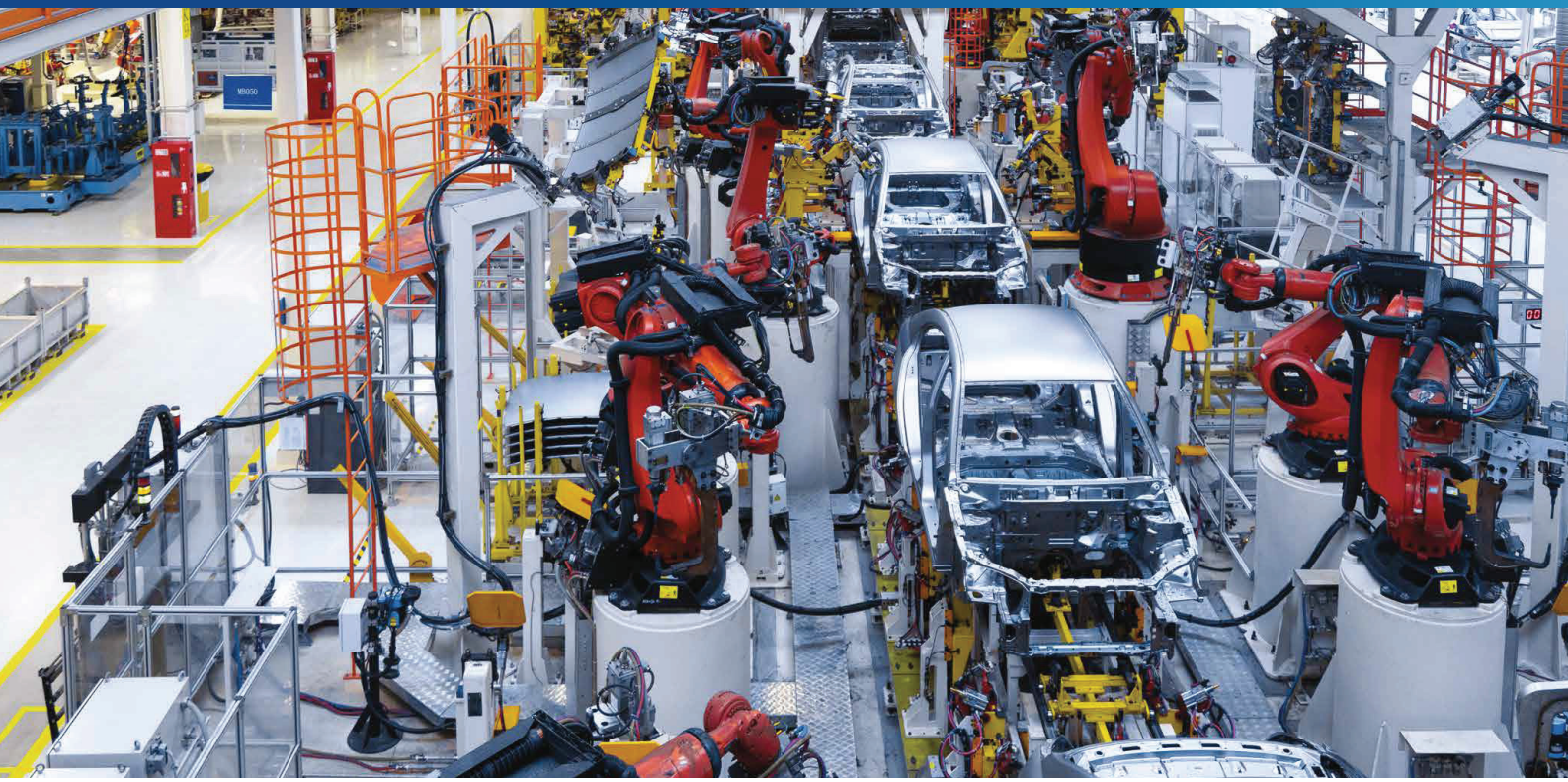
BELDEN
SENDING ALL THE RIGHT SIGNALS

HOPF
PARTNER | SOLUTIONS | COMPONENTS



Herausforderungen für Cybersicherheit in der Fabrikautomation

Anwendungsfälle und Lösungen aus dem Produktionsbereich

Gary DiFazio, Director of Marketing, Industrial Cybersecurity

Einleitung

Wie andere innovative Industrieunternehmen auf der ganzen Welt profitieren auch viele Betreiber von Fertigungsanlagen in der Fabrikautomation etwa in der Automobil-, Luft- und Raumfahrt- oder Elektronikindustrie deutlich vom Zugriff auf Echtzeitdaten aus dem Produktionsbereich. Sie setzen diese Informationen strategisch ein, um den Ertrag zu steigern, die Qualität zu verbessern, Ausschuss zu reduzieren und vieles mehr. Darüber hinaus sind viele dieser Unternehmen darauf ausgerichtet, im Zuge der kontinuierlichen Weiterentwicklung des Industrial Internet of Things (IIoT) und durch das Aufkommen neuer und leistungsfähigerer Technologien und den damit verbundenen Möglichkeiten noch größere Vorteile zu realisieren.

Mit der zunehmenden Vernetzung steigen jedoch die Risiken. Denn Steuerungsnetzwerke, die früher isoliert waren, sind nun für Außenstehende über eine wachsende Anzahl von Kontaktpunkten einschließlich des weltweiten Internets möglicherweise zugänglich. Dadurch sind die Produktionsprozesse nicht nur der Gefahr von Hackerangriffen und Schadsoftware aller Art ausgesetzt, sondern ebenso Geräteausfällen, menschlichem Versagen, böswilligen internen Vorfällen und andere Cybersicherheitsereignissen. Dies kann dazu führen, dass die Prozesse erheblich beeinträchtigt werden und sogar das Sicherheitsniveau des gesamten Produktionsbereichs darunter leidet. Solche Probleme können besonders in Fertigungsprozessen der Fabrikautomation von Bedeutung sein, wo ungeplante Stillstandzeiten oft mit Hunderttausenden oder sogar Millionen Dollar pro Stunde und mehr zu Buche schlagen - und übermäßiger Ausschuss oder Produktrückrufe können noch deutlich mehr kosten.

Inhaltsverzeichnis

- Einleitung 1
- Fertigungsanlagen der Fabrikautomation sind für Cybervorfälle äußerst anfällig 2
- Höherer Vernetzung = höhere Profitabilität = höheres Risiko 2
- Eine Vielzahl von Gefahren für Produktivität und Prozessintegrität 3
- Zahlreiche "Schuldige" für Cybervorfälle, ob in böswilliger Absicht oder versehentlich 3
- Einige Szenarien üblicher Cybervorfälle und was diese für Betreiber von Fertigungsanlagen in der Fabrikautomation bedeuten 3
- Vielfältige Bedrohungen der Cybersicherheit – Eine Strategie für den Schutz der Cybersicherheit 6
- Transparenz, Schutzmaßnahmen und kontinuierliche Überwachung 7
- Zusammenfassung 8

Be certain.
Belden.

Die Betreiber von Fertigungsanlagen in der Fabrikautomation haben jedoch zahlreiche Optionen, um das Risiko von Cybersicherheitsproblemen deutlich zu reduzieren. Mit anderen Worten: Sie können die Wahrscheinlichkeit von Cybervorfällen in unzähligen Produktionsprozessen auf der ganzen Welt, welche die Produktivität, Qualität, Sicherheit, Profitabilität und sogar das Markenimage erheblich schädigen, verringern.

Dieses White Paper informiert die Leser über das wahre Ausmaß und die Vielfalt der Cybersicherheitsbedrohungen, die in heutigen Fertigungsprozessen der Fabrikautomation auftreten, und erläutert die Möglichkeiten, wie diese Bedrohungen begrenzt werden können. Hierzu gehören effektive Cybersicherheitsvorkehrungen, die Optimierung der strategischen Nutzung intelligenter Cybersicherheitskonfigurationen in den Netzwerkgeräten, die Kenntnis und Umsetzung von Best Practices für Cybersicherheit wie etwa die umfassende dreistufige Lösung von Tripwire („Transparenz → Schutzmaßnahmen → Kontinuierliche Überwachung“) und der Einsatz innovativer Werkzeuge von Drittanbietern, die speziell für die Optimierung der Cybersicherheitsleistung Ihrer Anlagen entwickelt und getestet wurden.

Erfahrene Anwender moderner Automatisierungstechnik (Operations Technology, OT) können heute das Beste aus zwei Welten bekommen: die Nutzung und Ausweitung des Einsatzes datengesteuerter Technologien, welche die Produktivität steigern und gleichzeitig proaktiv vor den Schwachstellen schützen, von denen eine Gefahr für die Integrität der Prozesse ausgeht.

Anlagen der Fabrikautomation sind für Cybervorfälle äußerst anfällig

Prozessexperten für Fertigungsanlagen der Fabrikautomation müssen herausfordernde Ziele und Quoten erfüllen. Denn es kommt darauf an, eine Vielzahl von Teilen aus zahlreichen Quellen in großen Mengen in fertige Produkte umzusetzen und diese rechtzeitig und in höchster Qualität auf den Markt zu bringen, und zwar mit minimalen Abweichungen und optimalen Zielspezifikationen. Um dies zu erreichen, sind sie auf die Daten angewiesen, die sie von den vernetzten Komponenten der Anlagen in jedem Schritt des Fertigungsprozesses bis hin zur abschließenden Qualitätskontrolle erhalten. Was aber, wenn manche dieser Daten verfälscht wurden?

Außerdem birgt der typische Fertigungsbereich der Fabrikautomation zahlreiche Gefahren für das Leben und die Sicherheit von Menschen, weshalb dort Lichtgitter, Bewegungsmelder, Sensoren und andere Schutzmaßnahmen eingesetzt werden. Was passiert jedoch, wenn eine davon beeinträchtigt ist? Können wir den Schutzmaßnahmen auch dann noch vertrauen, wenn sie in ungewöhnlicher Weise auf Daten antworten oder auf falsche Daten reagieren?

Höherer Vernetzung = höhere Profitabilität = höheres Risiko

Diese beunruhigenden Szenarien sind heutzutage keine Seltenheit. Denn die zunehmende Vernetzung moderner Automatisierungsanlagen der Fabrikautomation ist ein zweischneidiges Schwert. Zwar setzen unterschiedliche Branchen wie Automobil, Luft- und Raumfahrt oder Elektronik im Produktionsbereich verschiedene Automatisierungsgeräte wie etwa Controller, Roboter, Motoren, Sensoren, HMIs, VFDs, E/A Module und prozessspezifische Maschinen aller Art bereits erfolgreich ein. Während diese wichtigen Geräte lange Zeit unabhängig voneinander gearbeitet haben, teilen sie sich heute jedoch häufig proaktiv Datenströme in Echtzeit und kommunizieren abgestimmt miteinander, um eine exaktere Steuerung der Prozesse zur Verbesserung der Präzision und Qualität zu ermöglichen. Darüber hinaus erzeugen und kommunizieren viele dieser Geräte wichtige Daten für Analysen, die sowohl eine weitere Feinabstimmung der Prozesse als auch die Archivierung der Produktionsdaten für die Gesamtanlageneffektivität, Audits, Lieferantenverantwortung und andere Zwecke erlauben. Im Zuge der ständigen Weiterentwicklung des IIoT, das eine noch höhere Vernetzung, Auslastung und Wertschöpfung der miteinander verbundenen Geräte und gemeinsam genutzten Daten verspricht, wird sich dieser Trend noch beschleunigen. Zugleich nehmen dadurch die Möglichkeiten für höhere Erträge, schnellere Produktionszyklen, weniger Ausschuss, verbesserte Qualität, zusätzliche Sicherheit für Personal und Geräte und vieles mehr zu.

Mit diesen Vorteilen ist jedoch eine ernsthafte Bedrohung der Effektivität der Fertigungsprozesse verbunden. Denn deren Steuerungsnetzwerke, die früher isoliert waren, sind jetzt möglicherweise direkt mit der Außenwelt verbunden, von anderen Bereichen der Fabrik über das IT Netzwerk des Unternehmens bis hin zum Internet. Dadurch entstehen neue Bedrohungsvektoren, welche die Fertigungsanlagen für vielfältige potenzielle Cyberereignisse anfällig machen, die sowohl böswillig als auch unbeabsichtigt sein können. Viele dieser Bedrohungen sind Neuland für OT Mitarbeiter, etwa Ransomware, Schadsoftware, Cybersabotage durch Mitarbeiter, Netzwerkausfälle, Benutzerfehler und vieles mehr. Während die Unternehmens IT mit solchen Problemen und den damit verbundenen Kosten vertraut ist, kann deren zunehmendes Auftreten im OT Bereich weitaus größeren Schaden anrichten. Denn in Branchen der Fabrikautomation ist die Produktion und die Auslieferung von Produkten das A und O des Business.

Eine Vielzahl von Gefahren für Produktivität und Prozessintegrität

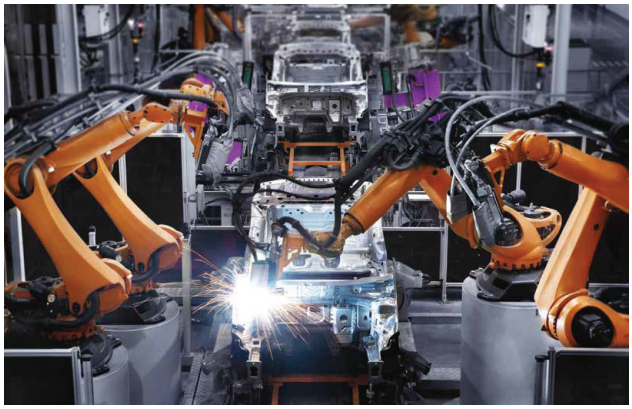
In Fertigungsprozessen der Fabrikautomation werden Produktionslinien häufig mit maximaler Auslastung betrieben. Und Stillstandzeiten, die durch entgangene Gewinne, vermehrten Ausschuss, nicht eingehaltene Lieferverpflichtungen und vieles mehr hohe Kosten verursachen, können in vielen Branchen pro Stunde mit Hunderttausenden oder sogar Millionen Dollar und mehr zu Buche schlagen.

Darüber hinaus gibt es bei Dutzenden, Hunderten oder sogar Tausenden von Montageprozessen, die exakt spezifiziert sein müssen, unzählige Möglichkeiten, dass eine Schlüsselbaugruppe wie eine Türverkleidung oder ein Motherboard oder sogar ein Endprodukt durch einen einzigen nicht spezifikationskonformen Fertigungsschritt zu Ausschuss wird. Das gilt selbst für so einfache Dinge wie einen Bolzen oder ein anderes Befestigungselement mit unzureichendem Drehmoment. Die Fertigungsvorschriften für all diese Teile können durch eine unsachgemäße Änderung der Geräte-konfiguration oder der Produktionsanforderungen beeinflusst werden. Dabei spielt es keine Rolle, ob es sich um einen Eingabefehler, eine böswillige Eingabe, fehlerhafte Komponenten oder eine andere unerwünschte Veränderung des Netzwerks handelt. Zwar haben die Betreiber von Fertigungsanlagen der Fabrikautomation theoretisch den Vorteil, dass sie nicht spezifikationsgerechte Unterbaugruppen bis hin zu Bauteilen nachbearbeiten können. Jedoch wird das oft als mühsam und zeitaufwändig angesehen, weshalb solche Produkte häufig als Ausschuss klassifiziert und kostspielig entsorgt werden.

Darüber hinaus kann es für viele Anlagenbetreiber zu teuren Rückrufaktionen, einer Verschlechterung des Markenimages oder sogar zu Rechtsstreitigkeiten kommen, wenn fehlerhafte Produkte nicht rechtzeitig erkannt werden.

Zahlreiche “Schuldige” für Cybervorfälle, ob in böswilliger Absicht oder versehentlich

Wie bereits erwähnt, handelt es sich bei Cybersicherheitsvorfällen nicht nur um Ereignisse, die von böswilligen Akteuren wie Hackern und Entwicklern von Schadsoftware ausgelöst werden, auch wenn diese eher für Schlagzeilen sorgen. Vielmehr betrachten Experten alles als Cybersicherheitsvorfall, was sich nachteilig auf das Netzwerk auswirkt und die Fähigkeit einschränkt, die Verfügbarkeit eines industriellen Prozesses einschließlich der Sicherheitssysteme zu visualisieren, zu überwachen, zu steuern und aufrechtzuerhalten - ob böswillig, versehentlich oder durch normalen Verschleiß. Dies umfasst etwa Hackerangriffe wie Denial of Service Attacken, böswillig herbeigeführte Schäden und Unternehmensspionage. Weitere Bedrohungsszenarien sind Angriffe mit Ransomware und Viren, unbeabsichtigte Fehler von Mitarbeitern, die weite Teile der Fertigung lahmlegen können, verärgerte Mitarbeiter, die von innen über das Netzwerk Produktionsstörungen herbeiführen oder ein allmähliches Versagen von Geräten und Komponenten, was die Prozesse verlangsamen oder nicht spezifikationsgerechte Betriebsbedingungen verursachen kann - all dies und vieles mehr, unabhängig von der Quelle oder der Absicht.



Einige Szenarien üblicher Cybervorfälle und was diese für Betreiber der Fertigungsanlagen in der Fabrikautomation bedeuten

Da die potenziellen Vorteile der Vernetzung ebenso zunehmen wie die Bedrohung durch Cybervorfälle, erscheint es für Spezialisten heutiger Automatisierungsnetzwerke an der Zeit, sich umfassend über die Risiken zu informieren. Das Personal im OT Bereich muss damit beginnen, die verfügbaren Cybersicherheitstechniken und -technologien zu nutzen, mit denen die IT schon lange vertraut ist, um seine Produktionsprozesse zu schützen. Möglicherweise steht sogar noch mehr auf dem Spiel, da die Bedrohung der Fabrikautomation die Verfügbarkeit der Produktion beeinträchtigen kann. Und anders als wichtige, aber unspezifische Administrationsfunktionen, ist die Herstellung von Produkten der Lebensnerv jedes Fertigungsunternehmens.

Der Schutz der Produktion beginnt mit den Grundlagen, die für viele im OT Bereich möglicherweise nicht so selbstverständlich sind wie für ihre Kollegen in der IT. Hierzu gehören bewährte Methoden für Cybersicherheit wie das Deaktivieren nicht verwendeter Ports, das Trennen der OT- und IT-Prozesse durch Firewalls, das Aktivieren integrierter Sicherheitseinstellungen bei entsprechend ausgestatteten Geräten und, was möglicherweise am wichtigsten ist, das Deaktivieren von Verbindungen zwischen Automatisierungsgeräten und dem weltweiten Internet. Obwohl all dies wichtig ist, liegt der Schlüssel für Cybersicherheit von IT- wie auch OT-Prozessen darin, minütlich in Echtzeit einen optimalen Einblick in den Netzwerkbetrieb zu haben und ständig aufrechtzuerhalten.

In diesem Zusammenhang muss darauf hingewiesen werden, dass Cybersicherheit in der IT häufig vor allem „defensiv“ angegangen wird. Eine proaktive Steuerung von Cybersicherheit in der OT kann jedoch die Prozessintegrität erhöhen und die Fähigkeit des Personals verbessern, Prozesse in immer differenzierter Weise zu betreiben. Denn für Steuerungsexperten geht es bei Cybersicherheit häufig nicht nur um den Schutz ihrer Anlagen. Vielmehr können die damit verbundene höhere Transparenz und effektivere Überwachung ebenso wichtige Aspekte sein, um sowohl die Stabilität der Prozesse zu verbessern als auch die Qualität und die Erträge zu steigern. Zum besseren Verständnis werden im Folgenden eine Reihe gängiger Szenarien und deren typische Auswirkungen auf Prozesse der Fabrikautomation vorgestellt. Diese Beispiele veranschaulichen, dass die Fähigkeit, jedes dieser Szenarien sofort zu erkennen, wenn es auftritt, anstatt im Dunklen zu tappen, der Schlüssel zur Optimierung von Cybersicherheit und der Prozessintegrität in der OT ist.

Nicht autorisierter böswilliger Zugriff von außerhalb des Unternehmens

Hackerangriffe sind vielleicht die „dramatischste" böswillige Bedrohung, da es sich in der Regel um gezielte Attacken handelt. Dies ist nicht der Fall, wenn beispielsweise jemand wahllos eine Schadsoftware versendet und nicht weiß, wen sie treffen wird. Im Gegensatz hierzu sind Hackerangriffe oft dadurch charakterisiert, dass sich ein Angreifer Zugang in ein Netzwerk verschafft und dann versucht herauszufinden, welche Informationen und Ressourcen verwertbar sein könnten. Wie bereits erwähnt, ist dies die Phase, in der solche Angriffe erkannt und vereitelt werden können. Voraussetzung ist jedoch, dass zuvor geeignete Maßnahmen getroffen wurden, um die Transparenz zu erlangen, welche die digitalen Fußabdrücke der Angreifer offenbart und die Netzbetreiber zum Handeln auffordert.

Hinter Hackangriffen stehen ganz unterschiedliche Akteure. Das können Personen sein, die im Auftrag eines Staates strategisch wichtige Unternehmen sabotieren sollen, Wettbewerber oder deren Partner, die organisatorische Informationen wie Stücklisten, Produktionsdaten und Konstruktionspläne erhalten möchten, oder einfach kriminelle Computerspezialisten.

Dabei ist es wichtig zu wissen, dass die Opfer von Hackerangriffen nicht immer das endgültige Ziel sein müssen. Beispielsweise beabsichtigt ein Hackerteam möglicherweise ein gut geschütztes Unternehmen wie einen großen Automobilhersteller anzugreifen. Dann geraten kleine Zulieferer sofort ins Visier, da sie möglicherweise über eine Onlineverbindung für Fakturierung oder Bestellungen einen nur unzureichend geschützten Zugang in die IT Systeme dieses Unternehmens haben. Oder wenn das kleinere Unternehmen über ein spezielles Gerät verfügt, etwa die bestimmte Ausführung einer SPS, das auch von dem größeren Unternehmen eingesetzt wird, hacken die Angreifer dieses Gerät häufig zunächst in dem kleineren Unternehmen, das sie sozusagen als „Testumgebung" nutzen. So können sie sich über die Verwendung der Firmware und mögliche Sicherheitslücken informieren, bevor sie versuchen, in dem größeren Unternehmen auf dieses Gerät zuzugreifen. Ein weiterer Grund, ein kleineres Unternehmen ins Visier zu nehmen, ist die „Versklavung" von Computerressourcen. Die so erbeuteten Kapazitäten werden dann zusammen mit anderen genutzt, um Denial-of-Service Attacken oder ähnliche Angriffe auf größere Unternehmen durchzuführen.

Sie sollten sich darüber im Klaren sein, dass die IP Adressen vieler Steuerungen, Kameras, Maschinen und anderer vernetzter Geräte - möglicherweise Ihrer - gerade jetzt im Internet für jeden verfügbar sind, der sie sich ansehen möchte. Diese Informationen stehen über professionelle Computer Suchmaschinen wie Shodan bereit, und was für illegale Zwecke im Darknet gefunden werden kann, lässt sich nur vermuten. Jeder kann diese leicht verfügbaren Informationen nutzen, um das Innere von Fabriken durch die Kameras der dortigen Anlagen zu betrachten. Das ist ebenso besorgniserregend wie aufschlussreich und zeigt, dass grundlegende Schutzmaßnahmen für Cybersicherheit wie die Deaktivierung von Ports, das Installieren von Firewalls oder das Suchen und Beseitigen unnötiger und gefährlicher Internetzugriffspunkte in diesen Unternehmen nicht umgesetzt wurden.

Angreifer innerhalb des Unternehmens

In OT Bereichen, die Erfahrung mit Schutzmaßnahmen für Cybersicherheit haben, wird häufig viel unternommen, um Angriffe von außen zu vereiteln. Dagegen wird die Möglichkeit böswilliger Handlungen von Mitarbeitern - die oft einfacher durchzuführen sind und mit größerer Wahrscheinlichkeit auftreten - jedoch übersehen und keine vorsorgliche Abwehrstrategie entwickelt. Der Aufbau eines zuverlässigen Perimeterschutzes reicht nicht aus, wenn sich der Angreifer bereits „innerhalb der Werkstore" befindet. Außerdem sind Mitarbeiter, die als Hacker agieren, bereits mit OT Prozessen und den entsprechenden Geräten vertraut und können sogar noch größeren Schaden anrichten als externe Angreifer.

Die Gründe für Cyberangriffe von Mitarbeitern können vielfältig sein. Die Motive reichen von Verärgerung und Rachsucht aufgrund tatsächlicher oder eingebildeter Ungerechtigkeiten über Bestechung, Geldgier sowie Bedrohung und Erpressung durch Dritte bis hin zu Nervenkitzel, Psychosen und Langeweile - oder einfach, weil die Mitarbeiter dazu in der Lage sind. Die Folgen können etwa die Störung der Produktion durch eine gezielte Änderung von Spezifikationen oder Arbeitsaufträgen sein, der Diebstahl und die Weitergabe geschützter Informationen an Außenstehende oder der Verkauf dieser Informationen an den Meistbietenden sowie die Beeinträchtigung von Sicherheitssystemen, um sich an vermeintlichen Feinden im Unternehmen und an diesem selbst zu rächen.

Eine andere Art von internen Angriffen besteht darin, dass der Angreifer gestohlene Zugangsdaten eines vertrauenswürdigen Mitarbeiters benutzt. Beispielsweise kann es vorkommen, dass Bediener - auch wenn sie die Protokolle überprüfen - bei Änderungen von Produktionsspezifikationen nicht misstrauisch werden, wenn diese offensichtlich von ihrem Vorgesetzten veranlasst wurden. Denn sie bemerken nicht, dass in Wahrheit ein anderer Mitarbeiter dahintersteckt, der die Zugangsdaten unerlaubt verwendet hat. Selbst wenn solche Änderungen markiert wurden, ist es unmöglich, darauf bezogene verdächtige Informationen wie etwa „Warum wurden diese Änderungen um 4 Uhr morgens vorgenommen?" oder „Warum wird mit fremden IP-Adressen kommuniziert?" einzubeziehen, um ein vollständiges Bild zu erhalten, falls keine zusätzlichen Werkzeuge eingesetzt werden.

Erstaunlicherweise fragen sich Mitarbeiter häufig, wie jemand ihr Passwort kennen kann, obwohl sie es auf einen Notizzettel geschrieben und unter die Tastatur ihres Engineering Arbeitsplatzes geschoben haben. Gängige Methoden zum Knacken von Passwörtern wie sogenannte Brute Force Attacken, psychografisches Rätselraten (Kindernamen, Geburtstage), Zugriff auf unverschlüsselte Passwortdatenbanken oder das Aufspüren von Zugangsdaten im Netzwerkverkehr sind weit verbreitet und äußerst effektiv, häufig jedoch nicht einmal erforderlich.

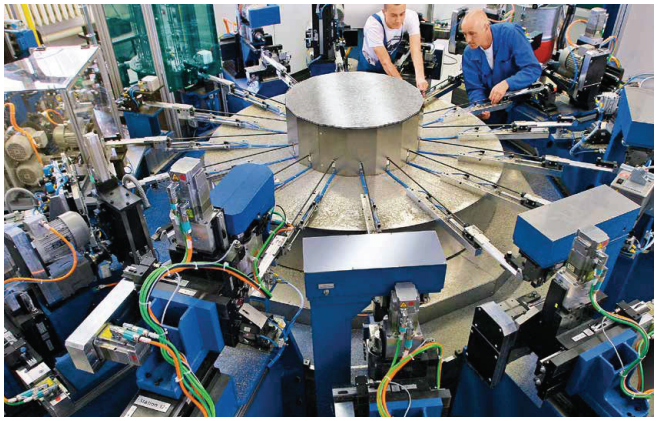
Unabhängig von der Bedrohungsquelle beginnt der Schutz vor Cyberangriffen mit Transparenz. Denn wenn bei jeder Änderung eine Warnung an den Bediener gesendet wird, kann jede Änderung anhand autorisierter Arbeitsaufträge überprüft werden. So lassen sich ungewöhnliche, nicht autorisierte Änderungen - ob in böswilliger Absicht oder nicht - sofort wieder auf die normale betriebliche Konfiguration zurücksetzen.

Schadsoftware - Viren, Trojaner, Würmer und vieles mehr

Der Begriff Schadsoftware beschreibt eine Reihe von durch Menschen entwickelte, codebasierte Programme, die das OT Netzwerk infizieren und die Produktion auf verschiedene Weise erheblich beeinträchtigen können. Die Auswirkungen reichen von skurril und ärgerlich (Ankündigung von „Star Wars Rules“ auf jedem Bildschirm) bis hin zum kompletten Stillstand der Anlagen. Gründe dafür können Bosheit, Sabotage oder Lösegeld sein. Ransomware, die zunächst für leichte Angriffe auf IT Prozesse diente, ist im OT Bereich offensichtlich eine noch wirkungsvollere Methode, da dort Stillstandzeiten häufig deutlich kostspieliger und zeitkritischer sind. Bei vielen aktuellen Ransomware Schadprogrammen wie WannaCry und (Not) Petya garantiert das Bezahlen des Lösegelds leider nicht, dass die Benutzer wieder die Kontrolle über die Daten oder den Betrieb der Anlagen bekommen - und ironischerweise hat dies nichts mit der „Ehrlichkeit“ der Angreifer zu tun. Denn häufig schließen die Behörden sofort die Bitcoin Konten oder andere von den Kriminellen geforderte elektronischen Zahlungswege, sodass die Opfer keinerlei Zugang zu einer möglichen „Lösung“ haben. In diesen und anderen Fällen besteht der einzige Ausweg darin, Geräte neu zu konfigurieren und die Prozessausfallzeit und den Datenverlust in Kauf zu nehmen.

Schadsoftware kann Viren enthalten, die an eine Datei angehängt sind, die von den Empfängern geöffnet werden muss, damit sie sich verbreiten können - daher die ständige Warnung, niemals auf unbekannte Anhänge oder Dateien zu klicken. Würmer sind heimtückischer. Denn sie duplizieren sich selbst und agieren im Hintergrund, ohne dass der Benutzer etwas tun muss. Sogenannte Trojanische Pferde sind vielleicht die heimtückischsten von allen, da sie sich häufig als nützliche Anwendung tarnen, aber beim Öffnen, Sperren oder Löschen von Dateien Schaden anrichten. Außerdem können sie eine Hintertür öffnen, die es böswilligen Angreifern ermöglicht, auf das Netzwerk zuzugreifen.

Schadsoftware kann auf verschiedene Weise in OT Netzwerke eingeschleust werden. Ein beliebter Weg ist das Infizieren von Benutzerhandbüchern und Schaltplänen im PDF-Format. Wenn ein Vertragspartner eine solche Datei öffnet, um ein Gerät im Produktionsbereich zu warten, wird die Schadsoftware gestartet und im gesamten OT Netzwerk verbreitet. Schadsoftware kann über einen Anhang eingegeben werden, der in einer E-Mail geöffnet wird - das ist ein weiterer Grund, warum mit dem Internet verbundene Geräte keine Verbindung zu Geräten im Produktionsbereich herstellen dürfen. Auch wenn keine Verbindung zur Außenwelt besteht, kann Schadsoftware durch eine absichtliche oder unwissende Komplizenschaft von Mitarbeitern in ein Netzwerk eindringen, beispielsweise durch Anschließen eines internetfähigen Laptops oder eines gefundenen „kostenlosen“ USB Sticks. Letzteres geschah mutmaßlich bei Stuxnet, einer Schadsoftware, die vermeintlich isolierte Fabriken im Iran infiltrierte und durch die Übermittlung falscher Werte an SPSen Zentrifugen lahmlegte. Durch Best Practices für Cybersicherheitsvorkehrungen können einige dieser Szenarien vermieden werden, etwa indem die Verwendung von USB Ports eingeschränkt oder die Verbindung nicht autorisierter Geräte mit dem Netzwerk verweigert wird.



Eine weitere Quelle für Schadsoftware, die nur selten in Betracht gezogen wird, ist das Huckepackverfahren auf einem ordnungsgemäß gekauften Gerät. Manchmal kann der Fertigungsbereich eines Geräteherstellers infiziert und die Schadsoftware in der Firmware der Geräte enthalten sein. Dadurch werden die Produktionsprozesse der Kunden, in denen sie installiert sind, infiziert. Häufig lässt sich das durch Transparenz vermeiden. Denn die richtigen Werkzeuge können diese Geräte markieren, wenn sie insgeheim Dinge tun, für die sie nicht vorgesehen sind wie etwa Port Scans oder Kommunikation mit der Außenwelt.

Schadsoftware ist jedoch häufig kein Selbstzweck, sondern der erste Schritt eines Hackerangriffs. Denn diese Software wurde entwickelt, um Konfigurationen zu ändern, Kennwörter zu erfassen, Firewalls zu deaktivieren oder andere versteckte Funktionen auszuführen, die es den Angreifern ermöglichen, ihre eigentlichen Ziele zu erreichen. Durch eine vorausschauende, auf Cybersicherheit ausgerichteten Strategie können solche Änderungen wieder rückgängig gemacht. Denn ähnlich wie bei Hackerangriffen hinterlässt die Implementierung von Schadsoftware Hinweise auf Änderungen im Netzwerk. Durch richtige Transparenz lassen sich diese sofort erkennen und Alarme auslösen.

Wie bereits erwähnt, wurden zahlreiche Schadsoftwareprogramme ursprünglich entwickelt, um IT Prozesse zu gefährden. Dennoch können sie im OT Bereich „Kollateralschäden“ verursachen, da es häufig IT Geräte und Dienste wie Windows, Linux, SQL Datenbanken und Webserver gibt, die auch dort vorhanden sind. Sie können unabhängig voneinander infiziert werden, und ohne eine angemessene Trennung der beiden Bereiche kann sich eine Infizierung der Unternehmensebene in die Produktion ausbreiten. In den vergangenen Jahren ist immer mehr Schadsoftware eingesetzt worden, die entwickelt wurde, um Produktionsprozesse mittels steuerungsspezifischer Protokolle wie IEC 101, IEC 104 oder Step7 anzugreifen. Ein besonders verheerendes Programm dieser Art ist Triton, das vermutlich von einem Staat initiiert worden ist. Es wurde speziell für Triconex, ein branchenführendes Sicherheitssystem (Safety Instrumented System, SIS) von Schneider Electric, geschrieben und scheint eher auf Schaden denn auf finanziellen Gewinn ausgerichtet zu sein.

Menschliche Fehler

Nicht alle Cybervorfälle werden böswillig herbeigeführt. Ein hoher Prozentsatz der schädlichen Auswirkungen auf das Netzwerk von Fertigungsprozessen der Fabrikautomation resultiert vielmehr aus unbeabsichtigten Fehlern. Stellen Sie sich vor, wie leicht es passieren kann, dass ein vielbeschäftigten Bediener einen Drehmomentwert von 60 PSI anstelle von 6,0 PSI eingibt oder eine SPS versehentlich über die Leitung 1 mit den Werten für die SPS auf Leitung 2 konfiguriert, was große Probleme auf der Leitung verursacht. Überlegen Sie, wie oft ein Wartungsmitarbeiter die Firewallregeln abschwächt, um eine Reparatur durchzuführen oder eine Testumgebung aufzubauen - und niemand wird die ursprünglichen Regeln jemals wiederherstellen.

Netzwerkänderungen lassen sich jedoch mit der richtigen Überwachungslösung anzeigen. So können die Bediener schnell erkennen, ob diese Änderungen korrekt waren und andernfalls - wenn erforderlich - sofort Maßnahmen ergreifen,

Ausfallende Geräte

Ein weiteres nicht böswillig herbeigeführtes Szenario, das sich häufig negativ auf die Integrität des Produktionsnetzwerks auswirken kann, ist ein bevorstehender Ausfall der physischen Infrastruktur, beispielsweise eines Kabels, eines Switches oder von Geräten wie einer SPS oder einer HMI. Denn dadurch können Produktionsdaten unvollständig oder verlangsamt übertragen werden bzw. ganz verloren gehen, was die Qualität und die Erträge der Fertigungsprozesse in der Fabrikautomation beeinträchtigt.

Häufig kann das Netzwerk Hinweise geben, von messbaren Änderungen der Antwortzeiten von Robotern und Förderbändern bis hin zu zunehmenden zyklischen Redundanzprüfungen (Cyclic Redundancy Check, CRC) oder anderen Fehler- und Diagnoseinformationen, die von Betriebsprotokollen erstellt werden, jedoch nicht rechtzeitig Berücksichtigung finden. Eine automatische Überwachung dieser Informationen in Verbindung mit entsprechenden Alarmen ist eine weitere Form der vorbeugenden Wartung. Sie ist wichtig, um Ereignisse präzise vorherzusehen, bevor sie sich negativ auf den Produktionsprozess auswirken können.

Vielfältige Bedrohungen der Cybersicherheit – Eine Strategie für den Schutz von Cybersicherheit

Wie in allen obigen Beispielen ausgeführt, hinterlässt jede Änderung des Netzwerks, ob absichtlich, versehentlich oder böswillig bzw. sinnvoll, leichtsinnig oder höchst nachteilig, sofort Spuren. Die Schwierigkeit besteht darin, dass solche Spuren häufig unvollständig, isoliert und irgendwo in Geräteprotokollen „versteckt“ sind oder gar nicht erst erfasst werden. Wenn die Ursache eines Vorfalls jedoch nicht genau zum Zeitpunkt seines Auftretens herausgefunden wird, lässt sich das Problem nicht erkennen und wird so lange bestehen bleiben, bis der Schaden behoben ist, was kostspieligen Folgen für Ihre Produktivität hat.

Deshalb denken Anlagenbetreiber über die Umsetzung von Lösungen nach, die speziell entwickelt wurden, um eine kontinuierliche Transparenz ihrer Netzwerkaktivitäten in Echtzeit zu gewährleisten. Normalerweise bestehen diese Lösungen aus drei Schritten: Bestandsaufnahme dessen, was vorhanden ist und welche Aufgaben es hat, Implementierung vielfältiger Schutzsteuerungen und schließlich Überwachung von Änderungen gegenüber der Ausgangssituation, das heißt jedwedes ungewöhnliche Netzwerkverhalten. Auf diese Weise erlangen Sie die Kontrolle über alles, was Sie steuern können.

Obwohl das Vorhaben, eine unsichere Anlage von Grund auf zu sichern, entmutigend sein kann, können Sie recht schnell ein hohes Schutzniveau erreichen. Denn es gibt grundlegende Cybersicherheitsmaßnahmen, mit denen Sie sofort beginnen können, um das betriebliche Risiko zu verringern und die Auswirkungen aller oben beschriebenen Bedrohungen zu erkennen und zu vermeiden. Bei diesen Maßnahmen handelt es sich um Basistechnologien, welche die höchste Transparenz und den besten Schutz gegen böswillige Aktivitäten bieten. Sie bilden die Grundlage für die meisten Cybersicherheitsrichtlinien der Branche wie etwa IEC 62443, den Leitfaden für das Prozesssteuerungsnetzwerk der American Water Works Association sowie NIST SP-800-82 und NERC CIP. Unabhängig davon, ob Ihr Unternehmen einen bestimmten Standard übernehmen möchte oder nicht, können Sie mit einigen der angesprochenen grundlegenden Cybersicherheitsmaßnahmen beginnen:

- Bestandsaufnahme der Hard- und Software
- Segmentierung des Netzwerks
- Schwachstellenmanagement
- Änderungsmanagement
- Netzwerkverwaltung
- Zentralisierte Protokollverwaltung

Diese Maßnahmen gehören alle zu der umfassenden dreiteiligen Strategie. Die Philosophie und der Antrieb dahinter lautet, wie wir oft sagen: „Wie können Sie etwas schützen, wenn Sie nicht wissen, was Sie haben, welche Aufgaben es hat und wie diese ausgeführt werden bzw. wie ein ‘normaler‘ Netzwerkbetrieb überhaupt aussieht?“ Die dreiteilige Strategie löst dieses Problem.

Transparenz, Schutzmaßnahmen und kontinuierliche Überwachung

Umfassende Cybersicherheit in drei Schritten:

Schritt 1: Transparenz herstellen

Sie können sofort mit dem „Ratespiel“ aufhören. Denn Sie wissen, was Sie haben und somit auch, was Sie sichern müssen. Wenn Sie für Ihr Steuerungsnetzwerk ganzheitliche Transparenz hergestellt haben, können Sie sowohl Ihre Geräte inventarisieren (Hersteller, Marke, Typ, Seriennummer, Firmwareversion etc.) als auch Kommunikationsmuster zwischen Geräten verwalten, Änderungen der Netzwerktopologie anzeigen, nicht autorisierte Geräte im Netzwerk identifizieren, Konfigurationsänderungen erkennen sowie Schwachstellenanalysen und andere prozessbezogene Unterlagen bereitstellen, ohne auf Vermutungen angewiesen zu sein. Zur Herstellung ganzheitlicher Transparenz gehört:

1. Erfassen und dokumentieren Sie die gesamte Netzwerkkommunikation zwischen dem industriellen Steuerungsnetzwerk und dem IT Netzwerk des Unternehmens.
2. Erfassen und dokumentieren Sie alle Fernzugriffe auf das industrielle Steuerungsnetzwerk, beispielsweise den Zugriff von Geräteherstellern via Einwahlmodems, VPN und Mobilfunkverbindungen.
3. Inventarisieren und aktualisieren Sie Informationen zu Hard- und Software, etwa Hersteller, Typ, Seriennummer, Firmwareversion und Versionen der installierten Software.
4. Erstellen und pflegen Sie ein Diagramm der Netzwerktopologie.
5. Erfassen Sie, über welche industriellen Protokolle kommuniziert wird und welche Geräte kommunizieren, beispielsweise HMIs und SPSen.
6. Erfassen Sie, wie die Geräte konfiguriert sind und ob sich diese Konfigurationen ändern.
7. Stellen Sie fest, welche Sicherheitslücken (Schwachstellen) in den Prozessen vorhanden sind.
8. Setzen Sie eine zentralisierte Lösung für die Verwaltung der Protokolle um.

Schritt 2: Umsetzung von Schutzmaßnahmen

Schutzmaßnahmen sind Funktionen, die dazu beitragen, Auswirkungen von Cybervorfällen zu verhindern oder zu verringern. Es ist jedoch ineffizient, Schutzmaßnahmen wahllos umzusetzen. Sie müssen vielmehr optimal für den jeweiligen industriellen Prozess, den Sie sichern und verwalten möchten, ausgelegt sein. Denn was für eine Anwendung geeignet ist, kann für eine andere möglicherweise nicht passen. Ein richtiger erster Schritt ist die Trennung zwischen dem IT Netzwerk des Unternehmens und dem industriellen Steuerungsnetzwerk. Dadurch wird jegliche nicht autorisierte Netzwerkkommunikation durch den Einsatz von Firewalls oder Zugriffssteuerungslisten (Access Control Lists) für Netzwerkgeräte verweigert.

Eine andere meist sehr effektive Vorgehensweis ist die Verbesserung des Schutzes von Anlagen/Geräten. Hierzu gehören folgende Maßnahmen:

1. Deaktivierung aller Dienste, die nicht unbedingt für einen industriellen Prozesse erforderlich sind, beispielsweise nicht sichere Protokolle wie Telnet, das Daten nur unverschlüsselt überträgt.
2. Aktivierung von Cybersicherheitsfunktionen wie Protokollierung, SSH und SNMPv3 sowie anderer Funktionen.
3. Überprüfung der Geräte/Anlagen auf ordnungsgemäße Konfigurationen, das heißt Änderung standardmäßiger Passwörter und Aktivierung der Verwaltung von Passwörtern (Länge, Sicherheitsniveau, Komplexität etc.).

Grundlegende Schutzmaßnahmen können Folgendes umfassen:

1. Segmentierung des Netzwerks
   a. Zwischen Produktionszonen
   b. Zwischen wichtigen unternehmenskritischen Anlagen/Geräten wie SPSen und RTUs
2. Wappnen von Anlagen und Geräten
   a. Gemäß Industriestandards oder Best Practices wie IEC 62443 oder NIST SP 800-82
   b. Zu den Geräten gehören etwa HMIs, SPSsen, Engineering Arbeitsplätze, ältere Geräte und industrielle Netzwerkgeräte
3. Zentralisierung des gesamten Fernzugriffs mit starker Authentifizierung
   a. Einrichtung einer separaten, geschützte „DMZ“ für alle Fernverbindungen
   b. Umsetzung einer Multi-Faktor Authentifizierung für Benutzer. Das ist ein zweistufiger Authentifizierungsprozess, bei dem manches wie etwa Passwörter bekannt ist und anderes wie etwa Softwaretoken nicht.

Schritt 3: Kontinuierliche Überwachung

Im dritten Schritt wird ein ständiges Monitoring umgesetzt. Denn ebenso wie Sie ein SCADA System zur Optimierung und Steuerung Ihrer industriellen Prozesse verwenden, benötigen Sie eine SCADA-ähnliche Cybersicherheitslösung. Sie trägt dazu bei, die Transparenz industrieller Cybersicherheitsvorfälle zu erhöhen als auch zu steuern und sicherzustellen, dass die von Ihnen umgesetzten Schutzmaßnahmen ordnungsgemäß funktionieren. Das ist jedoch keine einmalige Aktion, sondern muss kontinuierlich durchgeführt werden, da auch ständig neue Bedrohungen auf Sie zukommen.

Eine SCADA-ähnliche Überwachung der industriellen Cybersicherheit hilft, ständig auftauchende Fragen zu beantworten. Hierzu gehören etwa:

1. Woher weiß ich, ob sich die Konfigurationen meiner Geräte/Anlagen ändern und ob diese Änderungen die Geräte in einen nicht sicheren Zustand versetzen oder mit meinen ursprünglichen Spezifikationen nicht mehr übereinstimmen?
2. Woher weiß ich, ob sich meine betrieblichen Basisparameter (die Konfiguration eines Geräts oder einer Anlage, die für den Ablauf des jeweiligen Prozesses spezifisch ist) ändern?
3. Woher weiß ich, ob eines meiner Geräte demnächst ausfallen wird?
4. Woher weiß ich, ob in meinem Steuerungsnetzwerk zurzeit ein nicht autorisiertes Gerät oder Protokoll eingesetzt wird?
5. Woher weiß ich, ob sich meine Risikogefährdung geändert hat?

Wenn Sie imstande sind, all diese Fragen zu beantworten, können Sie Ihre industriellen Prozesse ohne Beeinträchtigung durch Cybersicherheitsvorfälle betreiben.

Da Sie nicht wissen können, ob Ihr Unternehmen ein Ziel für böswillige Angriffe von außen oder innen ist, sollten Sie Ihr Netzwerk genau kennen. Wenn das nicht so ist, wird sich ein anderer damit befassen, der sicherlich keine guten Absichten hat. Steuerungsnetzwerke lassen sich jedoch schützen. Außerdem kann die Cybersicherheit, wie bereits erwähnt, die wichtigsten Leistungskennzahlen industrieller Prozesse unterstützen: Sicherheit, Produktivität und Qualität. Das A und O ist aber, dieses Thema in Angriff zu nehmen. Überlegen Sie sich hierzu eine Strategie, die idealerweise von der Geschäftsführung top-down vorangetrieben wird.

Sie sollten keine Zeit verlieren, Transparenz, Schutzmaßnahmen und eine kontinuierliche Überwachung umzusetzen. Denn in jeder Minute, die Sie ungenutzt verstreichen lassen, ist Ihr Netzwerk vielfältigen Bedrohungen ausgesetzt, die großen finanziellen Schaden anrichten können.

Zusammenfassung

Die Produktion ist der Lebensnerv jedes Unternehmens in der Fabrikautomation. Spezialisten arbeiten dort rund um die Uhr, um qualitativ hochwertige Produkte termingerecht und mit immer knapperen Betriebsbudgets auf den Markt zu bringen. Fortschritte in der Automatisierungstechnik und der Vernetzung des Produktionsbereichs geben ihnen leistungsstarke Werkzeuge an die Hand, mit denen sich die Erträge steigern und der Ausschuss verringern lassen. Diese Werkzeuge können jedoch nicht guten Gewissens eingesetzt werden, ohne das damit verbundene Cybersicherheitsrisiko zu kennen. Mit diesem Bewusstsein und entsprechenden Maßnahmen können Experten für Netzwerk-, Cybersicherheits- und Automatisierungssteuerung in der Fabrikautomation und in vergleichbaren Prozessen die Profitabilität mit innovativen Automatisierungslösungen erhöhen, die durch das IIoT aufkommen, und gleichzeitig das bestmögliche Cybersicherheitsniveau für den Produktionsbereich gewährleisten.

Weitere Informationen zu den industriellen Cybersicherheitslösungen von Belden stehen unter **https://www.belden.com/de/solutions/industrial/cybersicherheit**.

Belden, Belden Sending All The Right Signals, GarrettCom, Hirschmann, Lumberg Automation, Tofino Security, Tripwire und das Belden-Logo sind Handelsmarken oder eingetragene Handelsmarken der Belden Inc. oder verbundener Unternehmen in den USA und anderen Regionen der Welt. Sonstige hierin verwendete Marken und Bezeichnungen können das Eigentum von Belden und anderer Unternehmen sein.

EMEA **+49 (0) 7127/14-1809** | **beldensolutions.com**

US **1-800-BELDEN-1** | **belden.com**

©Copyright 2019, Belden Inc.