Best Practices für eine sichere Nutzung der Ewon-Lösung

Dieses Dokument enthält Empfehlungen, die Ihnen helfen sollen, die Vorteile der Ewon-Lösung auf eine sehr sichere und effiziente Weise zu nutzen.

Die Fernzugriffslösung von Ewon wurde mit Blick auf zwei strategische Ziele entwickelt: Sicherheit und Benutzerfreundlichkeit. Dieses Dokument enthält eine Liste von Best Practices, die bei der Konfiguration und Nutzung der Fernwartungslösung von Ewon befolgt werden sollten, um optimale Sicherheit und Effizienz zu erreichen und die Maßnahmen zu ergänzen, die HMS bereits in die Lösung implementiert hat.

Wir empfehlen Ihnen dringend, dieses Dokument als Grundlage für die Definition oder Verbesserung Ihrer internen Prozesse im Zusammenhang mit der Verwaltung der Lösung zu verwenden. Dies wird dazu beitragen, die Qualität Ihres Sicherheitsstatus sowie die Akzeptanz bei Kunden und Partnern zu erhöhen.[1]

Auf der letzten Seite dieses Dokuments finden Sie eine Tabelle, in der unsere empfohlenen Best Practices zusammengefasst sind. Sie können diese Liste verwenden, um Ihre Implementierung zu beschreiben und Ihren Kunden zu zeigen, dass Sie über solide Sicherheitsprozesse verfügen. Damit werden Sie leichter die Akzeptanz der Remote-Lösung erreichen.

1. Governance

Konsistenz der Lösung

Die Definition von Remote-Konnektivität als Schlüsselelement für Ihr Unternehmen trägt nicht nur zur Steigerung Ihrer Wettbewerbsfähigkeit bei, sondern ermöglicht es auch, Mitarbeiter einzubeziehen, eine strukturierte und konsistente Lösung zu erstellen und einen soliden Sicherheitsstatus zu erreichen.

- Beziehen Sie Ihre Unternehmensleitung ein, um eine Fernwartungsstrategie sowie angemessene Erwartungen und Tools zu definieren.
- Verwenden Sie eine spezielle Hardware für die industrielle Remote-Konnektivität. Dadurch wird eine zusätzliche physische Sicherheitsebene zum Schutz Ihrer Geräte geschaffen und das Risiko einer Beeinträchtigung des Betriebs Ihrer industriellen Steuerungssysteme verringert.

[1]Dieses Dokument setzt die Verwendung eines „Talk2M Pro"-Kontos voraus.
Einige Funktionen sind in der Version „Talk2M Free+" möglicherweise nicht verfügbar.

- Harmonisieren Sie Ihre Fernwartungsaktivitäten mit einer einzigen Lösung. Dies reduziert die Komplexität der Verwaltung, die Sicherheitsrisiken und die Anzahl der Angriffsvektoren.

2. Kontoerstellung und -struktur

Ein Talk2M-Konto wird für die Verwaltung der Geräte, Benutzer und aller Sicherheitsaspekte der Fernzugriffslösung von Ewon verwendet.

Struktur des Kontos

Ihre Unternehmensaktivitäten, Anforderungen und Organisation sollten sich in der Struktur Ihres Kontos widerspiegeln.

- Definieren Sie eine klare Struktur für Ihre Wartungsaktivitäten innerhalb Ihrer Organisation und für die Zusammenarbeit mit Ihren externen Partnern. Verwenden Sie die Talk2M-Gerätepools und Benutzergruppen, um die Verwaltung von Benutzer- und Zugriffsrechten für verschiedene Gruppen von Ewon-Geräten zu vereinfachen.

Konto-Konsolidierung

Die Verwaltung mehrerer Konten mindert die Effizienz, da sie doppelten Aufwand erfordert.

- Konsolidieren Sie alle Ihre Ewon-Geräte in so wenigen Talk2M-Konten wie möglich (idealerweise nur ein Konto), um Ihren Wartungsaufwand zu reduzieren und Ihre Sicherheit zu erhöhen. Durch die Minimierung der Anzahl der zu erstellenden und zu verwaltenden Elemente (z. B. Benutzer, Gruppen und Pools) lässt sich auch die Wahrscheinlichkeit von Fehlern und Versäumnissen verringern.

Resilienz der Kontoverwaltung

Der Besitzer des Talk2M-Kontos (Hauptadministrator) sollte die Verantwortung dafür übernehmen, dass Best Practices auf dem Konto umgesetzt werden.

- Legen Sie mindestens zwei Benutzer mit Administratorrechten an, um das Risiko einer einzelnen Fehlerquelle im Falle des Ausscheidens eines einzelnen Administrators zu begrenzen.
- Nutzen Sie die „benutzerdefinierten Felder“, die für registrierte Geräte und Benutzer Ihres Talk2M-Kontos definiert werden können, indem Sie sie mit nützlichen Informationen füllen. Dies ermöglicht das Sortieren und Filtern nach einer größeren Anzahl von Kriterien und erhöht somit die Effizienz, indem es das Auffinden eines Geräts oder Benutzers erleichtert und gleichzeitig die Möglichkeit von Fehlern verringert.

  - *Beispiele für benutzerdefinierte Felder für Geräte: Gerätemodell, Kundenname, Land, Stadt, Standort.*
  - *Beispiele für benutzerdefinierte Felder für Benutzer: Team, Funktion, Qualifikationen, Region.*

3. Erstellung und Verwaltung von Benutzern

Benutzeridentifikation

Gemeinsame Benutzerkonten sollten unter allen Umständen vermieden werden, da sie die Verantwortlichkeit verhindern und zu großen Sicherheitsproblemen führen, wenn ein Mitarbeiter das Unternehmen verlässt.

- Erstellen Sie einen eindeutigen Benutzer für jede Person, die mit der Ewon-Lösung interagiert.

Authentifizierung:

Talk2M ermöglicht es Ihnen, Passwortrichtlinien zu konfigurieren, die alle Benutzer dazu zwingen, sichere Passwörter zu definieren.

- Definieren Sie Mindestanforderungen an die Passwortsicherheit.
- Konfigurieren Sie eine Gültigkeitsdauer für Passwörter, nach der diese ablaufen und geändert werden müssen.
- Aktivieren Sie die Zwei-Faktor-Authentifizierung für alle Benutzerkonten. Benutzernamen und Passwörter werden nicht mehr als ausreichende Authentifizierungsmethode anerkannt. Ein höheres Sicherheitsniveau bietet die Zwei-Faktor-Authentifizierung, bei der nicht nur das Wissen (Beispiel: ein Passwort), sondern auch der Besitz (Beispiel: eine Telefonnummer) nachgewiesen werden muss. Wenn die Anmeldeinformationen eines Benutzerkontos (Benutzername/ Passwort) durch eine Datenschutzverletzung kompromittiert wurden, kann das Konto durch Aktivierung der Zwei-Faktor-Authentifizierung geschützt werden.

Aufgabentrennung

Benutzer sollten nur Zugang zu Informationen oder Berechtigungen haben, die sie zur Erfüllung ihrer Aufgaben benötigen.

- Die meisten Benutzer sollten als Standardbenutzer mit eingeschränkten Rechten definiert werden.
- Verwenden Sie die Funktion „Benutzergruppe“ des Talk2M-Kontos, um Benutzerprofile zu definieren, denen bestimmte Berechtigungen, Zugriffsrechte und/oder Verwaltungsrollen zugewiesen werden. So ist es beispielsweise möglich, die Zugriffsrechte einer Benutzergruppe auf bestimmte Ewon-Gateways oder sogar auf bestimmte Geräte, die hinter diesen Ewon-Gateways verbunden sind, zu beschränken.
- Administratoren haben die Aufgabe, die Rechte und Berechtigungen anderer Benutzer zu verwalten. Daher sollte diese Aufgabe auf besonders vertrauenswürdige Personen innerhalb des Unternehmens beschränkt werden.
- Einigen Benutzern können begrenzte administrative Rollen zugewiesen werden, mit der sie berechtigt sind, bestimmte Gruppen von Benutzern oder Gerätepools zu verwalten.

Befristete Aktivierung von Benutzern

Um die Sicherheit weiter zu erhöhen, können Administratoren des Talk2M-Kontos Benutzer standardmäßig deaktivieren.

- Aktivieren Sie Benutzer Ihres Talk2M-Kontos nur dann, wenn sie eine Aufgabe ausführen müssen, z. B. eine Fernwartung einer Maschine, und deaktivieren Sie sie, sobald ihre Aufgabe erledigt ist.

4. Einsatz der Geräte

Planung der Installation von Geräten

In Kombination mit Talk2M ermöglichen Ewon-Gateways Fernzugriff auf Geräte, die auf ihrer LAN-Seite installiert sind. Die Installation und Konfiguration eines Ewon-Gateways muss entsprechend den Geräten erfolgen, auf die aus der Ferne zugegriffen werden soll.

- Installieren Sie ein Ewon-Gateway pro Maschine oder System (mit demselben Eigentümer), damit eine einfache und granulare Verwaltung der Zugriffsrechte möglich ist.
- Vermeiden Sie es, Zugriff auf ein ganzes Fabriknetzwerk einzurichten, da dies unter Sicherheitsgesichtspunkten nicht optimal ist und Zugriff auf einen sehr großen Bereich eröffnen würde, der die Verwaltung komplexer Benutzerzugriffsrechte erfordern würde.
- Um die Verwaltung der Benutzerzugriffsrechte zu vereinfachen, erstellen Sie eine kohärente Struktur von Pools von Ewon-Gateways (Beispiel: Gerätepools nach Region, Kunde oder Gerätetyp) und weisen Sie ein Ewon-Gateway immer dem bzw. den entsprechenden Pool(s) zu.

Konsistente Konfiguration von Geräten

Die Registrierung und Konfiguration von Geräten ist ein erster und wichtiger Schritt zu einer sicheren Einrichtung. Bei großen Installationen kann die manuelle Konfiguration jedes einzelnen Geräts lästig sein und zu Fehlern führen.

- Verwenden Sie keine Standard-Zugangsdaten und definieren Sie ein sicheres Passwort für den Zugriff auf die Konfigurationswebseite des Ewon-Gateways.
- Erwägen Sie, den globalen Registrierungsschlüssel Ihres Talk2M-Kontos zu verwenden, um eine gemeinsame Konfigurationsdatei zu erstellen, mit der Sie jedes neue Gerät mit geringem Aufwand und reduziertem Fehlerrisiko einrichten können. Diese gemeinsame Konfigurationsdatei kann auf einen USB-Stick oder eine SD-Karte kopiert und für die erste Initialisierung Ihrer Ewon-Gateways verwendet werden. Ein Talk2M-Administrator muss dann die Registrierung des neuen Geräts für das Konto genehmigen.

5. Fernverbindung zu Maschinen

Kontrolle der Remote-Konnektivität

Die Kontrolle der Remote-Konnektivität des Ewon-Gateways und des externen Zugriffs auf die Produktionsanlagen ist der Schlüssel zur Gewährleistung der Sicherheit und des Schutzes des Betriebs.

- Schließen Sie den digitalen Eingang eines Ewon-Gateways an einen Schlüsselschalter oder ein ähnliches Gerät an, mit dem Sie dann die VPN-Verbindung lokal aktivieren oder deaktivieren können.
- Alternativ kann die Konnektivität eines Ewon-Gateways oder eines Benutzers auch auf Cloud-Ebene gesteuert werden, indem Sie sie über Ihr Talk2M-Konto deaktivieren oder aktivieren.
- Um die Aufmerksamkeit und die Sicherheit des Bedienpersonals vor Ort zu verbessern, verwenden Sie den digitalen Ausgang des Ewon-Gateways (Produkt der neuen Generation) zum Anschluss einer Signallampe oder eines anderen Signalgebers. Die Anzeige leuchtet dann auf, wenn eine Fernverbindung aktiv ist.

Aufbau einer Fernverbindung

Einige bewährte Verfahren, bevor Sie eine Fernverbindung zu einem Gerät herstellen:

- Prüfen Sie, ob nicht bereits ein anderer Benutzer verbunden ist, indem Sie das Feld „Verbundener Benutzer“ in eCatcher überprüfen.
- Reservieren Sie bei Bedarf eine oder mehrere Verbindungen, um einer bestimmten Benutzergruppe Vorrang zu geben.

Beenden einer Fernverbindung

Einige bewährte Praktiken, wenn die per Fernzugriff durchgeführte Aktivität abgeschlossen ist:

- Lassen Sie einen Computer mit einer aktiven Fernverbindung nicht unbeaufsichtigt, um zu verhindern, dass Unbefugte einen Vorgang durchführen oder vertrauliche Informationen einsehen können.
- Beenden Sie die Verbindung, wenn der VPN-Tunnel nicht mehr benötigt wird.
- Dokumentieren Sie die per Fernzugriff durchgeführte Aktivität, z. B. mit der Logbuchfunktion von eCatcher. Dies ist nützlich, um den Überblick über Ihre Arbeit zu behalten und Informationen mit anderen Nutzern zu teilen.

6. Wartungsstrategie

Softwareupdates

In allen Informationssystemen können Schwachstellen entdeckt und dann von den Software- oder Hardwareanbietern entsprechend gepatcht werden. Anlagen, die nicht gepatcht sind, bieten potenzielle Sicherheitslücken für Hacker. Eine Risikominderung kann durch die Befolgung einiger einfacher Empfehlungen erreicht werden:

- Halten Sie die Firmware Ihrer Ewon-Gateways auf dem neuesten Stand.
- Halten Sie die Version Ihrer Ewon-Software, wie z. B. den Talk2M-Client eCatcher, auf dem neuesten Stand.
- Generell sollten Sie Ihre Ausrüstung (Computer, Mobilgeräte) auf dem neuesten Stand halten.
- Verwenden Sie ein Antivirenprogramm auf Ihrem PC.

Überwachung der Fernzugriffsnutzung

Die regelmäßige Einsichtnahme in die Verbindungsberichte und Protokolle gibt Ihnen einen guten Einblick in die per Fernzugriff durchgeführten Aktivitäten, die auf Ihrem Talk2M-Konto stattfinden.

- Überwachen Sie die Nutzungsmuster in Ihrem Team.
- Identifizieren Sie Geräte, die mehr Aufmerksamkeit benötigen.
- Vergleichen Sie die Nutzung des Datenverkehrs von Monat zu Monat, um wichtige Abweichungen zu erkennen.

Entfernung oder Anpassung von Zugriffsrechten

Es ist wichtig, dass Sie über effiziente Prozesse verfügen, um Benutzerregistrierungen und Zugriffsrechte systematisch anzupassen.

- Löschen Sie umgehend das Benutzerkonto eines Mitarbeiters, der Ihr Unternehmen verlässt.
- Überprüfen Sie regelmäßig Benutzer, Geräte und Berechtigungen (Gruppen- und Poolzuweisungen) und entfernen Sie übermäßige oder ungenutzte Rechte.

Überprüfung der Verfügbarkeit von Fernzugriff

Wenn ein Problem auftritt, das Unterstützung erfordert, ist höchste Reaktivität erforderlich, um sofort mit der Remote-Fehlersuche zu beginnen.

- Richten Sie Routinen ein, um regelmäßig zu überprüfen, ob Sie eine Verbindung zu Ihren Geräten herstellen können, insbesondere bei Ewon-Gateways, die keine permanente Verbindung zu Talk2M haben (Beispiel: VPN ist standardmäßig deaktiviert und wird über einen Schlüsselschalter aktiviert).

7. Organisatorische Maßnahmen

Dokumentation der Verwaltung von Fernzugriff

Die Fernzugriffslösung von Ewon ist ein wichtiges Element in Ihrem Unternehmen und sollte professionell beschrieben und verwaltet werden. Eine erfolgreiche Einführung und Kundenakzeptanz kann durch umfassende Prozesse und Materialien für die Kommunikation mit Partnern und Kunden erleichtert werden.

- Dokumentieren Sie Ihr Talk2M-Konto, die Liste der Geräte und die Benutzerorganisation.
- Erstellen Sie Prozesse und Richtlinien für interne/externe Benutzer der Lösung.

Kontrollmaßnahmen

- Überprüfen Sie regelmäßig, ob Ihre Dokumentation auf dem neuesten Stand ist und ob Ihre Richtlinien innerhalb Ihrer Organisation befolgt werden.

Schulung und Sensibilisierung

Mitarbeiter sollten sich der Bedeutung der Informationssicherheit und der Risiken bewusst sein, die sich aus einer mangelhaften Umsetzung von Sicherheitsmaßnahmen ergeben.

- Klären Sie Ihre Mitarbeiter über Sicherheit auf und schulen Sie sie in der Befolgung der Best Practices.

Weitere Einzelheiten zur Konfiguration eines Talk2M-Kontos finden Sie auf der Supportwebsite von Ewon: https://www.ewon.biz/technical-support/pages/talk2m/talk2m-service?ordercode=talk2m

Anwendung von Best Practices

Nachfolgend finden Sie eine Liste der von unserer Organisation umgesetzten Best Practices, um die effiziente und sichere Nutzung der Ewon-Lösung zu gewährleisten:

#	Thema		Anmerkungen zur Umsetzung
1	Governance	• Konsistenz der Lösung	
2	Erstellung und Struktur eines Kontos	• Struktur des Kontos • Konto-Konsolidierung • Resilienz der Kontoverwaltung	
3	Erstellung und Verwaltung von Benutzern	• Benutzeridentifikation • Authentifizierung: • Aufgabentrennung • Befristete Aktivierung von Benutzern	
4	Einsatz der Geräte	• Planung der Installation von Geräten • Konsistente Konfiguration von Geräten	
5	Fernverbindung zu Maschinen	• Kontrolle der Remote-Konnektivität • Aufbau einer Fernverbindung • Beenden einer Fernverbindung	
6	Wartungs-strategie	• Softwareupdates • Überwachung der Fernzugriffsnutzung • Entfernung oder Anpassung von Zugriffsrechten • Überprüfung der Verfügbarkeit von Fernzugriff	
7	Organisatorische Maßnahmen	• Dokumentation der Verwaltung von Fernzugriff • Kontrollmaßnahmen • Schulung und Sensibilisierung	