Für höchste IT-Sicherheit bei der Inbetriebnahme besitzt jeder Router bereits bei der Auslieferung ein individuelles Passwort. MB connect line hat bewusst auf Standardpasswörter im Auslieferungszustand verzichtet.

Security by Design

Leitlinie von MB connect line war und ist es, höchste IT-Sicherheit bereits bei der Entwicklung von Produkten und Systemen zu berücksichtigen und sämtliche Handlungen danach auszurichten. Die Umsetzung ist Security by Design.
Das Fundament der Vertrauenskette (Trusted Chain) bildet die Bootsoftware. Diese befindet sich auf einem Nur-Lese-Speicher (ROM). Eine Änderung dieser Software im Betrieb ist somit nicht möglich. Die Firmware ist mit einem Zertifikat von MB connect line signiert. Im Rahmen des Secure-Boot-Prozesses prüft die Bootsoftware die im Speicher abgelegte Firmware. Nur wenn die Firmware mit dem hinterlegten Zertifikat im Router signiert wurde, wird sie geladen und gestartet. Konfigurationsdaten und Benutzerdaten sind im nichtflüchtigen Speicher (FLASH) verschlüsselt abgelegt. Der individuelle Schlüssel dafür ist im Hardware-Secure-Element hinterlegt, das mit einem Safe vergleichbar ist. Damit kann nur der Router selbst auf die Daten zugreifen.

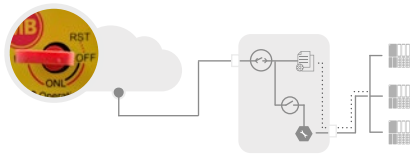
„Höchstes Maß an IT-Sicherheit.“

MASCHINENSEITE: DER ROUTER

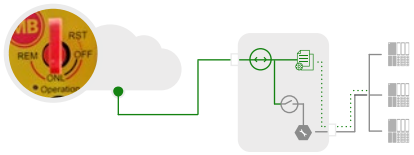
Router mit Schlüsselschalter

Der Router mbNET.rokey ist mit einem integrierten Schlüsselschalter ausgerüstet. Dieser Schalter kann drei Schlüsselstellungen einnehmen sowie eine zusätzliche tastende Stellung RST zur Rücksetzung des Routers auf Werkseinstellung.

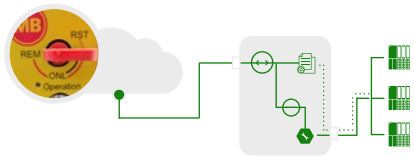
Router mbNET.rokey mit Schlüsselschalter



Bei der Stellung **OFF** baut der Router keine Verbindung zur Cloud auf und wird als offline angezeigt.



Bei der Stellung **ONL** ist der Router online, hat Zugriff auf die Cloud und wird in dieser auch als online angezeigt. In dieser Schalterstellung kann nur auf interne Dienste des Routers wie die Konfigurationsoberfläche oder die mbEDGE-Funktionen zugegriffen werden.



Erst mit der Schalterstellung **REM** ist auch die Verbindung zwischen dem Fernwarter und dem LAN-Netz freigeschaltet und das Routing zu dem Endgerät möglich. Wird ein Router mit Schlüsselschalter eingesetzt, ist für jeden Fernwartungszugriff einen Ansprechpartner vor Ort erforderlich. Er bedient den Schlüsselschalter und ermöglicht so den Zugriff aufs LAN-Netz. Um einen beliebigen Fernzugriff zu verhindern, ist jeder Router mit zwei Schlüsseln ausgerüstet: einem schwarzen und einem roten. Der schwarze Schlüssel kann nur die beiden Einstellungen ONL und OFF schalten. Die Einstellungen REM und RST sind nur mit dem roten Schlüssel erreichbar.

Interne Dienste, Daten, mbEDGE

Routing VPN/LAN

IT-Sicherheitseigenschaften

- Ausgestattet mit einer Stateful Inspection Firewall mit IP-Filter, Simple-NAT, 1:1 NAT und Portforwarding
- Im Auslieferungszustand sind sämtliche Sicherheitseinstellungen aktiviert (Security by Default)
- OpenVPN als VPN-Verbindungsprotokoll
- Regelmäßige Sicherheitsupdates
- Umfangreiche IT-Sicherheitsmerkmale wie Secure-Boot und Hardware-Secure-Element

MB CONNECT LINE

BENUTZERSEITE:

VERBINDUNGSAUFBAU ZUM REMOTE SERVICE PORTAL

BENUTZERSEITE: VERBINDUNGSAUFBAU ZUM REMOTE SERVICE PORTAL

Der dritte für die IT-Sicherheit relevante Aspekt ist der Verbindungsaufbau vom Benutzer zum Remote Service Portal. Hier hat der Benutzer zwei Möglichkeiten. Die einfachste Variante ist das Einwählen über eine mit HTTPS gesicherte Verbindung über einen Browser. Die Verbindung zum Endgerät erfolgt ebenfalls HTTPS gesichert per mbWEB2go. Muss dagegen eine transparente TCP/IP-Netzwerkverbindung geschaffen werden, erfolgt der Zugriff über einen PC mit dem VPN-Client-Programm mbDIALUP. Es stellt den dafür notwendigen gesicherten VPN-Tunnel her.

Webbasierte Visualisierung

Für die Überwachung und Visualisierung von Systemzuständen oder um auf Applikationen und Anwender-oberflächen zuzugreifen, bietet sich die webbasierte Variante an. Der Nutzer verbindet sich via HTTPS über einen Web-Browser mit der Cloud. Im Anschluss wird via mbWEB2go eine Verbindung zum Endgerät aufgebaut. Weitere Tools oder Programme sind nicht notwendig.

Auf der Maschinenseite ist der Router in diesem Fall nur für Protokolle wie RDP, VNC oder Web durchlässig. Über eine Remote Desktop Verbindung kann der Benutzer auf die Oberflächen von HMIs oder auf die Anzeigen von Steuergeräten zugreifen und gemäß der jeweiligen Applikation auch eingreifen. Es sind alle Zugriffe möglich, die auch auf dem entsprechenden Bediengerät vor Ort möglich wären.
Jeder Zugriff wird mit Benutzername, Zeitpunkt, Dauer und Endgerät protokolliert und ist somit transparent nachvollziehbar.

Technische Daten zum webbasierten Fernzugriff

- Mobiler und sicherer Webzugang per HTTPS
- Zugriff auf Webserver und IP-Kameras
- Unterstützt RDP- und VNC-Protokolle ohne spezielle Clients oder Apps
- HTML5-fähiger Standard-Browser genügt
- Unabhängig vom Betriebssystem auf dem Endgerät
- Ermöglicht die Überwachung und Visualisierung unabhängig von stationären PCs

Fernzugriff aufs Netzwerk

Um protokollunabhängige TCP/IP-Netzwerkverbindungen aufzubauen und beispielsweise Eingriff in die Steuerung vorzunehmen, muss auf dem PC des zugreifenden Benutzers die VPN-Client-Software mbDIALUP installiert sein. Nur wenn sich der Benutzer über diese Software auf das Remote Service Portal einwählt, kann er auf die Maschinensteuerung zugreifen. Auch diese Zugriffe werden jederzeit bezüglich Benutzer, Zeitpunkt und Dauer sowie ausgewähltem Router protokolliert.

Technische Daten zum Fernzugriff per Client-Software

- VCOM: Tunnelt virtuelle COM-Ports auf die COM-Schnittstelle vom mbNET
- SEARCHoverIP: Multicast für gängige SPS-Programmierumgebungen
- TCP/IP-Ethernet-Protokolle
- mbNET.S7 „Adapter“ für STEP7-Classic und TIA Portal, Zugriff über MPI/ PROFIBUS
- USBoverIP: Tunnelt virtuellen USB-Port auf die USB-Schnittstelle vom mbNET

MB CONNECT LINE

IT-SICHERHEIT

IT-SICHERHEIT

Als unabhängiges mittelständisches Unternehmen sind wir Vorreiter, wenn es um Lösungen für die industrielle Kommunikation via Internet geht. Konkret geht es um die sichere Verbindung von Maschinen und Anlagen für Fernwartung, Datenerfassung und IoT-Anwendungen.

„UNSERE DNA: 100% IT-SECURITY“

Sicherheit ist eine Frage des Bewusstseins

Welche Sicherheitsrisiken bestehen in der industriellen Kommunikation? Diese Frage stellen wir uns bei allen Entwicklungsschritten. Sichere Systeme und Geräte setzen einen sicheren Entwicklungsprozess voraus. Die Entwicklungsingenieure von MB connect line sind entsprechend zertifiziert. Dafür setzen wir auf ein TÜV Experten-Zertifizierungsprogramm im Bereich der sicheren Softwareentwicklung und auf Expertenwissen auf dem Gebiet der IT-Sicherheit (TeleTrusT T.P.S.S.E.).

Sicherheit als gemeinschaftliches Ziel

MB connect line arbeitet eng mit IT-Sicherheitsunternehmen zusammen. So können wir das Sicherheitsversprechen für unsere Lösungen gewährleisten und unsere Entwicklungen validieren. Wir engagieren uns aktiv in der Industrial-Security Arbeitsgruppe bei TeleTrusT. Daraus ist die Evaluierungsmethode für IEC62443-4-2 entwickelt worden, an der wir unsere Produktsicherheit messen und prüfen. Die breite Erfahrung und die verschiedenen Sichtweisen sind entscheidende Faktoren für die sichere Gestaltung unserer Produkte – ohne dabei den Blick auf die Benutzerfreundlichkeit zu verlieren.

Security by Design

Unser Ziel ist es, die Arbeitsabläufe und die Anwendungsfälle so sicher wie möglich zu gestalten und IT-Sicherheit von Anfang an in der Entwicklung zu betrachten. Auf diese Weise bestimmt der Blick auf mögliche Angriffsflächen den Arbeitsablauf der Entwickler. Ein weiterer Kernpunkt ist die Benutzerfreundlichkeit. Wir reduzieren die Komplexität stets so weit, dass der Anwender möglichst keine Fehler machen kann. Dabei wird der gesamte Lebenszyklus betrachtet. Auch aus einem am Ende zur Verschrottung bereitstehenden Gerät können keine Daten ausgelesen werden.

„IT-Sicherheit ist bei uns eine Management-Entscheidung und ganz klar die Basis für unseren zukünftigen Erfolg.
Das Verständnis von IT und OT zusammen ist die Herausforderung, die wir gerne annehmen.“

IT-SICHERHEIT

Sicherheit als Prozess

Wir sehen Penetrationstests als wichtige Schritte der Produktpflege und nicht als den letzten Schritt der Produktentstehung. Für uns beginnt die eigentliche Sicherheitsprüfung, bevor das Produkt formell freigegeben wird. Wir auditieren und validieren die F&E-Entscheidungen, führen regelmäßige Penetrationstests durch, überwachen neu auftretende Bedrohungen und deren Auswirkungen, erstellen systematische Updates und Patches. Für uns ist IT-Sicherheit ein Prozess über die gesamte Lebensdauer unserer Produkte.

Sicherheit als Kultur

IT-Sicherheit ist tief in unserer DNA verwurzelt. Unsere F&E-Mitarbeiter besuchen regelmäßig TÜV-zertifizierte Schulungen und in unserem Unternehmen haben wir ein aktives **Product Security Incident Response Team (PSIRT)** etabliert. Wir streben danach, kontinuierlich „State of the Art" sichere Produkte zu liefern.

Zertifizierung und Prüfung

In regelmäßigen Abständen werden unsere Produkte durch unabhängige IT-Sicherheitsunternehmen sowohl automatisierten als auch manuellen Penetrationstests ausgesetzt.
Den Abschluss eines Penetrationstests bildet stets ein intensiver Dialog zwischen dem Penetrationstester und den Entwicklern.

Industrielle Anwendungen basieren auf verschiedenen Zertifizierungsmöglichkeiten wie dem Standard IEC 62443. In Zusammenarbeit mit TeleTrusT wurde hierfür ein Prüfkatalog entwickelt, welcher für unsere Produkte angewendet wird. Zudem ist der publizierte „Stand der Technik" von TeleTrusT ein wichtiges Werkzeug für unsere Produktentwicklung.

Sicherheitsstrategie im Überblick

Wir engagieren uns aktiv in der Industrial-Security-Arbeitsgruppe bei TeleTrusT. Daraus ist die Evaluierungsmethode für IEC62443-4-2 entwickelt worden.

Das Dokument „Stand der Technik" von TeleTrusT stellt eine der IT-Sicherheits-Richtlinien für uns dar.

Unser Product Security Incident Response Team (PSIRT) überwacht stets sämtliche Entwicklungen und analysiert, wie sich neue Gefahren und neu entdeckte Schwachstellen auf unsere Produkte auswirken können.

Wir unterziehen unsere Produkte und Lösungen regelmäßig Penetrationstests bei zertifizierten, externen IT-Dienstleistern.

IEC 62443-4-1 ZERTIFIZIERT

Wir sind offiziell IEC 62443-4-1 zertifiziert. Diese Zertifizierung unterstreicht unser Engagement für höchste Standards in der Cybersicherheit und den Schutz industrieller Steuerungssysteme. Mit dieser Anerkennung setzen wir ein starkes Zeichen für Qualität, Sicherheit und Vertrauen in unsere Entwicklungsprozesse und Produkte.
Unsere DNA: 100% IT-Security seit mehr als 25 Jahren.


TÜVNORD

CERTIFICATE

Cybersecurity-related processes as per
IEC 62443-4-1 : 2018 (ML 2)

IEC 62443

MB connect line GmbH
Winnettener Straße 6
91550 Dinkelsbühl
Germany

Product development life-cycle requirements related to cyber security of access products intended for use in IACS environments

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

TeleTrusT

TeleTrusT ist der Bundesverband IT-Sicherheit e.V. In diesem Kompetenznetzwerk haben sich in- und ausländische Mitglieder aus Industrie, Verwaltung und Wissenschaft sowie thematisch verwandte Partnerorganisationen zusammengeschlossen. Unsere Produkte tragen das Label „IT-Security Made in Germany“ und „IT-Security Made in EU“, welche von TeleTrusT vergeben werden.

Allianz für Cyber-Sicherheit

Allianz für Cyber-Sicherheit

Die Allianz für Cyber-Sicherheit arbeitet aktiv mit dem Bundesamt für Sicherheit und Informationstechnik (BSI) zusammen. Als aktives Mitglied erhalten wir umgehend Kenntnis zu möglichen Sicherheitsbedrohungen. So können unsere Entwicklungsingenieure diesen Risiken nicht nur reaktiv, sondern vor allem präventiv entgegenwirken. Die Wirksamkeit dieser unmittelbar eingeleiteten Maßnahmen beweisen regelmäßig durchgeführte toolgestützte und manuelle Penetrationstests. Sie sind der Ansporn, jegliche Schwachstelle zu schließen und alles Mögliche für die Einhaltung der IT-Sicherheit zu tun.

VDE CERT

CERT@VDE

CERT@VDE ist eine IT-Sicherheitsplattform des VDE speziell für Unternehmen im Bereich Industrieautomation zur Koordination von IT-Security-Problemen. Sie bietet Herstellern, Integratoren, Anlagenbauern und Betreibern aus dem Bereich Industrieautomation die Möglichkeit zum intensiven und vertrauensvollen Informationsaustausch und konkrete Unterstützung beim Thema Cyber-Security. Häufig ist ein CERT (Computer Emergency Response Team) bereits eine Kundenanforderung und damit Bestandteil der Einkaufskonditionen. Um wettbewerbsfähig zu bleiben, müssen Unternehmen entsprechende Ressourcen bereitstellen.

MB connect line GmbH

Winnettener Straße 6
91550 Dinkelsbühl
DEUTSCHLAND

Tel.: +49 (0) 98 51 / 58 25 29 0
Fax: +49 (0) 98 51 / 58 25 29 99
E-Mail: info@mbconnectline.com

www.mbconnectline.com