Erweiterte Sicherheit für industrielle Netzwerke

Transparenz, sichere Authentifizierung und punktgenaue Zugriffsteuerung in unternehmenskritischen Netzwerken

WHITE PAPER

Autoren: Prof. Dr. Tobias Heer, Alexander Austein

Die Bedrohungsszenarien für industrielle Netzwerke verändern sich fortwährend. Neue Angriffsvektoren und -methoden tauchen auf und die Betreiber von Automatisierungsnetzwerken (Operational Technology, OT) bemühen sich, deren Sicherheit zu erhalten und zu verbessern. Darüber hinaus stellen neue Normen und Regularien die Betreiber von OT-Netzwerken vor zusätzliche Herausforderungen.

Insbesondere der Kontrolle über die im Netzwerk befindlichen Geräte und deren Kommunikation kommt dabei eine zentrale Rolle zu. Moderne Ansätze zur Netzwerkzugangskontrolle (Network Access Control – NAC) sind heute daher ein entscheidender Baustein in jedem Netzwerk- und Sicherheitskonzept.

In diesem Whitepaper wird eine leistungsstarke Möglichkeit zur Umsetzung eines solchen NAC-Konzepts, bestehend aus macmon NAC und Industrial Ethernet Switches von Hirschmann, vorgestellt.

HIRSCHMANN
A BELDEN BRAND

macmon nac

Neue Herausforderungen für die Cybersicherheit in unternehmens-kritischen Netzwerken

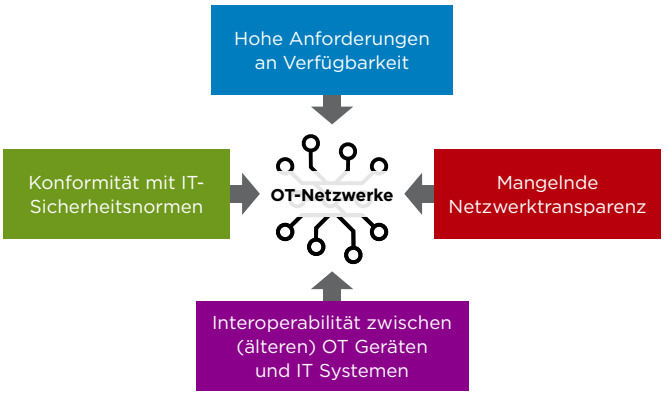
OT-Netzwerke befinden sich heute mehr und mehr im Umbruch. Ehemals geschlossene und relativ unzugängliche Netzwerke werden zunehmend mit dem Internet verbunden und öffnen sich anderen Unternehmensbereichen. Die Treiber dieser Entwicklung sind neue Anwendungen und Produkte, welche Einzug in die OT-Netzwerke gehalten haben. Ein einfaches Beispiel hierfür ist die heute fast allgegenwärtige Fernwartung und Fernüberwachung von Produktionsmaschinen.

OT-Netzwerke befinden sich heute mehr und mehr im Umbruch. Ehemals geschlossene und relativ unzugängliche Netzwerke werden zunehmend mit dem Internet verbunden und öffnen sich anderen Unternehmensbereichen.

Als weiteres Beispiel kann die Aggregation von Sensordaten aus der Feldebene genannt werden. Diese Aggregation ist für die Optimierung und Planung von Produktionsprozessen unerlässlich. Schlussendlich trägt auch der heutige Trend zur Unterstützung und Koordination von Produktionsprozessen und -mitteln durch Cloud-Dienste zur Öffnung der Netzwerke bei: Viele moderne in der Fertigung eingesetzte Produkte lassen sich nicht mehr ohne eine Verbindung zur Cloud im Intranet oder Internet betreiben. Leistungsfähige Anlagen benötigen daher vielfältige zusätzliche Verbindungen zwischen bisher meist unverbundenen Netzwerkteilen. In der Summe lässt sich in vielen Industrieanlagen ein Wandel von stark begrenzter lokaler Kommunikation hin zu weitreichenderer oder sogar globaler Kommunikation beobachten.

Die zunehmende Vernetzung von OT-Netzwerken mit der IT- und IoT-Welt, führt jedoch auch zu zusätzlichen Angriffsflächen. Um auf diese neuen Anforderungen und Bedrohungen zu reagieren, sind die Betreiber von OT-Netzwerken gezwungen, bewährte Best-Practices in der OT-Sicherheit zu überdenken. Einfache und früher wirksame Sicherheitsmethoden, wie der Perimeter-Schutz durch eine zentrale Firewall und der sprichwörtliche „Air Gap", also die vollständige Trennung des OT-Netzwerks von allen anderen vernetzten Ressourcen, sind nicht mehr praktikabel oder ineffektiv. Gezielte Angriffe auf Industriestandorte mit Malware wie Stuxnet, BlackEnergy und Industroyer können mithilfe infizierter Geräte oder USB-Medien den „Air Gap" überwinden.
Auch herkömmliche IT-Malware, wie Wannacry oder gezielte Ransomware Angriffe wie die Serie von HIVE-Angriffen, richten regelmäßig in OT-Netzwerken auf der ganzen Welt hohe Schäden an.
Insbesondere die Welle von Ransomware-Angriffen, die in den letzten Jahren über die deutschen Industriebetriebe hereingebrochen ist, verdeutlicht hier den Handlungsbedarf eindrücklich.

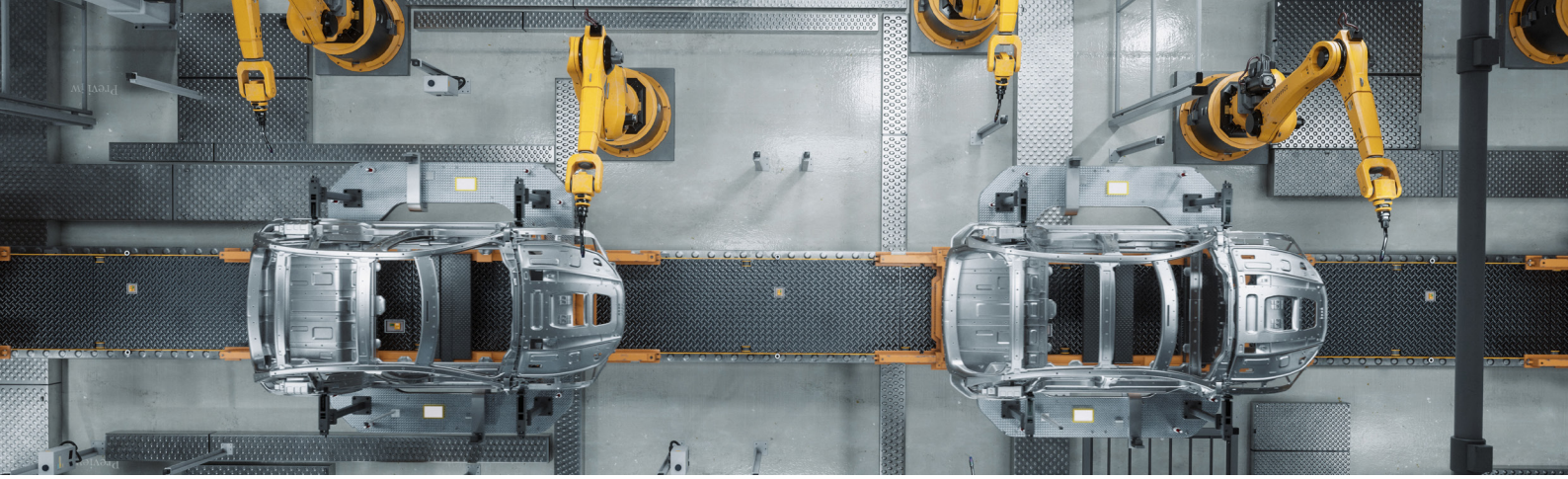
Bei der Umsetzung neuer Sicherheitsmaßnahmen stehen die Betreiber von OT-Netzwerken in der Regel vor vier großen Herausforderungen:



Herausforderung 1:

Mangelnde Netzwerktransparenz

Betreiber von bestehenden OT-Netzwerken haben oftmals Probleme aufgrund einer unzureichenden Transparenz ihrer Netzwerke. Insbesondere bei gewachsenen Netzen sind nicht immer alle Kommunikationsbeziehungen und -teilnehmer bekannt. Angreifer und deren Datenverkehr fallen so oftmals nicht oder zu spät auf. Selbst wenn alle Teilnehmer und deren Verkehr im OT-Netzwerk bekannt sein sollten, lässt sich eine Konformität des tatsächlichen Verkehrs mit den bekannten Verkehrsmustern ohne geeignete Werkzeuge praktisch nur schwer erzwingen: Zu vielfältig ist das Verhalten der Geräte und zu kleinteilig sind die Regeln, die sich daraus ergeben.
In größeren OT-Netzwerken herrscht zudem eine hohe Fluktuation an Netzwerkteilnehmern.
Viele Wartungsprozesse werden von den Betreibern immer noch manuell oder als Teil eines Wartungsvertrags mit ihren Gerätelieferanten durchgeführt.
Diese Lieferanten verwenden oft unterschiedliche mobile Systeme, um die Wartungsarbeiten durchzuführen. Darüber hinaus können „kreative" Lösungen und schnelle Problembehebungen zu einer beträchtlichen Anzahl von versteckten oder unbekannten



Geräten in der Fertigung führen. Diese sogenannte „Schatten-IT“ hat häufig unzureichende Sicherheitseinstellungen und verwendet veraltete Software mit bekannten Schwachstellen. Diese schwer kontrollierbaren IT-Landschaften in der OT stellen daher eine potenzielle Bedrohung dar und müssen überwacht und beherrscht werden.

Gegenmaßnahme:
Eine Netzwerkzugangssteuerung kann nicht nur den Netzwerkzugriff einschränken, sondern dem Administrator auch einen detaillierten Überblick über die Geräte im Netzwerk und deren Anbindung an dieses verschaffen. Das betrifft sowohl Geräte die gerade aktiv verbunden sind als auch Geräte, die zuvor mit dem Netzwerk verbunden waren oder nur sporadisch verbunden sind. Allein das Wissen um das Vorhandensein von Geräten ist jedoch nicht ausreichend. Auch die Identität der Geräte muss festgestellt werden. Für beide Problemstellungen (finden von Geräten und deren Identifikation) kann NAC einen entscheidenden Beitrag liefern.

Je nach Art der NAC-Lösung und je nach Fähigkeit der Geräte, kann die Bewertung der Identität eines Geräts auf starken individuellen Passwörtern und Zertifikaten basieren und sogar den inneren Zustand der Geräte berücksichtigen. So können z.B. durch das NAC-System weitere Prüfungen auf Endgeräten durchgeführt werden, um Systemeigenschaften, wie z.B. den Status der Antivirus-Definitionsdateien oder der Konfiguration des Geräts, festzustellen und darzustellen. Da sich in Industrieanlagen oftmals eine Mischung aus älteren und sehr heterogenen Geräten befindet, ist es wichtig, auch die Identität solcher Geräte möglichst sicher festzustellen.
Eine Überwachung des Netzwerk-Fußabdrucks (zum Beispiel die geöffneten Ports oder Zertifikate der Konfigurationsschnittstellen) kann solche zusätzlichen Identitätsinformationen liefern.
Das erlaubt einen tieferen Einblick in den Sicherheitsstatus eines Netzwerks und eine robustere Identifikation seiner Teile. Zusätzlich zur Überwachung der Endgeräte können auch die Switches in der Anlage Informationen zu den angeschlossenen Geräten und deren Verhalten liefern. So können nicht identifizierte Geräte schnell lokalisiert und Änderungen im Netzwerk präzise eingegrenzt werden.
Die Kombination solcher Funktionen mit industriegerechten OT-Switchen und -Routern sorgt für wichtige Transparenz, bis in den Produktionsbereich, wo potenzielle Angreifer andernfalls unautorisierte Geräte anschließen oder bestehende Geräte kompromittieren könnten.

Herausforderung 2:

Interoperabilität zwischen (älteren) OT-Geräten und IT-Systemen

Neuere OT-Geräte bieten aktuelle Netzwerksicherheitsprotokolle und -funktionen und lassen sich so einfach in moderne Netzwerksicherheitskonzepte integrieren. Zahlreiche Unternehmen haben jedoch auch eine große Anzahl von Geräten, die noch aus Zeiten stammen, in der Netzwerksicherheit für OT-Netzwerke eine untergeordnete Rolle spielte.
Ein Austausch dieser Geräte steht jedoch meistens nicht zur Debatte, da Automatisierungsgeräte jahrzehntelang betrieben werden, um eine solide Kapitalrendite zu erzielen. Die sich daher zwangsläufig ergebende Mischung aus Neu- und Alt-Geräten, macht die Umsetzung eines einfachen und einheitlichen Sicherheitskonzepts schwierig und führt oft zu verminderter Sicherheit, da moderne Sicherheitskonzepte ohne Geräteunterstützung nicht oder nur teilweise umgesetzt werden können.
Heute werden in Industrieanlagen vermehrt Endgeräte und Netzwerkkomponenten eingesetzt, die für IT-Umgebungen entwickelt wurden.
Diese verfügen jedoch nicht über wichtige industrielle Funktionen. Hierzu gehören Mechanismen zur Steigerung der Zuverlässigkeit und Redundanz, die in unternehmenskritischen Netzwerken von entscheidender Bedeutung sind. Für den Einsatz in rauen Industrieumgebungen werden zudem Produkte benötigt, die den teils hohen physischen Anforderungen (zum Beispiel Vibration und Temperatur) widerstehen. Durch die lange Lebensspanne einer Anlage verschärft sich die Situation weiter:

Viele IT-Hersteller bieten keine oder nur kurze Zusagen für die Verfügbarkeit ihrer Produkte und Software-Updates. Deshalb können IT-Geräte früher ausfallen als langlebige Automatisierungsgeräte. Ihr Austausch wird immer schwieriger, je länger eine Anwendung in Betrieb ist. Ohne die richtige Auswahl der Geräte und ein Augenmerk auf tatsächlich verfügbare Funktionen entwickelt sich daher ein schwer zu beherrschender „Zoo“ aus verschiedensten Geräten und Gerätegenerationen. Dies erschwert die Verwaltung und Gewährleistung der Sicherheit in einer Anlage signifikant.

Gegenmaßnahme:
Während moderne Endgeräte Authentifizierungsprotokolle wie IEEE 802.1X unterstützen, können ältere Endgeräte oft nur über ihre MAC-Adresse identifiziert werden. Eine effektive Netzwerkzugangskontrolle muss deshalb unterschiedliche Authentifizierungsoptionen unterstützen. Zeitgemäße NAC-Lösungen nehmen daher die Authentifizierung der verschiedensten Geräte automatisch vor und abstrahieren vom konkreten Mechanismus. Administratoren können so allgemeine Richtlinien für den Netzwerkzugriff festlegen und sich auf die Verfügbarkeit des Netzwerks konzentrieren, anstatt sich um die verschiedenen Authentifizierungsmethoden für einen heterogenen „Zoo“ aus OT-Endgeräten zu kümmern.
Authentifizierung allein genügt jedoch nicht, um eine angemessene Sicherheit des Netzwerks zu erreichen. Eine durch die Authentifizierung getroffene Zugriffsentscheidung muss auch korrekt umgesetzt werden. Dies sollte so nahe wie möglich an den industriellen Anlagen erfolgen, also in der Feldebene oder der Fabrikhalle, dem Shop-Floor. Deshalb sind leistungsstarke industrielle Switches erforderlich, die optimal in das NAC-System integriert sind. Hirschmann und macmon setzten hier auf eine enge Kooperation, um eine bestmögliche Unterstützung zu gewährleisten. Durch die hohe Kompatibilität von macmon NAC mit verschiedensten Hirschmann Geräten und durch unterschiedliche unterstützte Schnittstellen zu verschiedenen Switches (z.B. RADIUS, SNMP, SSH, telnet, etc), ist eine nachträgliche Einführung von macmon NAC in einer Industrieanlage fast immer ohne einen Austausch der vorhandenen Netzwerk-Hardware möglich.

Herausforderung 3:
Konformität mit IT-Sicherheitsnormen
Die Funktion des industriellen Prozesses, sowie die Datensicherheit, haben in Industrie- und Versorgungsunternehmen oberste Priorität und sind stark reguliert. Mit den neuesten Anforderungen und dem

sich ständig wandelnden Stand der Technik Schritt zu halten, ist für die Betreiber von OT-Netzwerken in vielen Industriebranchen zu einer großen Herausforderung geworden. Dieser Umstand konfrontiert Unternehmen mit schwer planbaren Investitionen in die IT-Sicherheit.

Die Erfassung der Compliance des Netzwerks und der enthaltenen Geräte ist ein wichtiger Aspekt vieler Sicherheitsstandards. Ebenso ist es wichtig, auf Abweichungen wie z.B. der Verbindung eines unbekannten Gerätes mit dem Netzwerk oder der Verletzung von Policies (z.B. aufgrund eines abgelaufenen Virenschutzes oder nicht konformer Kommunikation) effektiv zu reagieren und das Netzwerk wieder in einen definierten Zustand zu überführen. Eine effektive Netzwerkzugangskontrolle ist ein wichtiger Baustein hierfür, da sie nicht nur den Zugriff auf das Netzwerk beschränken kann, bevor ein infiziertes oder unbefugtes Gerät in das Netzwerk kommt, sondern auch fortwährend dessen Sicherheit bewerten und Folgeaktionen durchführen kann. Diese Funktionen können von einer zeitnahen Benachrichtigung des Administrators bis hin zur vollständigen Isolierung eines verdächtigen Geräts im Netzwerk reichen. Grundsätzlich hängt in industriellen Netzwerken die Auswahl der Maßnahmen jedoch immer von der erforderlichen Verfügbarkeit des jeweiligen Geräts ab und sollte deshalb von Fall zu Fall getroffen werden. Moderne NAC-Systeme erlauben die Definition verschiedener Reaktionen für unterschiedliche Gerätegruppen, um in allen Situationen schnell und angemessen reagieren zu können.

Ein weiteres wichtiges Sicherheitskonzept ist die Segmentierung eines industriellen Netzwerks in getrennte Funktionsbereiche, sogenannte Zonen.

Diese Segmentierung ist ein zentraler Aspekt der weithin akzeptierten ISO/IEC 62443 Standards [3] sowie anderer wichtiger Normen für die industrielle Sicherheit. Die Sicherheitszonen isolieren verschiedene unabhängige Bereiche einer Anlage voneinander. In der Regel werden Zonen als physikalisch getrennte Netzwerke oder logisch getrennte VLANs [4] umgesetzt. Die Trennung der Zonen lassen sich durch Firewalls oder Switches mit sehr restriktiven Regeln und Access Control Lists (ACLs) implementieren. Je feingranularer und präziser diese Segmentierung erfolgt, desto geringer sind die Bewegungsmöglichkeiten eines Angreifers nach einem erfolgreichen Eindringen in das Netzwerk.
In der Praxis gestaltet sich eine feingranulare Segmentierung jedoch aufwändig und zeitintensiv, insbesondere wenn viele Geräte und deren Zugangsberechtigungen berücksichtigt werden müssen.

Gegenmaßnahme:
Ohne technische Unterstützung lässt sich ein feingliedriges und dauerhaft tragfähiges Zonenkonzept nur mit viel Aufwand realisieren. Netzwerkzugangskontrolllösungen haben sich daher auf die technische Unterstützung dieses Vorgangs spezialisiert.
Zum einen lassen sich mit ihnen sehr einfach Zonen durch VLANs definierten, welche die NAC-Software bedarfsgerecht und gerätespezifisch automatisch zuweisen kann. Darüber hinaus lassen sich Geräte anhand ihrer Merkmale zu Gruppen zuweisen, welche einheitlich behandelt werden können. Eine individuelle und oft repetitive Konfiguration verschiedenster Geräte kann so vermieden werden.

In der Vergangenheit wurde in unternehmenskritischen Netzwerken häufig die Verfügbarkeit über die Sicherheit der Daten gestellt. Diese Vorgehensweise ist mittlerweile überholt.

Zusätzlich zur NAC-Lösung bedingt die Umsetzung auch leistungsstarke industriegerechte Firewalls und Switches mit Access Control Lists und modernen Endpunkt Authentifizierungsfunktionen, wie IEEE 802.1X, um die Vereinfachungen durch das NAC-System effizient umsetzen zu können. So können die durch das NAC-System definierten Zuweisungen auch auf Feldebene direkt bei den Endgeräten erzwungen und realisiert werden.

Älteren Industrieanlagen, deren Netzwerkinfrastruktur und Endgeräte oft kein 802.1X unterstützen, sollte eine moderne Netzwerkzugangskontrolle auch Alternativen zur Zonen- beziehungsweise VLAN-Zuweisung durch 802.1X bieten. Ein hybrider Betrieb aus SNMP-Konfigiration der Switches mit Regeln für Endgeräte (SNMP NAC) und 802.1X/Radius ist dafür notwendig. SNMP als generisches Netzwerkmanagement-Protokoll erlaubt die Rekonfiguration der Switches im Netzwerk, um eine Zuweisung eines Endgeräts zu einer Zone (also einem VLAN) ohne 802.1X zu bedingen. Da SNMP in Industrienetzwerken weit verbreitet ist, können so auch ältere Netzwerke mit Hilfe einer NAC-Lösung ein dynamisches und effizientes Zonenkonzept umsetzen.

Da die Umsetzung der Zonenzuweisung am äußersten Rand des Netzwerks, also auf dem Shop-Floor, erfolgt, müssen Switches, Access Points und Firewalls nicht nur die genannten Sicherheitsfunktionen, sondern auch die branchenüblichen industriellen Redundanzverfahren wie z.B. das Parallel Redundancy Protocol (PRP) oder das Media Redundancy Protocol (MRP) unterstützen. Die Wahl dedizierter Industriegeräte ermöglicht hier sowohl hochverfügbare Redundanz als auch zeitgemäße Zugriffskontrolle. Durch die nahtlose Integration von industrieller Kommunikations-Hardware in die Netzwerkzugangskontrolle werden die erforderlichen Komponenten bereitgestellt, um die Anforderungen der wichtigen industriellen Standards zu erfüllen.

Herausforderung 4:

Hohe Anforderungen an Verfügbarkeit
Der Ausfall eines unternehmenskritischen OT-Netzwerks führt in der Regel dazu, dass auch wichtige Unternehmensprozesse ausfallen. Die Folgen können nicht nur Produktionseinbußen, sondern auch verärgerte Kunden, Notfallreparaturkosten und aufsichtsrechtliche Bußgelder sein. In der Vergangenheit wurde deshalb in unternehmenskritischen Netzwerken häufig die Verfügbarkeit über die Sicherheit der Daten gestellt. Diese Vorgehensweise ist mittlerweile überholt. Die Betreiber von OT-Netzwerken haben erkannt, dass nur die Kombination aus Verfügbarkeit und Sicherheit langfristig zu Erfolg und Kundenbindung führen kann.

Da die Maschinen eine hohe Gesamtanlageneffektivität erreichen müssen, ist oft keine Zeit für Updates und Patches, die einen Neustart des Geräts erfordern. In einer Fertigungslinie ist es teilweise sogar unmöglich, dass nur bestimmte Teile des Netzwerks oder einzelne Maschinen offline gehen. Eine weitere große Sorge der Betreiber besteht darin, dass zusätzliche Sicherheit die Zuverlässigkeit und Verfügbarkeit des Netzwerks beeinträchtigen könnte.

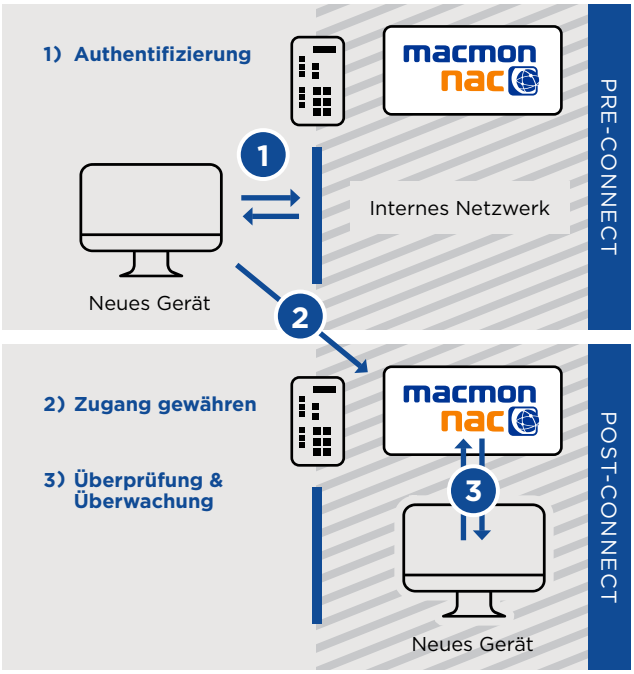
Gegenmaßnahme:
In den letzten Jahrzehnten haben industrielle Ethernet Netzwerke ein hohes Maß an Verfügbarkeit und Zuverlässigkeit erreicht. Mit dem Aufkommen redundanter Ringstrukturen und Punkt-zu-Punkt-Verbindungen (MRP und PRP), in Kombination mit der redundanten Übertragung von Frames, sind Ausfallszeiten von 0 Millisekunden Realität geworden.

Switches und Infrastrukturkomponenten wurden jedoch speziell unter dem Gesichtspunkt der Verfügbarkeit entwickelt. Da die einzige Aufgabe vieler dieser Geräte darin besteht, die Stabilität des Netzwerks auf einem hohen Niveau aufrechtzuerhalten, sind zusätzliche Sicherheitsanforderungen oft nicht berücksichtigt worden. Um ein bestehendes hochverfügbares Netzwerk zu modernisieren oder ein unternehmenskritisches Netzwerk für die heutigen Sicherheitsanforderungen auszulegen, ist spezielle Netzwerk-Hardware erforderlich. Diese muss sowohl den Anforderungen der Zuverlässigkeit als auch der Sicherheit gerecht werden. Darüber hinaus müssen die Switches in moderne Lösungen für die Netzwerkzugangskontrolle integrierbar sein.
Durch moderne industrielle Netzwerk-Hardware wie z.B. die Industrial Ethernet Switches und IP-Router von Hirschmann und die Kombination mit der Netzwerkzugangskontrolle von macmon secure, ermöglicht fortschrittliche Sicherheitsmechanismen in der gesamten Netzwerkinfrastruktur.
Dies gilt von der Feldebene einer Fabrikhalle bis zum Backbone Netzwerk eines lokalen industriellen Rechenzentrums. Die Kombination äußerst zuverlässiger industrieller Switches auf Feldebene und einer hochmodernen Softwarelösung ermöglicht maßgeschneiderte Sicherheitsfunktionen für die verschiedenen Bereiche eines unternehmenskritischen Netzwerks.

Die Rolle der Netzwerkzugangskontrolle in der IT- und OT-Sicherheit

Die Netzwerkzugangskontrolle besteht aus einer Reihe von Technologien, mit denen Richtlinien umgesetzt werden, die den Zugriff auf die Unternehmensinfrastruktur steuern.

Prinzipiell kann der Vorgang der Netzwerkzugangskontrolle in zwei Phasen aufgeteilt werden, die aufeinander aufbauend oder unabhängig einzeln angewendet werden können. Diese Phasen sind „Pre-Connect“ und „Post-Connect“ und finden entweder statt *bevor* eine Kommunikation eines neu ins Netzwerk eingetretenes Gerät im Netzwerk kommunizieren kann oder *nachdem* das Gerät ins Netzwerk aufgenommen wurde. Moderne Lösungen für die



Netzwerkzugangskontrolle sollten beide Phasen bzw. Ansätze unterstützen, da sie spezifische Vorteile und Einschränkungen haben.

Pre-Connect: Es wird die Identität eines Geräts überprüft, bevor es eine Verbindung zum Netzwerk herstellen kann. Damit wird geregelt, ob ein Gerät auf das Netzwerk zugreifen darf und welche Rechte und Funktionen es dort hat. Vor einer erfolgreichen Prüfung ist technisch nur eine Kommunikation mit dem Authentifizierungsserver möglich.
Diese Art der Netzwerkzugangskontrolle basiert meist auf dem Netzwerkauthentifizierungsstandard IEEE 802.1X [1] in Kombination mit Authentifizierungsservern wie RADIUS [2].

Post-Connect: Nachdem das Gerät im Netzwerk zugelassen wurde, wird die Identität des Geräts oder weitere Eigenschaften geprüft. Somit können Geräte und deren Verhalten überwacht werden, nachdem die Verbindung zum Netzwerk hergestellt wurde. Wird bei einer nachgeschalteten Überprüfung festgestellt, dass das Gerät nicht mehr den erforderlichen Sicherheitsstandard genügt oder sich nicht wie erwartet verhält, kann es beispielsweise (automatisiert) aus dem Netzwerk entfernt oder isoliert werden.
Post-Connect kann auch ähnlich zum Pre-Connect Verfahren eingesetzt werden. In diesem Fall wird das Gerät nicht direkt ins Produktivnetzwerk gelassen, sondern bekommt nur Zugriff auf ein isoliertes Netzwerk. In diesem Netzwerk kann dann der Zustand und die Identität geprüft werden.
Erst nach erfolgreicher Überprüfung wird das Gerät dem Produktivnetzwerk zugewiesen. Damit können auch Geräte ohne technische Unterstützung für

Pre-Connect Verfahren wie IEEE 802.1X vor der Integration ins Netzwerk geprüft werden.

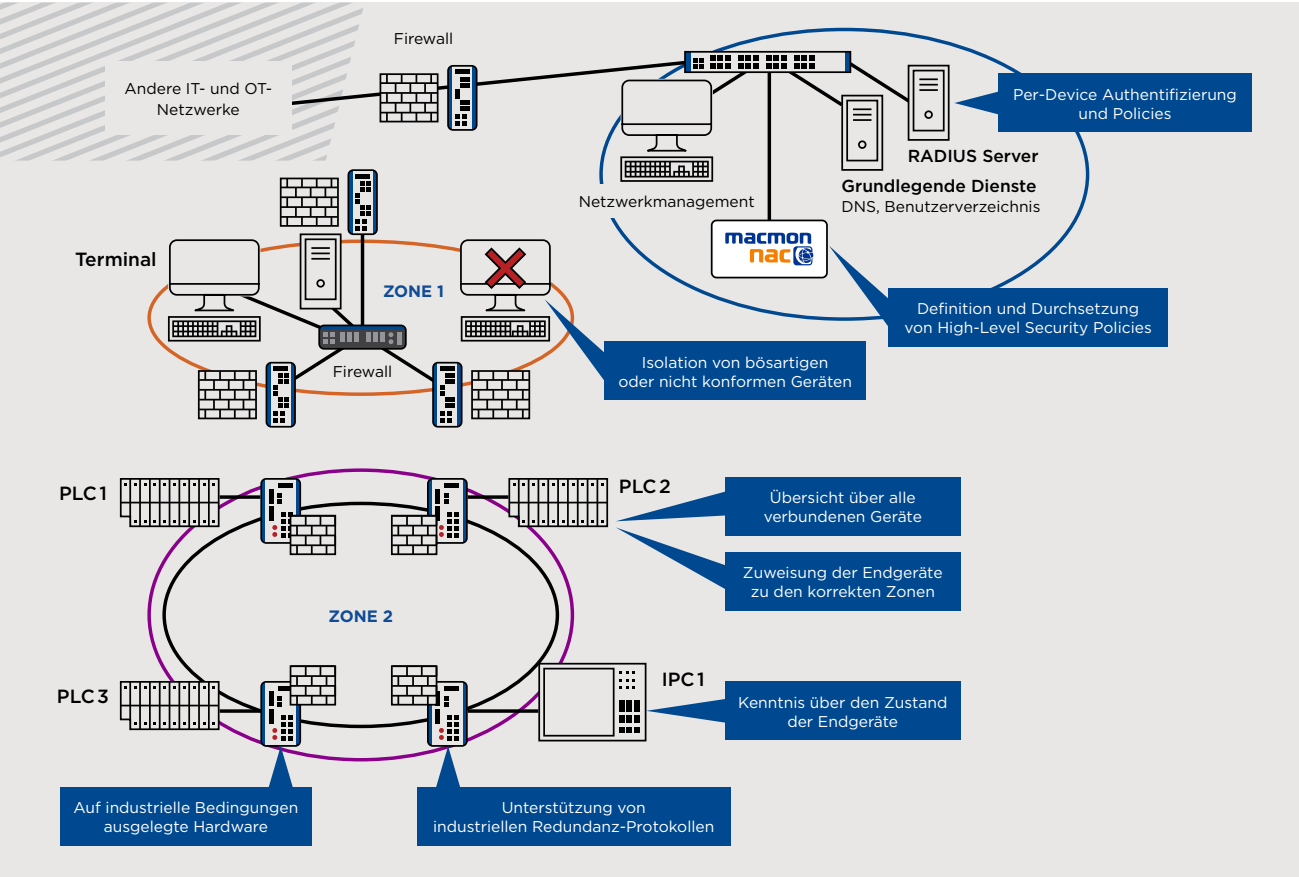
Besonders für Industriegeräte, bei denen die Unterstützung von IEEE 802.1X eher die Ausnahme als die Regel darstellt, ist ein Post-Connect Ansatz daher oft unerlässlich. Neben traditionellen Anwendungsfällen wie der unternehmensweiten Transparenz von Geräten, Gastgeräte-Zugriffsmanagement und Endpunktkonformität, sollte eine moderne Netzwerkzugangskontrolle auch die Möglichkeit bieten, Dritthersteller Sicherheits- und IT-Lösungen zu integrieren. Bei macmon und Hirschmann ist das bereits Alltag. Informationen können nahezu in Echtzeit bi-direktional ausgetauscht werden. Dazu zählen beispielsweise Firewalls, Intrusion-Detection und -Prevention, Deep Packet Inspection, Asset Management, Identity und Access Management. Insbesondere die Ermittlung von IoT-Geräten und das Asset Management, sowohl von IT- als auch OT-Geräten, gewinnt zunehmend an Bedeutung.

Die Lösung von Hirschmann und macmon im Überblick

Durch immer kürzere Innovationszyklen und die Forderung, neue Technologien einzuführen, ohne die Sicherheit zu beeinträchtigen, wird Agilität in OT-Netzwerken zu einem Schlüsselfaktor. Um den zuvor beschriebenen Herausforderungen gerecht zu werden, benötigen Sicherheitsexperten eine Lösung, die das Sicherheitsrisiko minimiert und gleichzeitig Transparenz und ein effizientes Arbeiten ermöglicht. Gleichzeitig muss die Lösung auch vorhersehbar und kontrollierbar sein.

> Mit dem voreingestellten macmon NAC-Regelwerk funktioniert die Konfiguration und Verwaltung der Netzwerkzugänge „out of the box“. Komplexe Richtlinien müssen in der Regel nicht erstellt werden.

Dies bedeutet, dass weder die Fertigung in der Fabrik noch in einer anderen Betriebsstätte eines Unternehmens im Betrieb gestört werden darf. macmon secure und Hirschmann kooperieren eng, um eine optimale Lösung mit höchstmöglicher Kompatibilität zwischen der NAC-Lösung und den industriellen Netzwerkgeräten zu bieten. Das Ziel dieser Kooperation ist, eine möglichst



Die obige Abbildung zeigt die Komponenten und einige Vorteile der integrierten Lösung

reibungsfreie Integrierbarkeit der NAC-Lösung ohne Zwischenfälle sicherzustellen.

macmon NAC übernimmt die Konfiguration und Verwaltung der Netzwerkzugänge. Damit lässt sich die Identität der Geräte einfach erkennen und es können regelbasiert verschiedene Zonen bzw. VLANs konfiguriert werden. Mit dem voreingestellten macmon NAC-Regelwerk funktioniert das „out of the box". Komplexe Richtlinien müssen in der Regel nicht erstellt werden. Die Durchsetzung der Richtlinien erfolgt durch die Hirschmann-Geräte im Produktionsbereich und an den Netzwerkzugangspunkten. Hirschmann ist mit seiner langjährigen Erfahrung bei industriellen Netzwerken einzigartig positioniert, um die Sicherheit innerhalb der spezifischen Rahmenbedingungen einer industriellen Umgebung unter Beibehaltung der Anlagenverfügbarkeit effektiv umzusetzen.

Autorisierte Geräte lassen sich beispielsweise anhand ihrer MAC-Adresse, gerätespezifischen Zugangsdaten oder Zertifikaten identifizieren, bevor sie automatisch ihren jeweiligen Sicherheitszonen zugeordnet werden. Dadurch ist es möglich die Forderung nach einem fein abgestuften Zonenkonzept zu erfüllen.

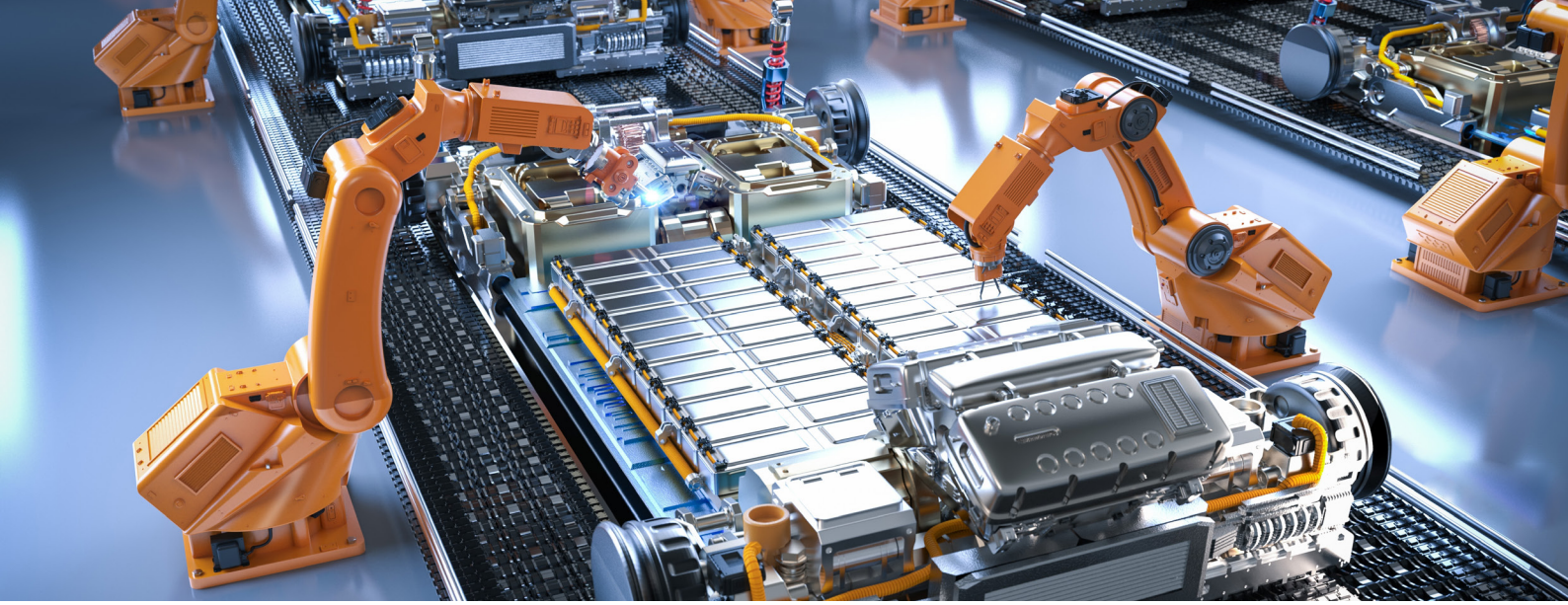
Unautorisierten Geräten wird standardmäßig der Netzwerkzugriff verweigert, alternativ können sie in Quarantäne Zonen verschoben werden.
Zusätzlich können Endgeräte mittels nachgelagerter Checks überprüft werden. Eigenschaften der Endgeräte, wie Domain-Zugehörigkeit und Art des Betriebssystems werden als zusätzliche Kriterien verwendet. Erfüllen Endgeräte die Sicherheitsvorgaben nicht, kann darauf automatisch reagiert werden. OT-Administratoren können beispielsweise per E-Mail, Syslog und weiteres informiert werden, um geeignete Maßnahmen zu ergreifen.
Eine vollständige Isolation des Endgerät ist in OT-Umgebungen typischerweise nicht erwünscht, da das Endgerät weiterhin seinen eigentlichen Zweck in der Anlage erfüllen soll. Um die Angriffsfläche zu verringern, könnte das Endgerät aber in ein spezielles VLAN verschoben werden, das als „Einbahnstraße" fungiert.
Zugriffe aus diesem VLAN auf andere Geräte der Anlage sind so weiterhin möglich, Zugriffe auf das verwundbare Gerät werden jedoch unterbunden.

Mehrere Eigenschaften machen die Lösung von macmon und Hirschmann gegenüber anderen Netzwerkzugangslösungen überlegen. Diese Eigenschaften bieten Industriekunden deutliche Vorteile.

Die Verwaltung des Netzwerkzugangs kann nur dann effektiv sein, wenn sie an den richtigen Stellen im Netzwerk umgesetzt wird. Die Sanktionierung muss in den meisten Fällen direkt dort erfolgen, wo der erste Switch oder Access Point eine Verbindung zu den Endgeräten herstellt. Eine gute Integration der NAC-Lösung und der Switches auf Feldebene ist daher sehr wichtig. In industriellen Anwendungen müssen diese Feldebenen-Switches hochwertige industriegerechte Switches sein, die extremen Temperaturen, Vibrationen und elektromagnetischen Störungen widerstehen. Zudem sind häufig spezielle Industrieprotokolle erforderlich.
Die industrielle Kommunikations-Hardware sollte auch aktuelle Sicherheitsmechanismen, wie IEEE 802.1X und Paketfilterung, auf dem neuesten Stand der Technik unterstützen. Das ermöglicht Zugriffsüberwachung und wesentliche Sicherheitskonzepte wie Segmentierung. Router, Switches und Access Points von Hirschmann zeichnen sich in all diesen Bereichen durch ihre Qualität aus und eignen sich deshalb hervorragend für eine enge Integration in macmon NAC. Die Kombination beider Lösungen ermöglicht eine effektive Netzwerkzugangskontrolle bis in den Produktionsbereich.

Mehrere Eigenschaften machen die Lösung von macmon und Hirschmann gegenüber anderen Netzwerkzugangslösungen überlegen. Diese Eigenschaften bieten Industriekunden deutliche Vorteile:

Sichtbarkeit: Geräte werden mittels nahtloser Zusammenarbeit mit der Netzwerkinfrastruktur erkannt und können manuell oder automatisiert Endgerätegruppen (Sensor, CNC Fräse, Drucker) zugeordnet werden. Die Zuordnung erfolgt hierbei primär über



die MAC-Adresse des Geräts. Das hat den Vorteil, dass keine aktiven Scans – das sogenannte Profiling – durchgeführt werden müssen. Speziell im OT-Umfeld kommen heute oft noch Geräte zum Einsatz, die sensibel auf aktive Scans reagieren. Dies könnte in weiterer Folge zu einer Beeinträchtigung des Geräts bis hin zum Absturz oder Ausfall führen. Ergänzend bietet macmon NAC aber auch feingranulare Möglichkeiten für sensitive Scans beziehungsweise Identifizierungsoptionen wie kryptografisches Fingerprinting welches speziell für OT-Geräte konzipiert wurde.

Keine Abhängigkeit von speziellen Technologien:
IEEE 802.1X gewährleistet eine umfassende Authentifizierung vor dem Verbindungsaufbau zum Layer 2 Netzwerk zwischen dem Gerät und dem Netzwerk-Switch. Deshalb ist 802.1X die effektivste Lösung für die Zugangskontrolle in IT- und OT-Netzwerken. Obwohl Geräte von Hirschmann 802.1X vollständig unterstützen, funktioniert macmon NAC auch in Netzwerkarchitekturen ohne 802.1X.
Das ist eine sehr wichtige Eigenschaft für industrielle Netzwerke, da diese oft über einen sehr langen Zeitraum betrieben werden und nicht alle Geräte 802.1X unterstützen.
Insbesondere im industriellen Bereich stehen viele Unternehmen vor der Herausforderung, die vollständige Kompatibilität mit den Anforderungen zu gewährleisten, die eine 802.1X Implementierung verlangt. Hierzu gehören etwa Software-Agenten (Supplicants) auf jedem Gerät, Zertifikate, sowie eine PKI-Infrastruktur für eine umfassende Authentifizierung, außerdem voll funktionsfähige Netzwerkgeräte, die ordnungsgemäß und 802.1X-kompatibel konfiguriert sind. Diese Anforderungen sind bei industriellen Anlagen oftmals nicht erfüllt.
macmon NAC kann auch in einem Hybridmodus effektiv arbeiten. Netzwerksegmente ohne 802.1X werden damit ebenfalls gesichert, ohne Störungen durch Veränderungen in diesem Bereich zu erzwingen.

Die Authentifizierung gemäß 802.1X wird dagegen in drahtlosen und neueren Teilen des Netzwerks eingesetzt.
Hirschmann hat sich der Verwendung offener und etablierter Standards verschrieben.

Hirschmann-Produkte können daher problemlos in bestehende industrielle Netzwerke integriert werden, selbst wenn sie auf Geräten anderer Hersteller basieren. Mit anderen Worten: Die Kombination aus macmon NAC und Hirschmann ist bestens geeignet, um bereits installierte Netzwerke hinsichtlich Leistung, Sicherheit und Verwaltbarkeit zu erweitern und zu verbessern.

Netzwerke mit unterschiedlichen Endgeräten:
In der Industrie gibt es selten Netzwerke mit Endgeräten, die vollständig auf Komponenten einzelner Hersteller basieren. In der Regel werden Fertigungsgeräte, Sensoren und andere Komponenten von vielen hochspezialisierten Anbietern bereitgestellt oder sogar speziell für eine Anlage konstruiert.
macmon NAC kann verschiedene von der Netzwerkinfrastruktur bereitgestellte Zugriffsmethoden wie beispielsweise VLAN-Zuweisungen verwenden, um unterschiedliche Endgeräte sicher zu integrieren.

Um Industriekunden bestmöglich zu unterstützen, hat macmon die Layer 2 und Layer 3 Geräte von Hirschmann integriert, getestet und zertifiziert. Dies umfasst insbesondere auch Produkte, die für den Einsatz unter rauen Umgebungsbedingungen konzipiert sind. Etwa die Switches der OCTOPUS-Familie oder die robusten Switches und Router der MACH-Familie. Die Geräteprüfungen und die Integration wurden sowohl für das neueste HiOS-Betriebssystem als auch für das Classic Switch Software Betriebssystem durchgeführt, um die vollständige Kompatibilität des gesamten Geräteportfolios von Hirschmann sicherzustellen.

Dies reicht vom Classic Basic Rail Switch RSB bis zum industriellen HiOS Backbone Switch/Router DRAGON MACH 4000.

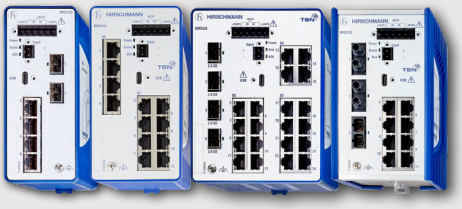
Um Industriekunden bestmöglich zu unterstützen, hat macmon die Layer 2 und Layer 3 Geräte von Hirschmann integriert, und getestet.
Dies umfasst insbesondere auch Produkte, die für den Einsatz unter rauen Umgebungs-bedingungen konzipiert sind.

Die kombinierte Lösung aus industriellen Kommunikationsgeräten von Hirschmann und macmon ist ideal, um die kritischen Punkte der industriellen Netzwerksicherheit anzugehen. Sie ermöglicht eine hervorragende Transparenz und integriert sich durch die Verwendung offener Standards nahtlos in bestehende Anlagen und Netzwerke.

MACH 1000 Rack Mount Fast/Gigabit Full Gigabit Switches

OCTOPUS Managed Fast/Gigabit Ethernet IP67/IP65 Switches und Router

BOBCAT Next-Generation Compact Managed Switches



macmon NAC ist für die Layer 2 und Layer 3 Geräte der OCTOPUS-Familie sowie die robusten Switches und Router der MACH- und auch der neuen BOBCAT-Familie von BELDEN optimiert.

Die Herausforderung meistern

Wie Sie eine umfassende Netzwerksicherheitsstrategie mit Hirschmann und macmon NAC erfolgreich umsetzen

Die heutigen Betreiber von OT-Netzwerken stehen vor zahlreichen Herausforderungen bei der Planung und Umsetzung einer umfassenden Netzwerksicherheitsstrategie in industrieellen Umgebungen. Diese Herausforderungen stellen ein Risiko für industrielle Anlagen und Anwendungen dar, weil sie die Transparenz der Aktivitäten im gesamten Netzwerk beeinträchtigen und die Einhaltung verbindlicher Standards und Vorschriften gefährden.

Eine leistungsstarke Netzwerkzugriffskontrolle erfüllt in Kombination mit industriegerechten Netzwerkgeräten für den Produktionsbereich diese Herausforderungen. Insbesondere die Integration von macmon mit Switches, Routern und Access Points von Hirschmann bringt die Zugriffskontrolle der nächsten Generation bis tief in die industriellen Netzwerke. Diese Lösung bietet modernste Sicherheit, während bewährte industrielle Funktionen wie extreme Zuverlässigkeit und hohe Verfügbarkeit durch Einsatz von Redundanzprotokollen erhalten bleiben. Die geprüfte Integration der Produkte beider Unternehmen stellt sicher, dass der Zugriffsschutz industrieller Netzwerke dort durchgeführt werden kann, wo es am wichtigsten ist: im Produktionsbereich.

HIRSCHMANN
A BELDEN BRAND

macmon nac

Referenzen:

[1] IEEE 802.1X-2010 – IEEE Standard for Local and metropolitan area networks – Port-Based Network Access Control
[2] IETF RFC2865 – Remote Authentication Dial In User Service (RADIUS)
[3] IEC 62443 – Security for Industrial Automation and Control Systems (IACS)
[4] IEEE 802.1Q-2014 - IEEE Standard for Local and metropolitan area networks – Bridges and Bridged Networks

Let's build the future.

Wenn Sie bereit sind, Ihre Netzwerksicherheitsinitiativen zu realisieren, steht Ihnen unser Team gerne zur Verfügung. Besuchen Sie **www.belden.com/networksecurity** um mehr darüber zu erfahren.

Über Belden

Belden Inc. liefert die Infrastruktur, die den digitalen Wandel einfacher, intelligenter und sicherer macht. Unser Fokus liegt nicht nur auf der Verbindungstechnik, sondern auch auf dem, was wir durch ein leistungsorientiertes Portfolio, zukunftsorientiertes Know-how und maßgeschneiderte Lösungen möglich machen. Mit mehr als 120 Jahren Erfahrung in Sachen Qualität und Zuverlässigkeit verfügen wir über ein solides Fundament, auf dem wir auch in Zukunft aufbauen können. Wir haben unseren Hauptsitz in St. Louis und verfügen über Produktionsstätten in Nordamerika, Europa, Asien und Afrika.

Für weitere Informationen besuchen Sie uns unter:
www.belden.com
www.beldensolutions.com

und folgen Sie uns auf **Linkedin** und **Facebook**