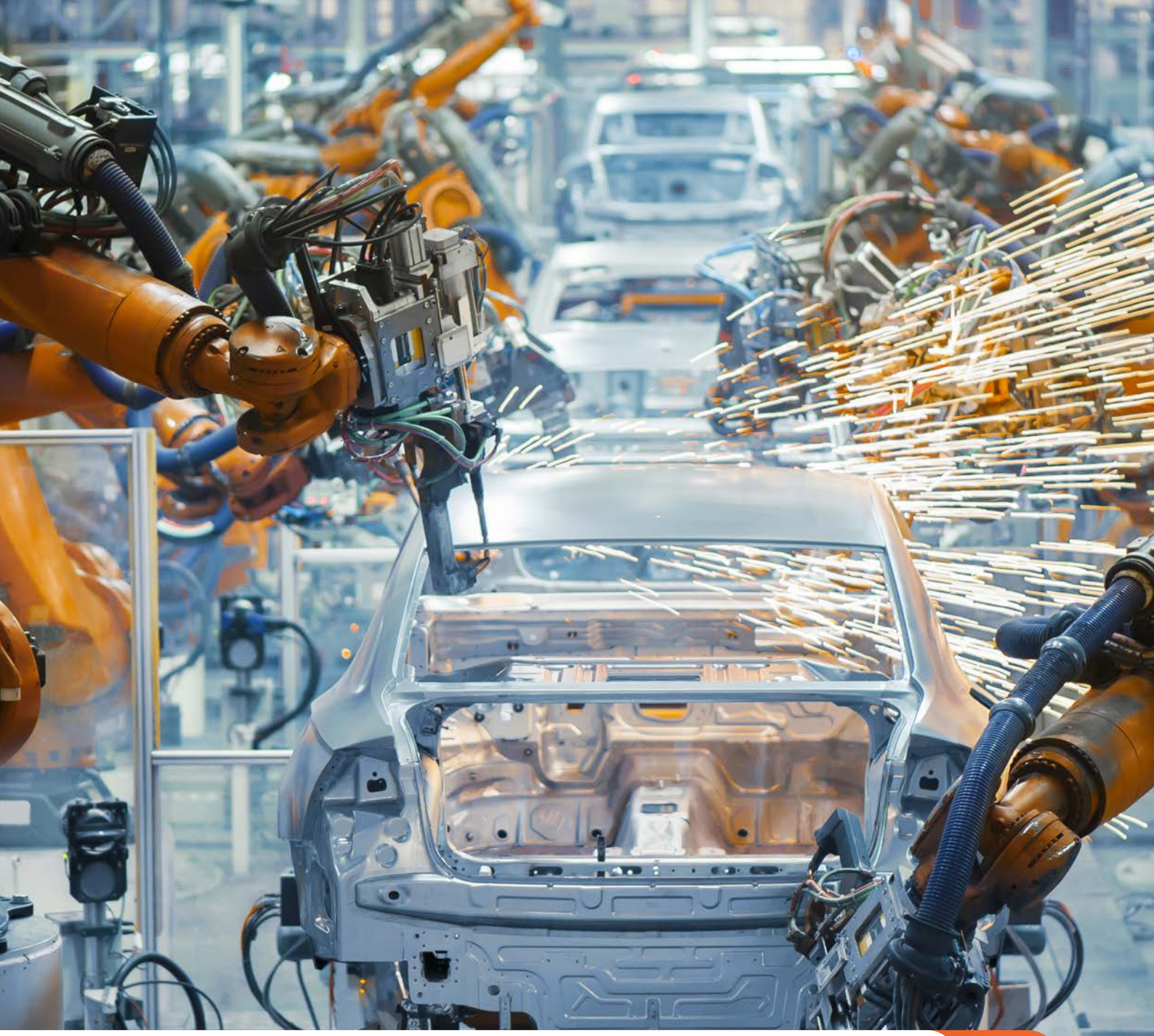


Rockwell Automation

Die nächste Generation der intelligenten Automobilfertigung setzt proaktive Cybersicherheit voraus

Inhaltsverzeichnis

Einleitung

Von der Einführung fahrerloser Autos bis zur Verbreitung batteriebetriebener Fahrzeuge – die Automobilindustrie erlebt derzeit einen Wandel, der schneller und weitreichender ist als je zuvor in ihrer Geschichte. Branchenführer arbeiten an Innovationen, damit Fahrzeuge mit rein elektrischem und mit Hybridantrieb mehr Fahrspaß bieten, während Neuentwicklungen bei Verbrennungsmotoren für weniger Emissionen und höhere Leistung sorgen. Gleichzeitig bietet sich den Automobilherstellern die einmalige Gelegenheit, durch zunehmende Automatisierung, Digitalisierung und Konnektivität im Fertigungsbereich neue Effizienzsteigerungen zu erzielen.

Diese rasante digitale Transformation und die Öffentlichkeitswirksamkeit der Automobilindustrie machen die Automobilfertigung zu einem zunehmend attraktiven Ziel für Cyberkriminalität. Bedrohungsakteure sind sich der hohen Kosten von Ausfallzeiten in Automobilwerken bewusst und wissen, dass diese Kosten Ransomware-Opfer dazu bewegen können, hohe Zahlungen zu leisten, um die Produktion schnell wieder aufzunehmen.

Cyberkriminelle wissen auch, dass die installierte Basis von Automobilmontageanlagen, einschließlich Industriesteuerungssystemen und Manufacturing Execution Systems (MES), in der Regel einen langen Lebenszyklus hat und dass das Schwachstellenmanagement eine ständige Herausforderung in der Betriebstechnologie (OT) darstellt.

In der heutigen Welt sind die Cyberrisiken, denen sich die Automobilhersteller gegenübersehen, schwerwiegend und bedeutend. Die Bedrohungslandschaft ist nach wie vor eine Herausforderung: Prognosen zufolge werden die durch Cyberkriminalität verursachten Schäden bis zum Jahr 2025 weltweit mit mehr als 10,5 Billionen USD beziffert werden, wobei die Kosten Jahr für Jahr um 15 % steigen werden.[1] Gleichzeitig werden die ausgefeiltesten und finanzstärksten Bedrohungsakteure, die von Nationalstaaten gesponsert werden, immer geschickter und dreister. Forscher schätzen, dass sich die Häufigkeit „signifikanter" staatlich finanzierter Cyberangriffe zwischen 2017 und 2021 verdoppelt hat.[2] Von den Industrieunternehmen haben mindestens 53 % in den letzten beiden Jahren eine Verletzung der Cybersicherheit in einer ihrer Anlagen erlebt.[3]

[1] *Cybersecurity Ventures*, [2] *States, Cybercontflict and the Web of Profit*, [3] *LNS Research*

Warum Automobilhersteller anfällig für Cyberangriffe sind

Automobilhersteller sind ein bevorzugtes Ziel für Cyberkriminelle, unter anderem weil sie viele Gemeinsamkeiten mit anderen Herstellern haben, darunter veraltete Infrastrukturen, die oft nicht gepatcht werden, und ein Mangel an qualifizierten Ressourcen für das Risikomanagement. Jüngste Studien zeigen, dass von den 100 bedeutendsten Automobilherstellern 49 % „sehr anfällig" für Ransomware-Angriffe sind. Kompromittierte Kennwörter oder gestohlene Anmeldeinformationen von 91 % dieser Unternehmen waren im Dark Web leicht zugänglich, während 79 % der Automobilhersteller und Tier-1-Zulieferer schlechte Bewertungen für das Patch Management erhielten. 90 % wurden als „sehr anfällig" für Phishing-Angriffe eingestuft.[4]

Automobilhersteller sind auch deshalb ein bevorzugtes Ziel, weil sie einzigartigen industriespezifischen Risiken ausgesetzt sind. Die Lieferketten in der Automobilindustrie sind zwangsläufig komplex, da die Automobilhersteller für eine Vielzahl von Teilen, einschließlich Software und elektronischer Hardwarekomponenten, auf weltweit verteilte Netzwerke von Drittherstellern angewiesen sind. Da die heutigen Fahrzeuge immer mehr softwaregesteuerte und mit dem Internet verbundene Systeme enthalten, ist die Gewährleistung der Lieferkettenintegrität von entscheidender Bedeutung, um die funktionale Sicherheit der Fahrzeuge – und damit den Schutz des Lebens ihrer Insassen – aufrechtzuerhalten.

Sicherheit während der rasanten digitalen Transformation

Die digitale Transformation betrifft die gesamte Industrielandschaft. Der Automobilsektor ist einer der am schnellsten wachsenden Sektoren. Die Digitalisierung der Prozesse in der Automobilfertigung führt zu höherer Produktivität, Produktqualität und besserer Konsistenz sowie optimierten Workflows, die die Sicherheit und Effizienz der Anlagen erhöhen. Die Möglichkeit, Daten zwischen IT- und OT-Systemen auszutauschen, ermöglicht Analysen, die die Betriebsabläufe verbessern und somit zu besseren Geschäftsergebnissen für die Automobilhersteller führen.

Diese Fortschritte können auch das Cyberrisiko erhöhen, insbesondere wenn die Automobilhersteller kein umfassendes Programm für die industrielle Cybersicherheit im Unternehmen entwickelt haben. Eine Defense-in-Depth-Sicherheitsstrategie, die mit dem NIST Cybersecurity Framework übereinstimmt, ist für die Sicherung von Netzwerken und einzelnen Geräten unerlässlich, um Systeme vor externen Angriffen zu schützen.

Automobilhersteller müssen außerdem kontinuierliche, schnelle Erkennungs- und Reaktionsfähigkeiten entwickeln, um anomale Aktivitäten zu erkennen und Angriffe zu unterbinden, bevor sie zu schwerwiegenden Ausfallzeiten oder finanziellen und materiellen Verlusten führen. Außerdem müssen sie in der Lage sein, sich schnell von Cybervorfällen zu erholen. Dies erfordert einen vielschichtigen Ansatz mit den richtigen Mitarbeitern, Prozessen und Technologien, einschließlich Secure-by-Design-Industriesteuerungen und robusten Sicherheitslösungen, die speziell für industrielle Umgebungen entwickelt wurden.

[4] *Black Kite*

ZUKÜNFTIGER SCHWERPUNKT:

Die Absicherung vernetzter Fahrzeuge ist entscheidend, um das Vertrauen der Verbraucher von heute zu gewinnen

Als vernetzt gelten Fahrzeuge, wenn sie Daten mit cloudbasierten Systemen, fahrzeuginternen Anwendungen und anderen Systemen wie der Straßeninfrastruktur, anderen Fahrzeugen, mobilen Geräten oder Telematikdiensten austauschen. Seit GM im Jahr 1996 das erste automatische, im Fahrzeug integrierte Notrufsystem eingeführt hat, ist die Konnektivität von Personenkraftwagen sprunghaft angestiegen. **Schätzungen zufolge werden vernetzte Fahrzeuge bis Ende 2023 mehr als 25 % und bis 2025 mehr als 75 % des weltweiten Automobilmarkts ausmachen.**[5]

Die technologisch anspruchsvollsten Fahrzeuge von heute, die über moderne Fahrerassistenzsysteme (ADAS) verfügen, enthalten mehr als 150 mikroprozessorgestützte elektronische Steuergeräte und über 150 Millionen Codezeilen.[6] Nach Schätzungen von Deloitte entfallen bis zu 40 % der Kosten eines Neuwagens auf halbleiterbasierte elektronische Systeme,[7] und wie gut die Software funktioniert, ist häufig ein entscheidender Faktor für die Leistung und Effizienz eines Fahrzeugs – und damit für die Präferenzen der Verbraucher für ein bestimmtes Fahrzeugmodell oder eine bestimmte Automarke.

Schätzungen zufolge werden vernetzte Fahrzeuge bis Ende 2023 mehr als 25 % und bis 2025 mehr als 75 % des weltweiten Automobilmarkts ausmachen.

Autos sind jetzt „geborene Zuhörer"

Viele Autofahrer erwarten heute, dass ihr Auto mit Software gesteuert werden kann und sich wie ein schnelles, mobiles Rechenzentrum verhält. Auch auf fahrzeuginterne Cybersicherheit wird mehr Wert gelegt. Als Sicherheitsforscher vorführten, dass sie aus der Ferne die Kontrolle über einen Jeep übernehmen konnten, der mit hoher Geschwindigkeit auf der Autobahn unterwegs war, und sich über das Internet in die integrierten Systeme hackten, veranlasste der Vorfall Chrysler zu einem Rückruf von 1,4 Millionen Fahrzeugen. Auch die Mainstream-Medien wurden darauf aufmerksam.[8]

In einer anderen Machbarkeitsstudie konnten Hacker mit einer Drohne, die einen WLAN-Dongle mitführte, die Türen eines beliebten Elektrofahrzeugs öffnen und sogar in den zentralen Command-and-Control(C2)-Server eindringen, der zur Kommunikation mit der gesamten Kundenflotte des Herstellers dient.[9]

Mehr denn je ist kompromisslose Cybersicherheit in vernetzten Fahrzeugen ein Muss für Automarken, die das Vertrauen der Verbraucher gewinnen und erhalten möchten. Laut einer vor Kurzem durchgeführten Umfrage würden 80 % der Autokäufer niemals ein Fahrzeug von einem Hersteller kaufen, wenn dieser von einem Hackerangriff auf Fahrzeuge betroffen wäre.[10] Und eine weitere Umfrage ergab, dass 84 % der Verbraucher kein Fahrzeug mehr bei einem Händler kaufen würden, bei dem sie in der Vergangenheit ein Fahrzeug gekauft haben, wenn sie herausfinden würden, dass ihre Daten durch eine Sicherheitsverletzung kompromittiert worden sind.[11]

[5]Capgemini, [6]IEEE Future Directions, [7]Deloitte, [8]Wired, [9]Electrek, [10]After Market News, [11]Total Dealer Compliance

Die größten Bedrohungen für die Cybersicherheit in der Automobilindustrie

Die digitale Transformation betrifft die gesamte Industrielandschaft. Der Automobilsektor ist einer der am schnellsten wachsenden Sektoren. Die Digitalisierung der Prozesse in der Automobilfertigung führt zu höherer Produktivität, Produktqualität und besserer Konsistenz sowie optimierten Workflows, die die Sicherheit und Effizienz der Anlagen erhöhen. Die Möglichkeit, Daten zwischen IT- und OT-Systemen auszutauschen, ermöglicht Analysen, die die Betriebsabläufe verbessern und somit zu besseren Geschäftsergebnissen für die Automobilhersteller führen.

Diese Fortschritte können auch das Cyberrisiko erhöhen, insbesondere wenn die Automobilhersteller kein umfassendes Programm für die industrielle Cybersicherheit im Unternehmen entwickelt haben. Eine Defense-in-Depth-Sicherheitsstrategie, die mit dem NIST Cybersecurity Framework übereinstimmt, ist für die Sicherung von Netzwerken und einzelnen Geräten unerlässlich, um Systeme vor externen Angriffen zu schützen.

Automobilhersteller müssen außerdem kontinuierliche, schnelle Erkennungs- und Reaktionsfähigkeiten entwickeln, um anomale Aktivitäten zu erkennen und Angriffe zu unterbinden, bevor sie zu schwerwiegenden Ausfallzeiten oder finanziellen und materiellen Verlusten führen. Außerdem müssen sie in der Lage sein, sich schnell von Cybervorfällen zu erholen. Dies erfordert einen vielschichtigen Ansatz mit den richtigen Mitarbeitern, Prozessen und Technologien, einschließlich Secure-by-Design-Industriesteuerungen und robusten Sicherheitslösungen, die speziell für industrielle Umgebungen entwickelt wurden.

Häufige Cybersicherheitsangriffe auf Automobilhersteller

Zu den drei häufigsten Angriffsszenarien gehören heute Ransomware-Angriffe, Phishing-Angriffe (die zum Diebstahl von Anmeldeinformationen führen) und die Ausnutzung ungepatchter Schwachstellen der Geräte im Fertigungsbereich.

DIE RANSOMWARE-BEDROHUNG

Ransomware-Angriffe sind die weltweit am schnellsten wachsende Form der Cyberkriminalität, und die durch Ransomware verursachten Schäden werden derzeit auf über 20 Milliarden USD geschätzt. Forscher schätzen, dass heute alle 11 Sekunden ein Unternehmen von einem Ransomware-Angriff betroffen ist.[12]

Die Fertigungsindustrie gehört zu den Branchen, die am ehesten von Ransomware-Angreifern ins Visier genommen werden. Industrieunternehmen verzeichnen fast doppelt so viel Netzwerkverkehr im Zusammenhang mit Ransomware wie die nächstgrößere Branche.[13] Und unter den Fertigungsunternehmen sind Automobilhersteller ein besonders attraktives Ziel, da die mit einem Produktionsstopp verbundenen Kosten so hoch sind. Tatsächlich führt dasselbe Phänomen, das Autohersteller eher dazu bringt, Lösegeldzahlungen in Betracht zu ziehen – nämlich die Intoleranz gegenüber Ausfallzeiten – auch dazu, dass viele von ihnen Schwachstellen nur zögerlich beheben.

Ransomware-Angriffe beginnen oft mit erfolgreichen Phishing-Versuchen. Ransomware-Angreifer nutzen häufig auch öffentlich sichtbare kritische Ports, um Malware in die Umgebung hochzuladen, oder sie nutzen gestohlene Anmeldeinformationen, um dezentralen Zugriff auf Systeme zu erhalten. Die ordnungsgemäße **Segmentierung** von Industrie- und Unternehmensnetzwerken ist von entscheidender Bedeutung, um die Ausbreitung von Ransomware vom ersten Infektionspunkt an zu verhindern. Wenn sichergestellt wird, dass industrielle Demilitarized Zones (DMZs) und kritische Sicherheitszonen logisch von den IT-Netzwerken des Unternehmens abgeschottet sind, können Versuche unterbunden werden, sich seitlich durch OT-Umgebungen zu bewegen, wenn der Zugriff in der IT oder OT erfolgt.

[12] *Cybersecurity Ventures*, [13] *Cisco*

PHISHING-ANGREIFER NEHMEN AUTOMOBILHERSTELLER INS VISIER

E-Mail-basierte Angriffe, die speziell auf Automobilhersteller abzielen, sind allgegenwärtig. Bedrohungsforscher, die sich näher mit dem Phishing-Risiko in der Automobilindustrie befassen, fanden mehr als 18 000 gefälschte oder Phishing-Domains, die explizit für die 100 bedeutendsten Automobilhersteller und OEMs erstellt wurden.[14] Phishing ist eine äußerst effektive Taktik, mit der Cyberkriminelle Berechtigungen auf Insiderebene für IT- oder Industriesteuerungssysteme, einschließlich administrativer Anmeldeinformationen, abgreifen können.

Sobald ein Phishing-Versuch erfolgreich war, können die Abwehrmaßnahmen nachfolgende Angriffsphasen möglicherweise nur schwer erkennen, da die Aktivitäten der Bedrohungsakteure von denen eines Insiders nicht zu unterscheiden sind. Ihre Fähigkeit, unmittelbaren Schaden anzurichten, wird nur durch ihren Kenntnisstand in Bezug auf die Bedienung von Anlagensystemen und die Manipulation von Komponenten der Industriesteuerungssysteme zum Erreichen bestimmter Ziele begrenzt. Der Schutz vor dieser Art von Bedrohungen erfordert Kontrollen auf Netzwerk-, Anwendungs- und Geräteebene sowie eine kontinuierliche IT/OT-Sicherheitsüberwachung, um Verhaltensanomalien oder ungewöhnliche Anmeldeversuche schnell zu erkennen.

Durch ein umfassendes Schulungsprogramm zum **Sicherheitsbewusstsein**, in dem die Mitarbeiter lernen, Phishing-Versuche zu erkennen und zu vermeiden, können diese Risiken gemindert werden, ebenso wie durch die Umsetzung geeigneter Richtlinien zur Kontrolle des administrativen Zugriffs auf Betriebssysteme in der Fertigung und in der Industrie. Wichtig sind auch Investitionen in die Aus- und Weiterbildung, um die Mitarbeiter über aktuelle Sicherheitsbedrohungen und bewährte Verfahren auf dem Laufenden zu halten.

UNGEPATCHTE SICHERHEITSLÜCKEN IN DER INSTALLIERTEN BASIS

Das Patch Management der installierten Basis ist für Automobilunternehmen eine große Herausforderung, aber diejenigen, die weiterhin nicht in der Lage sein werden, Schwachstellen in den Systemen des Fertigungsbereichs schnell zu beseitigen, werden sich mit einem inakzeptablen Risiko konfrontiert sehen.

In einem kürzlich veröffentlichten Forschungsbericht wurde festgestellt, dass 91 % der Automobilhersteller mindestens eine schwerwiegende Schwachstelle in ihrer OT- oder Industriesteuerungssoftware aufweisen.[15] Einige davon waren im Internet offengelegt, und viele konnten nicht gepatcht werden, weil die Hersteller keine Updates für die auslaufende Hardware mehr bereitstellten.

Die Entwicklung eines effektiven und leicht verständlichen Verfahrens für den Umgang mit Schwachstellen in der installierten Basis und die Erfüllung von Patching-Anforderungen ist von entscheidender Bedeutung. **Die Identifizierung und Inventarisierung aller Netzwerkressourcen** in der gesamten OT-Umgebung, einschließlich Hardware, Anlagen, Servern, Sensoren und mobilen Geräten, sowie die **kontinuierliche Überwachung der Ressourcen** zur Erkennung nicht autorisierter Ressourcen oder Benutzer in Netzwerken ist ein wichtiger Schritt.

Regelmäßige **Penetrationstests** sind ebenfalls von großer Bedeutung. Dabei versuchen Experten, in die Systeme einzudringen, und können eine realistische Beurteilung der Schwachstellen und Sicherheitslücken vornehmen, sodass diese behoben werden können.

[14] *Intsights*, [15] *Black Kite*

Die sich verändernde Natur der zu schützenden Werte

In der Vergangenheit mussten die IT-Netzwerke der Automobilhersteller ebenso geschützt und verteidigt werden wie die speicherprogrammierbaren Steuerungen (SPS) und Industriesteuerungssysteme im Fertigungsbereich.

Heute müssen diese Systeme ebenso gesichert werden wie die immer komplexeren und vernetzten IT-/IoT-/IIoT-Ökosysteme und die vernetzten, softwarebasierten Fahrzeuge. Dies wirft für die Automobilhersteller eine ganze Reihe neuer Fragen auf:

- Wie kann ein Hersteller die Software eines Fahrzeugs, das bereits im Einsatz ist, patchen?
- Müssen Automobilhersteller neue Security Operations Center (SOC) bauen, nur um ihre bereits produzierte Fahrzeugflotte überwachen zu können?
- Welche zusätzlichen regulatorischen Anforderungen werden in den kommenden Jahren auf die Automobilindustrie zukommen?
- Wie können Automobilhersteller einen besseren Einblick in die Sicherheitsmaßnahmen ihrer Zulieferer für elektronische Steuergeräte erhalten?

Ein grundsolider Ansatz für die Cybersicherheit in der Automobilindustrie

Da Automobilhersteller zunehmend End-to-End-Konnektivität in ihren Produktionsanlagen und unternehmensweiten Computer-Ökosystemen einsetzen, wächst die Notwendigkeit, einen umfassenden Ansatz für die Cybersicherheit zu verfolgen, um Menschen, geistiges Eigentum, Produktivität und betriebliche Kontinuität zu schützen.

OT-Netzwerke sind von Natur aus komplex; es gibt keinen Königsweg oder eine einfache, einmalige Lösung, die eine dauerhaft sichere Umgebung garantieren kann.

Stattdessen ist es wichtig, einen kontinuierlichen, risikobasierten Ansatz zu verfolgen, bei dem die besonderen Risiken für Menschen, Prozesse und Technologien im Unternehmen ermittelt werden. Eine eindeutige Beurteilung der Schwachstellen und der damit verbundenen Risiken kann dem Unternehmen helfen, die richtigen Ressourcen zuzuweisen, die richtigen Richtlinien und Verfahren zu implementieren und die richtigen Technologien einzusetzen.

Automobilhersteller sollten sich zunächst ein Bild von der Sicherheitslage ihrer installierten Basis machen, indem sie eine gründliche Bestandsaufnahme der Anlagen und eine umfassende Risikobeurteilung durchführen.

Chronologie der folgenschwersten Angriffe auf Automobilhersteller

März 2019

In einem ganz gezielten Angriff, der wahrscheinlich von einer APT-Gruppe (Advanced Persistent Threat) durchgeführt wurde, verschafften sich Cyberkriminelle Zugang zu Servern mit Kundendaten, was möglicherweise bis zu 3,1 Millionen Menschen betraf.[16]

Dezember 2019

Eine APT-Gruppe, die im Verdacht steht, Verbindungen zur vietnamesischen Regierung zu haben, APT 32 (Ocean Lotus), soll in die Netzwerke zweier großer Automobilhersteller eingedrungen sein.[17]

Februar 2020

Sicherheitsforscher entdeckten 19 Schwachstellen in Fahrzeugen, über die sie mit den Backend-Servern der Hersteller kommunizieren konnten, um Autotüren zu öffnen und Motoren aus der Ferne zu starten.[18]

April 2020

Durch Reverse-Engineering der Telematik-Steuereinheit eines einzelnen Fahrzeugs konnten die Sicherheitsforscher die Telematikverbindung nutzen, um in das Unternehmensnetzwerk des OEM einzudringen und sich Zugang mit sämtlichen administrativen Rechten zu verschaffen.[19]

Mai 2020

Der Quellcode für vernetzte Komponenten, die in den Transportern eines Automobilherstellers eingebaut sind, wurde veröffentlicht, nachdem Git-Repositories mit Bildern, Code, detaillierter Dokumentation und Entwicklungsumgebungen für die integrierten Logikeinheiten der Transporter an die Öffentlichkeit gelangt waren.[20]

Juni 2020

Bei einem gezielten Ransomware-Angriff auf einen japanischen Automobilhersteller wurden interne Server infiziert, was dazu führte, dass das Unternehmen die Produktion in Werken rund um den Globus aussetzen musste.[21]

August 2020

Einem Sicherheitsforscher ist es gelungen, die Kontrolle über die gesamte vernetzte Fahrzeugflotte eines Automobilherstellers zu erlangen, indem er eine serverseitige Schwachstelle im Netzwerk des OEM ausnutzte.[22]

August 2020

Ein Autohaus wurde Opfer der Gruppe, die mit der Ransomware Ryuk operiert. Die Angreifer stahlen während des Vorfalls Unternehmensdaten und veröffentlichten sie auf ihrem eigenen Leak-Portal.[23]

Februar 2021

Ein Automobilhersteller wurde Opfer eines mutmaßlichen Angriffs mit der Ransomware DoppelPaymer, der sich auf interne und kundenseitige Systeme auswirkte und zu einem längeren Ausfall führte.[24]

Mai 2021

Ein Teilezulieferer, der Tochtergesellschaft dieses großen Automobilherstellers ist, wurde Opfer eines gezielten Ransomware-Angriffs. Finanz- und Kundendaten wurden exfiltriert und offengelegt, während die Muttergesellschaft des Unternehmens aufgrund von Lieferkettenproblemen mit Produktionsausfällen zu kämpfen hatte.[25]

[16] CPO Magazine, [17] ZD Net, [18] Upstream, [19] Pen Test Partners, [20] ZDNet,
[21] Dark Reading, [22] Electrek, [23] TechNadu, [24] CPO Magazine, [25] The Register

Das NIST Cybersecurity Framework

Das Cybersecurity Framework des National Institute of Standards and Technology (NIST) stellt eine Reihe von Richtlinien und Best Practices zur Verfügung, die in den unterschiedlichsten Sektoren und Branchen als Standard übernommen wurden. Das NIST Cybersecurity Framework bietet neben Anleitungen, wie Unternehmen mit Cybersicherheitsrisiken umgehen und diese minimieren können, auch eine Reihe von Empfehlungen, wie Cybersicherheitsvorfälle verhindert und erkannt werden können und wie darauf reagiert werden muss, um eine schnelle Wiederherstellung nach einem Komplettausfall zu ermöglichen. Es wird allgemein als das maßgebliche Fundament verstanden, auf dem ein Unternehmen ein solides Sicherheitsprogramm aufbauen kann.

Das Framework umfasst fünf Kernfunktionen: **Identifizieren, Schützen, Erkennen, Reagieren und Wiederherstellen**. Zusammen decken sie das gesamte Angriffskontinuum und den Lebenszyklus des Sicherheitsmanagements ab. Die fünf Funktionen strukturieren Schlüsselbereiche, auf die sich Automobilhersteller konzentrieren können, um ihre allgemeine Sicherheitslage zu verbessern, die Zahl der ausnutzbaren Angriffsschwachstellen zu verringern und den Schaden zu minimieren, den einen OT-Cybersicherheitsvorfall verursachen könnte.

Im Folgenden wird jeder dieser Bereiche eingehender beschrieben, um eine Roadmap der Maßnahmen zum Aufbau einer Defense-in-Depth-Sicherheitsstrategie zu erstellen, die sich am NIST Cybersecurity Framework orientiert.

IDENTIFIZIEREN

In der ersten Funktion des NIST Framework wird den Unternehmen empfohlen, geschäftskritische Prozesse und Anlagen zu ermitteln sowie eine Bestandsaufnahme der Systeme und Software in ihren IT- und OT-Umgebungen durchzuführen. Auf diese Weise ist es möglich, die Quellen von Cybersicherheitsrisiken besser zu verstehen, indem sie Systemen, Anlagen, Daten und Fähigkeiten zuordnet werden. Mit diesem Verständnis kann ein Unternehmen seine Bemühungen auf die Unternehmensziele und die Risikomanagementstrategie ausrichten und entsprechende Prioritäten setzen.

Da in den heutigen Produktionsstätten zunehmend neue vernetzte Geräte in Betrieb genommen werden, können Sicherheitsteams immer schwerer einschätzen, welche OT-Hardware vernetzt ist. Es ist nahezu unmöglich, etwas zu schützen, das man nicht sehen kann.

Die Pflege eines aktuellen und präzisen Anlagenbestands (einschließlich Informationen über gerätespezifische Merkmale wie Konnektivität und Risiken oder Schwachstellen, die in den Anlagen vorhanden sind) ist unerlässlich. Wenn Sicherheitsteams wissen, was sich im Netzwerk befindet, können sie Systemarchitekturen und Datenflüsse mithilfe von Standarddarstellungen dokumentieren, die es weltweit operierenden Teams ermöglichen, Hardwaretopologien – und Risiken – standortübergreifend zu vergleichen.

Ein umfassender Anlagenbestand bietet Basiswerte für die Ermittlung von Mängeln und die Entwicklung und Umsetzung eines Sicherheitsprogramms, um diese zu beheben. Nach einer ersten Bestandsaufnahme sollten die Automobilhersteller fortlaufende Sicherheitsbeurteilungen einplanen, um zu gewährleisten, dass die Sicherheitsziele weiterhin erreicht und die Industriestandards eingehalten werden. Außerdem gibt die Aufnahme des Anlagenbestands Aufschluss über nicht genehmigte oder unzulässig genutzte Anlagen.

Sicherheitsbeurteilungen sind auch für die Ermittlung von Softwareschwachstellen (CVEs) unerlässlich. Sie bilden die Grundlage für die sofortige Entschärfung bestehender Schwachstellen und ermöglichen es Unternehmen, einen proaktiven Ansatz zum Erkennen und Beheben künftiger Schwachstellen zu entwickeln.

SCHÜTZEN

Die Schutzfunktion umfasst Aktivitäten, die die Cyberhygiene verbessern und eine Defense-in-Depth-Sicherheitsstrategie unterstützen. Auf diese Weise werden verschiedene Sicherheitsvorkehrungen getroffen, die das Cyberrisiko verringern und die Integrität und Geheimhaltung wertvoller Daten sowie die Verfügbarkeit geschäftskritischer Systeme schützen. Zu diesen Schutzmaßnahmen gehören Identitäts- und Zugriffsmanagementkontrollen, Netzwerksegmentierung, CIP-Sicherheit, CPwE-Architektur, Programme für das Schwachstellenmanagement, Backuplösungen, Sicherheitsschulungen für Mitarbeiter und gerätebasierte Konfigurationskontrollen.

Die Netzwerksegmentierung ist ein entscheidender Faktor für Automobilhersteller und andere Industrieunternehmen. Ältere OT-Netzwerke weisen in der Regel eine flache Architektur auf, aber falsch segmentierte IT- und OT-Netzwerke ermöglichen es Angreifern, die sich Zugang zu IT-Systemen verschaffen, sich schnell seitlich durch die Betriebsumgebung zu bewegen und möglicherweise Ransomware zu verbreiten, Zugang zu geschützten Informationen zu erhalten oder die Produktion zu gefährden.

Ein geeignetes Netzwerkdesign und eine effektive Segmentierung industrieller DMZs und Sicherheitszonen ermöglichen es Sicherheitsteams, die betroffenen Systeme im Falle eines Angriffs schnell zu isolieren. So kann die normale Produktion an anderer Stelle in der Einrichtung fortgesetzt werden.

Hersteller, die neue automatisierte oder vernetzte Lösungen einsetzen, können eine validierte Referenzarchitektur nutzen, um sicherzustellen, dass sie ein zukunftsfähiges Netzwerk entwickeln, das richtig segmentiert ist und auf Leistung, Verfügbarkeit und Sicherheit getestet wurde. Die Verwendung einer Architektur, die aus zuvor validierten Designs besteht, mit dokumentierten Best Practices und Konfigurationseinstellungen, ermöglicht es Unternehmen, ein stabiles konvergiertes IT/OT-Netzwerk zu realisieren, das alle Anforderungen an Leistung, Skalierbarkeit und Sicherheit erfüllt.

ERKENNEN

Die Aktivitäten innerhalb der Funktion „Erkennen" ermöglichen es Cybersicherheitsteams, anomales Netzwerkverhalten oder ungewöhnliche Datenflüsse, die auf einen Angriff hindeuten, schnell zu identifizieren. Zu diesen Aktivitäten gehören das Erfassen und Überwachen von Protokollen und die kontinuierliche Überwachung der logischen und physischen Sicherheit von IT- und OT-Umgebungen. Ein rund um die Uhr erreichbares Security Operations Center (SOC) sorgt für die erforderlichen Funktionen zur Alarmierung, Untersuchung von Ereignissen und Reaktion.

Bedrohungserkennungsdienste von Drittanbietern können Zugang zu Technologien zur Erkennung von Anomalien und Sicherheitsverletzungen bieten. Ihre Verwendung ermöglicht es den Abwehrsystemen, normale Betriebsbasiswerte festzulegen und Situationen zu erkennen und zu untersuchen, die nicht mit diesen erwarteten Mustern übereinstimmen.

Um die Auswirkungen eines Sicherheitsereignisses auf den Anlagenbetrieb zu bestimmen, ist eine konsequente und gründliche Dokumentation aller Anlagensysteme, OT-Netzwerke und IoT/IIoT-Geräte – einschließlich derjenigen, die potenziell unsicher sind – unerlässlich. In vielen Produktionsumgebungen wurde das Know-how über die OT-Systemarchitekturen – und darüber, welche Systeme mit externen Netzwerken verbunden sind – als „Insiderwissen" unter dem Werkspersonal gepflegt. Durch eine formale Dokumentation wird die Zusammenarbeit zwischen Ingenieuren und Sicherheitsteams gestärkt und produktiver gestaltet.

REAGIEREN

Wenn ein Cybersicherheitsvorfall erkannt wird, können Organisationen, die die Aktivitäten im Rahmen der Funktion „Reagieren" durchgeführt haben, schnell Maßnahmen ergreifen, um den Vorfall einzudämmen und seine Auswirkungen zu verringern. Die Funktion „Reagieren" umfasst sowohl technische Fähigkeiten als auch Prozesse und Kommunikationsabläufe. Organisationen sollten die Rollen und Zuständigkeiten der wichtigsten Beteiligten proaktiv festlegen, die bei einem OT-Cybervorfall zum Einsatz kommen würden.

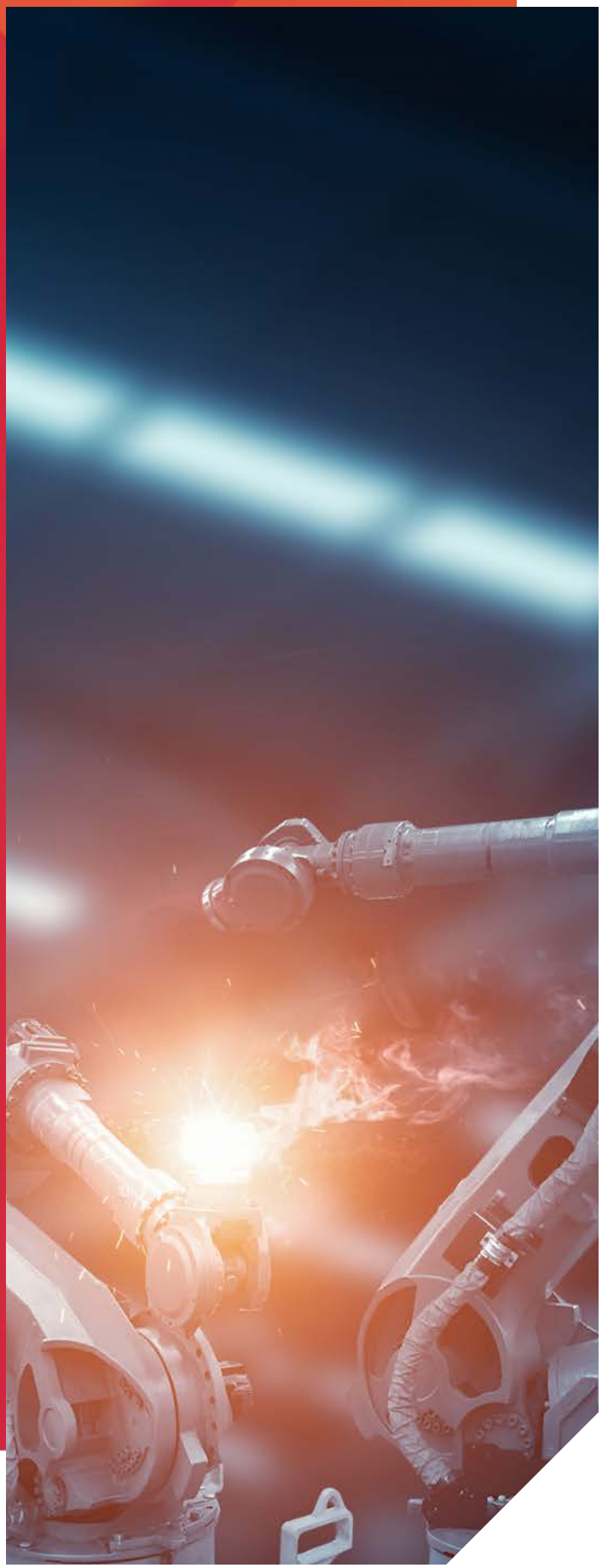
SOC-Teams und Anlageningenieure müssen sich die Verantwortung für die Untersuchung von Ereignissen teilen. Alle Mitarbeiter vor Ort und außerhalb des Unternehmens werden von regelmäßigen Notfallübungen profitieren, um die bestehenden Verfahren zu überprüfen und sicherzustellen, dass sie im Krisenfall schnelle und präzise Entscheidungen treffen können.

WIEDERHERSTELLEN

Die Funktion „Wiederherstellen" geht über unmittelbare, kurzfristige Reaktionsmaßnahmen hinaus. Organisationen sollten Pläne entwickeln, die es ihnen ermöglichen, Fähigkeiten oder Services, die durch Cybersicherheitsvorfälle beeinträchtigt wurden, schnell wiederherzustellen. Dadurch lässt sich die Ausfallsicherheit erhöhen und die Betriebskontinuität schützen.

Alle industriellen Fertigungsbetriebe sollten nicht nur umfassende Backups erstellen, sondern auch sicherstellen, dass eine vollständige Wiederherstellung so schnell realisiert werden kann, dass keine schwerwiegenden betrieblichen Auswirkungen entstehen. Das Testen von Backupfunktionen ist genauso wichtig wie die Durchführung regelmäßiger Notfallübungen, um Lücken in der Ausfallsicherheit von Geschäftsprozessen zu erkennen und zu schließen.

Die Wiederherstellung von Industriesteuerungssystemen erfordert spezielle Qualifikationen und Fähigkeiten. Die Sicherheitsteams müssen nicht nur die forensische Untersuchung und die Schadensbeurteilung abschließen und sicherstellen, dass die gesamte Schadsoftware entfernt wurde, sondern auch die Laufwerke wieder in Betrieb nehmen und die SPS-Prozesse wiederherstellen, damit sie voll funktionsfähig sind. Die Teams sollten über Erfahrung darin verfügen, wie Prozesse schnell wieder aufgenommen und in Gang gesetzt werden können.



Das Kernkonzept von Zero Trust lautet „Niemals vertrauen, immer prüfen“.

Zero Trust für Automobilhersteller

Zero Trust ist ein Ansatz für die Netzwerksicherheit, der vor mehr als einem Jahrzehnt erstmals von John Kindervag von Forrester Research vorgestellt wurde. Seitdem hat dieser Ansatz unter IT-Sicherheitsexperten an Akzeptanz gewonnen, vor allem, weil er sich ideal für die Absicherung moderner Cloud-First- und remotefähiger IT-Umgebungen eignet. Und mittlerweile wird er auch von OT-Sicherheitsexperten immer häufiger eingesetzt.

Das Kernkonzept von Zero Trust lautet „Niemals vertrauen, immer prüfen“. Die zugrunde liegende Annahme ist, dass keinem Benutzer, keiner Rechneridentität, keinem Datenverkehrsfluss und keiner Anwendung von vornherein vertraut werden sollte. Stattdessen sollten Identitäten und Risikostufen laufend überprüft und die Richtlinien für jede Verbindung kontinuierlich durchgesetzt werden.

In der heutigen Welt, in der Angriffe an der Tagesordnung sind, wird die Einführung eines Zero Trust-Ansatzes die Risiken mindern und die Wahrscheinlichkeit eines erfolgreichen Angriffs verringern. Die Automobilhersteller können durch Zero Trust wie folgt profitieren:

- Verkleinerung der Angriffsfläche durch die Einrichtung detaillierter Zugangskontrollen für wichtige Anlagen.
- Deutliche Verringerung der Anzahl böswilliger Eindringlinge in das Netzwerk durch strengere Anforderungen an die Authentifizierung und Identitätsüberprüfung.
- Abbau von übermäßigem Vertrauen in die Netzarchitektur, um die Arbeit von Angreifern zu erschweren

Heutige Zero Trust-Strategien lassen sich am besten mit einer anderen von Kindervag bereitgestellten Methodik entwickeln, die sich darauf konzentriert, die Schutzflächen des Unternehmens zu identifizieren – also die Daten, Anlagen, Anwendungen und Services (DAAS), die für die Betriebsabläufe am kritischsten sind – und diese mit Zero Trust-Kontrollen in der Reihenfolge ihrer Priorität zu schützen.

Wie Ihnen Rockwell Automation helfen kann

Rockwell Automation ist der weltweit führende Anbieter für industrielle Automatisierung und blickt auf mehr als hundert Jahre Erfahrung in der Entwicklung und Herstellung von OT-Systemen zurück.

Das Unternehmen nutzt dieses umfassende Know-how, um kritische Anlagen, Ressourcen und Netzwerke auf der ganzen Welt zu sichern. Mit Tausenden von Kunden im Bereich Industriesteuerungssysteme und Automatisierung weltweit weiß Rockwell Automation genau, worauf es ankommt, um Infrastrukturen zu schützen, Ausfallzeiten zu vermeiden und den Schaden durch Cyberangriffe zu begrenzen. Rockwell bietet auf die Industrie abgestimmte Cybersicherheitsservices, die den Produktionsbetrieb schützen, auf den Sie und Ihre Kunden täglich angewiesen sind – vom Fertigungsbereich bis in die Cloud.

Die von Rockwell Automation angebotenen Managed Services umfassen die Aktivitäten aller fünf Funktionen des NIST Cybersecurity Framework, einschließlich Anlagenidentifikation, Penetrationstests und -beurteilungen, Überwachung von Schwachstellen und Patching, Entwurf und Implementierung von Sicherheitsprogrammen, Erkennung und Sicherung von Bedrohungen sowie Reaktion auf Vorfälle und Wiederherstellungsservices.

Außerdem bietet Rockwell ein umfassendes Portfolio an projektbasierten Services an, mit denen Kunden ihre OT-Sicherheit schneller ausbauen können. Darüber hinaus pflegt Rockwell enge Partnerschaften mit führenden Unternehmen der IT- und Sicherheitsbranche wie Cisco, Claroty, Microsoft, Dragos und Crowdstrike. Gemeinsam mit Cisco hat das Unternehmen die Converged Plantwide Ethernet(CPwE)-Architektur entwickelt, um Kunden eine Reihe von vorab validierten und dokumentierten Architekturplänen sowie praktische Anleitungen für deren Umsetzung und Konfiguration bereitzustellen.

Das Produktportfolio von Rockwell Automation umfasst sowohl Secure-by-Design-Lösungen für Industriesteuerungen als auch Sicherheitstechnologien, die speziell entwickelt wurden, um die Produkte von Rockwell mit zusätzlichen Sicherheitsebenen auszustatten. Diese eigens entwickelten Sicherheitslösungen bieten Perimeterschutz, Netzwerksegmentierung, sichere Kommunikation zwischen Steuerungselementen und Datenschutz für die Benutzer ihrer Geräte.

Wenn Sie mehr darüber erfahren möchten, wie Automobilhersteller den nächsten Schritt zum Aufbau von cybersicheren Produktionsanlagen realisieren können, wenden Sie sich noch heute an einen Experten von Rockwell Automation.

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

Publikation GMSN-BR004A-DE-P – Mai 2022