Ewon® BY HMS NETWORKS

White Paper:
Beginnen Sie mit dem industriellen Fernzugriff

Einfacher und sicherer Fernzugriff auf Ihre Maschinen

Entdecken Sie alles, was man über den Fernzugriff wissen muss

Überreicht durch:

WACHENDORFF Prozesstechnik GmbH & Co. KG

HMS

Inhaltsverzeichnis

Einführung

Im Industriesektor müssen Ingenieure und Techniker regelmäßig die Fabriken besuchen, um verschiedene Geräte und Maschinen zu warten. Wäre es nicht – sowohl für den Maschinenbauer als auch für den Hersteller – fantastisch, diese Arbeiten aus der Ferne durchführen zu können und die meisten Probleme unabhängig von dem Ort, an dem man sich aufhält, einfach und sicher zu lösen?

Situationen

Wir gehen davon aus, dass Sie in der Industrie und/oder der Automatisierungstechnik tätig sind. Während Sie also mit den Maschinen und ihren SPS, die Sie vermarkten, bauen, warten oder nutzen, sehr vertraut sind, kennen Sie sich vielleicht weniger mit Technologien wie Fernzugriff, Internet, Sicherheit, Cloud Computing und der Nutzung der von Ihren Maschinen bereitgestellten Daten aus.

In diesem White Paper verwendete Symbole

In diesem White Paper verwenden wir spezielle Symbole, um auf wichtige Informationen hinzuweisen. Hier sind sie:


Erinnerung

Dieses Symbol weist auf wichtige Informationen hin, die man sich merken muss.


Technischer Inhalt

Dieses Symbol weist auf technischen Inhalt hin.


Tipp

Diese Symbol weist auf zweckdienliche Informationen hin.


Achtung

Wenn Sie diese Tipps beherzigen, vermeiden Sie potenziell kostspielige Fehler.

Über das White Paper hinaus

Der Einfachheit halber beschränken wir uns hier auf eine Einführung in den industriellen Fernzugriff. Wenn Sie sich eingehender mit dem Thema befassen möchten, laden wir Sie ein, unsere Website zu besuchen: **https://www.ewon.biz**

Was ist der industrielle Fernzugriff und was sind seine Vorteile?

In diesem Kapitel stellen wir uns die nachfolgenden Fragen:

- Warum ist der Fernzugriff notwendiger denn je geworden?
- Welche Möglichkeiten gibt es für den Fernzugriff auf Ihre Maschinen?
- Welche Vorteile hat der Fernzugriff?

Definition des Bedarfs an Fernzugriff

Die Hersteller von Industriemaschinen haben schon immer davon geträumt, sich aus der Ferne mit ihren Maschinen verbinden zu können. Für Erstausrüster (OEM) mit Parks von fernab installierten Maschinen an mehreren Kundenstandorten sowie für Unternehmen, die an mehreren Standorten produzieren, bietet die Möglichkeit, den Betrieb von Maschinen aus der Ferne zu überwachen, einen klaren Wettbewerbsvorteil.


Tipp

Häufige Anwendungsfälle für den Fernzugriff auf Industriemaschinen sind:

- Fehlersuche und Fernprogrammierung von speicherprogrammierbaren Steuerungen (SPS)
- Fernanzeige und-steuerung Ihrer Mensch-Maschine-Schnittstelle (HMI)
- Verbinden mit einer Webcam, um Hilfe zu erhalten
- Unterstützung der Techniker vor Ort bei der Inbetriebnahme

Vorteile des Fernzugriffs

Die Möglichkeit des Fernzugriffs auf das Steuersystem einer Maschine kann bei der Fehlersuche und -behebung helfen und erspart Technikern oder Ingenieuren die Reise zum Einsatzort. Diese Probleme erfordern oft weniger die Reparatur der Maschine als die Anpassung ihrer Programmierung oder Einstellungen. So handelt es sich beispielsweise häufig um Veränderungen bei den Rohstoffen, um Verschleißerscheinungen an der Maschine oder um andere Produktionsparameter, die sich im Laufe der Zeit geändert haben können. Der Fernzugriff ist der erforderliche erste Schritt zur Digitalisierung und Nutzung von Daten.

Tipp

Der Fernzugriff ermöglicht es Ihnen, von einem reaktiven zu einem proaktiven Supportmodell überzugehen, das Ihnen hilft, wettbewerbsfähig zu bleiben. Sobald Sie eine Fernverbindung zu Ihrer Maschine (oder Ihrem Maschinenpark) hergestellt haben, können Sie nicht nur Fehler beheben und schnell eingreifen, sondern auch die Daten für andere Zwecke analysieren. Zum Beispiel:

- Verbesserung der Reaktionsfähigkeit
- Verringerung der Auswirkungen von Notfällen
- Optimierung der Arbeitsbelastung der Ingenieure
- Maximierung der Verfügbarkeit und Produktivität der Maschinen
- Senkung der Reisekosten
- Minimierung der Umweltauswirkungen
- Steigerung Ihrer Nachhaltigkeit
- Minimierung der Stillstandzeiten Ihrer Maschinen
- Maximierung der OEE („Overall Equipment Effectiveness“ bzw. Gesamtanlageneffektivität)
- Maximierung der Sicherheit

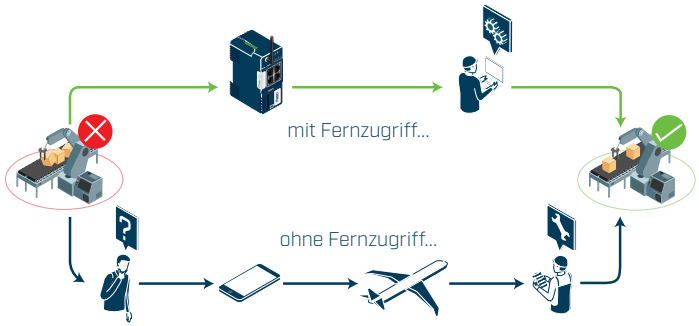
Eine schnelle Problemlösung bedeutet weniger Ausfallzeiten und eine schnellere Rückkehr zur Produktion für den Endkunden. In Fällen, in denen ein physisches Eingreifen vor Ort noch erforderlich ist, kann der Fernzugriff dazu beitragen, dass die reisende Person über die richtigen Kenntnisse, Ersatzteile und Werkzeuge verfügt, was die Chancen erhöht, das Problem bei einem einzigen Besuch zu beheben. All dies trägt zu einem besseren Kundenerlebnis bei und minimiert die Ausfallzeiten der Maschinen.

Der Druck auf die Industrie, Fernzugriffsstrategien einzuführen, hat sich in den letzten Jahren noch verstärkt. Dazu hat beispielsweise auch das weltweite Aufkommen der Telearbeit beigetragen. Der ultimative Beschleuniger waren die Covid-19-Krise und die Angst der Industrie, Außenstehende in ihre Einrichtungen zu lassen und dabei das Risiko einer Infektion des Personals einzugehen.

Es liegt auf der Hand, dass auch ökologische, wirtschaftliche und gesellschaftliche Aspekte eine wichtige Rolle spielen. Nachhaltigkeit und Umweltverträglichkeit werden bei unseren Lebensweisen immer wichtiger. In dieser Hinsicht ist es offensichtlich, dass der industrielle Fernzugriff ein wirksamer und sicherer Weg ist, um dieses Ziel zu erreichen und gleichzeitig die Kosten zu minimieren sowie die Effizienz (OEE) der Anlagen zu erhöhen.

Auch die Maschinenbauer erkennen die Chance, die der Fernzugriff bietet, um ihren Kunden neue umsatzfördernde, proaktive und präventive Dienstleistungen anzubieten. Wir sprechen hier von der Nutzung von Daten, die auf einfache Weise eine vorausschauende Wartung ermöglichen.

Letztlich ermöglicht der Fernzugriff mehr Effizienz für alle. Maschinenbauer können sich Wettbewerbsvorteile verschaffen, wie in Abbildung 1-1 dargestellt, um mehr Kunden zu bedienen und neue Märkte zu erschließen, während Maschinenanwender ihre OEE steigern können.



- Reduzieren Sie kostspielige Besuche vor Ort
- Live- und Online-Support für Ihre Kunden
- Regelmäßiger Kontakt mit Ihren Anlagen
- Geringere Umweltbelastung
- Reduzierte Maschinenstillstandzeiten
- Maximierte OEE
- Erhöhte Sicherheit
- Höhere Produktivität

Abbildung 1-1: Erhalten Sie mehr Effizienz und Wettbewerbsvorteile durch Fernzugriff

Geschichte des Fernzugriffs

Anfangs bestand der Fernzugriff auf die Maschinen aus einer „Punkt-zu-Punkt“-Verwaltung über eine Terminalkonsole, die über ein analoges Festnetztelefon und ein Modem angeschlossen war. Diese Systeme waren langsam, häufig schwierig zu installieren und teuer in Betrieb und Wartung.

Der Fernzugriff über eine Routerverbindung ist jedoch dank der Verfügbarkeit von Hochgeschwindigkeits-Mobilfunknetzen auch heute noch beliebt. Der Hauptvorteil dieser Methode des Fernzugriffs besteht darin, dass der Zugriff auf die Daten der Maschinensteuerung (SPS) möglich ist, wobei die Nutzung des Computernetzes des Kunden vermieden wird. Drahtlose Router, die über die Datennetze von Mobilfunkanbietern kommunizieren, sind bei vielen Anbietern programmierbarer Steuerungen erhältlich.

Bei diesem Ansatz ist weder eine Telefonleitung noch ein Anschluss an das Computernetz des Unternehmens erforderlich, obwohl die Verfügbarkeit von Funksignalen in Produktionsbereichen manchmal problematisch sein kann.

Das bedeutet ständigen Netzzugang und Nutzungsgebühren, die sich schnell summieren können.

Nutzung des Internets

Eine bessere Methode, um aus der Ferne auf Maschinen zuzugreifen, besteht darin, die Vorteile der Internettechnologie und des Cloud Computing zu nutzen. Die größte Herausforderung besteht darin, die Verbindung der Maschine mit dem Unternehmensnetz des Endbenutzers und damit mit dem Internet *sicher* zu verwalten. Die IT-Abteilungen der meisten Unternehmen zögern aus offensichtlichen Sicherheitsgründen, Nicht-Mitarbeitern Zugang zum Firmennetz zu gewähren.

On-Demand-Fernzugriff

Maschinenbauer benötigen nicht unbedingt durchgehende Verbindungen. Der Fernzugriff für Fehlersuche, Wartung oder Maschinenservice kann über eine On-Demand-Verbindung erfolgen, was die Kosten minimiert und die Sicherheit erhöht.

Was sind die Vorteile des On-Demand-Zugriffs? Erstens möchte der Endbenutzer möglicherweise den ständigen Fernzugriff auf die Maschine verhindern. Das Trennen der Maschine vom lokalen Netzwerk (LAN) ist für die Sicherheit nicht unbedingt erforderlich, aber es verschafft dem Endbenutzer die physische Kontrolle darüber, wann und wie lange die Maschine zugänglich ist. In diesem Fall ist die Maschine in der Regel nicht mit dem LAN verbunden. Die Maschine wird nur bei Bedarf oder auf Wunsch des Herstellers angeschlossen.

Beruht die Fernverbindung auf einer volumenbasierten Preisgestaltung wie z. B. bei der Mobilfunktechnologie, kann es außerdem wünschenswert sein, eine Verbindung herzustellen und nur bei Bedarf zu bezahlen ;-).

Ausgehende Verbindungen

Virtuelle private Netzwerke (VPN) sind aus technischer Sicht eine hervorragende Lösung.

Es kann jedoch eine komplexe Aufgabe sein, einen angemessenen Zugang zum Netz zu ermöglichen und gleichzeitig die Sicherheit zu gewährleisten. Jeder Hersteller speicherprogrammierbarer Steuerungen (SPS) verwendet in der Regel einen anderen Satz von Netzwerkanschlüssen und die Festlegung eines klaren Pfads durch die Firewalls eines Kunden erfordert eine sorgfältige Konfiguration. Darüber hinaus wird diese von den IT-Abteilungen regelmäßig abgelehnt, da sie keine Sicherheitslücken schaffen wollen.

Wenn Sie eine ausgehende Verbindung im lokalen Netz der Fabrik nutzen, können Sie viele Firewall-Probleme von Anfang an lösen. Denn wenn keine eingehende Verbindung hergestellt wird, müssen in der Firewall des Unternehmens keine Ports für eingehende Verbindungen freigegeben werden, und es sind keine IT-technischen Änderungen erforderlich, um die Kommunikation herzustellen; und das alles bei vollständiger Sicherheit. Diese Konfiguration ermöglicht dem Techniker den Zugriff auf autorisierte Maschinen, verhindert jedoch den Zugriff auf das Fabriknetz (LAN).

Auf Software basierende Lösungen

Über das Internet kann ein lokaler Kontroll-PC mit Hilfe der Virtual-Network-Computing(VNC)-Technologie oder einer anderen PC-basierten Fernzugriffssoftware ferngesteuert werden. In diesem Szenario repliziert die Software die Kontrolle über den über Fernzugriff zugänglichen Computer der Benutzerschnittstelle und gibt sie an diesen ab. Diese Art von Lösung kann zwar für die Fernverbindung zu einem PC akzeptabel sein, bietet dem Benutzer aber in der Regel Zugriff auf das gesamte Netzwerk, was unter Sicherheitsaspekten nicht akzeptabel ist.
Dieser Ansatz setzt voraus, dass in der Remote-Maschine ein Industrie-PC vorhanden ist, auf dem die Anwendung ausgeführt werden kann. Diese Hardware und Software sind mit zusätzlichen Kosten verbunden, sodass die Gesamtkosten höher sind als bei einer spezifischen Lösung.

Auf einem sicheren Industrierouter basierende VPN-Lösungen

Die beste Lösung ist die Verwendung einer On-Demand-VPN-Verbindung mit einem Industrierouter und einer sicheren cloudbasierten Infrastruktur. Eine Verbindung vom Typ VPN SSL (Secure Sockets Layer) stellt die IT-Abteilung eines Kunden im Allgemeinen vor wenig Probleme.

Diese Methode ist aus einer Sicherheitsperspektive sogar noch interessanter, da sie automatisch eine logische Netzwerktrennung zwischen der Maschine und dem LAN der Fabrik herstellt. Maschinenbauer können ihre Maschinenparks über eine einfache und sichere Schnittstelle verwalten. Endbenutzer können die Plattform verwenden, um Fernzugriffsrechte zu verwalten.

Da dies die beste Lösung ist, wird sie in den nachfolgenden Kapiteln ausführlich beschrieben.

Verständnis und Verwendung der Fernzugriffslösung Ewon

Dies werden Sie in diesem Kapitel erfahren:

- Einführung und Funktionsweise des Ewon Cosy und der Talk2M Industrial Cloud
- Wie verbindet man sich mit der Talk2M Industrial Cloud
- Wie verwendet man eCatcher für die Verbindung mit der Maschine über Talk2M
- Wie kommuniziert man über eine VPN-Verbindung
- Andere Ewon-Lösungen

Einführung in den Industrierouter Ewon Cosy

Der Ewon Cosy ist ein sicherer Industrierouter, der eine sichere Fernverbindung zu einer Maschine oder Anlage ermöglicht. Mit dem Ewon Cosy können Maschinenbauer und Hersteller Fehler an ihren Maschinen beheben, SPS-Fehler korrigieren, eine Mensch-Maschine-Schnittstelle (HMI) oder eine IP-Kamera aus der Ferne bedienen, ohne dafür reisen zu müssen. Der Ewon Cosy ist mit der überwiegenden Mehrheit der SPS und auch mit älteren Geräten („legacy/brown field equipment“) kompatibel.

Dieser Ansatz ermöglicht:

- die Kosten erheblich zu senken
- die Effizienz der Maschinen zu verbessern
- den CO^2-Fußabdruck zu minimieren
- eine einfache Nachrüstung älterer Geräte durchzuführen

Wie funktioniert der Ewon Cosy?

Der Ewon Cosy stellt jederzeit und überall eine sichere VPN-Verbindung zwischen Ihnen und Ihrer Maschine her. Die Verbindung wird über Talk2M, eine hochsichere industrielle Cloud, hergestellt. Der Ewon Cosy lässt sich über Ethernet oder drahtlos (4G oder WLAN) verbinden, um in jeder Situation einen einfachen Fernzugriff zu ermöglichen.

Der Ewon Cosy in Verbindung mit Talk2M macht es den Benutzern leicht, sich über das Internet mit ihren Maschinen zu verbinden, wie dies in Abbildung 4-1 dargestellt ist. Dies ist eine sehr einfach zu bedienende Lösung, die keine speziellen Computerkenntnisse erfordert.

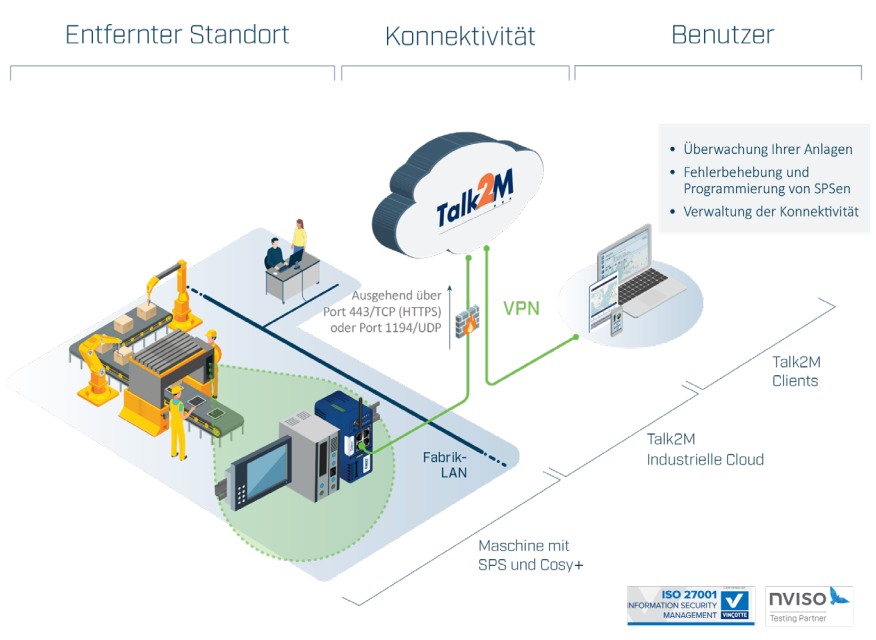


Abbildung 4-1: Talk2M ist eine industrielle Cloud, die es Benutzern ermöglicht, sich über das Internet mit ihren Maschinen zu verbinden.

Ewon bietet Anwendern drei Lösungen, um sich über Talk2M mit ihren Maschinen zu verbinden:

- eCatcher: eine Talk2M-Client-Software
- eCatcher mobile: eine Smartphone-Anwendung
- M2Web: ein spezielles Webportal

Tipp

Sie können auch einen Webbrowser (z. B. Google Chrome, Microsoft Internet Explorer/Edge oder Mozilla Firefox etc.) verwenden, ohne die eCatcher-Anwendung zu installieren, um eine Verbindung zu Ihren Maschinen herzustellen (dieser Dienst wird M2Web genannt).

Verbindung Ihrer Maschine mit dem Internet über den Ewon Cosy

Um Ihre Maschinen mit dem Internet zu verbinden, gibt es mehrere Möglichkeiten:

- **Kabelgebundenes Netz (Ethernet):** Die meisten Industriestandorte sind damit ausgestattet, um sich mit dem Internet zu verbinden. Dies ist häufig die bevorzugte Methode. Ein Ethernet-LAN-Anschluss ist in der Regel kostenlos und bietet einen zuverlässigen Hochgeschwindigkeitszugang. In einigen Fällen unterliegen lokale Netzwerke komplexen Sicherheitsrichtlinien, welche die Verbindung Ihrer Maschinen einschränken können. In diesen Fällen kann eine drahtlose Verbindung eine Alternative sein.

- **Drahtloses Netzwerk (WLAN)**: WLAN-Netzwerke werden in Fabriken immer häufiger eingesetzt. Wie LAN-Verbindungen ist auch der WLAN-Zugang in der Regel kostenlos und bietet Hochgeschwindigkeitsverbindungen. Viele Fabriken bieten „Gast"-WLAN-Netzwerke an, die in logischer Hinsicht vom LAN des Unternehmens getrennt sind. Diese Lösung ermöglicht es Maschinenbauern und Benutzern, auf das Internet zuzugreifen, ohne dass Änderungen an der Firewall-Konfiguration erforderlich sind.

- **Mobilfunknetz (4G)**: Wenn keine LAN- oder WLAN-Verbindung verfügbar ist, sind Mobilfunktechnologien eine gute Alternative. Der Mobilfunkdienst ist im Allgemeinen weltweit mit unterschiedlichen Geschwindigkeiten verfügbar, aber die Signalabdeckung kann in einigen Gebieten begrenzt oder unzuverlässig sein. Darüber hinaus können die Kosten für die Datennutzung in einem Mobilfunknetz hoch sein und die Mobilfunktechnologie ist nicht überall gleich, sodass möglicherweise unterschiedliche SIM-Module in den Routern der Maschine installiert werden müssen. Aus diesen Gründen werden im Allgemeinen LAN- oder WLAN-Verbindungen bevorzugt, wenn sie verfügbar sind.

Verbindung der Maschine mit Talk2M

Sobald Sie mit dem Internet verbunden sind, wird Ewon in drei Phasen versuchen, eine Verbindung zu Talk2M herzustellen:

1. Der Ewon verbindet sich mit einem zentralen Zugangsserver (AS) und authentifiziert sich über eine HTTPS-Sitzung (Hyper Text Transfer Protocol Secure).
2. Der Ewon fragt die IP-Adresse des zu verwendenden VPN-Servers (die Adressen der VPN-Server können sich von einer Verbindung zur anderen ändern) über eine HTTPS-Verbindung ab.
3. Der Ewon baut einen VPN-Tunnel mit dem VPN-Server auf.

Diese Phasen sind in Abbildung 4-2 dargestellt.

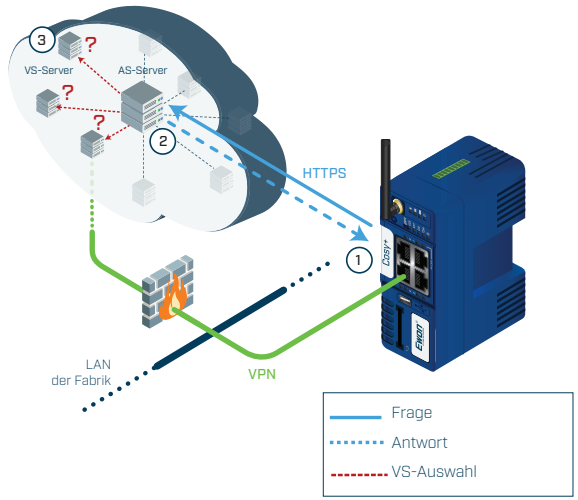


Abbildung 4-2: Verbindung des Ewon mit Talk2M in drei Phasen.

Verbindung des Benutzers mit Talk2M

Wenn der Benutzer die eCatcher-Software startet, muss er sich zunächst mit den nachfolgenden Informationen authentifizieren:

- **Name des Kontos:** Mit eCatcher kann ein Talk2M-Konto angelegt werden. Es kann eine unbegrenzte Anzahl an Konten angelegt werden. Jedes Konto enthält alle Benutzer, die sich an den in diesem Konto registrierten Ewon-Geräten anmelden dürfen.
- **Name des Benutzers:** In einem Konto kann eine unbegrenzte Anzahl an Benutzern registriert werden. Benutzernamen in einem Konto müssen eindeutig sein.
- **Passwort**: Jeder Benutzer hat sein eigenes Passwort.

Achtung

Nach der Authentifizierung können Sie auf die Liste der Ewon-Geräte zugreifen, die in einem Talk2M-Konto registriert sind und für die Sie Zugriffsrechte haben. Die Liste beinhaltet die nachfolgenden Informationen:

- Den Namen und den Zustand eines jeden Ewon
- Eine Kurzbeschreibung des Ewon und der angeschlossenen Maschine
- Alle derzeit mit dem Ewon verbundenen Benutzer
- Alle verbundenen Parks (Gruppen von Ewon-Geräten)
- Den Steuerungstyp (SPS)
- Die Art der Remote-Verbindung (wie LAN oder Mobilfunk)
- Die IP-Adresse der anderen im Netz des Ewon angegebenen Geräte

Wenn Sie auf einen aufgelisteten Ewon klicken und sein Verbindungsstatus als „Online“ angezeigt wird (was bedeutet, dass eine VPN-Verbindung besteht), baut eCatcher einen VPN-Tunnel zu dem zugewiesenen Ewon auf.

Sie können auch verschiedene andere Aktionen in eCatcher durchführen, wie z. B.:

- Registrieren eines neuen Ewon im aktuellen Konto
- Ändern und Löschen von Informationen über Ewon-Geräte
- Hinzufügen, Bearbeiten oder Löschen von Benutzerinformationen oder Gruppen im aktuellen Konto (eine Gruppe ist eine Gruppe von Benutzern)
- Hinzufügen, Ändern oder Löschen von Parks im aktuellen Konto (ein Park ist eine Gruppe von Ewon-Geräten)
- Ändern der Informationen des Kontos

Verwendung der VPN-Verbindung

Wenn eine VPN-Verbindung aufgebaut wird, werden zwei „Tunnel“ erstellt: einer zwischen dem Ewon und dem VPN-Server, der andere zwischen eCatcher und dem VPN-Server. Dies ist in Abbildung 4-3 dargestellt. Jedem Tunnel wird automatisch eine eindeutige VPN-IP-Adresse zugewiesen. Obwohl die VPN-Adressen von Seiten des Ewon und von Seiten des eCatcher zugänglich sind, sind sie von Seiten des VPN-Servers nicht zugänglich.

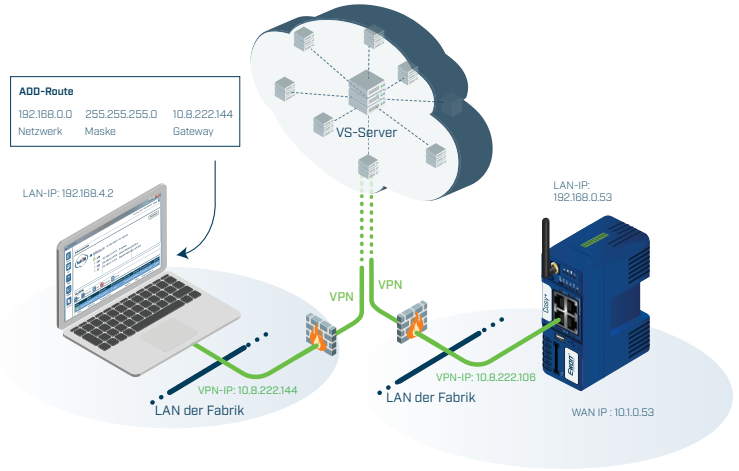


Abbildung 4-3: Die eCatcher-Software fügt automatisch eine Route zur LAN-IP-Adresse des Ziel-Ewon hinzu.

Technischer Inhalt

Um die Maschinenseite des Ewon zu erreichen, muss Ihr Computer/Tablet/Smartphone wissen, dass der gesamte Datenverkehr, der eine Ziel-IP-Adresse innerhalb des IP-Adressbereichs des LAN des Ewon enthält, über seine virtuelle Schnittstelle weitergeleitet werden muss. Um dies zu aktivieren, fügt eCatcher automatisch eine Route hinzu, wenn eine VPN-Verbindung geöffnet wird, und entfernt die Route automatisch, wenn die VPN-Verbindung geschlossen wird, wie dies in Abbildung 4-3 erläutert wird. Die eCatcher-Software kennt die LAN-IP-Adresse des Ewon, da sie bei der Registrierung eines jeden Ewon für ein Talk2M-Konto angegeben wird. Wenn Sie eine Verbindung zu einem anderen Ewon herstellen möchten, löscht eCatcher automatisch die vorherige Route und fügt eine neue Route mit dem entsprechenden Zieladressbereich hinzu.

Auf der Maschinenseite wird der Verkehr, der durch den VPN-Tunnel läuft, automatisch an die LAN-Seite (Maschinenseite) des Ewon weitergeleitet. Damit eine Maschine auf der LAN-Seite mit dem Benutzer kommunizieren kann, haben Sie zwei Optionen:

- Eine Funktion aus dem Bereich der Network Address Translation (NAT) (auch Plug'n Route genannt) kann die LAN-IP-Adresse des Ewon durch die IP-Adresse des Benutzers ersetzen (dies ist die Standardkonfiguration im Ewon).
- Einzelne Maschinen auf der LAN-Seite des Ewon können auf manuelle Weise so konfiguriert werden, dass sie die LAN-IP-Adresse des Ewon als Standardgateway verwenden.

Sich mit den anderen Ewon-Lösungen vertraut machen

Der Fernzugriff über Ewon Cosy und Talk2M ist ein erster Schritt auf dem Weg zur Digitalisierung. Um noch einen Schritt weiter zu gehen, bietet Ewon mit Ewon Flexy und Talk2M Lösungen zur Überwachung und Datenerfassung an.

Der Ewon Flexy ist ein vielseitiges IIoT-Gateway und ein fortschrittlicher Industrierouter. Neben dem Fernzugriff ermöglicht er Ihnen die Überwachung und Erfassung von Leistungskennzahlen (KPIs), die für die Maximierung der Effizienz (OEE) unerlässlich sind. Außerdem können Sie diese Daten von der Maschine in die Cloud zurückspeisen und auf diese Weise analysieren, um eine vorausschauende Wartung zu organisieren.

Die Funktionen des Ewon Flexy beinhalten:

- Sicherer VPN-Fernzugriff: Der Ewon Flexy umfasst auch ein sicheres VPN, das mit Talk2M kompatibel ist und einen hochsicheren Fernzugriff für die Wartung, Überwachung und Datenerfassung bietet. Er ermöglicht die Fernverbindung zu SPS, IP-Kamera, HMI etc.

- Erweiterungskarten: Zusätzlich zur Grundfunktionalität kann der Ewon Flexy durch das Hinzufügen von Erweiterungskarten (Ethernet, WLAN, 4G, USB, seriell...) an Ihre spezifischen Konnektivitätsanforderungen angepasst werden.

- Datenerfassung: Die lokale Datenerfassung erfolgt durch den Ewon Flexy über die serielle oder die Ethernet-Schnittstelle. Der Erfassungsprozess basiert auf einer Datenbank mit Variablen, in der die einzelnen Variablen einem Eingangs-/Ausgangsserver (I/O-Server) zugeordnet werden.

- Alarmmanagement und Benachrichtigungen: Der Ewon Flexy ermöglicht die Auslösung und Nachverfolgung von Alarmen und Benachrichtigungen. Für jede Variable können Alarmschwellen und Parameter festgelegt werden. Der gesamte Alarmzyklus wird aufgezeichnet und steht für die Überwachung und Analyse zur Verfügung. Die Alarmbenachrichtigung kann über E-Mail, SMS, SNMP-Traps (Simple Network Management Protocol) und/oder FTP (File Transfer Protocol) erfolgen.

- Aufzeichnung und Abruf von Daten: Für jede Variable kann eine kontinuierliche Datenaufzeichnung und-pufferung durchgeführt werden. Jede Variable kann in festgelegten Intervallen oder bei Änderung der Auslöser aufgezeichnet werden. Das Ewon Flexy speichert die Datenwerte und Zeitstempel in seiner internen Datenbank (bis zu einer Million zeitgestempelter Punkte), um statistische Analysen und spätere Überprüfungen durchzuführen (historische Aufzeichnung) oder um aktuelle Trends zu analysieren (Echtzeitaufzeichnung).

- Web-HMI-Server (Mensch-Maschine-Schnittstelle): Der Ewon Flexy verfügt über einen integrierten Webserver zur Konfiguration und Datenvisualisierung, der in jedem Standard-Webbrowser angezeigt werden kann.**- Talk2M SPS:** Nutzen Sie die SPS für die Integration von Software und Cloud-Lösungen von Drittanbietern (z. B. Ewon-IIoT-Partner: AmazonWeb Services, Microsoft Azure, Siemens MindSphere, IBMBluemix etc.) in das Unternehmen.

Der Ewon Flexy wird für die Verbindung in den Bereichen des Cleantech, der Photovoltaik, des Gebäudemanagements, der intelligenten Zähler, des Wasser- und Abwassermanagements, der Energieüberwachung, der Bewässerungssysteme etc. verwendet.

Abbildung 4-4 erläutert diese Anwendungsbereiche.

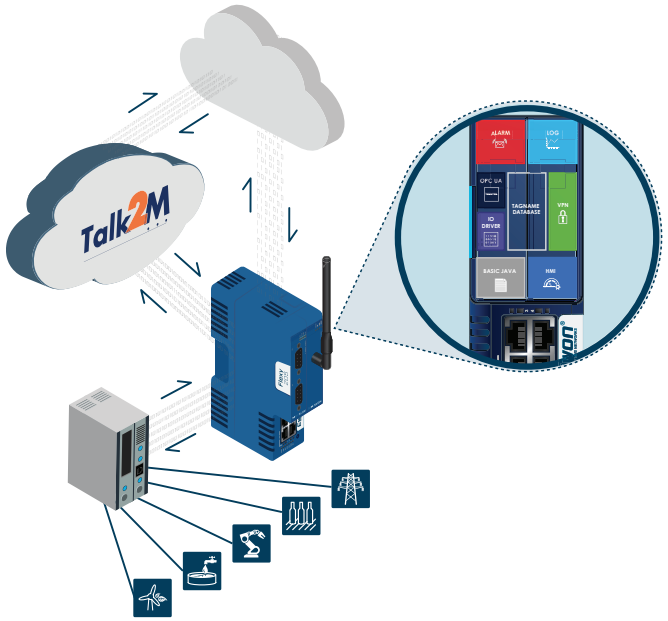


Abbildung 4-4: Der Ewon Flexy verbindet entfernte Feldgeräte mit Hilfe verschiedener Kommunikationsprotokolle.

Tipp

Wenn Sie mehr über den Ewon Flexy erfahren möchten, besuchen Sie die Website www.ewon.biz/flexy

Einen sicheren und zuverlässigen Fernzugriff gewährleisten

In diesem Kapitel können Sie insbesondere:

- Tipps für mehr Sicherheit entdecken
- Mehr über Bedrohungen der Cybersicherheit erfahren
- Mehr über Firewalls und VPN erfahren
- Sich für eine Web-gehostete Architektur entscheiden
- Einen „mehrschichtigen“ Sicherheitsansatz einführen
- Den Ewon Cosy und seine Funktionen entdecken

Tipps für mehr Sicherheit

Sicherheit ist wie eine Kette, die jederzeit infolge ihres schwächsten Glieds reißen kann. Es ist daher wichtig, den besten Kompromiss zwischen Sicherheit und Benutzerfreundlichkeit zu finden. Zu diesem Zweck finden Sie hier einige Tipps, die vor der Implementierung einer Lösung des industriellen Fernzugriffs leicht zu überprüfen sind:

1. Die Firewall der Fabrik darf nicht verändert werden, um ihre Integrität zu gewährleisten. Wenn Sie eine ausgehende Verbindung verwenden, minimieren Sie das Risiko, eine Lücke in Ihren Netzen zu schaffen. Mit einem Schlüsselschalter oder einer HMI-Taste hingegen behält der Endbenutzer die physische Kontrolle über den Fernzugriff. „Man muss nur den Schlüssel umdrehen“.
2. Seien Sie in der Lage, Ihre Verbindungen zu auditieren! Der Administrator muss feststellen können, wer, wann und worauf Zugriff hatte
3. Multi-Faktor-Authentifizierung: Zusätzlich zu den traditionellen Anmeldedaten (Benutzer-ID/ Passwort) ist es sinnvoll, eine zweite Sicherheitsebene durch Multi-Faktor-Authentifizierung zu verwenden. Zum Beispiel mit Hilfe eines Identifikationsschlüssels, der per SMS verschickt wird und bei jeder Verbindung anders ist.
4. Zertifizierung: Es ist wichtig, dass die von Ihnen verwendeten Lösungen auf professionelle Weise auditiert und zertifiziert werden. Die Norm ISO 27001 ist in dieser Hinsicht natürlich die Referenz. Es ist jedoch wichtig, den Kontext dieser Zertifizierung zu kennen und zu wissen, was sie tatsächlich bescheinigt. Die Zertifizierung kann sich beispielsweise auf die Erstellung der Gebrauchsanweisung beschränken, was uns nicht viel nützt. Wir empfehlen

Ihnen sicherzustellen, dass die Cloud, die Verbindungen und der Industrierouter alle der betreffenden Norm entsprechen.

5. Audit und Penetrationstests: Stellen Sie sicher, dass Ihr Anbieter von einem seriösen externen Unternehmen, das seine Tests regelmäßig aktualisiert, ordnungsgemäß auditiert wird. Ziel ist es natürlich, auf dem neuesten Stand zu bleiben und zu vermeiden, dass jedes Jahr derselbe Test und dasselbe Verfahren wiederholt bzw. ein zu restriktiver Teil auditiert werden.
6. Seien wir nicht naiv: „Es ist nicht alles Gold, was glänzt" – wählen Sie also einen seriösen, etablierten und spezialisierten Partner.

Die Bedrohungen der Cybersicherheit

Große Sicherheitsverletzungen, bei denen in der Regel Millionen von Zugangsdaten offengelegt werden, sind häufig Gegenstand von Medienberichten. Es gibt jedoch eine weitaus größere und potenziell verheerendere Bedrohung: Cyberangriffe auf kritische Infrastrukturen und Maschinen. Dazu gehören insbesondere Versorgungseinrichtungen, Notfallsysteme, Umgebungskontrollen in Gebäuden und Industrieanlagen.

Ein Beispiel: Im Mai 2021 war die Colonial Pipeline, die 45 % aller an der Ostküste der Vereinigten Staaten verbrauchten Kraftstoffe liefert, das Ziel eines Cyberangriffs. Der Ransomware-Angriff zwang das Unternehmen, seine 8.000 Meilen langen Pipelines für mehrere Tage abzuschalten.

Gruppen von Hackern, die in der Regel finanziell, aber auch politisch oder sozial motiviert sind, können versuchen, Lösegeld zu erpressen oder mit dem Internet verbundene Industrieanlagen zu beschädigen. Einige Staaten sind auch an Cyberangriffen beteiligt, um verschiedene strategische Ziele zu erreichen.

So wurde beispielsweise der Computervirus Stuxnet im Jahr 2010 angeblich von einem oder mehreren Staaten entwickelt, um das iranische Atomprogramm anzugreifen. Der Virus infizierte anfällige SPS und die Step7-Software von Siemens in der iranischen Nuklearanlage in Natanz und bewirkte, dass sich die Zentrifugen mit unterschiedlichen Geschwindigkeiten drehten, um übermäßige Vibrationen zu erzeugen und sie so zu zerstören.

In jüngster Zeit soll die Einschleusung von bösartigen Codes in die Sicherheitssoftware des Unternehmens Solarwinds mehr als 18.000 Kunden infiziert und die Exfiltration von Daten ermöglicht haben. Herr Mandia, der CEO des Unternehmens, sagte, dass dieser Angriff nur „von einem Land mit erstklassigen Offensivfähigkeiten" durchgeführt worden sein könne. *Sicherheit sollte daher für alle Maschinenbauer, Erstausrüster (OEM) und Systemintegratoren, die eine Fernverbindung zu den Maschinen ihrer Kunden herstellen wollen, an erster Stelle stehen.*

Einem aktuellen Bericht von Palo Alto Networks zufolge sind 98 % des IoT-Datenverkehrs unverschlüsselt und fast 60 % der Geräte anfällig für (mittelschwere bis schwere) Cyberangriffe. Mehr denn je ist es wichtig, Fabriken vor bösartigen Angriffen zu schützen, die immer komplexer und raffinierter werden.

Firewalls und virtuelle private Netzwerke (VPN) verstehen

Firewalls kontrollieren den Datenverkehr zwischen Netzwerken, z. B. einem lokalen Netzwerk (LAN) und dem Internet. Eine Firewall wird in der Regel am Rande des Netzwerkes installiert, das sie schützt, und kann aus einem Hardware-Gerät, einer Software oder einer Kombination aus Hardware und Software bestehen.

Sie können sich einen Router als Eingang zu einer mittelalterlichen Burg und die Firewall als Zugbrücke am Eingang, die den Zugang zur Burg kontrolliert, vorstellen.

Obwohl es viele fortschrittliche Konzepte und Technologien gibt, besteht die grundlegende Funktion der Firewall darin, den gesamten eingehenden Datenverkehr aus einem nicht vertrauenswürdigen Netz (z. B. dem Internet) auf Grundlage einer Reihe von vorkonfigurierten Regeln zu filtern. *Standardmäßig wird der gesamte aus dem vertrauenswürdigen Netz ausgehende Datenverkehr zugelassen* (z. B. vom LAN ins Internet). Eingehender Verkehr, der als Antwort auf eine aktive ausgehende Verbindung gesendet wird, ist ebenfalls zulässig. Eingehender Datenverkehr von der Ewon-Webseite www.ewon.biz wird als Reaktion auf eine Webbrowser-Anfrage automatisch durch die Firewall zugelassen.

Eingehender Verkehr, der sich nicht ausdrücklich einer ausgehenden Anfrage zuordnen lässt, wird jedoch standardmäßig blockiert. Um bestimmten, aus dem Internet eingehenden Verkehr zuzulassen, müssen Firewall-Regeln konfiguriert werden, um festzulegen, welche Art von Verkehr von welcher Quelle zu welchem Zielort durchgelassen werden soll.

Eine Firewall schützt zwar Systeme (einschließlich Maschinen) und Daten im LAN vor unbefugtem Zugriff, aber sie schützt nicht die Vertraulichkeit und Integrität des Internetverkehrs, der über das LAN gesendet und empfangen wird. *Das ist die Aufgabe eines virtuellen privaten Netzwerks bzw. VPN.* Die VPN-Technologie schafft einen Tunnel zwischen zwei Maschinen oder zwei Netzen. Zwischen den beiden Enden wird ein Verschlüsselungscode generiert, der dazu verwendet wird, einen verschlüsselten „Wrapper" zu erstellen, welcher die Daten an der Quelle schützt. Am anderen Ende des Kommunikationstunnels „entpackt" das Zielgateway die Daten und entschlüsselt sie.

Eine Web-gehostete Architektur nutzen

Sie können auch selbst eine VPN-Lösung auf Ihrem PC installieren. Dazu müssen Sie die Software installieren und konfigurieren, damit die Kommunikation hergestellt und gesichert ist. Dies liegt nicht unbedingt auf der Hand und eine falsche Konfiguration der Sicherheitseinstellungen würde den gewünschten Zweck verfehlen. Wir sind der Meinung, dass sich die Maschinenbauer nur auf die Wartung ihrer Maschinen konzentrieren sollten, ohne sich um die IT kümmern zu müssen. Aus diesem Grund haben wir Talk2M entwickelt. Dank unserer gehosteten Lösung ist keine komplizierte Konfiguration durch die Benutzer erforderlich. Die Konfiguration des VPN-Servers wird vom PC in die Cloud verlagert und die technischen und sicherheitstechnischen Konfigurationen werden von unseren Fachleuten eingerichtet. Die Benutzer können sich problemlos mit ihren Maschinen verbinden und sich auf ihre Aufgaben konzentrieren, wie dies in Abbildung 3-1 erläutert wird.

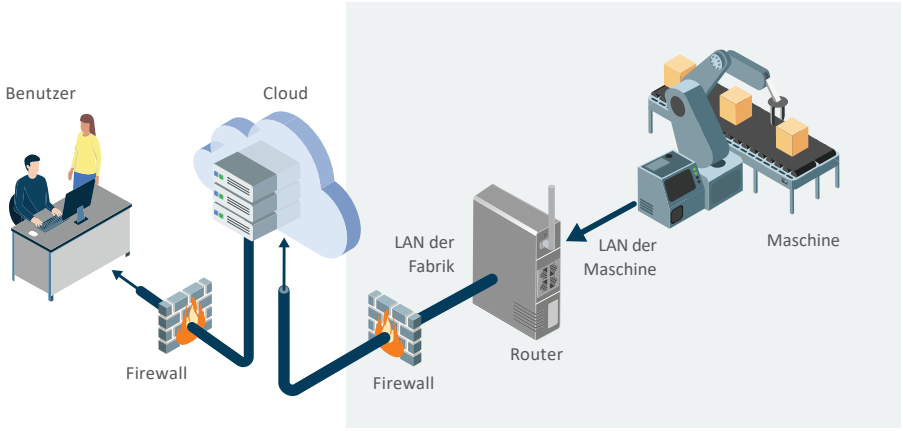


Abbildung 3-1: Verwendung eines VPN-Servers für eine sichere Verbindung zu Ihren entfernten Maschinen.

Wenn der VPN-Server jedoch nicht auf einem einzigen Gerät (PC) installiert ist, sondern von einer unabhängigen Organisation in einem Cloud-Service (SaaS) gehostet wird, kann er von mehreren Maschinenbauern gemeinsam genutzt werden, die jeweils über ein privates Konto verfügen und ihre Kunden und Maschinen individuell konfigurieren können.*Eine cloudbasierte Architektur bietet grundsätzlich eine bessere Skalierbarkeit als eine rein hardwarebasierte Architektur,* die auf Hardware-Gateways oder internen Softwareanwendungen basiert.

Eine cloudbasierte Architektur ermöglicht einen Lastenausgleich, indem die erforderlichen VPN-Verbindungen und-Tunnel auf mehrere Server verteilt werden. Außerdem bietet sie Redundanz und gewährleistet so die Ausfallsicherheit der Fernzugriffsdienste im Falle einer Betriebsunterbrechung oder einer Katastrophe.

Den „mehrschichtigen“ Sicherheitsansatz von Ewon entdecken

Eine der zentralen Herausforderungen bei Remote-Verbindungen zu industriellen Steuerungssystemen besteht darin, die richtige Balance zwischen den Anforderungen eines Ingenieurs oder Automatisierungsspezialisten und den Anforderungen der IT-Abteilung, die für die Netzwerksicherheit, Datenintegrität und Zuverlässigkeit verantwortlich ist, zu finden. Eine Lösung zu finden, die von beiden Seiten problemlos akzeptiert wird, ist seit vielen Jahren eine Herausforderung sowie eine Quelle der Frustration und Ineffizienz für alle Beteiligten. Die Aufrechterhaltung der Netzwerksicherheit ist entscheidend für die Akzeptanz durch die IT-Abteilung, aber die Benutzer wollen keine Lösungen, die komplex oder schwierig zu implementieren sind bzw. die Produktivität beeinträchtigen. *Durch die Konzentration auf Sicherheit und Benutzerfreundlichkeit hat Ewon eine Fernzugriffslösung geschaffen, die sowohl für Endbenutzer als auch für IT-Manager geeignet ist.*
Sicherheit und Zuverlässigkeit sind zwei Schlüsselaspekte der Ewon-Lösungen. Sie basieren auf einer „mehrschichtigen Sicherheitsstrategie“, bei der mehrere Ebenen von Sicherheitsmaßnahmen zum Einsatz kommen, wie dies in Abbildung 3-2 dargestellt ist.

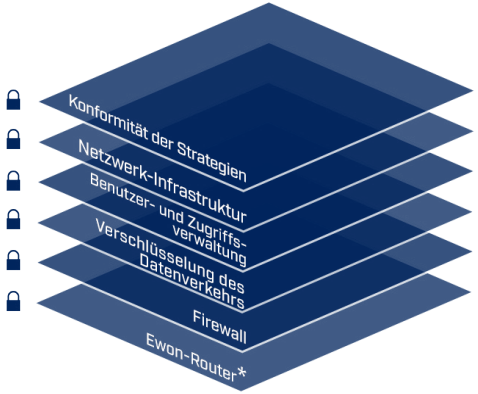


Abbildung 3-2: Die mehrschichtige Verteidigungsstrategie von Ewon.

Ziel ist es insbesondere, die Integrität des Konnektivitäts- und Informationssystems der industriellen Cloud Talk2M basierend auf zahlreichen fachspezifischen Veröffentlichungen, Richtlinien, Best Practices und etablierten Sicherheitsstandards zu schützen wie:

- ISO/IEC 27001 (International Organization for Standardization und International Electrotechnical Commission)
- U.S. National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0
- Open Web Application Security Project (OWASP)
- Handbuch zur Methodik der Sicherheitsprüfung (OSSTMM)

Von der Hardware bis hin zu Richtlinien und Verfahren ist die Sicherheit eine wesentliche Komponente, die vollumfänglich in jede Ebene der Ewon-Lösungen integriert ist. Die verschiedenen Schichten der Ewon-Strategie der tief gestaffelten Verteidigung bestehen aus den nachfolgenden Elementen:

- **Ewon-Router*:*** Die Benutzer müssen authentifiziert sein. Der maschinen-/LAN-seitige Verkehr wird vom WAN der Kundenseite getrennt und die Benutzer können nur auf autorisierte Geräte im LAN zugreifen. Die spezifischen Kontrollen umfassen vier Schlüsselaspekte
  - Netzwerktrennung: Industrierouter werden üblicherweise in das Bedienfeld einer Maschine eingebaut und dabei wird die Maschine auf der einen Seite (LAN) und das Firmennetz (WAN) auf der anderen Seite angeschlossen. Wenn eine Verbindung aufgebaut werden muss, funktioniert das Ewon-Gerät als Gateway, durch das der gesamte Verkehr läuft. Bei der anfänglichen Konfiguration des Ewon beschränken die Sicherheitseinstellungen des Gerätes den Verkehr zwischen diesen beiden Netzwerkschnittstellen. Diese Netzwerktrennung beschränkt den Fernzugriff auf die Geräte, die mit dem lokalen Netz von Ewon verbunden sind, und verhindert den Zugriff auf den Rest des Netzes.
  - Authentifizierung des Geräts: Ewon-Router haben andere Zugriffsrechte als Talk2M. Nur Benutzer mit den entsprechenden Anmeldedaten und Zugriffsrechten können die Sicherheitseinstellungen auf Ewon-Routern ändern. Ebenso können bei Geräten mit Datendiensten nur autorisierte Benutzer diese einsehen oder ändern.
  - Physischer Schalter: Alle Ewon-Hardwaregeräte verfügen über einen digitalen Eingang. An diesen Eingang kann ein physischer Schalter angeschlossen werden, um den WAN-Anschluss zu aktivieren oder zu deaktivieren. So kann der Endbenutzer vor Ort selbst bestimmen, ob auf das Gerät aus der Ferne zugegriffen werden kann oder nicht.
  - IP-Vergabe und-Kontrolle: Der Ewon benötigt dieselben Einstellungen wie ein PC, der an dasselbe Netzwerk angeschlossen ist (IP-Adresse, Subnetzmaske und Gateway sowie eventuelle Proxy-Einstellungen). Der Ewon kann so konfiguriert werden, dass er diese Einstellungen automatisch über das DHCP-Protokoll erhält. Der Ewon kann jedoch auch so konfiguriert werden, dass er eine statische IP-Adresse verwendet, die von der IT-Abteilung zugewiesen und kontrolliert wird, falls Sie dies wünschen.
- **Firewall:** In der eCatcher-Anwendung können Talk2M-Administratoren Filter- und Firewall-Regeln definieren, die angeben, auf welche am Ewon angeschlossenen Geräte aus der Ferne zugegriffen werden kann, und sogar auf welchen Ports (Ethernet, USB oder seriell) und mit welchen Protokollen sie erreicht werden können. Talk2M bietet vier verschiedene Firewall-Konfigurationen, die auf den IP-Adressen, den Ports, den Gateways und dem Zugang zu Ewon-Diensten der angemeldeten Geräte basieren. Ausgehend von der am wenigsten restriktiven bis zur sichersten Firewall-Ebene lassen sie sich wie folgt beschreiben:
  - Standard: Zugriff auf alle Geräte, die mit dem Ewon-Netzwerk verbunden sind.
  - Hoch: Zugriff nur auf explizit aufgeführte Ewon-LAN-Geräte; auch Port-Einschränkungen sind möglich.
  - Verstärkt: Der Zugang zum Ewon-Gateway kann gesperrt werden.
  - Ultra: Der Zugriff auf Ewon-Gerätedienste wie HTTP, FTP und SNMP kann gesperrt werden.

In Kombination mit der Talk2M-Benutzerrechteverwaltung können Administratoren die Fernzugriffsrechte an bestimmte Benutzergruppen anpassen.

- **Verschlüsselung:** Die Kommunikation zwischen dem Remote-Benutzer und den Ewon-Geräten wird vollumfänglich mithilfe des Transport Layer Security (TLS) verschlüsselt, um die Authentizität, Integrität und Vertraulichkeit der Daten zu gewährleisten. Alle Benutzer und Ewon-Geräte werden mit x.509-Zertifikaten authentifiziert und der End-to-End-Datenverkehr wird mit starken symmetrischen und asymmetrischen Algorithmen verschlüsselt.
- **Benutzerverwaltung und Verantwortlichkeit:** Jedes Talk2M-Konto kann über eine unbegrenzte Anzahl von Benutzern verfügen. Für jeden Benutzer, der Zugriff auf das Remote-Gerät benötigt, können die Administratoren eindeutige Anmeldedaten erstellen. Dies vereinfacht die Gewährung und gegebenenfalls den Entzug von Zugriffsrechten. Darüber hinaus können Talk2M-Administratoren einschränken, auf welche Maschinen die

einzelnen Benutzer zugreifen können, welche Dienste zugänglich sind und sogar welche Ports und Protokolle erlaubt sind. So kann ein Administrator z. B. Remote-Benutzern den Zugriff auf Webdienste auf einem bestimmten Gerät zu Überwachungszwecken gestatten, die zur Durchführung von Änderungen verwendeten Ports jedoch auf bestimmte Techniker beschränken. Die Kontrollen beinhalten:

- Auf Rollen basierte Zugriffskontrolle (RBAC), die festlegt, welche Benutzer auf welche Maschinen zugreifen dürfen, und unterschiedliche Zugriffsebenen zulässt
- Eindeutige Benutzer-ID mit benutzerdefinierten Kennwortanforderungen (von einer minimalen Länge, aus Buchstaben, Ziffern und Sonderzeichen bestehend, mit einem Ablaufzeitraum versehen und mit einer eindeutigen Kennworthistorie)
- Multi-Faktor-Authentifizierung (MFA), bei der die Benutzer nach Eingabe ihres Benutzernamens und Passworts einen per SMS zugesandten Code eingeben müssen
- Auditjournale und Verbindungsprotokolle für jedes Gerät, um zu sehen, wer sich wann und wie lange angemeldet hat

- **Talk2M-Infrastruktur:** Ewon bewertet regelmäßig die Talk2M-Architektur als Teil des Risikomanagements. Geeignete Kontrollen werden implementiert, um eine maximale Sicherheitseffektivität und die Einhaltung der geltenden gesetzlichen Vorschriften zu gewährleisten.

Technischer Inhalt

Ewon hat mehrere erstklassige Hosting-Unternehmen unter Vertrag genommen, welche die nachfolgenden Anforderungen erfüllen:

- Hochwertige Hosting-Provider: Um die Zuverlässigkeit zu erhöhen, die Redundanz zu verbessern und die Latenz zu verringern, arbeitet Ewon mit 21 führenden Hosting-Providern auf der ganzen Welt zusammen.
- 24/7/365-Überwachung: Unser Servernetzwerk wird 24 Stunden am Tag überwacht, um maximale Verfügbarkeit und Sicherheit zu gewährleisten.
- Zertifizierte Rechenzentren: Zu den relevanten Zertifizierungen gehören Service Organization Control (SOC) 1/2 Statements on Standards for Attestation Engagements (SSAE) 16/International Standard for Assurance Engagements (ISAE) 3402, SOC 2 und International Organization for Standardization (ISO) 27001/27002/27017/27018.
- Mitglied der Cloud Security Alliance (CSA): Ewon arbeitet mit Hosting-Partnern zusammen, die Mitglieder der CSA sind.

- **Richtlinien und Verfahren**: Die Talk2M-Fernzugriffslösung ist so konzipiert, dass sie mit den bestehenden Sicherheitsrichtlinien der Kunden kompatibel ist. Durch die Verwendung von ausgehenden Verbindungen über häufig geöffnete Ports (z. B. 443 und 1194) und die Kompatibilität mit den meisten Proxy-Servern ist der Ewon-Router so konzipiert, dass er nur minimal in das Netzwerk eingreift und innerhalb der bestehenden Firewall-Regeln funktioniert. Talk2M-Administratoren können die Passwortrichtlinien an die Unternehmensrichtlinien anpassen und den Benutzerzugriff einschränken. Talk2M-Administratoren können auch den Talk2M-Verbindungsbericht (Audit) einsehen, um zu sehen, welche Benutzer sich wann mit welchen Geräten verbinden, und so überprüfen, ob die Fernzugriffsrichtlinien des Unternehmens eingehalten werden.

Um die bestmögliche Geschäftskontinuität zu gewährleisten, stehen den Kunden zwei Serviceangebote zur Verfügung:

- Talk2M Free+ bietet einen effizienten kostenlosen Service ohne Service Level Agreement (SLA)
- Talk2M Pro besteht aus einem aufwändigeren, kostenpflichtigen Dienst mit Service Level Agreement

Der Dienst Talk2M Pro garantiert eine Verfügbarkeit von 99,6 %. Um diese beiden Service Levels bereitzustellen, wird die Talk2M-Architektur durch mehrere Richtlinien- und Kontrollziele verstärkt, darunter:

- Service Level Agreement der Hosting-Provider: Die Dienste von Talk2M Pro werden bei erstklassigen Hosting-Partnern gehostet, die uns eine Verfügbarkeit von 99,99 % garantieren. Für die Dienste von Talk2M Free+ werden mehrere Hosting-Provider genutzt, die in der Regel eine Verfügbarkeit von über 99 % bieten.
- Leistungsindikatoren: Die Leistung jedes Servers wird kontinuierlich überwacht.
- Server-Redundanz: Mehrere Anbieter ermöglichen eine schnelle Umleitung von VPN-Verbindungen im Falle von Problemen.
- Kontinuierliche Überwachung: Die Talk2M-Dienste werden rund um die Uhr durch Ingenieure überwacht.

Um schließlich die Latenzzeiten im Netz zu verringern, befinden sich die Rechenzentren auf fünf Kontinenten (Nordamerika, Europa, Asien, Afrika und Australien) und werden sich auf immer mehr Regionen erstrecken. Einige SPS-Protokolle, die auf sehr kleinen Paketgrößen beruhen und sehr viel empfindlicher auf Netzunterbrechungen reagieren, erfordern nämlich eine geringe Latenzzeit. Ewon-Produkte verbinden sich mit dem geografisch nächstgelegenen Server, um die Verbindungsleistung zu optimieren.

Künftige Lösung: Der Ewon Cosy+ und seine noch höhere Sicherheit

In Zukunft wird der Ewon-Industrierouter Cosy+ ein mehrschichtiges Sicherheitskonzept beinhalten (siehe Abbildung 3-2) und den Standard für die Branche setzen, die immer mehr Wert auf Sicherheit legt.
Mit dem Cosy+ hebt Ewon den Markt für Fernzugriff auf ein noch nie dagewesenes Sicherheitsniveau. Dieser neue Ansatz integriert ein hohes Maß an Hardwaresicherheit als Teil der Vertrauenskette, um die strengsten IoT-Standards zu erfüllen. Hier sind nur einige der hochmodernen Sicherheitsfunktionen, die der Ewon Cosy+ bietet:

- Garantierte Vertrauenskette von der Hardware bis zur Cloud: Der Ewon Cosy+ verfügt über einen eingebauten Secure Element (SE) Chip, der geheime Informationen schützt und einen Hardware-Vertrauensanker („Hardware Root of Trust“) bietet. Er enthält auch ein Stammzertifikat, um Klonen oder Fälschungen zu verhindern.
- Es wurde eine sichere Startsequenz („Secure Boot“, kontrollierte Startform) implementiert, um sicherzustellen, dass nur ein von Ewon signierter Code ausgeführt wird. Eine hohe Verschlüsselung der gesamten Kommunikation mit der T2M Cloud ist ebenfalls gewährleistet.
- Alle Vorgänge, die Geheimnisse im Zusammenhang mit dem Ewon Cosy+ betreffen, werden über „Key Ceremonies“ abgewickelt. Eine „Key Ceremony (KC)“ oder Schlüsselzeremonie ist eine Sitzung, die regelt, wie kryptografische Objekte erzeugt und gespeichert werden.
- Erhöhte Sicherheit durch digitalen Ausgang, der eine aktive Fernverbindung anzeigt.

Beispiele für die Verwendung des Fernzugriffs

In diesem Kapitel finden Sie vier konkrete Beispiele:

1. Hersteller von Tiefziehmaschinen (MAAC)
2. Industriebäckerei (Bakkersland)
3. Stapelung von Materialien (A.G. Stacker)
4. Zyklotrone im Gesundheitssektor (IBA)

1. Hersteller von Tiefziehmaschinen

Das in Chicago ansässige Unternehmen MAAC ist auf die Herstellung von Tiefziehmaschinen und anderen ergänzenden Produkten spezialisiert. MAAC-Produkte werden weltweit eingesetzt und kommen in vielen Branchen wie z. B. in der Luft- und Raumfahrt, der Medizintechnik und der Automobilindustrie zum Einsatz.

MAAC erkannte schon früh, dass die Automatisierungstechnik der Schlüssel zum Erfolg im Maschinensektor sein würde. Leslie Adams, Leiterin der technischen Dienste, ist seit langem eine Verfechterin der elektronischen Automatisierung. Adams: „Die von einem Ewon VPN-Router bereitgestellte Kommunikation ist einfach unglaublich. Mit einer Internetverbindung können wir fast überall auf Maschinen zugreifen.“

Die sichere VPN-Verbindung, welche die Ewon-Technologie bereitstellt, bietet eine vollständige Integration von IT-Sicherheitsstandards. Die einzigartige Fernzugriffslösung von Ewon ermöglicht es MAAC, sich mit den Maschinen vor Ort genauso einfach und flexibel zu verbinden wie mit einer Maschine in der Werkshalle des Unternehmens.

Der Fernzugriff ermöglicht es dem Unternehmen, sich mit einer Maschine zu verbinden, als wäre es vor Ort, und auf SPS, Antriebe und HMI-Geräte sowie alle anderen mit der Maschine verbundenen Geräte zuzugreifen. Vor der Installation der Ewon-Router nutzte MAAC Telefonmodems für die Verbindung zu seinen Maschinen, aber die Latenz war ein großes Problem. „Ich erinnere mich an die Frustration, die mit der Überwachung der Maschinen verbunden war, als die Informationen über die Modemverbindung lange auf sich warten ließen. Wir haben mit einer Maschine in Australien gearbeitet und die Verzögerung konnte bis zu 15 Sekunden betragen“, erinnert sich Adams.

Die Fernwartung, die eine schnelle und effiziente Fehlersuche ermöglicht, wirkt sich positiv auf die Kundendienstkosten aus. Leslie Adams kommentiert: „Mit Ewon können wir 50–70 % unserer Supportkosten einsparen und auch die Maschinenstillstandzeiten, die normalerweise mit dem Warten auf einen Servicetechniker verbunden sind, erheblich reduzieren. Die mit Reisen vor Ort verlorene Zeit entspricht einer Menge Geld. Auf Flughäfen zu sitzen und zu Kunden zu fahren entspricht einer Menge verlorener Zeit – Zeit, die unsere Programmierer lieber mit der Arbeit an neuen Maschinen oder der Feinabstimmung bestehender Systeme verbringen sollten. Wenn diese Personen nicht anwesend sind, arbeiten sie einfach nicht an den wichtigen Dingen."

2. Industriebäckerei (Bakkersland)

Bakkersland ist die größte industrielle Bäckerei in den Niederlanden. Die Hauptsorge von Bakkersland gilt dem möglichen Stillstand von Maschinen in einem Produktionsprozess. Jede Ausfallzeit kann zu Verzögerungen im Logistikprozess führen.

Um diese Art von Unterbrechungen zu vermeiden, hat Bakkersland ein Projekt eingeleitet, bei dem

jede seiner Maschinen mit einem Ewon-Industrierouter ausgestattet ist. Die Ewon-Router werden im Kontrollraum neben der SPS auf der DIN-Schiene (einer Metallschiene, die für die Montage von Leistungsschaltern und industriellen Steuergeräten in Geräteschränken verwendet wird) installiert. Die Einrichtung arbeitet online und kann dem Bediener über eine sichere VPN-Verbindung die Fernüberwachung der Maschine ermöglichen.

Bakkersland hat sich für den Cosy-Router von Ewon als Fernwartungssystem für seine Maschinen entschieden. Dennis van Scheijndel von Bakkersland erläutert die Vorteile der Ewon-Architektur: „Im Falle eines Alarms kann der Bediener darauf hinweisen, dass ein bestimmter Sensor verschmutzt oder dass die Verbindung nicht vollständig sicher ist. Falls erforderlich, kann der Lieferant Änderungen an der Steuerung vornehmen. Nicht nur wir als Anwender sparen Zeit, auch der Maschinenhersteller muss keinen Ingenieur mehr an Ort und Stelle entsenden. Davon profitieren vor allem die Anbieter im Ausland."

3. Stapelung von Materialien (A.G. Stacker)

A.G. Stacker ist ein Hersteller von Staplern und Zusatzgeräten. Als Clarence und Helen Allen das Unternehmen 1996 gründeten, war es ihr Ziel, innovative Geräte mit besserem Kundendienst als jeder andere in der Branche anzubieten. Heute arbeitet A.G. Stacker bei gleichzeitigem Augenmerk auf Innovation und Kundenservice mit Ewon zusammen, um die nächste Generation der Kundeninteraktion zu entwickeln.

Die Maschinen von A.G. Stacker werden von Kunden in der ganzen Welt eingesetzt. Jede dieser Maschinen verfügt über ein ausgeklügeltes Automatisierungssystem mit Antrieben, programmierbaren Steuerungen und anderen modernen Funktionen. Obwohl A.G. Stacker über ein Team von hochqualifizierten Ingenieuren, Technikern und Ausbildern verfügt, die den Kunden helfen, den Wert der Maschine zu maximieren, erfordern die Kundenbedingungen manchmal eine Feinabstimmung und Systemänderungen vor Ort. Bei in Betrieb befindlichen Automatisierungsanlagen muss sich manchmal jemand zum Kunden begeben, um selbst kleine Änderungen vorzunehmen. Da die Kosten für Last-Minute-Flüge in die Höhe geschossen sind, hat A.G. Stacker nach einem neuen und innovativen Weg zur Lösung dieses Problems gesucht. In diesem Moment kam Ewon ins Spiel.

Ewon bietet einen schnellen und einfachen, aber dennoch sicheren Ansatz für Remote-Konnektivität. Kennedy Larramore, der Elektro- und IT-Techniker von A.G. Stacker, erklärt: „Auch wenn wir drei Techniker für die Betreuung unserer Kunden abgestellt haben, sind „herumreisende Techniker" sowohl für unsere Kunden als auch für A.G. Stacker kostspielig. Im Grunde genommen könnte die Zeit, die wir mit Reisen verbringen, von unseren Mitarbeitern besser genutzt werden, und Ausfallzeiten bei unseren Kunden sind sehr teuer. Darüber hinaus stoßen wir häufig auf Probleme, bei denen der Kunde Schwierigkeiten hat, die genaue Art des Problems zu beschreiben."

„Wir haben damit begonnen, die Ewon-Geräte als Option für unsere Maschinen anzubieten. Aber nachdem wir die Leistungsfähigkeit der kostenlosen Talk2M-Lösung und der Geräte von Ewon in der Praxis gesehen haben, haben wir Ewon in alle Maschinen integriert, die wir bauen", fügt Herr Larramore hinzu.

4. Zyklotrone im Gesundheitssektor (IBA)

IBA entwickelt hochpräzise Lösungen für die Krebsdiagnose und-behandlung – zum Beispiel Zyklotrone. IBA hat sich für Ewon und die Talk2M-Technologie entschieden, um einen globalen Remote-Service anzubieten.

„Unser Ziel ist es vor allem, den Kunden im Falle einer Störung oder bei Fragen aus der Ferne helfen zu können", erklärt Patrick Delcour, Projektleiter für den Kundendienst bei IBA. „Mit Talk2M kann ich mich einloggen und innerhalb von drei Sekunden vom Standort in Melbourne, Australien, zum Standort in Gent, Belgien, wechseln."

Störungen werden für den Kunden vom Kontrollraum aus auf Grundlage der vom Status der Anzeigeleuchten und Displays bereitgestellten Informationen behoben. „Die Informationen aus dem Kontrollraum sind jedoch sehr bruchstückhaft", so Delcour. Vor dem Einsatz von Ewon musste der Bediener des Kunden im Falle eines Problems eine IBA-Hotline anrufen.

Die Talk2M-Lösung hat die Arbeitsweise von IBA revolutioniert. Talk2M bietet eine einfache Bedienung und Verbindung bei gleichzeitiger Verbesserung der Effizienz der Antworten. „Drei Klicks und ich bin verbunden“, sagte Delcour. Die Komplexität, die mit Firewalls oder Proxys verbunden ist, bleibt für den Benutzer völlig verborgen.

Sobald die Verbindung zu Talk2M hergestellt wurde, werden alle IP-Adressen auf der lokalen

Netzwerkseite des Ewon transparent und für den Benutzer zugänglich. Der Benutzer kann sich mit wenigen Klicks mit der SPS und der IP-Kamera verbinden oder auf dem Kontroll-PC einen Remote-Desktop starten, um den lokalen PC fernzusteuern und das HMI zu starten.

Weitere Beispiele für die Verwendung von Ewon finden Sie unter**www.ewon.biz/customers.**

Inbetriebnahme des Ewon Cosy in 5 einfachen Schritten

In diesem Kapitel erfahren Sie, wie Sie:

- Ihr Talk2M-Konto anlegen und konfigurieren können
- Ihren Ewon Cosy konfigurieren können
- Sich mit einer Remote-Maschine verbinden können

Wenn Sie noch keinen Ewon Cosy besitzen, aber gerne einen erwerben möchten, besuchen Sie bitte **www.ewon.biz/contact**, um einen Händler in Ihrer Region/Ihrem Land zu finden.

Befolgen Sie diese Schritte:

1. **eCatcher herunterladen, installieren und starten.**
   eCatcher ist ein kostenloses Tool, mit dem Sie den Fernzugriff über das Talk2M VPN initiieren und eine Verbindung zu allen Geräten herstellen können, die mit Ihrem Ewon verbunden sind. Sie können eCatcher von der Ewon-Website unter https://ewon.biz/technical-support/pages/all-downloads herunterladen. Nachdem Sie den Installationsassistenten ausgeführt haben, folgen Sie den Anweisungen, um die Installation abzuschließen und eCatcher zu starten.

2. **Legen Sie auf der Anmeldeseite Ihr Konto an, indem Sie auf „Kostenloses Konto erstellen“ klicken.**
   Erstellen Sie einen eindeutigen Kontonamen, geben Sie Ihren Namen und Ihre E-Mail-Adresse ein und erstellen Sie ein Passwort. Außerdem müssen Sie Ihr Konto aktivieren, indem Sie auf den an Ihre E-Mail-Adresse gesendeten Link klicken.

Klicken Sie auf „Verfügbarkeit prüfen“, um zu überprüfen, ob Sie einen eindeutigen Kontonamen ausgewählt haben.

3. **Melden Sie sich bei eCatcher an und fügen Sie Ihr Ewon hinzu, indem Sie auf die Schaltfläche „Hinzufügen“ klicken.**
   Dieser Schritt ist in Abbildung 6-1 dargestellt. Fahren Sie mit dem Einrichtungsassistenten fort. Wählen Sie Ihre Version von Ewon Cosy (Ethernet, WLAN oder Mobiltelefon). Die Konfiguration erfolgt entweder über eine(n) vorkonfigurierte(n) USB-Stick/SD-Karte, der/die in den Ewon eingeführt wird, oder über die Webschnittstelle des Ewon.

Auf die Webschnittstelle des Ewon kann über einen Webbrowser zugegriffen werden, der mit demselben LAN wie der Ewon verbunden ist (oder direkt an den Ethernet-Anschluss

angeschlossen ist). Der einfachste Weg, um auf die Webschnittstelle zuzugreifen, ist der Start des Programms „eBuddy“, das automatisch Ewons erkennt, die mit demselben LAN verbunden sind. Wenn Sie den Ewon gefunden haben, klicken Sie mit der rechten Maustaste auf den Ewon und wählen Sie „Im Browser öffnen“.

Bei diesem Schritt haben Sie die Möglichkeit, die IP-Adresse des LAN (standardmäßig 10.0.0.53) zu ändern und das WAN über DHCP oder eine statische IP-Adresse einzustellen. Wenn Sie dazu aufgefordert werden, führen Sie einen USB-Stick/eine SD-Karte in Ihren PC ein, um die Konfiguration zu speichern. Wenn Sie fertig sind, schließen Sie die eCatcher-Anwendung.

Abbildung 6.1: Hinzufügen eines Ewon in eCatcher

4. **Schalten Sie Ihren Ewon Cosy ein, schließen Sie Ihr WAN-Kabel an und führen Sie Ihren USB-Stick/Ihre SD-Karte ein.**
   Stecken Sie Ihr WAN-Ethernet-Kabel wie in Abbildung 6-2 dargestellt in den WAN-Anschluss ein, der neben dem entsprechenden Anschluss eine orangefarbene Kontrollleuchte aufweist. Jeder Anschluss des Ewon hat eine Nummer, die neben ihm angezeigt wird. Standardmäßig ist 1 ein LAN-Anschluss und 4 ein WAN-Anschluss.

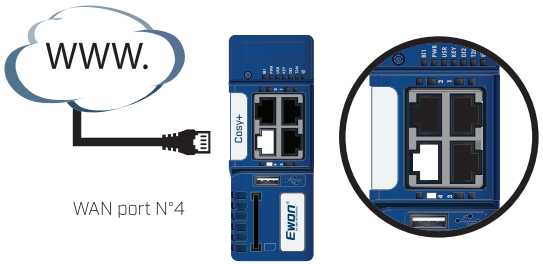


ABBILDUNG 6-2: Identifizierung des WAN-Anschlusses auf Ihrem Ewon.

Wenn die PWR-Anzeige grün leuchtet und die USR-Anzeige grün blinkt (siehe Abbildung 6-3), führen Sie Ihren konfigurierten USB-Stick/Ihre konfigurierte SD-Karte in Ihren Ewon Cosy ein. Die USR-Anzeige beginnt schnell orange zu blinken und zeigt damit an, dass eine gültige Konfigurationsdatei erkannt wurde.

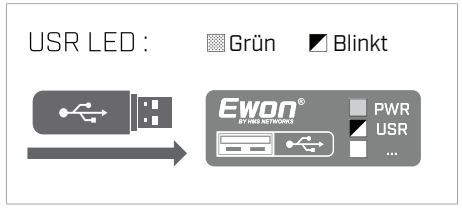


Abbildung 6-3: Die LED-Anzeige, wenn Sie den USB-Stick anschließen und die Datei erfolgreich war.

Sobald die USR-Anzeige dauerhaft grün leuchtet, wurde die Datei erfolgreich geladen. Sie können den USB-Stick oder die SD-Karte entfernen und Ihr Ewon Cosy wird nun neu gestartet. Wenn die USR-Anzeige rot leuchtet, liegt ein Fehler in Ihrer Konfiguration vor. Diese Modelle sind in Abbildung 6-4 dargestellt.

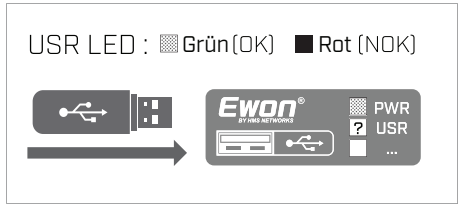


Abbildung 6-4: Warten Sie, bis die Benutzeranzeige dauerhaft grün (erfolgreich geladen) oder rot (Fehler) leuchtet.

Erinnerung

Die Konfiguration der Talk2M-Verbindung kann einige Minuten dauern. Am Ende des Einrichtungsvorgangs sollte die Talk2M-Anzeige aufleuchten. Siehe Abbildung 6-5.

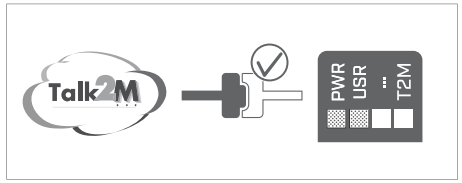


ABBILDUNG 6-5: Die Talk2M-Anzeige leuchtet auf und zeigt an, dass der Einrichtungsvorgang abgeschlossen ist..

5. **Sobald Ihr Computer mit dem Internet verbunden ist, starten Sie eCatcher.**
Der Status Ihres Ewon Cosy muss „Online“ sein. Markieren Sie einfach Ihr Ewon-Gerät und klicken Sie auf die Schaltfläche „Verbinden“.

Sobald Sie über eCatcher mit Ihrem Ewon verbunden sind, müssen Sie, wenn Sie ein Ethernet-Gerät an den LAN-Anschluss Ihres Ewon Cosy angeschlossen haben und sich im selben Subnetz befinden, dessen IP-Adresse anpingen können, um die Verbindung zu überprüfen.

Empfehlungen für den Benutzer, der sich für eine Lösung des industriellen Fernzugriffs entscheidet:

1. Achten Sie besonders auf den Sicherheitsaspekt (siehe Kapitel 3).
2. Stellen Sie sicher, dass Sie Ihre Verbindungen einfach verwalten können und dass Sie wissen, wer wann und auf welche Maschine(n) Zugriff hat. Außerdem ist es wichtig, dass frühere Zugriffe über ein integriertes Auditsystem nachvollzogen werden können.
3. Alle Verbindungen müssen vertraulich und verschlüsselt sein.
4. Definieren Sie Ihre Netzzugangsarchitektur innerhalb Ihrer Fabriken: Maschinenlieferanten dürfen keinen Zugang zu Ihrem gesamten LAN haben. Akzeptieren Sie nur ausgehende Verbindungen. Daher brauchen Sie keine weiteren Ports zu öffnen und Sie sollten keine feste IP-Adresse benötigen.
5. Vergewissern Sie sich, dass die Cloud-Architektur Ihres Lieferanten Ihnen den Zugang über ein korrektes SLA garantiert. Denn nichts ist schlimmer, als wenn Ihr Cloud-System von einem einzigen Rechenzentrum abhängt, das nicht mehr verfügbar ist. Denken Sie an die Ereignisse in Frankreich im Jahr 2021.
6. Entscheiden Sie sich für eine Lösung, die auf Grundlage bewährter und ständig weiterentwickelter Lösungen, vorzugsweise als Open Source, entwickelt wurde.
7. Stellen Sie sicher, dass Ihr Lieferant die Firmware und die Programme ständig aktualisiert. Es gibt nichts Schlimmeres als einen Lieferanten, der aus rein opportunistischen Gründen einsteigt und sich nach ein paar Jahren wieder zurückzieht.
8. Stabilität der Gruppe: Vergewissern Sie sich, dass Ihr Lieferant solide und rentabel ist.

2G: Die 1991 auf Grundlage von GSM kommerziell eingeführte zweite Generation der drahtlosen Telekommunikationstechnologie ermöglichte digitale Datendienste für Mobiltelefone einschließlich SMS-Textnachrichten. Siehe auch Global System for Mobile Communications (GSM) und Short Message Service (SMS).

3G: Die 1998 kommerziell eingeführte dritte Generation der drahtlosen Telekommunikationstechnologie bietet Datenübertragungsraten von 2 Megabit pro Sekunde (Mbit/s) oder mehr für drahtlose Sprachtelefonie, mobilen Internetzugang, festen drahtlosen Internetzugang, Videotelefonie und mobiles Fernsehen.

4G: Die 2008 kommerziell eingeführte vierte Generation der drahtlosen Telekommunikationstechnologie bietet Spitzen-Datenübertragungsraten von 100 Mbit/s für die Kommunikation mit hoher Mobilität (z. B. von einem fahrenden Fahrzeug aus) und 1 Gigabit pro Sekunde (Gbit/s) für die Kommunikation mit geringer Mobilität (wie bei einem Fußgänger).

Advanced Encryption Standard (AES): Ein symmetrischer Blockverschlüsselungsalgorithmus, der zur Verschlüsselung von Netzwerkverkehr und sensiblen Daten verwendet wird. AES ist der Ersatzverschlüsselungsalgorithmus für DES und 3DES. Siehe auch Data Encryption Standard (DES).

Application Programming Interface (API): Satz von Regeln und Spezifikationen, die Softwareprogramme befolgen können, um miteinander zu kommunizieren; dient als Schnittstelle zwischen verschiedenen Softwareprogrammen und erleichtert deren Interaktion.

Data Encryption Standard (DES): Ein symmetrischer Verschlüsselungsalgorithmus, der in den frühen 1970er Jahren entwickelt wurde, heute aber aufgrund seiner geringen Schlüsselgröße (56 Bit) als unsicher gilt.

DB9: Ein gebräuchlicher elektrischer Steckverbinder für serielle RS232-Computerverbindungen, der seinen Namen von seiner charakteristischen D-förmigen Metallabschirmung und seinen zwei parallelen Reihen von insgesamt neun Stiften hat. Siehe auch RS232.

DF1: Asynchrones, byteorientiertes Protokoll für die Kommunikation mit den meisten RS232-Schnittstellenmodulen von Allen Bradley. Siehe auch RS232.

Drahtloses Modem: Ein Modem, welches das Telefonsystem umgeht und sich direkt mit einem drahtlosen Netzwerk verbindet, über das es Zugang zu dem von einem Internetdienstanbieter (ISP) bereitgestellten Internet hat.

Encapsulating Security Payload (ESP): Teil der IPsec-Protokollsuite, der für die Sicherstellung der Authentizität, Integrität und Vertraulichkeit der ursprünglichen Pakete verantwortlich ist.

Envelope Encryption (EVP): Eine High-Level-Schnittstelle zu den kryptografischen Funktionen von OpenSSL. Siehe auch OpenSSL.

Ethernet: Ein Netzwerkprotokoll, das steuert, wie Daten über ein lokales Netzwerk übertragen werden. Technisch gesehen handelt es sich um das IEEE 802.3-Protokoll. Dieses Protokoll wurde im Laufe der Zeit weiterentwickelt und verbessert und kann nun Daten mit einer Geschwindigkeit von 1 GB pro Sekunde übertragen.

Erstausrüster (Original Equipment Manufacturer, OEM): Ein Unternehmen, das Teile und Geräte herstellt, die von einem anderen Hersteller vermarktet werden können.

Ethernet-Kabel (gekreuzt): Ein aus verdrillten Kupfer-Adernpaaren bestehendes Kabel mit zwei RJ45-Steckern, das benutzt wird, um zwei Computergeräte direkt miteinander zu verbinden.

Ethernet-Kabel (ungekreuzt): Ein aus verdrillten Kupfer-Adernpaaren bestehendes Kabel mit zwei RJ45-Steckern, das benutzt wird, um Computergeräte in einem LAN miteinander zu verbinden; dies geschieht normalerweise über einen Hub oder einen Switch. Siehe auch Lokales Netzwerk (LAN).

File Transfer Protocol (FTP): Ein Standard-Netzwerkprotokoll, das zur Übertragung von Computerdateien zwischen einem Client und einem Server über ein Netzwerk verwendet wird.

Firewall: Ein Netzsicherheitssystem, das den unbefugten Zugang zu einem oder von einem privaten Netz verhindern soll. Firewalls können sowohl als Hardware als auch als Software bzw. als eine Kombination aus beidem implementiert werden. Netzwerk-Firewalls werden häufig eingesetzt, um zu verhindern, dass unbefugte Internetnutzer auf private, mit dem Internet verbundene Netze zugreifen.

Global System for Mobile Communications (GSM): Vom Europäischen Institut für Telekommunikationsnormen (ETSI) entwickelte drahtlose Telekommunikationsnorm für 2G-Protokolle. Siehe auch 2G.

Hyper Text Transfer Protocol Secure (HTTPS): Ein sicheres Kommunikationsprotokoll über einen Webbrowser im Internet, welches das Secure-Sockets-Layer(SSL)-Protokoll zur Verschlüsselung verwendet. Siehe auch Secure Sockets Layer (SSL).

Hash-based Message Authentication Code (HMAC): Ein Nachrichtenauthentifizierungscode, der eine kryptografische Hash-Funktion und einen geheimen kryptografischen Schlüssel verwendet.

Internet Protocol Security (IPsec): Eine Reihe von Netzwerkprotokollen zur Authentifizierung und Verschlüsselung von Datenpaketen, die über ein Netzwerk gesendet werden.

Internetanbieter (ISP): Eine Organisation, die ihren Kunden den Zugang zum Internet ermöglicht.

Internetprotokoll (IP): Das Hauptkommunikationsprotokoll der TCP/IP-Kommunikationssuite für die Weiterleitung über Netzwerkgrenzen (Router) und das Internet. Siehe auch Übertragung.

Intrusion Detection System (IDS): Ein Hardware-Gerät oder eine Software-Anwendung, das/die ein Netzwerk oder System auf bösartige Aktivitäten überwacht.

IP-Kamera: Eine Videokamera, die über eine Fast Ethernet-Verbindung vernetzt ist. Die IP-Kamera sendet ihre Signale über eine Internet- oder Netzwerkverbindung an den Hauptserver oder den Computerbildschirm. Sie wird hauptsächlich für die IP-Überwachung, das geschlossene Fernsehsystem (CCTV) und die digitale Videografie verwendet. IP-Kameras ersetzen weitgehend analoge Kameras, da sie über einen digitalen Zoom und Fernüberwachungsfunktionen über das Internet verfügen.

Lokales Netzwerk (LAN): Computernetzwerk, das Computer und Geräte (einschließlich Maschinen) in einem Gebäude, einer Fabrik, einem Labor, einer Schule oder einem anderen relativ kleinen Bereich miteinander verbindet.

Machine-to-Machine (M2M): Drahtgebundene oder drahtlose Kommunikation, die direkt zwischen zwei Geräten stattfindet

Mensch-Maschine-Schnittstelle (HMI): Die Benutzeroberfläche in einem Fertigungs- oder Prozesssteuerungssystem.

Modbus: Ein serielles Kommunikationsprotokoll, das ursprünglich von Modicon (jetzt Schneider Electric) zur Verwendung in seinen SPS veröffentlicht wurde. Siehe auch speicherprogrammierbare Steuerung (SPS).

Multi-Faktor-Authentifizierung (MFA): Eine Art der Zugangskontrolle, die den Zugang nur nach mindestens zwei Formen der Authentifizierung gewährt.

Network Address Translation (NAT): Ein Verfahren zur Zuordnung einer IP-Adresse zu einer anderen IP-Adresse, z. B. einer privaten IP-Adresse zu einer öffentlichen IP-Adresse.

Netzlatenz: Jede Art von Verzögerung, die bei der Datenkommunikation über ein Netz auftritt. Netzverbindungen, bei denen geringe Verzögerungen auftreten, werden als Netze mit geringer Latenz bezeichnet. Netzverbindungen, die lange Verzögerungen aufweisen, werden als Netze mit hoher Latenz bezeichnet.

Netzwerktrennung: Aufteilung eines Netzes in zwei LANs, wobei ungesicherte Computer im ersten Netz verbleiben und die zu schützenden Computer in ein zweites abgeschirmtes Netz verlegt werden.

Object Linking and Embedding (OLE): Eine Microsoft-eigene Technologie, mit der Dokumente eingebettet und mit anderen Objekten verknüpft werden können.

OEE (Overall Equipment Effectiveness, d. h. Gesamtanlageneffektivität) ist eine Maßnahme, mit der Sie die Effizienz Ihrer Produktionsabläufe einschätzen und die Ausfallzeiten einer Produktionsmaschine reduzieren können, um so die Produktivität zu verbessern.

OpenSSL: Eine Open-Source-Implementierung der SSL- und TLS-Protokolle. Siehe auch Secure Sockets Layer (SSL) und Transport Layer Security (TLS).

Out-of-Band-Management: Ein spezieller Kommunikationskanal, der für die Verwaltung von vernetzten Geräten wie z. B. für die Fernüberwachung und-konfiguration verwendet wird. Ein Out-of-Band-Kommunikationskanal ist unabhängig von einem In-Band-Kommunikationskanal und hängt daher nicht vom betrieblichen Kommunikationskanal des Geräts (z. B. einer Netzverbindung) ab.

Paketvermittlung: Ein in Kommunikationsnetzen verwendetes Verfahren, bei dem Daten in Paketen – bestehend aus einem Header und einer Nutzlast – an ihr Ziel übertragen werden. Anhand der Informationen im Header leitet die Netzwerkhardware die einzelnen Pakete über den besten verfügbaren Pfad zum Ziel und setzt die Daten am Zielort wieder in der richtigen Reihenfolge zusammen.

Ping: Ein Softwareprogramm, mit dem die Erreichbarkeit eines Hosts (z. B. eines Geräts oder einer Maschine in einem IP-Netzwerk) getestet werden kann.

Process Field Bus (PROFIBUS): Ein Standard für die Feldbuskommunikation in der Automatisierungstechnik.

Programmable Logic Controller (PLC): Ein robuster Industriecomputer, der für die Steuerung von Fertigungsprozessen angepasst wurde.

Public Key Infrastructure (PKI): Satz von Rollen, Richtlinien und Verfahren, die zur Erstellung, Verwaltung, Verteilung, Verwendung, Speicherung und zum Widerruf digitaler Zertifikate sowie zur Verwaltung der Verschlüsselung mit öffentlichen Schlüsseln (auch als asymmetrische Verschlüsselung bezeichnet) verwendet werden.

Public Switched Telephone Network (PSTN): Das weltweite leitungsvermittelte Telefonnetz, das von nationalen, regionalen und lokalen Telefongesellschaften betrieben wird.

RJ45: Standardschnittstelle für Telekommunikationsnetze („registrierte Buchse“), die zum Anschluss von Sprach- und Datengeräten verwendet wird.

Rollenbasierte Zugriffskontrolle (RBAC): Eine Methode zur Kontrolle des Zugriffs auf Computer- oder Netzressourcen auf Grundlage von definierten Rollen, die einzelnen Benutzern innerhalb einer Organisation zugewiesen werden.

RS232: Ein Telekommunikationsstandard für die serielle Datenübertragung.

RS485: Eine standardisierte serielle Schnittstelle, die von der Telecommunications Industry Association und der Electronic Industries Alliance (EIA/TIA) definiert wurde. Auch bekannt als TIA485 und EIA485.

Secure Hash Algorithm (SHA): Eine Familie von kryptografischen Hash-Funktionen, die vom National Institute of Standards and Technology (NIST) der Vereinigten Staaten veröffentlicht wurde.

Secure Sockets Layer (SSL): Kryptografisches Protokoll zur Sicherung der Kommunikation über ein Computernetz.

Speicherprogrammierbare Steuerung (SPS): Eine speicherprogrammierbare Steuerung ist ein spezieller Computertyp, der zur Steuerung industrieller Prozesse durch sogenannte „sequentielle Verarbeitung“ verwendet wird. Sie dient der Automatisierung von Industrieprozessen. Eine Aktion löst eine andere aus, die wiederum eine andere auslöst, und dies entsprechend verschiedenen Parametern, Bedingungen etc. Diese Geräte werden in großem Umfang in Montagelinien und zur Maschinensteuerung eingesetzt.

Service Level Agreement (SLA): Eine formelle Verpflichtung zwischen einem Dienstleistungsanbieter und einem Kunden, die bestimmte Aspekte der erbrachten Dienstleistung wie Qualität, Leistung, Verfügbarkeit und Verantwortlichkeiten regelt.

Short Message Service (SMS): Ein Textnachrichtendienst.

Siemens Multi-Point Interface (MPI): Proprietäre serielle Schnittstelle, die auf dem EIA485-Standard (früher RS485) basiert und zum Anschluss von PCs, Konsolen und anderen Geräten an speicherprogrammierbare Steuerungen vom Typ Siemens SIMATIC S7 verwendet wird. Siehe auch RS485 und speicherprogrammierbare Steuerung (SPS).

Simple Network Management Protocol (SNMP): Standard-Internetprotokoll, das zum Sammeln und Organisieren von Informationen über die in einem Netz verwalteten Geräte verwendet wird.

Subscriber Identity Module (SIM): Ein integrierter Schaltkreis (IC), in dem die Nummer der International Mobile Subscriber Identity (IMSI) und der zugehörige Schlüssel, die zur Identifizierung und Authentifizierung von Teilnehmern auf mobilen Geräten verwendet werden, gespeichert sind.

Supervisory Control and Data Acquisition (SCADA): Eine Kontrollsystemarchitektur, die Computer, vernetzte Datenkommunikation und grafische Benutzeroberflächen (GUIs) für das Management der Prozessüberwachung auf hoher Ebene verwendet.

Transmission Control Protocol (TCP): Eines der Hauptprotokolle der Internetprotokollsuite; TCP ist eine der beiden ursprünglichen Komponenten der Suite und ergänzt das Internet-Protokoll (IP), weshalb die gesamte Suite gemeinhin als TCP/IP bezeichnet wird. TCP gewährleistet die zuverlässige und ordnungsgemäße Übermittlung eines Bytestroms von einem Programm auf einem Computer zu einem anderen Programm auf einem anderen Computer. TCP ist das Protokoll, auf dem die wichtigsten Internetanwendungen wie das World Wide Web, E-Mails, Fernverwaltung und Dateiübertragung beruhen. Siehe auch Internetprotokoll (IP).

Transport Layer Security (TLS): Kryptografisches Protokoll zur Sicherung der Kommunikation über ein Computernetz.

Universal Serial Bus (USB): Industriestandard, der Kabel, Stecker und Kommunikationsprotokolle für die Verbindung, Kommunikation und Stromversorgung zwischen Computern und Peripheriegeräten definiert.

Virtual Network Computing (VNC): Ein grafisches Desktop-Sharing-System, mit dem eine Fernverbindung zu einem anderen PC hergestellt und dieser gesteuert werden kann, indem Tastenanschläge und Mausbewegungen an einen entfernten PC gesendet werden.

Virtuelles privates Netzwerk (VPN): Eine Technologie zur sicheren Erweiterung eines privaten Netzwerks (z. B. eines LAN) über ein öffentliches Netzwerk (z. B. das Internet) mit Hilfe einer verschlüsselten Verbindung und Datenkapselung. Siehe auch Lokales Netzwerk (LAN).

Wide Area Network (WAN): Ein Telekommunikations- oder Computernetz, das sich über ein großes geografisches Gebiet erstreckt.

X.509: Ein kryptografischer Standard, der das Format von Zertifikaten für öffentliche Schlüssel definiert.

Zertifizierungsstelle (ZS): Eine Einrichtung, die digitale Zertifikate ausstellt und den Besitz eines öffentlichen Schlüssels durch das im Zertifikat genannte Subjekt bescheinigt.

Wenn Sie mehr erfahren möchten...

In diesem White Paper werden die Vorteile des Fernzugriffs und der Fernüberwachung für Maschinen- und Anlagenbauer (OEM) untersucht. Sie ermöglichen es ihnen, ihre Geräte mit einer optimalen Organisation zu unterstützen und dabei die Daten auf lokaler Ebene aufzubewahren.

Diese Art von Dienstleistung wird als Wettbewerbsvorteil, als Quelle der Kundenzufriedenheit und häufig auch als Gewinnbringer angesehen.

https://www.ewon.biz/de/produkte/flexy/kpis-als-einfache-iot-anwendung/flexy-kpis-whitepaper

In diesem White Paper werden fünf Anwendungsfälle zur zentralen Datenerfassung vorgestellt, die Maschinenbauer heute mit einem Ewon Flexy und Talk2M umsetzen können.

Datengesteuerte Projekte können Maschinenbauern dabei helfen, ihr Geschäft auszubauen, indem sie ihnen einen besseren Einblick in den Zustand ihrer Maschinen geben und ihnen ermöglichen, die Nutzungsmuster ihrer Kunden zu verstehen.

https://www.ewon.biz/de/loesungen/remote-data/whitepaper-ewon-solutions-for-iiot

DE- Rev. Sept 2021