Rockwell Automation

EINBLICKE IN DIE CYBERSICHERHEIT DER AUTOMOBILINDUSTRIE:

Gängige Bedrohungen, proaktive Prävention

Zusammenfassung

Bedrohungsakteure nehmen Automobilunternehmen mit erfolgreichen Cyberangriffen ins Visier. Die jüngsten öffentlichkeitswirksamen Vorfälle zeigen, dass der derzeitige Cybersicherheitsschutz in der Automobilindustrie offensichtlich nicht stabil genug ist:

- Februar 2021. Ein führender Automobilhersteller in Südkorea wurde Opfer eines Ransomware-Angriffs, der zu Ausfällen bei Zahlungsdiensten, seiner mobilen Apps und interner Systeme von Händlern führte.
- Juni 2020. Japans führender Automobilhersteller wurde Opfer eines Cyberangriffs, der zu Betriebsunterbrechungen seiner Werke in Großbritannien, Nordamerika und Italien führte.
- April 2020. Die Untersuchung einer Automobilzeitschrift ergab schwerwiegende Sicherheitsmängel in zwei der meistverkauften Fahrzeugmodelle.

Mehrere Faktoren tragen zu einer breiteren Angriffsfläche bei Automobilherstellern bei, darunter:

- Vermehrter Datenfluss, verstärkte Kommunikation, Konnektivität und Integration der OT- und IT-Infrastruktur.
- Mangel an qualifizierten Ressourcen für die Bewältigung von Risiken im Zusammenhang mit Industriesteuerungssystemen, SCADA- (Supervisory Control and Data Acquisition) und anderen OT-Systemen.
- Mangelhafte Transparenz in Bezug auf die Anzahl und die Art der an Fahrzeugnetzwerke angeschlossenen Geräte.
- Die anhaltende Pandemie hat die Lieferkette unter Druck gesetzt und das Risiko sowie die Kosten von Produktionsausfällen in einer Zeit, in der die Lagerbestände knapp sind, noch weiter erhöht. Leider ist es unwahrscheinlich, dass sich diese Situation in nächster Zeit entspannen wird.
- Der Ausbau der Infrastruktur für Elektrofahrzeuge bringt neue Bedrohungen für vernetzte Fahrzeuge, öffentliche Ladestationen und sogar das Stromnetz mit sich. Und das Fehlen von Sicherheitsstandards zur Absicherung von Ladestationen erschwert deren Schutz nur noch weiter.

Angreifer zielen auf Schwachstellen in der installierten Netzwerkbasis ab, unter anderem auf Maschinen und Geräte in den Fertigungsbereichen. Da fast die Hälfte der 100 größten Automobilhersteller als hochgradig anfällig für Ransomware-Vorfälle gilt[1], ist klar: Das Risikomanagement in der Automobilindustrie ist noch immer zu reaktiv, um der zunehmenden Dynamik und Raffinesse der Angriffe zu begegnen.

[1] Black Kite

Kosten und Konsequenzen

Schwachstellen, die von Bedrohungsakteuren ausgenutzt werden, können zu einer Vielzahl negativer betrieblicher Folgen führen, die über die typischen IT-Probleme, wie z. B. Datenschutzverletzungen, hinausgehen.

AUSFALLZEITEN IN DER PRODUKTION

Außerplanmäßige Ausfallzeiten sind eines der größten Risiken für Unternehmen der Automobilindustrie, da Betriebsausfälle sehr kostspielig sind. Eine Schätzung ergab Kosten von 22 000 USD pro Minute bzw. 1,3 Millionen USD pro Ausfallstunde. Einigen Schätzungen zufolge belaufen sich die Kosten auf 50 000 USD pro Minute.[2] Cyberangriffe verursachen häufig Ausfallzeiten in OT-Umgebungen, und Angreifer wissen, dass Unterbrechungen der Fahrzeugproduktion mit solch hohen Kosten verbunden sind, was die Automobilindustrie zu einem primären Ziel macht.

Zu den Kosten für Ausfallzeiten kommen noch die Kosten für betriebliche und materielle Schäden sowie die Kosten für Reaktion, Schadensbehebung und Wiederherstellung nach einem Cyberangriff hinzu, die in der Regel auf über 1 Million USD bis zu 13 Millionen USD oder mehr pro Vorfall geschätzt werden.

GEFÄHRDUNG SENSIBLER DATEN

Das Potenzial für eine Gefährdung sensibler Daten reicht von der Informationstechnologie (IT) bis hin zur Betriebstechnologie (OT). Vertrauliche Daten im Fertigungsbereich liegen jedoch in einer anderen Form vor. Geschäftsgeheimnisse, einschließlich Formeln, Techniken, Software oder Maschinen- bzw. Rezepturdaten, sind äußerst wertvolles geistiges Eigentum und stark wettbewerbsorientierte Geschäftsgüter. Die Automobilhersteller schätzen diese Informationen, weil sie ihnen einen Wettbewerbsvorteil in Bezug auf die betriebliche Effizienz oder die Produktmerkmale verschaffen können, insbesondere im Zusammenhang mit der Umstellung auf Elektrofahrzeuge und Ladestationen.

Angreifer, denen es gelingt, in Umgebungen mit Betriebstechnologie (OT)/Industriesteuerungssystemen einzudringen, können wichtige Informationen und/oder sensible Kundendaten ausspähen und exfiltrieren.

ENGPÄSSE IN DER LIEFERKETTE

Doch nicht nur die Automobilhersteller sind im Visier der Angreifer. Die Risiken erstrecken sich auch auf Zulieferer, die Automobilunternehmen mit kritischen Produktionsbauteilen wie Klimaanlagen und Heizungssystemen beliefern. Schwere Cyberangriffe auf Zulieferer können einen Dominoeffekt auslösen, der zu längeren Engpässen in der Lieferkette führen kann.

Cyberkriminelle nehmen Schwachstellen auf allen Ebenen der Lieferkette in der Automobilindustrie ins Visier. Im Oktober 2021 wurde beispielsweise der deutsche Automobilzulieferer Eberspächer Group[3], der 50 Werke unterhält, Opfer eines Ransomware-Angriffs auf seine weltweiten Netzwerke und Server, bei dem Daten verschlüsselt wurden. Das Unternehmen schaltete seine IT-Systeme vorsorglich ab, musste jedoch erhebliche Störungen hinnehmen, die dazu führten, dass Mitarbeiter in bezahlten Urlaub geschickt wurden, was weitere Verluste zur Folge hatte.

BEDROHUNG DER PHYSISCHEN SICHERHEIT

Cyberangriffe, die in OT-Umgebungen der Automobilbranche vordringen, können auch zu einer potenziellen Bedrohung für die physische Sicherheit werden. Malware, Würmer und Viren können industrielle Systeme wie speicherprogrammierbare Steuerungen (SPS) sabotieren und Angreifern die Kontrolle über die Maschinen in Produktionsstraßen geben. Unerwartete Anpassungen der Prozesse in der Produktionsstraße oder des Verhaltens der Anlagen können ebenfalls eine Gefahr für die Sicherheit der Arbeiter im Fertigungsbereich darstellen. Zudem könnte eine absichtliche OT-Beschädigung die Produktintegrität beeinträchtigen und die Sicherheit der Kunden gefährden.

[2] TPC, [3] Eberspächer

Bedrohungsakteure und gängige Cyberangriffe in der Automobilindustrie

Um einen vollständigen Überblick über die Cybersicherheitslandschaft in der Automobilindustrie zu erhalten, ist es wichtig, mehr über die bösartigen Bedrohungsakteure, die es auf Automobilunternehmen abgesehen haben, und die bei Angriffen üblicherweise verwendeten Methoden zu erfahren. Ein weiterer wichtiger Punkt ist, dass die meisten erfolgreichen Cyberangriffe bekannte Schwachstellen ausnutzen, die mit den verfügbaren Tools und bewährten Verfahren behoben werden können, auch wenn die Raffinesse der Angriffe exponentiell zunimmt.

BEDROHUNGSAKTEURE

Böswillige Cybersicherheitsakteure, wie z. B. Ransomware-Banden, versuchen, Netzwerke zu infiltrieren, um daraus einen finanziellen Nutzen zu ziehen. Andere Bedrohungsakteure können Automobilunternehmen mit der Absicht angreifen, physischen Schaden anzurichten oder wertvolles geistiges Eigentum, personenbezogene Daten oder andere wertvolle Informationen zu stehlen.

Darüber hinaus ist die Automobilindustrie Teil des kritischen Fertigungssektors, der von der Cybersecurity and Infrastructure Security Agency (CISA)[4] als entscheidend für den wirtschaftlichen Wohlstand und die Kontinuität der USA eingestuft wird. Der wirtschaftlich kritische Charakter der Automobilherstellung macht die Unternehmen dieser Branche auch anfällig für Cyberangriffe von Nationalstaaten. Zur Durchsetzung ihrer eigenen nationalen Interessen können Länder Bedrohungsakteure damit beauftragen, Informationen zu sammeln oder wichtige industrielle Ziele zu sabotieren.

Sicherheitsforscher entdecken und veröffentlichen darüber hinaus Schwachstellen in den Cybersicherheitsmaßnahmen von Automobilunternehmen. Bei einem unlängst aufgetretenen Vorfall[5] analysierten Sicherheitsforscher die Computersysteme eines beliebten Modells eines großen US-Autoherstellers und entdeckten eine Reihe von WLAN-Anmeldedaten für ein Montagewerk.

Natürlich haben es Sicherheitsforscher nicht darauf abgesehen, Schwachstellen böswillig auszunutzen, doch sie können Lücken aufdecken, die für die Öffentlichkeitsarbeit ein Alptraum sind und die Glaubwürdigkeit bei den Kunden beeinträchtigen.

Befassen wir uns nun mit den gängigen Angriffen, denen Automobilhersteller und ihre Zulieferer häufig ausgesetzt sind.

RANSOMWARE

Ransomware ist ein schnell zunehmender Angriffstyp, der in allen Branchen Probleme verursacht. Der Bericht „2021 Third Party Breach Report"[6] von Black Kite hat ergeben, dass Ransomware mittlerweile die häufigste Ursache für Datenschutzverletzungen durch Dritte ist und 27 % der Angriffe im Jahr 2021 ausmachte. 53 % der CISOs gaben an, dass sie im letzten Jahr mindestens einmal von Ransomware betroffen waren.

Bei einem typischen Ransomware-Angriff dringen die Bedrohungsakteure in das Netzwerk ein und übertragen bösartige Daten, die mehrere Dateien und Geräte verschlüsseln. Bei vielen Ransomware-Vorfällen werden Daten exfiltriert und verschlüsselt, da die Bedrohungsakteure davon ausgehen, dass eine Erpressung eher erfolgreich ist, wenn sie damit drohen können, gestohlene sensible Informationen zu veröffentlichen. Da die Grenzen zwischen IT und OT fließend sind, können Ransomware-Angriffe zu den gefürchteten Produktionsunterbrechungen im Fertigungsbereich führen.

[4] CISA, [5] Which.co, [6] Black Kite

ANGRIFFE AUF INDUSTRIESTEUERUNGSSYSTEME

Integrierte Konnektivität und eine zunehmend offene Kommunikation zwischen IT-, OT- und Internet-of-Things(IoT)-Geräten haben auch die Angriffsfläche in Umgebungen mit Industriesteuerungssystemen vergrößert und machen oft jahrzehntealte Technologien erstmals dem Internet und cloudbasierten Anwendungen zugänglich. Organisationen, die ihr „Air Gapping" für ausreichend halten, werden eines Besseren belehrt.

Zu den häufigen Angriffen zählen die Ausnutzung unsicherer Kommunikationsprotokolle, ungepatchte Software, schwache IoT-Sicherheit und Malware-Angriffe auf die Lieferkette, die sich auf Fertigungssysteme auswirken. Und die Angriffe auf Industriesteuerungssysteme nehmen zu, wie die Offenlegung von 41 % mehr Schwachstellen von Industriesteuerungssystemen[7] in der ersten Hälfte des Jahres 2021 gegenüber dem gleichen Zeitraum des Jahres 2020 zeigt.

HACKERANGRIFFE AUF VERNETZTE FAHRZEUGE

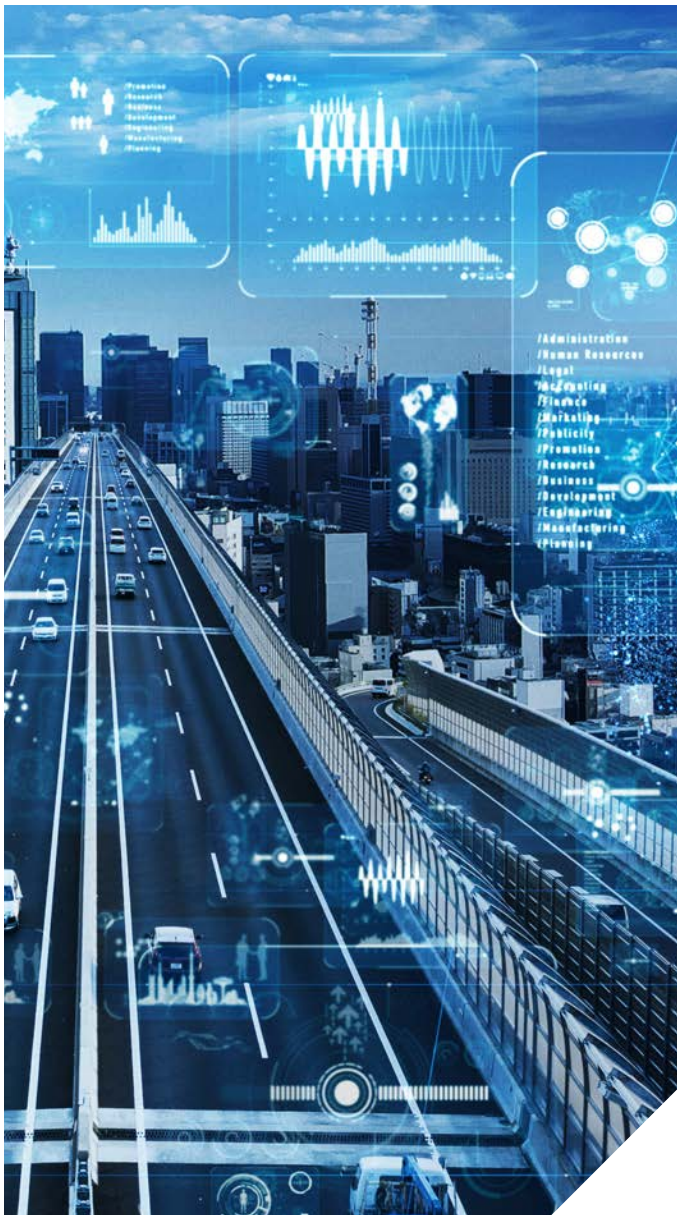
Moderne vernetzte Kraftfahrzeuge sind mit verschiedenen integrierten Computersystemen ausgestattet, auf die Bedrohungsakteure mit dezentralen und physischen Angriffen abzielen können. Moderne Fahrzeuge „wachen auf" und werden vernetzt, noch bevor sie vom Band laufen, und sind mit Systemen ausgestattet, die potenzielle Sicherheitslücken darstellen.

- Die Telematik-Steuereinheit kann anfällig für Hackerangriffe sein. Bei einem Vorfall[8] entwendeten Forscher ein Telematikgerät aus einem Fahrzeug, zogen die SIM-Karte (Subscriber Identity Module) heraus und konnten über den SIM-Zugang die vollständige Kontrolle über das Unternehmensnetzwerk des OEM (Original Equipment Manufacturer) erlangen, indem sie die Zugangsdaten des Administrators verwendeten.
- Der Controller Area Network(CAN)-Bus ermöglicht die Kommunikation zwischen verschiedenen Mikrosteuerungen und Sensoren in Kraftfahrzeugen. Untersuchungen[9] zeigen, dass ein typischer CAN-Bus sehr anfällig für Angriffe ist, die Schwachstellen wie fehlende Authentifizierung oder Verschlüsselung ausnutzen, was zur Übernahme des Fahrzeugs oder zur Preisgabe sensibler Daten führen kann.

MOBILE APPS

In unserer zunehmend mobilen Welt bieten viele OEMs mobile Apps an, mit denen sich Kunden mit ihren Fahrzeugen verbinden können. Einige dieser Apps ermöglichen es den Nutzern, ihr Fahrzeug zu orten, die Türen zu öffnen und den Motor zu starten. Hacker können Schwachstellen in der Codierung, der Kommunikation oder der Datenspeicherung der App ausnutzen.

Die Konsequenzen von Angriffen auf mobile Anwendungen reichen von der Preisgabe sensibler Daten bis hin zu potenziellen Sicherheitsrisiken. Im Jahr 2018 gab beispielsweise ein Autohersteller[10] versehentlich die persönlichen Daten von mehr als 50 000 App-Nutzern in einem ungesicherten Cloud-Speicherbereich preis.



[7] CPO Magazine, [8] Pen Test Partners, [9] University of Washington, [10] Bleeping Computer

Proaktive Cybersicherheit in der Automobilfertigung

Automobilunternehmen brauchen einen proaktiveren Ansatz, um die Flut von Bedrohungen zu bewältigen, denen sie heute ausgesetzt sind. Unsere Empfehlungen decken wichtige Aspekte der Defense-in-Depth-Sicherheitsstrategie ab und stehen im Einklang mit dem Cybersecurity Framework (CSF) von NIST.

BESTANDSAUFNAHME UND RISIKOBEURTEILUNG

Proaktive Sicherheit beginnt mit dem Schließen von Transparenzlücken. Welche Anlagen im Fertigungsbereich befinden sich im Netzwerk? Welche Software wird in OT-Umgebungen eingesetzt, und welche besonderen Risiken bestehen für diese Anlagen und Software? Automobilhersteller können nicht schützen, was sie nicht kennen.

Eine gründliche Bestandsaufnahme und Risikobeurteilung kann Ihnen dabei helfen, die wichtigsten Abhilfemaßnahmen zu ergreifen, bevor böswillige Akteure offensichtliche Schwachstellen ausnutzen können. Die ersten Maßnahmen, die Sie ergreifen können, entsprechen der Kategorie „Identifizieren" des NIST CSF, die dazu dient, den Sicherheitsschutz auf die Schwachstellen mit der höchsten Priorität zu konzentrieren und zu priorisieren. Ziel ist es, die wertvollsten Unternehmensressourcen zuerst zu sichern, basierend auf den erkannten Bedrohungen und Risiken für die Organisation.

PATCH MANAGEMENT

Das Patch Management im OT-Bereich ist eine Herausforderung, da jede Ausfallzeit kostspielig ist und vermieden wird, und für das Patchen von veralteter Software oft eine Maschine außer Betrieb genommen werden muss.

In den meisten Fällen werden bei einer Bestandsaufnahme der Anlagen und einer Risikobeurteilung im Fertigungsbereich mehrere Anlagen mit veralteten Betriebssystemen entdeckt. Durch diese Schritte werden auch nicht autorisierte Ressourcen aufgedeckt, die im Netzwerk verborgen sind und die Organisation kritischen Sicherheitsrisiken aussetzen.

Ein proaktiver Sicherheitsansatz muss ein methodisches Patch Management umfassen, um Schwachstellen im Einklang mit der Schutzfunktion („Protect") des NIST CSF zu beheben. Unternehmen in der Automobilindustrie benötigen Prozesse, um Patches mit minimaler Betriebsunterbrechung zu implementieren. Einige Unternehmen entscheiden sich für einen Infrastructure-as-a-Service-Ansatz, der das Patching und andere Betriebs- und Cybersicherheits-Managementprozesse erheblich vereinfacht.

Sicherheitsteams sollten beim Bestimmen der Patching-Prioritäten folgende Faktoren berücksichtigen:

- Das potenzielle Risiko für Anlagen, wenn eine Sicherheitslücke ausgenutzt wird
- Die Bedeutung jedes anfälligen Geräts oder Systems für den gesamten Fertigungsprozess
- Die Sicherheitsmaßnahmen, die die einzelnen Patches bieten.

ZONENÜBERWACHUNG LOGISCHER NETZWERKE UND CPWE

Die Netzwerkarchitektur spielt eine entscheidende Rolle für die Sicherheit vernetzter IT- und OT-Umgebungen. Angriffe können sich von einzelnen Maschinen, Switches und anderen Anlagenkomponenten in das IT-Netzwerk ausbreiten, aber auch umgekehrt – von IT- zu OT-Netzwerken. Dies ist häufig der Grund für die Entscheidung, Produktionssysteme bei IT-Sicherheitsvorfällen offline zu schalten.

Im vorherigen Beispiel des Eindringens in die Telematik-Steuereinheit eines Fahrzeugs hatte der OEM keine ordnungsgemäße Netzwerksegmentierung vorgenommen. Die Zonenüberwachung logischer Netzwerke hilft bei der Erstellung der richtigen Strategien einer Zonenüberwachung für die ganzheitlichere werksweite Sicherheit und schützt den Betrieb vor einer Vielzahl von Angriffen.

Eine bewährte Referenzarchitektur, wie z. B. Converged Plantwide Ethernet (CPwE), stellt außerdem eine solide Grundlage für eine ordnungsgemäße Netzwerksegmentierung dar, damit Bedrohungsakteure keine Schwachstellen ausnutzen und zwischen IT- und OT-Umgebungen wechseln können.

Häufig entstehen OT-Architekturen aus funktionalen und effizienten Produktionskonzepten, statt dass die Sicherheit von Anfang an integriert wird. OT-Systeme werden entwickelt, um in Betrieb genommen zu werden und reibungslos zu funktionieren. Oft wird nur wenig oder gar nicht darauf geachtet, wie sich eine bestimmte Entscheidung während der Entwicklung auf die Netzwerksicherheit auswirken könnte.

Automobilhersteller benötigen jedoch reibungslos funktionierende OT-Systeme mit den richtigen Cybersicherheitsmaßnahmen zu deren Schutz. Auch wenn die Anzahl und Schwere der Angriffe zunimmt, ist es wichtig, einen reibungslosen und sicheren Informationsfluss aufrechtzuerhalten, um die zuverlässige Betriebszeit zu maximieren.

CPwE nutzt eine industrielle Demilitarized Zone (IDMZ), um Informationen zwischen IT- und OT-Systemen sicher auszutauschen und gleichzeitig die Produktionssysteme vor bösartigem Datenverkehr aus den unternehmenseigenen IT-Systemen oder aus dem Internet zu schützen. Front- und Back-Firewalls sorgen für starken Schutz und die Durchsetzung von Sicherheitsrichtlinien, indem sie den Datenverkehr in allen Netzwerken überprüfen.

KONTINUIERLICHE ERKENNUNG VON UND REAKTION AUF BEDROHUNGEN

Die Erkennung von und die Reaktion auf Bedrohungen ist ein wichtiger Bestandteil der Sicherheitsmaßnahmen jedes Unternehmens.

Ein proaktiver Ansatz für die Cybersicherheit in der Automobilindustrie beginnt mit Präventionsmaßnahmen, die die Cyber-Resilienz verbessern. Die Implementierung von Kontrollen zur Erkennung von Bedrohungen und zur Reaktion auf Vorfälle kann Unternehmen dabei helfen, Angriffe schnell zu identifizieren, auf Bedrohungen zu reagieren und deren Ausbreitung zu verhindern sowie betroffene Systeme im Falle eines Angriffs schneller wiederherzustellen.

Lösungen zur Erkennung von Bedrohungen sollten kontinuierlich Bedrohungssignaturen, wie anomale Geräte und Aktivitäten im Netzwerk, identifizieren. Basiswerte zu normalen Benutzeraktivitäten und Datenverkehrsflüssen können sich bei der Analyse als nützlich erweisen und die Zeit bis zur Erkennung von Vorfällen verkürzen, insbesondere in komplexen Netzwerken mit einem hohen Maß an IT/OT-Konvergenz.

Die Erkennung von Angriffen in Echtzeit ermöglicht auch eine schnelle Reaktion auf Vorfälle, wie z. B. das Abschotten von Geräten oder das Entfernen von Zugängen, was den Automobilherstellern hilft, eine Eskalation des Schadens zu vermeiden.

Cybersicherheits-Know-how von Rockwell Automation für die Automobilindustrie

Rockwell Automation schützt mit seinen Cybersicherheitsservices für die Industrie die Fertigungsprozesse in der Automobilindustrie, auf die Sie und Ihre Kunden täglich angewiesen sind. Unser proaktiver Ansatz deckt den gesamten Lebenszyklus der Cybersicherheit ab, von der Beurteilung bis zur Wiederherstellung – damit Ihr Unternehmen auf die Situationen vor, während und nach einem Angriff vorbereitet ist.

Wir verfügen über ein fundiertes Fachwissen aus dem Bereich Produktionsbetriebe, das auf den Erkenntnissen aus mehr als 100 Jahren industrieller Automatisierung beruht. Beginnend mit einer gründlichen Bestandsaufnahme und Risikobeurteilung können wir Ihnen helfen, sich einen klar strukturierten Überblick über die installierte Architektur, die Netzwerkinfrastruktur und die vorhandenen Schwachstellen in Ihrer Umgebung zu verschafffen.

Unsere Erfahrung mit Converged Plantwide Ethernet gewährleistet eine ganzheitliche Defense-in-Depth-Sicherheitsstrategie zur Abwehr von Bedrohungen, die sich zwischen IT- und OT-Betrieb ausbreiten können. Und eine industrietaugliche Erkennung und Reaktion mit einem rund um die Uhr erreichbaren SOC (Security Operations Center) für die Betriebstechnologie kann helfen, Angriffe zu stoppen, bevor Bedrohungsakteure den Betrieb stören.

Wenn Sie mehr darüber erfahren möchten, wie proaktive Sicherheitsstrategien in der Automobilindustrie vor Cyberangriffen schützen können, kontaktieren Sie uns noch heute.

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-WP004A-DE-P – Mai 2022

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