Rockwell Automation

Anwenderberichte zur industriellen Cybersicherheit

Herausforderungen, Lösungen und Ergebnisse verschiedenster Industriezweige

Inhaltsverzeichnis

AUSTAUSCH VON ERKENNTNISSEN 01

Eine Mitteilung von Rockwell Automation

DER MARKT IM ÜBERBLICK 02

Cybersicherheitsbedrohungen in der OT-Branche: Ransomware sorgt weiter für Beeinträchtigungen

PHARMABRANCHE 06

Ein globales Pharmaunternehmen erzielt Echtzeittransparenz hinsichtlich der Bedrohungen seiner Industriesteuerungssysteme sowie tägliche Einblicke in den Anlagenbestand an 64 Standorten weltweit

LIFE SCIENCES 08

Ein Hersteller medizinischer Geräte modernisiert seine Netzwerkinfrastruktur, um die OT-Cybersicherheit zu verbessern und das Unternehmenswachstum zu fördern

ENERGIEVERSORGER 10

Ein Energieversorgungsunternehmen verbessert die Cybersicherheit in 62 Kompressorstationen und Terminals mit Echtzeit-Bedrohungserkennung und einer Überwachung des Anlagenbestands

ÖL UND GAS 12

Ein Öl- und Gasunternehmen reduziert das Risiko von Ausfallzeiten aufgrund von Cybervorfällen in nur einem Monat durch Bedrohungserkennung und Identifizierung des Netzwerkbestands in Echtzeit

AUTOMOBILINDUSTRIE 14

Wie ein Automobilhersteller seine OT-Sicherheit in zwei Tagen auf Verbesserungsmöglichkeiten hin überprüft hat

KONSUMGÜTERINDUSTRIE 16

Ein Lebensmittelhersteller setzt ein vereinheitlichtes Risikomanagement an 46 Standorten weltweit ein, um die Cybersicherheit in Dutzenden übernommenen Unternehmen zu vereinheitlichen

LEBENSMITTEL UND GETRÄNKE 18

Ein Lebensmittel- und Getränkehersteller verbessert die Cybersicherheit und die Reaktion auf Vorfälle und steigert die Gesamtanlageneffektivität um 5 %.

LEBENSMITTEL UND GETRÄNKE 20

Ein Lebensmittel- und Getränkeunternehmen optimiert und vereinfacht die OT-Cybersicherheit mit Managed Support Services rund um die Uhr

KONSUMGÜTERINDUSTRIE 22

Ein Konsumgüterunternehmen realisiert eine sichere digitale Transformation und senkt seine durchschnittliche Netzwerkreaktionszeit auf 3,5 Minuten – eine Verbesserung um 90 %

CHEMIE 24

Ein Chemieunternehmen bietet seinen Mitarbeitern während der Pandemie sicheren dezentralen Zugriff auf das Steuerungssystem für 8000 E/A-Punkte

AUSTAUSCH VON ERKENNTNISSEN

Eine Mitteilung von Rockwell Automation

Verehrte Leser,

wir wissen, dass es für Anbieter kritischer Infrastrukturen schwierige Zeiten sind. Angesichts schonungsloser Cyberangriffe, komplexer Initiativen zur digitalen Transformation und einer scheinbar nie endenden Pandemie müssen sich viele Unternehmen mit der Sicherung ihrer OT-Systeme auseinandersetzen.

Die OT-Sicherheit wird immer wichtiger, da Bedrohungsakteure erwiesenermaßen in IT-Systeme eindringen können und werden, um OT- und Industriesteuerungssysteme zu infiltrieren. Sie werden feststellen, dass diese Art der Sicherheitsverletzung auch IT-Systeme und kritische Infrastrukturen lahmlegen kann.

Wenn es eine Bedrohung gibt, die Führungskräften in Unternehmen besondere Sorgen bereitet, dann sind es die weltweit zunehmenden Ransomware-Angriffe. Angesichts der zunehmenden Spannungen nach dem Einmarsch Russlands in die Ukraine hat die Agentur für Cybersicherheit und Infrastruktursicherheit (Cybersecurity and Infrastructure Security Agency, CISA) beispielsweise die Betreiber von Netzwerken der staatlichen und lokalen Behörden in den USA, der Luftfahrt und des Energiesektors vor einem erhöhten Risiko von Ransomware-Angriffen aus Russland gewarnt.

Hinzu kommt, dass viele Organisationen mit kritischen Infrastrukturen nicht über automatisierte Funktionen zur Erkennung von und Reaktion auf Bedrohungen verfügen, wie etwa die kontinuierliche Überwachung von Netzwerken und Systemen. Weitere häufige Probleme sind Risiken im Zusammenhang mit der digitalen Transformation, mit älteren Systemen und Anwendungen, nicht vernetzten digitalen Ressourcen und dem Mangel an zentralem Netzwerk- und Bedrohungsmanagement.

Darüber hinaus hat COVID-19 eigene Herausforderungen mit sich gebracht, wie z. B. den Bedarf an sicheren dezentralen Arbeitsplätzen sowie regelmäßige Betriebsunterbrechungen und Ausfälle der Lieferkette.

Haben Sie sich schon einmal gefragt, wie Unternehmen mit diesen unzähligen Risiken umgehen? In dieser Zusammenfassung von Anwenderberichten der Kunden von Rockwell Automation gehen wir der Frage nach, was sich für andere Organisationen in den unterschiedlichsten Branchen bewährt hat, darunter Pharmaindustrie, Life Sciences, Energie, Öl und Gas, Automobilbau, Lebensmittel und Getränke, Konsumgüter und vertikale Fertigung.

Wenn Sie sich Gedanken über Bedrohungen für Ihre OT- und Industriesteuerungsinfrastruktur machen, sollten Sie die folgenden Anwenderberichte aufmerksam lesen. Unsere erfahrenen Teams haben Unternehmen aus verschiedenen Branchen dabei geholfen, sicherere industrielle Abläufe zu realisieren. Zwar ist kein Infrastrukturprogramm garantiert zu 100 % risikofrei, doch gibt es bewährte Lösungsansätze, die die Sicherheitsrisiken für kritische Infrastrukturen effektiv und effizient verringern können.

Kamil Karmali

Global Manager, Cybersecurity Consulting Services

Rockwell Automation

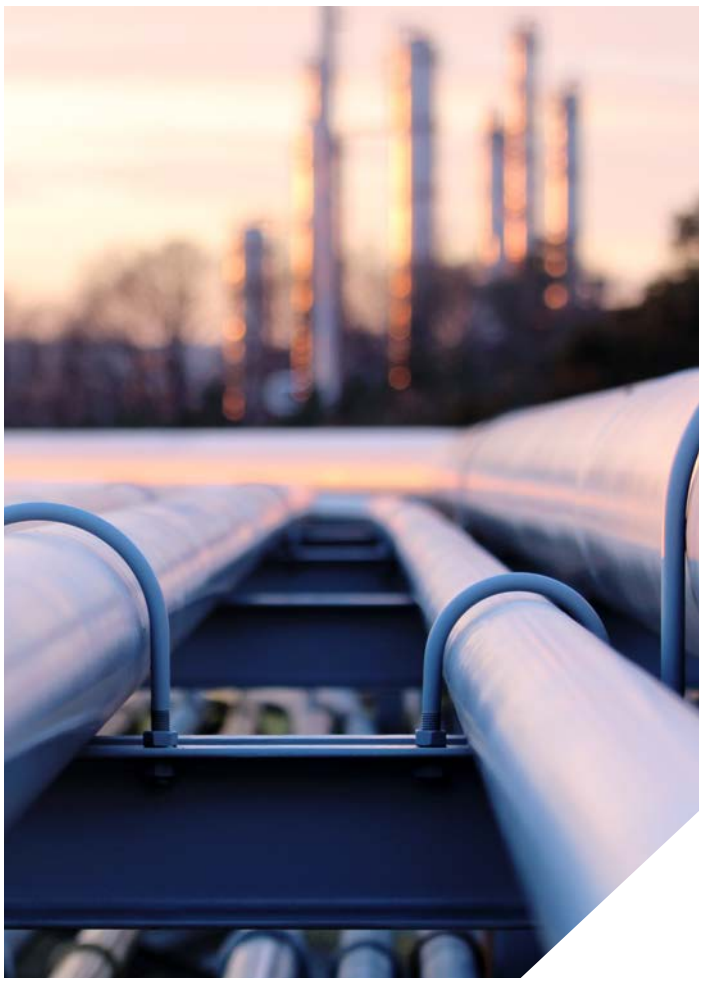
DER MARKT IM ÜBERBLICK

Cybersicherheitsbedrohungen in den OT-Industrien

RANSOMWARE SORGT WEITERHIN FÜR STÖRUNGEN

Wenn Erfahrung der beste Ratgeber ist, dann sind die Lektionen, die Sie von anderen in Ihrer Branche lernen können, vielleicht die zweitbesten. Organisationen, die von internen oder externen Bedrohungsakteuren angegriffen werden, lernen in der Regel wertvolle Lektionen über Cybersicherheit – unter anderem, wie sie Schwachstellen erkennen und schließen und wie sie sich gegen künftige Angriffe schützen können.

Die folgenden Anwenderberichte zeigen auf, wie 10 Anbieter kritischer Infrastrukturen ihre Sicherheitsvorkehrungen verbessert haben, bevor Cyberkriminelle Kennwörter abgreifen und in Netzwerke und Anwendungen eindringen konnten. Doch zunächst erhalten Sie einen Überblick über den aktuellen Stand der Cyberangriffe und der Sicherheit in sechs von 16 Branchen mit kritischen Infrastrukturen, die von der Cybersecurity and Infrastructure Security Agency (CISA) ermittelt wurden.



PHARMAINDUSTRIE UND LIFE SCIENCES

Angriffe auf das Herzstück der Reaktionen auf COVID-19

Unternehmen aus den Bereichen Pharmaindustrie und Life Sciences stehen im Mittelpunkt der Reaktionen auf COVID-19.

Cyberkriminelle nutzen die Pandemie weiterhin zu kommerziellen Zwecken aus, indem sie Malware, Ransomware, Phishing und URL-Betrug einsetzen, wobei sie häufig Themen zu COVID-19 und zum Coronavirus als Lockmittel verwenden. Wie in anderen Branchen auch, versuchen Bedrohungsakteure, sich Zugang zu Infrastrukturen zu verschaffen, die neu mit einem dezentralen Zugriff für von zuhause aus arbeitende Mitarbeiter ausgestattet wurden.

Hinzu kommt, dass Angriffe aus Ländern wie Nordkorea, Russland und China, die darauf abzielen, Unternehmen, die COVID-19-Impfstoffe, Heilmittel und medizinische Geräte entwickeln, zu schädigen, immer raffinierter werden. Zu den Angriffszielen zählen beispielsweise Industriespionage, Diebstahl von geistigem Eigentum und Zugriff auf geschützte Gesundheitsinformationen von Patienten.

Bedrohungsakteure nehmen auch Hersteller medizinischer Geräte ins Visier und versuchen, sich in tragbare und implantierbare medizinische Geräte einzuhacken. Einige dieser Geräte, wie z. B. vernetzte Herzschrittmacher und Blutzuckermessgeräte, werden über das Internet mit Krankenhausnetzwerken verbunden. Viele Führungskräfte der Medizinbranche befürchten, dass vernetzte medizinische Geräte Cyberangriffen auf Krankenhäuser und medizinische Einrichtungen Tür und Tor öffnen, was Menschenleben gefährden könnte.

In Anbetracht der hohen Risiken hat die Food and Drug Administration, die diese Geräte reguliert, der Notwendigkeit von Aktualisierungen zur ordnungsgemäßen Sicherung dieser Geräte Priorität eingeräumt.

86 % DER UNTERNEHMEN GEBEN AN, DASS SIE NUR EINEN BEGRENZTEN ODER GAR KEINEN EINBLICK IN DIE UMGEBUNG IHRER INDUSTRIESTEUERUNGSSYSTEME HABEN.

QUELLE: DRAGOS

ÖL UND GAS

Pipelinesicherheit und der Angriff, der weltweit für Aufsehen sorgte

Nach dem Angriff auf Colonial Pipeline, dem größten Treibstoffpipeline-Anbieter der USA, machen sich Führungskräfte der Öl- und Gasindustrie verständlicherweise Sorgen um Ransomware-Angriffe. Der Angriff legte einige Geschäftssysteme lahm und führte im Osten der USA zu Gasmangel.

Laut Bloomberg verschafften sich die Hacker am 29. April 2021 über ein VPN-Konto, das zum Zeitpunkt des Angriffs nicht mehr genutzt wurde, aber immer noch für den Zugriff auf das Netzwerk von Colonial Pipeline verwendet werden konnte, Zugang zu den entsprechenden Netzwerken. Und in einem kürzlich veröffentlichten Bericht wurde festgestellt, dass bei 77 % der großen US-Energieunternehmen mindestens ein Kennwort online geleakt wurde.

Auch bei Öl- und Gasunternehmen häufen sich die Sicherheitsvorfälle, da die Unternehmen ihre OT-Systeme digitalisieren und mit Industriesteuerungssystemen verbinden, um Betriebsabläufe zentral zu verwalten. In den USA ist der Öl- und Gassektor nach Finanzdienstleistern und dem verarbeitenden Gewerbe die Branche, die am dritthäufigsten angegriffen wird.

Der Angriff auf Colonial Pipeline verdeutlicht nicht nur, wie leicht Bedrohungsakteure in OT-Systeme eindringen können, sondern zeigt auch die potenziell katastrophalen Auswirkungen von Angriffen auf Anbieter kritischer Infrastrukturen – und damit auf das tägliche Leben der Verbraucher.

AUTOMOBILINDUSTRIE

Zunehmende Konnektivität weckt neue Sorgen um die Cybersicherheit

In der Automobilbranche sehen sich Fahrzeug- und Teilehersteller mit einer steigenden Zahl von Ransomware-Angriffen konfrontiert, die die Sicherheit von konvergierten IT- und OT-Systemen gefährden können. Eine Studie ergab, dass 49 % der führenden Automobilhersteller sehr anfällig für Ransomware-Angriffe sind. In zahlreichen Fällen beginnen diese Angriffe mit dem Eindringen in IT-Systeme und breiten sich dann auf angeschlossene OT-Anlagen aus.

Bei einem unlängst erfolgten Angriff auf einen globalen Automobilhersteller starteten Cyberkriminelle beispielsweise eine Phishing-Kampagne, die Ransomware in das IT-System des Unternehmens einschleuste, die sich dann auf die OT-Anlagen ausbreitete. Der Angriff führte zum Stillstand von Produktionsanlagen auf der ganzen Welt und legte die IT- und E-Mail-Systeme des Unternehmens lahm.

Ransomware ist nicht die einzige Bedrohung, die Führungskräften schlaflose Nächte bereitet. Störungen durch Cyberangriffe auf Automobilzulieferer haben zu Problemen in der Lieferkette geführt, die sich branchen- und länderübergreifend auswirkten und zu Betriebseinschränkungen und in einigen Fällen sogar zur Schließung ganzer Werke führten.

KONSUMGÜTERINDUSTRIE

Häufigkeit und Kosten von Cyberangriffen nehmen zu

Konsumgüterunternehmen verzeichnen immer mehr Vorfälle im Bereich der Cybersicherheit. Mehr als 40 % der Konsumgüterhersteller wurden im Jahr 2020 Opfer eines Cyberangriffs. Und die finanziellen Folgen der Beeinträchtigungen sind hoch – Tendenz steigend. Die durchschnittlichen Kosten von Datenschutzverletzungen im Konsumgütersektor stiegen 2021 auf 3,7 Millionen USD, was einem Anstieg von 42,9 % gegenüber dem Vorjahr entspricht.

Zu den Trends, die die Anforderungen an die Cybersicherheit vermutlich noch erhöhen werden, gehören der verstärkte Einsatz von Sensoren und Geräten des Internets der Dinge (IoT), die zunehmende Verfügbarkeit von 5G und die Konvergenz von IT- und OT-Netzwerken. Immer mehr Geräte und Betriebssysteme werden miteinander vernetzt sein und Daten über Netzwerke übertragen, was die Angriffsfläche erheblich vergrößert.

Die Auseinandersetzung mit den Angriffen auf die Lieferkette hat die Konsumgüterhersteller auch dazu veranlasst, die Beschaffung zu überdenken, Lagerflächen anzupassen und Liefermodelle zu überdenken sowie die Wirtschaftlichkeit ihrer Anbieter und Lieferanten neu zu bewerten.

LEBENSMITTEL UND GETRÄNKE

Die zerstörerischen Auswirkungen von Ransomware-Angriffen nehmen zu

Die Branche sah sich erdrutschartigen Veränderungen bei den Kundenwünschen nach gesünderen Lebensmitteln und ansprechenden Einkaufserlebnissen gegenüber. Jüngere Verbraucher tendieren zum Beispiel zu nährstoffreichen Lebensmitteln auf pflanzlicher Basis, die aus lokaler Produktion stammen und in umweltfreundlichen Verpackungen angeboten werden. Gleichzeitig wurden die Folgen von Cyberangriffen auf Lebensmittel- und Getränkeunternehmen hinsichtlich der Kosten und Ausfallzeigen immer gravierender.

Und dann kam die COVID-19-Pandemie. Lebensmittel- und Getränkeunternehmen führten in kurzer Zeit dezentrale Arbeitsplattformen ein, um den neuen Anforderungen an die Sicherheit und den Schutz der Privatsphäre ihrer Mitarbeiter gerecht zu werden. Die Unternehmen stellten fest, dass ihre älteren Systeme und Anwendungen oft nicht mit modernen Cybersicherheitslösungen kompatibel waren. Die Notwendigkeit aktueller, risikobasierter Sicherheitsprogramme wurde immer offensichtlicher, vor allem angesichts der zunehmenden Angriffe.

Der Ransomware-Angriff auf JBS, einen großen brasilianischen Fleischverarbeitungsbetrieb, betraf beispielsweise Werke in den USA, Kanada und Australien. Bedrohungsakteure verschlüsselten die Systeme und Daten des Unternehmens und forderten dann ein Lösegeld in Höhe von mehreren Millionen Dollar, um den Zugang wiederherzustellen. JBS bezahlte 11 Milliarden USD. Darüber hinaus gab es in den 12 Monaten vor dem Angriff auf JBS schätzungsweise 40 weitere Angriffe auf Lebensmittelunternehmen, wie die Chicago Tribune berichtet.

Diese Art von Malware-Kampagne verdeutlicht den Trend, dass immer mehr Lebensmittel- und Getränkeunternehmen ins Visier genommen werden, die konvergierte IT- und OT-Systeme zur besseren Verwaltung der Produktion einsetzen. Ohne angemessene Cybersicherheitsplanung und -kontrollen können OT-Systeme durch diese Konvergenz einer Reihe von hochentwickelten Cyberbedrohungen ausgesetzt werden.

Lehren aus dem Erfolg anderer

Die folgenden Anwenderberichte zeigen, wie vielfältig die Herausforderungen sind, mit denen Kunden von Rockwell Automation konfrontiert sind. Dennoch weisen alle gemeinsame Elemente auf.

Die besten OT-Cybersicherheitslösungen – in Bezug auf die Qualität des Schutzes, die Geschwindigkeit der Bereitstellung und den laufenden Service, der Ausfallzeiten minimiert und Cyberangriffe abwehrt – erfordern Erfahrung im industriellen Betrieb.

Suchen Sie in diesen Berichten nach Parallelen zu Ihren eigenen Herausforderungen. Wir sind uns bewusst, dass die in dieser Zusammenfassung vermittelten Einblicke für das Verständnis der Lösungsmöglichkeiten, die zur Bewältigung von OT-Bedrohungen in verschiedenen Branchen eingesetzt werden können, von großem Wert sind.

PHARMABRANCHE

Ein internationales Pharmaunternehmen erzielt Transparenz hinsichtlich der Bedrohungen seiner Industriesteuerungssysteme und führt eine tägliche Bestandsaufnahme seiner Anlagen an 64 Standorten weltweit in Echtzeit durch

Pharmaunternehmen sind seit langem ein beliebtes Ziel für raffinierte Cyberkriminelle. Die COVID-19-Pandemie hat jedoch die Notwendigkeit eines risikobasierten Cybersicherheitsprogramms noch verstärkt – und zwar in kürzester Zeit.

Ein weltweit operierender Pharmahersteller benötigte Unterstützung beim Aufbau eines Cybersicherheitsprogramms für seine IT- und OT-Systeme. Nicht gepatchte OT-Systeme erhöhten die Sicherheitsrisiken für Produktionsanlagen, und die fehlende Echtzeittransparenz von Bedrohungen für Industriesteuerungssysteme machte es nahezu unmöglich, OT-Malware zu erkennen.

Erschwerend kam hinzu, dass der Pharmakonzern seine Unternehmensnetzwerke nicht von den Netzwerken der Industrieanlagen isoliert hatte und auch den Datenverkehr sowie die Verbindungen zu und von kritischen Produktionssystemen nicht eingeschränkt hatte.

Mit Blick auf die Zukunft wusste das Unternehmen, dass es seine Teams in guter Cybersicherheitshygiene schulen musste, um dauerhafte Verbesserungen der Sicherheitskultur zu erreichen.

88 % DER US-FÜHRUNGSKRÄFTE IN DER MEDIZINTECHNIK GLAUBEN NICHT, DASS IHRE UNTERNEHMEN AUF EINEN CYBERSICHERHEITSVORFALL VORBEREITET SIND.

QUELLE: IRDETO

WAS WURDE BEREITGESTELLT?

Nach einer Risikobeurteilung ging der Pharmariese eine Partnerschaft mit Rockwell Automation ein und unternahm wichtige Schritte zur Verbesserung der Cybersicherheitsmaßnahmen durch Netzwerksegmentierung und Stärkung der Endpunkt- und Perimetersicherheit.

Zu Beginn wurde schnell ein dreistufiges Cybersicherheitsprogramm entwickelt und realisiert.

Erste Priorität hatte die Trennung der logischen und physischen Netzwerke an 64 Standorten weltweit, um die Ausbreitung von Bedrohungen einzudämmen, sobald Netzwerke und Systeme von diesen betroffen waren. Außerdem verstärkte das Unternehmen die Sicherheit von Perimeter-Geräten, um Bedrohungsakteure zu behindern, und setzte zum Schutz der Endgeräte „Zulassungslisten" für Anwendungen ein, um die Nutzung von Anwendungen nur dann zuzulassen, wenn diese zuvor genehmigt wurden.

Als Nächstes führte das Unternehmen eine Reihe von Services zur Bedrohungserkennung ein und implementierte die USB-Datenbereinigung zur zentralen Verwaltung und Überwachung von USB-Medien im OT-Netzwerk, um sich vor Bedrohungen oder Angriffen zu schützen – sowohl von innerhalb als auch von außerhalb des Netzwerks. Die Bedrohungserkennungsdienste bestimmen auch das normale Netzwerkverhalten, das als Basiswert verwendet werden kann, und setzen rund um die Uhr Bedrohungsüberwachungsfunktionen ein, um anormale Aktivitäten zu erkennen und entsprechend zu signalisieren. So kann das Unternehmen Aktivitäten, die seine Systeme gefährden könnten, schneller oder noch vor einem Angriff erkennen.

ERGEBNISSE

Rockwell Automation unterstützte das Pharmaunternehmen bei der Entwicklung und Implementierung einer erweiterten Sicherheitsstrategie für 64 Standorte weltweit in nur neun Monaten. Auf diese Weise ist das Unternehmen nun besser in der Lage, seine OT-Anlagen und Industriesteuerungssysteme vor den immer raffinierteren Cyberbedrohungen zu schützen. Das Unternehmen hat nun einen durchgängigen Echtzeitüberblick über Bedrohungen der Industriesteuerungssysteme im gesamten Konzern.

DIE FAKTEN

Schneller Aufbau eines ausgefeilten Schutzes gegen Cyberbedrohungen

AUFGABENBEREICH

- Umsetzung innerhalb von 9 Monaten
- 64 Standorte weltweit

LÖSUNGEN

- Cybersicherheitsplan
- Netzwerksegmentierung
- Endgeräte- und Perimetersicherheit
- Bedrohungserkennung
- Management von USB-Medien

LIFE SCIENCES

Ein Hersteller medizinischer Geräte modernisiert seine Netzwerkinfrastruktur, um die OT-Cybersicherheit zu verbessern und das Unternehmenswachstum zu steigern

Ein in den USA ansässiger Hersteller medizinischer Geräte hatte ehrgeizige Pläne zur Erweiterung seiner globalen Produktionskapazitäten.

Aufgrund der Wachstumsprognosen wurde ein standardisiertes Infrastrukturkonzept benötigt, das die Ausweitung der digitalen Transformation und die Modernisierung der OT-Infrastruktur unterstützen konnte. Außerdem musste das Unternehmen die Cybersicherheit durch die Segmentierung seiner IT- und OT-Netzwerke verbessern.

Im Laufe der Jahre hatten die Investitionen in die OT nicht mit denen in die IT Schritt gehalten, und das Unternehmen musste die IT- und OT-Systeme umgestalten, um die Cybersicherheitsmaßnahmen für ein wachsendes und expandierendes digitales Unternehmen zu verbessern.

Schnelligkeit war von entscheidender Bedeutung Der Gerätehersteller musste eine zentrale Cybersicherheits- und Modernisierungsstrategie entwickeln und schnell umsetzen, um seine erweiterten Netzwerke und digitalen Ressourcen zu schützen. Allerdings fehlten dem Unternehmen die Ressourcen, um die neuen Funktionen schnell genug zu implementieren, damit der Zeitplan eingehalten werden konnte.

80 % DER WELTWEIT FÜHRENDEN SICHERHEITSEXPERTEN HALTEN RANSOMWARE FÜR EINE GEFÄHRLICHE UND WACHSENDE BEDROHUNG DER ÖFFENTLICHEN SICHERHEIT.

QUELLE: WELTWIRTSCHAFTSFORUM

WAS WURDE BEREITGESTELLT?

Rockwell Automation entwickelte gemeinsam mit dem Medizingerätehersteller einen umfassenden Plan zur Beurteilung und Neugestaltung von Netzwerken sowie zur Einrichtung einer industriellen Demilitarized Zone (IDMZ) für sieben Standorte in vier Regionen weltweit.

Als Nächstes wurde ein Standardkonzept für die virtuelle Infrastruktur des Unternehmens entwickelt. Das Unternehmen begann mit der Segmentierung seiner IT- und OT-Netzwerke, um die Daten, die zwischen den Umgebungen ausgetauscht werden, besser zu schützen. Eine weitere wichtige Initiative war die Schaffung einer digitalen Sicherheitsgrenze, einer so genannten IDMZ, zwischen IT- und OT-Netzwerken. Bei dieser Technologie werden Netzwerk- und Anwendungssicherheitskontrollen eingesetzt, um den zonenübergreifenden Datenfluss zu verwalten und zu schützen.

Während der 12-monatigen Initiative benötigte das Unternehmen eine Einschätzung der genauen Anforderungen und Kosten der Automatisierung sowie Informationen zur Netzwerk- und IDMZ-Realisierung und einheitliche Netzwerkdesign-Standards. Das Unternehmen arbeitete mit mehreren Partnern aus dem Rockwell Automation-Ökosystem zusammen, um diese Einschätzung zu erlangen und die Implementierung zu unterstützen, darunter Panduit für die physische Installation und Verkabelung und unser LifecycleIQ Services-Geschäftsbereich für die globale Bereitstellung von Supervisory Control and Data Acquisition(SCADA)-Systemen.

Außerdem führte das Unternehmen ein Managed Services-Programm zur Überwachung und Verwaltung seiner Netzwerke, Rechenzentren und Anwendungen ein.

ERGEBNISSE

Mit der Lösung erreichte das Unternehmen sein Ziel, ein standardisiertes Netzwerk und eine IDMZ-Infrastruktur zu schaffen, um ein schnelles und sicheres Wachstum zu fördern und gleichzeitig die Produktionskapazität zu erhöhen. Das Konzept bot die richtige Struktur für eine schrittweise Umsetzung an neu errichteten Standorten und kann auch für die Modernisierung der Netzwerkinfrastruktur an bestehenden Standorten sowie für das dezentrale Management verwendet werden, wenn die Netzwerkanforderungen nach einer Erweiterung verlangen.

Der Hersteller medizinischer Geräte hat nun einen Überblick über seine Investitionskosten (CapEx) für diese Anforderungen, sodass eine bessere strategische Planung und Entscheidungsfindung möglich ist und sichergestellt werden kann, dass die Cybersicherheit mit dem Wachstum des Unternehmens Schritt hält.

DIE FAKTEN

Sichere Skalierung mit einer modernen Netzwerkinfrastruktur

AUFGABENBEREICH

- Umsetzung in 12 Monaten
- 7 Standorte weltweit

LÖSUNGEN

- Netzwerkdesign und -konzept
- IDMZ
- Managed Services für die Cybersicherheit

ENERGIEVERSORGER

Das Unternehmen für Erdgasspeicherung und Pipelines verbessert die Cybersicherheit in 62 Kompressorstationen und Terminals mit Echtzeit-Bedrohungserkennung und einer Überwachung des Anlagenbestands

Da Öl- und Gasunternehmen zunehmend versuchen, sich vor der steigenden Zahl an Cyberangriffen zu schützen, erkennen viele die Notwendigkeit, ein umfassendes Cybersicherheitsprogramm zum Schutz ihrer IT- und OT-Netzwerke einzuführen.

So war es auch bei einem großen zwischenstaatlichen Gaspipeline-Anbieter in den USA. Das Fehlen eines einheitlichen Cybersicherheitsprogramms führte dazu, dass die Geschäfts- und IT-Führungskräfte des Unternehmens bestenfalls über ein minimales Verständnis der aktuellen und zukünftigen Bedrohungen für Geräte, Netzwerke und die Produktionsbetriebszeit verfügten. Ein Angreifer hätte jederzeit die Möglichkeit, unbemerkt in die digitalen Systeme des Unternehmens einzudringen, wodurch der Betrieb gestört und sogar Anlagen und Einrichtungen beschädigt oder stillgelegt werden könnten.

Als das Unternehmen im Rahmen seiner digitalen Transformation IT- und OT-Systeme vernetzte, erkannten die Führungskräfte die Notwendigkeit, ein zentrales, risikobasiertes Cybersicherheitsprogramm zu implementieren, das es dem Unternehmen ermöglichen würde, Cyberbedrohungen in allen Netzwerken schnell zu erkennen und auf sie zu reagieren.

BEI 77 % DER GROSSEN US-ENERGIEUNTERNEHMEN WURDE MINDESTENS EIN KENNWORT ONLINE GELEAKED, SODASS SIE ANFÄLLIG FÜR ANGRIFFE SIND.

QUELLE: THE HOUSTON CHRONICLE

WAS WURDE BEREITGESTELLT?

Rockwell Automation unterstützte das Unternehmen für Erdgaspipelines bei der Entwicklung und Umsetzung der Grundlagen für einen vereinheitlichten Risikoschutz in 62 nordamerikanischen Kompressorstationen und Terminals.

In Zusammenarbeit mit dem Ökosystempartner Claroty entwickelte Rockwell Automation Managed Services zur Bedrohungserkennung mit Überwachung des Anlagenbestands, um alle IT- und OT-Anlagen im Unternehmensnetzwerk zu identifizieren. Die Bestandsaufnahme der installierten Basis ist ein entscheidender Schritt zur Aufdeckung von Sicherheitslücken und zur Entwicklung eines Plans zur Abwehr interner und externer Bedrohungen, der eine schnellere Reaktion und Eindämmung von Cyberangriffen ermöglicht. Der Pipeline-Anbieter konnte in Zusammenarbeit mit Claroty auch dessen Lösung zur Echtzeit-Bedrohungsüberwachung implementieren und Workflows für die Reaktion auf Vorfälle definieren.

Mit modernen Funktionen zur Bedrohungserkennung ist der Pipeline-Anbieter nun in der Lage, Cybersicherheitsbedrohungen von außen und an den Unternehmensstandorten schnell zu erkennen und darauf zu reagieren. Darüber hinaus wurden Best Practices für die Belegschaft entwickelt, die einen eindeutigen Überblick über die sich wandelnden Anforderungen geben.

ERGEBNISSE

Rockwell Automation unterstützte das Unternehmen dabei, in rund 11 Monaten die Grundlage für eine moderne Sicherheitsinitiative zu schaffen – eine kurze Zeitspanne für eine komplexe, aber dringende Aufgabe. Heute hat das Unternehmen dank der vollständigen Transparenz aller digitalen Ressourcen in IT- und OT-Netzwerken seine Sicherheitslage verbessert und kann Sicherheitsbedrohungen kontinuierlich in Echtzeit erkennen und schnell auf Vorfälle reagieren, um die Auswirkungen von Sicherheitsverletzungen zu verringern.

DIE FAKTEN

Verbesserung der Sicherheit in der Pipeline

AUFGABENBEREICH

- Umsetzung in 11 Monaten
- 62 Standorte in Nordamerika

LÖSUNGEN

- Verwaltete Bedrohungserkennung
- Bedrohungsüberwachung
- Bestandsaufnahme der Anlagen
- Planung der Reaktion auf Vorfälle.

ÖL UND GAS

Öl- und Gasunternehmen reduziert das Risiko von Ausfallzeiten aufgrund von Cybervorfällen in nur einem Monat durch Echtzeit-Bedrohungserkennung und Identifizierung des Netzwerkbestands

Die Cyberbedrohungen für Öl- und Gassysteme nehmen zu, da Bedrohungsakteure den Energiesektor mit Ransomware und anderer Malware ins Visier nehmen. Der Angriff auf Colonial Pipeline hat bewiesen, dass Sicherheitsverletzungen die Services und Versorgung kritischer Infrastrukturen empfindlich stören, Millionen von Menschen in Mitleidenschaft ziehen und erhebliche finanzielle Verluste verursachen können.

Parallel dazu hat COVID-19 die Entwicklung der Digitalisierung beschleunigt und dazu geführt, dass Mitarbeiter dezentral arbeiten müssen, was die Sicherheitsrisiken weiter erhöht.

Zur Verringerung der Risiken musste ein multinationales Energieunternehmen seine Risikomanagementstrategie verbessern. Ein wesentliches Element dabei war die Aktualisierung der OT-Systeme, um die Risiken im Falle eines Cyberangriffs zu minimieren.

Dem Unternehmen war auch bewusst, dass es seine digitalen Ressourcen proaktiv schützen musste, indem es eine skalierbare Plattform zur Erkennung von Bedrohungen implementierte, die Schwachstellen und potenzielle Bedrohungen schnell identifizieren und datengestützte betriebliche Erkenntnisse zur Verbesserung der Entscheidungsfindung generieren konnte.

Das Unternehmen benötigte außerdem Unterstützung bei der Verwaltung von Kosten im Zusammenhang mit der Veralterung und Modernisierung von Technologien sowie bei der Umgestaltung von inkonsistenten Lösungen in eine einheitlichere Infrastruktur.

79 % DER ÖL- UND GASUNTERNEHMEN BERICHTEN VON EINER ZUNAHME GEFÄHRLICHER ANGRIFFE IN DEN LETZTEN 12 MONATEN.

QUELLE: EY GLOBAL STATE OF SECURITY SURVEY 2021

WAS WURDE BEREITGESTELLT?

In Zusammenarbeit mit Rockwell Automation wurde ein umfassendes Programm zur Bedrohungserkennung entwickelt und umgesetzt. Die Lösung ermittelt einen Basiswert des normalen Netzwerkverhaltens und stellt eine Bestandsaufnahme der Netzwerkressourcen in Echtzeit zur Verfügung. Außerdem überwacht sie kontinuierlich die Aktivitäten, um ungewöhnliches Verhalten zu erkennen und zu melden, bevor Bedrohungen zu Sicherheitsverletzungen führen. Die Lösung zur Bedrohungserkennung ermöglichte auch ein umfassendes Verständnis von OT-Systemen und Netzwerkaktivitäten, was die Entscheidungsfindung insgesamt verbesserte.

In Zusammenarbeit mit dem Energieunternehmen implementierten Rockwell Automation und der Ökosystempartner Claroty Bedrohungsmanagementlösungen für insgesamt 12 Raffinerien, 3 Midstream-Anlagen, 1 SCADA-System und 1 zentrale Unternehmensmanagementkonsole.

49 % DER FÜHRENDEN US-ENERGIEUNTERNEHMEN WEISEN EINE KRITISCHE SCHWACHSTELLE AUF, DIE AUF VERALTETE SYSTEME ZURÜCKZUFÜHREN IST.

QUELLE: BLACK KITE RESEARCH

ERGEBNISSE

Dieses Öl- und Gasunternehmen verfolgt nun eine einheitliche Strategie zum Schutz von OT- und IT-Netzwerken vor Sicherheitsverletzungen, einschließlich Services zur Bedrohungserkennung und Echtzeit-Inventarisierungsfunktionen, die es dem Unternehmen ermöglichen, Cybersicherheitsbedrohungen zu erkennen, auf sie zu reagieren und sie zu entschärfen, während gleichzeitig die Wahrscheinlichkeit von Ausfallzeiten aufgrund von Cybersicherheitsvorfällen verringert wird, was das Risiko von Betriebsunterbrechungen minimiert.

Bereits einen Monat nach der Einführung des Pilotprojekts bot die Lösung verbesserte Sicherheitsfunktionen. Derzeit unterstützt sie die Unternehmensleitung dabei, die Leistungsfähigkeit von Betrieb und Belegschaft besser zu verstehen, die Überlastung der Sicherheitsteams zu verringern und datengestützte Entscheidungen zu treffen.

DIE FAKTEN

Minimierung der Risiken für die Geschäftskontinuität durch verbesserte Bedrohungserkennung

AUFGABENBEREICH

- 1 Monat Pilotprojekt
- 17 Standorte
- Ökosystempartner: Claroty

LÖSUNGEN

- Bedrohungserkennung
- Aufnahme des Anlagenbestands in Echtzeit

AUTOMOBILINDUSTRIE

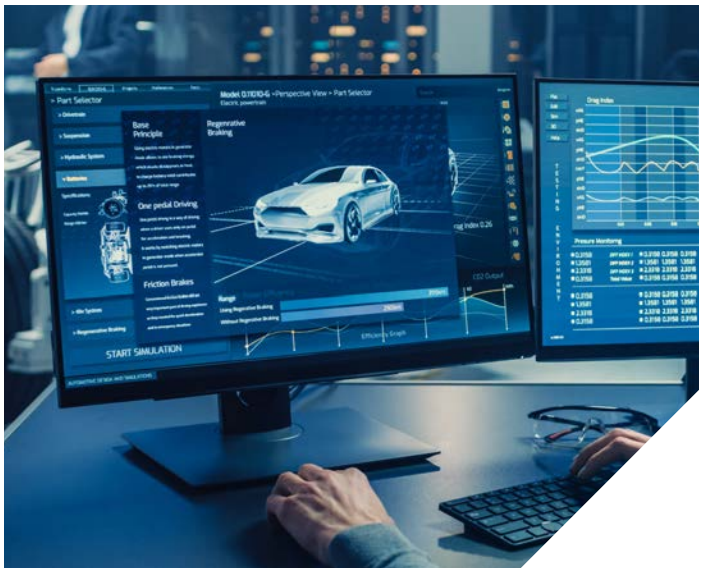
Wie ein Automobilhersteller die OT-Sicherheit in Rekordzeit auf Verbesserungsmöglichkeiten hin überprüft hat

Automobilhersteller stehen vor zahlreichen Herausforderungen, wenn sie sich mit den sich schnell entwickelnden Produktanforderungen und einem sich wandelnden Ökosystem auseinandersetzen. Inmitten chaotischer Zustände machte sich ein weltweit tätiger Automobilhersteller Sorgen um seine mangelnde Cybersicherheit.

Insbesondere befürchtete das Unternehmen, dass Cyberkriminelle durch OT-Schwachstellen in IT- und OT-Netzwerke eindringen könnten, um sensible Informationen zu stehlen und Betriebsabläufe sowie Produktionslinien zu beeinträchtigen. Zwar hatte das Unternehmen vor Kurzem in die Sicherung seiner kritischen Produktionsumgebung investiert, doch die Verantwortlichen waren der Ansicht, dass die Netzwerke weiterhin anfällig für Sicherheitsverletzungen waren. Und da eine Flut von Phishing- und Ransomware-Angriffen auf einzelne Mitarbeiter abzielte, wusste das Unternehmen, dass ein erhöhtes Bewusstsein für Bedrohungen bei den Mitarbeitern dazu beitragen würde, die Cybersicherheitsrisiken für die IT- und OT-Infrastrukturen des Unternehmens zu verringern.

48 % DER AUTOMOBILHERSTELLER HABEN EIN HOHES RISIKO FÜR EINEN RANSOMWARE-ANGRIFF.

QUELLE: BLACK KITE, RANSOMWARE RISK: AUTOMOTIVE MANUFACTURING IN 2021, JUNI 2021



WAS WURDE BEREITGESTELLT?

Rockwell Automation unterstützte das Automobilunternehmen bei der Bewertung der Cybersicherheitsfähigkeiten mithilfe eines Penetrationstests – einem simulierten Cyberangriff auf Systeme, der von Experten durchgeführt wird, um Sicherheitslücken aufzudecken.

In diesem Fall wollte das Automobilunternehmen feststellen, ob externe Akteure in IT- und OT-Umgebungen eindringen und die Kontrolle über diese erlangen könnten. Dank der OT-Cybersicherheits-Expertise des Rockwell Automation-Teams konnten die erforderlichen Tests sechs Wochen schneller abgeschlossen werden als bei einem durchschnittlichen Drittanbieter.

Und tatsächlich stellte das Team innerhalb von zwei Tagen fest, dass in mehreren Bereichen der Fertigungseinrichtung eine Fernsteuerungssoftware installiert worden war, um den Sicherheitsexperten eine schnelle Verbindung zu ermöglichen. Unsere Cybersicherheitsexperten testeten die Anwendung gemeinsam mit dem CIO und dem CISO des Unternehmens und erkannten, dass es möglich war, eine direkte Verbindung vom öffentlichen Internet zu den einzelnen Produktionsumgebungen herzustellen und dabei die mit Firewalls gesicherten Perimeter zu umgehen.

Mit anderen Worten: In einem zweitägigen Penetrationstest stellte Rockwell Automation fest, dass Cyberkriminelle die vollständige Kontrolle über IT- und OT-Netzwerke erlangen und auf digitale Ressourcen und Geräte zugreifen konnten, darunter Human Machine Interface(HMI)-Server und Steuerungssysteme, geheime Fertigungspläne, sensible Kundendaten, Überwachungskameras und sogar Benutzerkennwörter für Microsoft Office 365-E-Mail-Konten, einschließlich des Kontos des CEO.

ERGEBNISSE

Mithilfe von Penetrationstests und -beurteilungen ließen sich schnell mehrere kritische Schwachstellen aufdecken, über die Bedrohungsakteure die Kontrolle über die Anlagen und Produktionsumgebungen des Herstellers erlangen konnten. Führungskräfte sind nun in der Lage, die Schwachstellen in der Praxis zu erkennen, und wissen, wie sie ihre IT- und OT-Infrastrukturen besser schützen können. Die Beurteilung führte dazu, dass Rockwell Automation auf der Grundlage der bei den Penetrationstests entdeckten Schwachstellen einen vollständigen, auf die Bedürfnisse des Automobilherstellers zugeschnittenen Schutzplan erstellte. Das Automobilunternehmen plante, die Sicherheitsbeurteilungen und die Beseitigung von Sicherheitslücken auszuweiten und den Mitarbeitern die Bedeutung einer guten Cybersicherheitshygiene zu vermitteln.

DIE FAKTEN

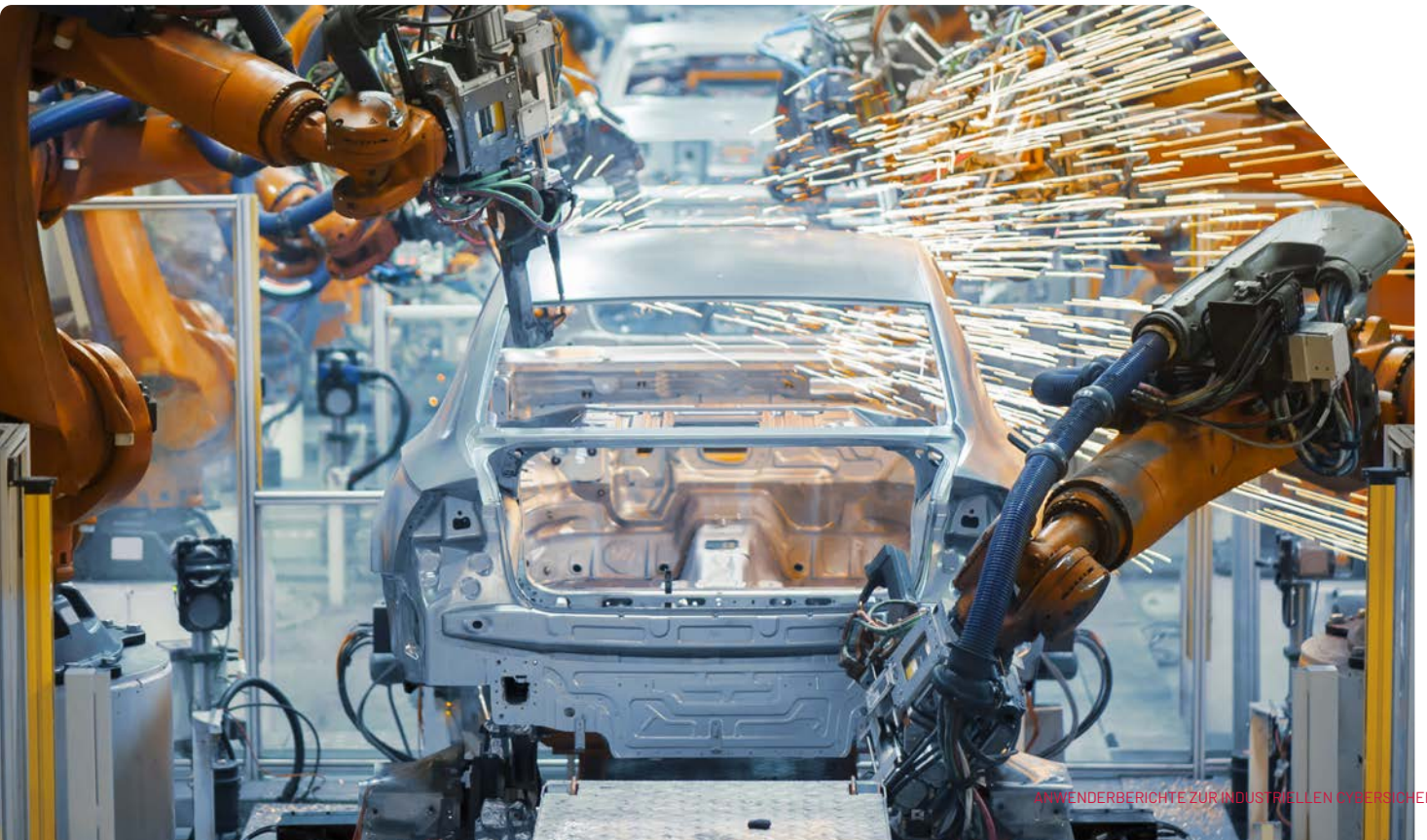
Penetrationstests decken kritische Schwachstellen auf

AUFGABENBEREICH

- 2 Wochen
- 6 Standorte

LÖSUNGEN

- Penetrationstests



KONSUMGÜTERINDUSTRIE

Ein Lebensmittelhersteller setzt ein vereinheitlichtes Risikomanagement an 46 Standorten weltweit ein, um die Cybersicherheit in Dutzenden übernommenen Unternehmen zu vereinheitlichen

Während einige Konsumgüterhersteller während der COVID-19-Pandemie florierten – man denke nur an Lebensmittelgeschäfte und Anbieter von Gesundheitsprodukten – sind andere ins Straucheln geraten. Dennoch stehen beide vor gewaltigen Herausforderungen. Cyberangriffe werden immer alltäglicher und kostspieliger, vernetzte OT- und IT-Systeme können industrielle Steuerungssysteme gefährden, und die sich ständig ändernden Anforderungen an die öffentliche Sicherheit erfordern Flexibilität.

Zur Überwindung dieser Hürden musste sich ein Fortune-500-Lebensmittelhersteller ein genaues Bild von den Cybersicherheits-Schwachstellen in seinen OT- und IT-Netzwerken machen. Kompliziert wurde die Angelegenheit dadurch, dass das Unternehmen in den letzten zwei Jahrzehnten Dutzende von Lebensmittelunternehmen mit jeweils unterschiedlichen Technologie- und Sicherheitsökosystemen erworben hatte.

Somit fehlte dem Hersteller ein zentraler Echtzeiteinblick in die Sicherheit der Systeme an seinen 46 globalen Produktionsstandorten. Die Schaffung von Transparenz würde eine standardisierte risikobasierte Sicherheitsstrategie und vereinheitlichte Risikomanagementfunktionen erfordern.

DIE DURCHSCHNITTLICHEN KOSTEN EINER DATENSCHUTZVERLETZUNG BEI KONSUMGÜTERHERSTELLERN STIEGEN IM JAHR 2021 AUF 3,7 MIO. USD, EIN ANSTIEG UM 42,9 % GEGENÜBER 2020

QUELLE: IBM SECURITY, COST OF A DATABREACH REPORT 2021, JULI 2021

WAS WURDE BEREITGESTELLT?

Gemeinsam mit dem Leiter der Cybersicherheitsabteilung des Unternehmens und dem Ökosystempartner Claroty entwickelte und realisierte Rockwell Automation zentralisierte Services zur Bedrohungserkennung an 46 globalen Produktionsstandorten. Auf diese Weise konnte ohne Betriebsunterbrechung ein Basiswert für die Netzwerkaktivität bestimmt und eine kontinuierliche Überwachung auf ungewöhnliche Aktivitäten, die auf Cyberangriffe hindeuten könnten, ermöglicht werden.

Im Falle einer Sicherheitsverletzung kann nun auf einen maßgeschneiderten Workflow zur Wiederherstellung der gefährdeten Systeme und Netzwerke zurückgegriffen werden. Und da die Schulung der Mitarbeiter für eine effektive Sicherheit unerlässlich ist, wurde ein Programm zur Förderung einer unternehmensweiten Kultur der Cybersicherheitshygiene eingeführt.

ERGEBNISSE

Dieser Lebensmittelhersteller verfügt derzeit über zentralisierte und vereinheitlichte Risikomanagementsysteme, die dazu beitragen, Cybersicherheitsrisiken zu minimieren, indem sie die Transparenz von der IT auf die OT-Umgebung ausweiten und Cyberbedrohungen erkennen und darauf reagieren, bevor diese sich zu Sicherheitsverletzungen entwickeln. Die Mitarbeiter haben durch das unternehmensweite Schulungsprogramm ein neues Bewusstsein für Cybersicherheit entwickelt.

In Zukunft wird das Unternehmen in der Lage sein, konsistente Cybersicherheitsprogramme zu realisieren, während es durch zukünftige Übernahmen weiter wächst.

DIE FAKTEN

Zentralisierung der Bedrohungserkennung, Minimierung des Risikos für globale OT- und IT-Netzwerke

AUFGABENBEREICH

- 46 Standorte weltweit
- Ökosystempartner: Claroty

LÖSUNGEN

- Bedrohungserkennungs-dienste

LEBENSMITTEL UND GETRÄNKE

Ein Lebensmittel- und Getränkehersteller verbessert die Cybersicherheit und die Reaktion auf Vorfälle und steigert die Gesamtanlageneffektivität um 5 %.

Nach einem Malware-Angriff, bei dem Computersysteme und Produktionslinien gestört wurden, musste ein internationaler Snack-Hersteller seine Cybersicherheitsmaßnahmen verstärken und seine Netzwerkinfrastruktur an 80 Standorten weltweit modernisieren. Zuvor hatte das Unternehmen versucht, eine Plattform für die Gesamtanlageneffektivität einzuführen, um Sicherheitsrisiken zu messen und einzudämmen und die Leistung bestehender Anwendungen zu verbessern. Die Initiative kam jedoch aufgrund von Inkompatibilitäten zwischen der Software zur Messung der Gesamtanlageneffektivität und der unternehmenseigenen Steuerungsebene und den Netzwerkanforderungen des Unternehmens nicht richtig voran.

Das Unternehmen bat Rockwell Automation um Unterstützung bei einer globalen Bestandsaufnahme seiner digitalen Ressourcen und bei der Modernisierung seiner Reaktionsmöglichkeiten auf Vorfälle sowie seiner übergreifenden Cybersicherheitsfunktionen.

2021 STIEGEN DIE DURCHSCHNITTLICHEN GESAMTKOSTEN EINER DATENSCHUTZVERLETZUNG BEI KONSUMGÜTERUNTERNEHMEN UM 43 %.

IBM SECURITY, COST OF A DATA BREACH REPORT 2021, JUNI 2021

HERAUSFORDERUNGEN

Die Zeiten im Segment der Konsumgüterindustrie sind hart. Die erdrutschartigen Veränderungen der letzten zehn Jahre in Bezug auf Produkt- und Einkaufspräferenzen, die angeschlagenen globalen Lieferketten, die Pandemiepolitik, durch die die Größe von Personengruppen begrenzt wird, und der Fachkräftemangel sind für niemanden fremd.

Dazu kommt die sprunghaft zunehmende Häufigkeit von Cyberangriffen.

WAS WURDE BEREITGESTELLT?

In Zusammenarbeit mit dem Global Director of Engineering des Unternehmens bewertete Rockwell Automation dessen Netzwerke und sorgte dafür, dass die zur Messung der Gesamtanlageneffektivität erforderlichen Daten mit den Unternehmensnetzwerken und -anwendungen kompatibel waren.

Anschließend führte Rockwell Automation umfassende Netzwerkbeurteilungen an den weltweiten Standorten des Unternehmens durch und implementierte kompatible industrielle Rechenzentren zur dezentralen Überwachung und Verwaltung der digitalen Ressourcen. Nach einer eingehenden Beurteilung entwickelte unser Team einen Plan für die Entschärfung von Netzwerkkonflikten mit der Anwendung zur Messung der Gesamtanlageneffektivität und für die Implementierung einer dezentralen Überwachung und Verwaltung rund um die Uhr durch das Supportteam von Rockwell Automation.

ERGEBNISSE

Nachdem die neue Netzwerkinfrastruktur eingerichtet war, konnte dieser Snack-Hersteller schnell Verbesserungen hinsichtlich der Datengenauigkeit und der standardisierten globalen Berichterstellung erkennen. Eine einheitliche Infrastruktur, verbunden mit unseren Managed Services, half dem Unternehmen, Ausfallzeiten zu reduzieren, die Datengenauigkeit zu verbessern und mithilfe von Service Level Agreements (SLAs) schneller auf Cybersicherheitsvorfälle zu reagieren.

Gemeinsam trugen diese Faktoren dazu bei, dass das Lebensmittel- und Getränkeunternehmen seine Gesamtanlageneffektivität um 5 % steigern konnte. Selbst eine Verbesserung der Gesamtanlageneffektivität um 1 % kann bei einer großen Produktionslinie eine enorme Kostenersparnis bedeuten und den wirtschaftlichen Nutzen einer Verstärkung der OT-Cybersicherheitsmaßnahmen eines Unternehmens unterstützen.

DIE FAKTEN

Verbesserung der Cybersicherheit und Steigerung der Gesamtanlageneffektivität

AUFGABENBEREICH

- 80 % der Standorte weltweit
- 5 % bessere Gesamt-anlageneffektivität
- Ökosystempartner: World Wide Technology

LÖSUNGEN

- Lösungen
- Netzwerkbeurteilung
- Aufnahme des weltweiten Anlagenbestands
- Bereitstellung industrieller Rechenzentren für dezentrale Überwachungs- und Managementfunktionen rund um die Uhr
- Reaktion auf Vorfälle

LEBENSMITTEL UND GETRÄNKE

Ein Lebensmittel- und Getränkeunternehmen optimiert und vereinfacht die OT-Cybersicherheit mit Managed Support Services rund um die Uhr

HERAUSFORDERUNGEN

Viele Hersteller versäumen es im Laufe der Jahre, ihre Altsysteme und Software zu aktualisieren. Dies kann das Risiko von Cyberangriffen erhöhen, betriebliche Ineffizienzen zur Folge haben, die die Margen schmälern, und die Bemühungen um die digitale Transformation erschweren.

Vor dieser Situation stand ein weltweit tätiger Lebensmittel- und Getränkehersteller, als er mit der Planung eines mehrjährigen Modernisierungsprojekts begann. Es galt, drei wesentliche Herausforderungen zu bewältigen. Ein Hauptziel war es, das Management der kritischen OT-Systeme zu optimieren und neue Anlagen zu integrieren, die nicht konsequent mit den veralteten Technologien, die noch im Einsatz waren, umgesetzt wurden. Ohne diese Integration fehlten den Mitarbeitern des Unternehmens die Kompetenz für ein konsistentes Management der OT-Systeme.

Erschwerend kam hinzu, dass während der COVID-19-Pandemie die Nachfrage nach Lebensmitteln anstieg. Die Geschäftsleitung des Unternehmens befürchtete, dass die technologische Infrastruktur dem zunehmenden Datenverkehr nicht standhalten und letztlich zu Ausfallzeiten und Umsatzeinbußen führen könnte.

Außerdem benötigte das Unternehmen Hilfe bei der Einrichtung eines sicheren dezentralen Zugriffs, um sich vor den zunehmenden Cybersicherheitsvorfällen zu schützen, da immer mehr Mitarbeiter und Dritte von zu Hause aus arbeiteten. Zusammengenommen führten diese Faktoren zu einem instabilen und unzuverlässigen technologischen Ökosystem, das unvorhergesehene finanzielle Verluste verursachte. Der Hersteller benötigte Hilfe bei der Implementierung eines konsistenten, zuverlässigen Managements seiner digitalen OT-Anlagen, um inmitten der Herausforderungen eine zuverlässige Betriebszeit zu gewährleisten.

WAS WURDE BEREITGESTELLT?

Das Lebensmittel- und Getränkeunternehmen beauftragte Rockwell Automation mit der Bereitstellung von Managed Services zum besseren Schutz vor Cyberangriffen und zur Schaffung einer stabilen und effizienten Betriebsumgebung.

Gemeinsam mit dem Unternehmen entwickelte Rockwell Automation ein unternehmensweites Managed Support Services-Programm für die Betriebstechnologie, das alle Systeme der digitalen Infrastruktur unterstützt. Es wurden zusätzliche Lösungen implementiert, um eine konsistente Bereitstellung und Support für kritische Anwendungen, Software und Infrastruktur sowie eine dezentrale Überwachung rund um die Uhr zu ermöglichen.

Rockwell Automation half dem Unternehmen auch bei der Einrichtung von 19 industriellen OT-Rechenzentren mit einer Plattform zur kontinuierlichen Erkennung von Bedrohungen, um Cybersicherheitsrisiken zu begegnen. Und zum Schutz von Mitarbeitern, die von zu Hause aus arbeiten, wurde an 40 nordamerikanischen Standorten ein sicherer dezentraler Zugriff entwickelt und eingerichtet.

ERGEBNISSE

Dank der modernisierten Infrastruktur und der unterstützenden Managed Services kann dieser Hersteller Cybersicherheitsbedrohungen für seine Unternehmens- und OT-Netzwerke durch eine Rund-um-die-Uhr-Überwachung der Bedrohungen reduzieren und gleichzeitig die Risiken von Ausfallzeiten minimieren. Die konsequente Einführung und Integration von Technologiekomponenten hat dazu beigetragen, die Systeme zuverlässiger zu machen, das Anwendungsmanagement zu verbessern und die Betriebszeit der Anlage zu erhöhen. Der Einsatz von sicheren Funktionen für den dezentralen Zugriff schützt Mitarbeiter, Dritte und die betriebliche Infrastruktur des Unternehmens vor Cyberrisiken.

Durch diese Initiativen konnte das Unternehmen die betriebliche Effizienz steigern und gleichzeitig die Kosten senken.

DIE FAKTEN

Aktualisierung von älteren Systemen und wirksamer Schutz vor Cyberangriffen

AUFGABENBEREICH

- 40 Standorte
- 19 industrielle OT-Rechenzentren

LÖSUNGEN

- Managed Support für alle digitalen Infrastrukturgeräte
- Industrielle OT-Rechenzentren
- Sicherer dezentraler Zugriff
- Erkennen von Bedrohungen rund um die Uhr

KONSUMGÜTERINDUSTRIE

Konsumgüterunternehmen realisiert eine sichere digitale Transformation und senkt die durchschnittlichen Netzwerkreaktionszeiten um 90 %

Die scheinbar nicht enden wollende COVID-19-Pandemie hat die Abläufe an den Arbeitsplätzen auf den Kopf gestellt, die Einkaufsgewohnheiten der Verbraucher verändert und die globalen Lieferketten lahmgelegt. Erschwerend kommt hinzu, dass Häufigkeit, Schwere und Kosten von Cyberangriffen stark zunehmen. So gaben zum Beispiel in einer Studie 61 % der Hersteller an, dass sie 2021 von einem Cyberangriff betroffen waren, und 75 % mussten Systemausfälle hinnehmen.

Ein Nebeneffekt der Herausforderungen während der Pandemie war die Beschleunigung der digitalen Transformation, um neue Herausforderungen wie die Home-Office zu bewältigen, und die parallele Anforderung an die industrielle Cybersicherheit, um neu vernetzte Abläufe und Netzwerke zu schützen.

Wie ein multinationaler Lebensmittel- und Getränkehersteller feststellte, können digitale Transformation und Cybersicherheit nicht länger als zwei getrennte Initiativen betrachtet werden, sondern müssen ganzheitlich umgesetzt werden. Das Unternehmen plante, eine sicherheitsorientierte Digitalisierungsinitiative zu lancieren, um von den Echtzeitdaten zu profitieren, die von seinen zunehmend digitalen Geschäftssystemen erzeugt werden. Zunächst mussten jedoch die technischen Defizite behoben werden, die sich im Laufe der Jahre angesammelt hatten.

Die älteren Systeme und Anwendungen des Lebensmittelherstellers waren beispielsweise nicht mit modernen Cloud-Computing- und Cybersicherheitsplattformen kompatibel. Die heterogenen Netzwerke und die virtuelle Infrastruktur unterstützten weder kritische Datenanalysen noch Technologien der künstlichen Intelligenz. Zudem trugen unzureichende Programme zur Sensibilisierung und Schulung der Mitarbeiter für die Cybersicherheit zu einer Kultur mangelnder Sicherheitshygiene bei.

61 % DER BETRIEBE WURDEN 2021 OPFER EINES SICHERHEITSVORFALLS

QUELLE: TRENDMICRO, THE STATE OF INDUSTRIAL CYBERSECURITY, MAI 2021

WAS WURDE BEREITGESTELLT?

Der Konsumgüterhersteller beauftragte Rockwell Automation mit der Modernisierung und Vereinheitlichung seiner IT- und OT-Systeme, der Implementierung einer automatischen Überwachung und Verwaltung des neuen Netzwerks sowie der Aktualisierung der Cybersicherheitsfunktionen an 44 Standorten in Nordamerika. Dafür wollte das Unternehmen jedoch keine Mittel für Investitionsausgaben (CapEx) verwenden.

Rockwell Automation entwickelte und implementierte eine moderne cloudbasierte Lösung mit unserem Infrastructure-as-a-Service(IaaS)-Angebot. Gemeinsam mit dem Konsumgüterhersteller entwickelte unser Team das IaaS-Netzwerk und implementierte Cybersicherheitsfunktionen wie Netzwerksegmentierung, Patch Management für Betriebssysteme und Antivirenlösungen. World Wide Technology, ein Ökosystempartner von Rockwell Automation, kümmerte sich um die Lieferung der Hardware für diese Initiative. Die gesamte Netzwerk- und Recheninfrastruktur wurde dann auf einen Managed Service in der OT migriert.

Außerdem implementierte das Unternehmen die TechConnectSM- und Anwendungs-Support-Services von Rockwell Automation, um den 24/7-Helpdesk-Support für Anwendungen und Infrastruktur zu verbessern und damit Außendienstmitarbeiter vor Ort für den praktischen Support direkt am System entsendet werden. Während die Service Level Agreements (SLAs) eine Reaktion auf IaaS-Warnungen innerhalb von maximal 10 Minuten vorschrieben, betrugen die tatsächlichen Reaktionszeiten im Durchschnitt nur 3,5 Minuten.

ERGEBNISSE

Durch diese sichere Lösung für die digitale Transformation wurden große Cybersicherheitslücken geschlossen. Hierfür implementierte das Unternehmen eine moderne Netzwerkinfrastruktur mit einem Infrastructure-as-a-Service-Angebot sowie ein effektives OT Patch Management – eine bekanntermaßen komplexe Sicherheitsanforderung – und Virenschutzmaßnahmen.

Mithilfe des Application Support Service von Rockwell Automation konnte das Unternehmen die Reaktionszeit für kritische Alarme und Warnungen um 90 % verbessern, was wiederum die Ausfallzeiten verringerte. Die Mittel für die Initiative wurden aus den Betriebsausgaben des Unternehmens bereitgestellt, sodass die digitale Transformation ohne Inanspruchnahme der Investitionsrücklagen finanziert werden konnte. Dank des weltweit unterstützten, servicefähigen Supportmodells konnte der Mangel an qualifizierten IT- und Cybersicherheitsmitarbeitern in den neuen digitalen Geschäftsbereichen behoben und das Unternehmen auf eine künftige Skalierung vorbereitet werden.

DIE FAKTEN

Sichere digitale Transformation, 90 % bessere Reaktionszeit

AUFGABENBEREICH

- 44 Standorte in Nordamerika
- Das IaaS-SLA mit einer Reaktionszeit von 10 Minuten konnte auf durchschnittlich 3,5 Minuten reduziert werden
- Ökosystempartner: World Wide Technology

LÖSUNGEN

- Infrastructure as a Service (IaaS)
- OT Patch Management
- Antivirus
- TechConnectSM- und Anwendungs-Support

CHEMIE

Chemieunternehmen bietet seinen Mitarbeitern während der Pandemie sicheren dezentralen Zugriff auf das Steuerungssystem für 8000 E/A-Punkte

HERAUSFORDERUNGEN

Angesichts der anhaltenden COVID-19-Pandemie arbeitet eine große Zahl von Menschen weiterhin von zu Hause aus. Biokraftstoffunternehmen bilden da keine Ausnahme.

Ein südamerikanischer Hersteller von Ethanol, Bioenergie und Viehfutter musste einen gesicherten dezentralen Zugriff auf die IT- und OT-Netzwerke des Unternehmens einrichten. Eine der obersten Prioritäten war die Implementierung eines sicheren Zugangs für eine Neugründungsinitiative mit dezentralen Lieferanten. Das Biokraftstoffunternehmen musste auch Auflagen zur Verringerung der Reisetätigkeit erfüllen und gleichzeitig die Überprüfung aller dezentralen Interaktionen mit dem Industriesteuerungssystem ermöglichen.

WAS WURDE BEREITGESTELLT?

Gemeinsam mit Rockwell Automation entwickelte und implementierte das Biokraftstoffunternehmen Sicherheitslösungen mit komplexen Stromversorgungsoptionen.

Erste Priorität hatte dabei das Neugründungsprojekt. Rockwell Automation beriet das Unternehmen hinsichtlich des komplexen Spektrums an Stromversorgungsoptionen, die zur Erreichung der Projektziele in Frage kamen. Eine der vorgeschlagenen Optionen war Intelligent Packaged Power (IPP) mit Mittel- und Niederspannungsanlagen, die in das Prozessleitsystem (Distributed Control System, DCS) des Unternehmens integriert werden sollten.

DIE WELTWEITE NACHFRAGE NACH BIOKRAFTSTOFFEN WIRD ZWISCHEN 2021 UND 2026 VORAUSSICHTLICH UM 28 % STEIGEN

INTERNATIONAL EMERGENCY AGENCY, RENEWABLES 2021 ANALYSIS AND FORECAST TO 2026, DEZEMBER 2021

Anschließend unterstützte Rockwell Automation das Unternehmen bei der Verbesserung der zentralisierten Überwachung von Sicherheitsinformationen, indem es eine Lösung mit einem industriellen Rechenzentrum und dezentralen Überwachungs- und Managementfunktionen rund um die Uhr für die virtuelle Umgebung implementierte. Unser Team konzipierte und implementierte außerdem eine industrielle Demilitarized Zone (IDMZ), um die Geschäftsnetzwerke und Industriesteuerungssysteme des Unternehmens sicher zu isolieren.

Sichere Möglichkeiten für dezentralen Zugriff und Konfiguration waren angesichts der Reisebeschränkungen und des Social Distancings während der COVID-19-Pandemie ebenfalls entscheidend. Auf diese Weise konnte das Biokraftstoffunternehmen die Interaktionen dezentraler Bediener mit dem Industriesteuerungssystem überwachen und alle dezentralen Interaktionen mit einem Schlüssellieferanten überprüfen, der 1243 Meilen vom Standort entfernt ist. Dieser Ansatz wird auch bei den künftigen neu gegründeten Standorten verfolgt werden.

ERGEBNISSE

Mithilfe der Lebenszyklusservices von Rockwell Automation, in Verbindung mit der Bereitstellung einer IDMZ und einem sicheren dezentralen Zugriff, konnte das Unternehmen die Anforderungen des Neugründungsprojekts erfüllen und gleichzeitig die Cybersicherheitsrisiken für Unternehmens- und OT-Netzwerke reduzieren. Die Initiative vereinfachte auch die Kontrolle und Überwachung von dezentralen Zugriffen auf OT und Industriesteuerungen, erhöhte die Systemzuverlässigkeit, verbesserte die Mitarbeitereffizienz und optimierte die Systemunterstützung durch eine dezentrale Überwachung rund um die Uhr.

Das Team von Rockwell Automation unterstützte das Biokraftstoffunternehmen auch bei der Verbesserung der Sicherheitsprotokolle für Mitarbeiter im Hinblick auf aktuelle und zukünftige Pandemien.

DIE FAKTEN

Sicherer dezentraler Zugriff während der Pandemie

AUFGABENBEREICH

- 2 Standorte
- Ökosystempartner: Claroty

LÖSUNGEN

- Bedrohungserkennungsdienste

Rockwell Automation: Sichern, worauf die Welt angewiesen ist

Rockwell Automation bietet eine Reihe von industriellen Sicherheitslösungen und -services, die Sie bei der Abwehr von Bedrohungen unterstützen und die Widerstandsfähigkeit Ihres OT- und IT-Betriebs erhöhen. Unsere Experten können eine zuverlässige und sichere Netzwerkinfrastruktur entwerfen, während sie gleichzeitig Bedrohungen abwehren und mit einer 24/7-Überwachung schnell auf Vorfälle reagieren. Neben unserem umfassenden Know-how und unseren Kenntnissen der neuesten Best Practices bringen wir das Wissen aus mehr als 100 Jahren Erfahrung in der industriellen Automatisierung in den Produktionsbetrieb ein.

Unsere Standorte auf der ganzen Welt ermöglichen es unseren Kunden, Cybersicherheitsschutz konsequent auf globaler Ebene und über mehrere Standorte hinweg umzusetzen – und dies mit einer Logistik, die so fein abgestimmt ist, wie Sie es vom Branchenführer der industriellen Automatisierung erwarten.

Ressourcen für den Einstieg

- Erfahren Sie mehr über gängige Angriffe auf die OT-Cybersicherheit. Sehen Sie sich die Präsentation einer Sitzung der Automation Fair®-Konferenz an: Die 10 folgenschwersten Angriffe auf die OT-Cybersicherheit.
- Melden Sie sich für unsere Cybersecurity Preparedness Assessment (Beurteilung der Cybersicherheitsbereitschaft) an und erhalten Sie einen individuellen Bericht, der sich an den ursprünglichen Umfrageteilnehmern orientiert. Informieren Sie sich, wie Ihr Unternehmen im Vergleich zu anderen Unternehmen abschneidet – abhängig von Branche, Unternehmensgröße und Region.
- Sprechen Sie mit einem Experten von Rockwell Automation und erfahren Sie, wie wir Sie mit dem richtigen OT-Cybersicherheitsprogramm unterstützen können, um Ihre industriellen Abläufe optimal zu schützen.

Folgen Sie uns.

rockwellautomation.com — expanding **human possibility**®

AMERIKA: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: +1 414 382 2000, Fax: +1 414 382 4444
EUROPA/NAHER OSTEN/AFRIKA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgien, Tel: +32 2 663 0600, Fax: +32 2 663 0640
ASIEN/AUSTRALIEN/PAZIFIKRAUM: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: +852 2887 4788, Fax: +852 2508 1846
DEUTSCHLAND: Rockwell Automation GmbH, Parsevalstraße 11, 40468 Düsseldorf, Tel: +49 (0)211 41553 0, Fax: +49 (0)211 41553 121
SCHWEIZ: Rockwell Automation AG, Industriestrasse 20, CH-5001 Aarau, Tel: +41(62) 889 77 77, Fax: +41(62) 889 77 11, Customer Service – Tel: 0848 000 277
ÖSTERREICH: Rockwell Automation, Kotzinastraße 9, A-4030 Linz, Tel: +43 (0)732 38 909 0, Fax: +43 (0)732 38 909 61

Allen-Bradley und expanding human possibility sind Marken von Rockwell Automation, Inc.
Marken, die nicht Rockwell Automation gehören, sind das Eigentum der jeweiligen Unternehmen.

Publikation GMSN-AP001A-DE-P – Mai 2022

Copyright © 2022 Rockwell Automation, Inc. Alle Rechte vorbehalten. Printed in USA.