1201 South Second Street

Milwaukee, WI 53204

www.rockwellautomation.com

**Pressemitteilung**



      

 **Führungskräfte der industriellen Sicherheit diskutieren Herausforderungen und Chancen der Cybersicherheit in neuer Video-Reihe von Rockwell Automation**

*Chief Information Security Officers (CISOs) und Sicherheitsspezialisten analysieren die kurz-, mittel- und langfristige Cybersicherheitslandschaft*

**BRÜSSEL, 20. Juni 2024 –** Rockwell Automation, Inc. (NYSE: ROK), das weltweit größte Unternehmen für industrielle Automatisierung und digitale Transformation, hat heute eine neue Reihe seiner Vordenker-Videos veröffentlicht, die sich eingehend mit der sich ständig weiterentwickelnden Welt der industriellen Cybersicherheit befasst.

Die 11-teilige Video-Reihe umfasst Interviews mit IT/OT-Vordenkern und Chief Information and Security Officers (CISO) von Unternehmen mit kritischen Infrastrukturen, unterstützt von hochrangigen Spezialisten und Branchenvertretern von Rockwell Automation.

Die Reihe befasst sich mit den sich weiterentwickelnden Cyber-Bedrohungen und den Herausforderungen, die sich aus der Einhaltung strenger Gesetze ergeben, darunter [NIS2](https://www.rockwellautomation.com/en-gb/capabilities/industrial-cybersecurity/nis2.html?utm_source=Marketing&utm_medium=Public_Relations&utm_campaign=MultiInitiative_MultiIndustry_EMEA_CMP-05431-R0T3R4&utm_content=news_wire), und zeigt die vielfältigen Möglichkeiten und Kosten-/Zeit-/Effizienzeinsparungen auf, die sich durch robuste, ganzheitliche Cybersicherheitsprogramme ergeben.

Die Interviews mit Sicherheitsverantwortlichen sind für alle wichtig, die an Projekten zur digitalen Transformation und IT/OT-Konvergenz beteiligt sind:

* [Die Bedeutung von Teamarbeit](https://www.rockwellautomation.com/en-gb/company/news/presentations/rokstudios/why-cybersecurity-needs-to-be-seen-as-a-cultural-pillar.html?utm_source=Marketing&utm_medium=Public_Relations&utm_campaign=MultiInitiative_MultiIndustry_EMEA_CMP-05431-R0T3R4&utm_content=news_wire) (IT + OT), kulturellem Engagement und flexiblen Strategien, mit Beiträgen eines Beauftragten für Informationssicherheit bei einem führenden globalen Energieunternehmen.
* Einblick in [die Unterstützung eines OT-Cybersicherheitsprogramms auf Vorstandsebene](https://www.rockwellautomation.com/en-gb/company/news/presentations/rokstudios/how-to-get-board-level-buy-in-for-cybersecurity.html?utm_source=Marketing&utm_medium=Public_Relations&utm_campaign=MultiInitiative_MultiIndustry_EMEA_CMP-05431-R0T3R4&utm_content=news_wire) aus der Sicht eines CISOs eines großen Energieversorgungsunternehmens.
* [NIS2-Gesetzgebung und -Einhaltung](https://www.rockwellautomation.com/en-gb/company/news/presentations/rokstudios/effective-cybersecurity-and-nis2-compliance.html?utm_source=Marketing&utm_medium=Public_Relations&utm_campaign=MultiInitiative_MultiIndustry_EMEA_CMP-05431-R0T3R4&utm_content=news_wire), aus der Sicht eines OT-Sicherheitsleiters eines führenden Kraftstoffversorgungsunternehmens.
* [Grundlegende Strategien, bewährte Praktiken und die Bewertung der Ausrüstung](https://www.rockwellautomation.com/en-gb/company/news/presentations/rokstudios/cybersecurity-trends-a-view-from-a-ciso.html?utm_source=Marketing&utm_medium=Public_Relations&utm_campaign=MultiInitiative_MultiIndustry_EMEA_CMP-05431-R0T3R4&utm_content=news_wire), wie von einem CISO eines weiteren europäischen globalen Energieunternehmens vorgeschlagen.

Dragos Inc., ein weltweit führender Anbieter von Cybersecurity für OT-Umgebungen und Partner von Rockwell Automation, spielt eine wichtige Rolle in dieser Serie:

* Ben Miller, Chief Information Security Officer bei Dragos Inc. teilt seine Gedanken zum [Kampf gegen die ständige Bedrohung durch OT-Cybersicherheitsangriffe](https://www.rockwellautomation.com/en-gb/company/news/presentations/rokstudios/combating-the-constant-threat-cybersecurity-attacks.html?utm_source=Marketing&utm_medium=Public_Relations&utm_campaign=MultiInitiative_MultiIndustry_EMEA_CMP-05431-R0T3R4&utm_content=news_wire) und gibt Einblicke in den jährlichen OT-Cybersicherheits-Jahresbericht des Unternehmens.
* Phil Tonkin, Field Chief Technology Officer, Dragos, und John Speakman, Cybersecurity Services Team Lead, EMEA North Region bei Rockwell Automation, diskutieren gemeinsam über die [Absicherung industrieller Prozesse](https://www.rockwellautomation.com/en-gb/company/news/presentations/rokstudios/navigating-the-evolving-cyber-threat-landscape.html?utm_source=Marketing&utm_medium=Public_Relations&utm_campaign=MultiInitiative_MultiIndustry_EMEA_CMP-05431-R0T3R4&utm_content=news_wire).

„Da Industrieunternehmen immer stärker vernetzt sind, sehen sie sich mit einer Reihe von Bedrohungen konfrontiert, von immer raffinierteren staatlichen Akteuren über Hacktivisten bis hin zu kriminellen Gruppen, die Ransomware-Angriffe starten“, so Miller. „Die gute Nachricht ist, dass es Schlüsselkontrollen gibt, die Unternehmen priorisieren können, um sich besser gegen OT-Cyber-Bedrohungen zu schützen, einschließlich der Überwachung, um Einblick in die Anlagen, Schwachstellen und Bedrohungen in ihrer Umgebung zu erhalten.“

Zu den Gesprächen mit den Spezialisten von Rockwell Automation gehören:

* Maria Else, Senior Global Product Manager, Cybersecurity, und Andreu Cuartiella, Lifecycle Services Commercial Manager EMEA, befassen sich mit [der IT/OT-Konvergenz](https://www.rockwellautomation.com/en-gb/company/news/presentations/rokstudios/everything-you-need-to-know-about-the-nis2-directive.html?utm_source=Marketing&utm_medium=Public_Relations&utm_campaign=MultiInitiative_MultiIndustry_EMEA_CMP-05431-R0T3R4&utm_content=news_wire) und der Frage, wie Abteilungen Mauern einreißen und zusammenarbeiten müssen, um ihre Cybersicherheit zu prüfen, zu planen und weiterzuentwickeln.
* David Maine-Reade, Program Manager, Standards & Regulierungen, und Manju Venugopal, Senior Engineering Manager, Produktsicherheit, befassen sich mit dem, was David als „[Tsunami of regulations](https://www.rockwellautomation.com/en-gb/company/news/presentations/rokstudios/navigating-eu-cybersecurity-regulations.html?utm_source=Marketing&utm_medium=Public_Relations&utm_campaign=MultiInitiative_MultiIndustry_EMEA_CMP-05431-R0T3R4&utm_content=news_wire)“ beschreibt, und wie eine gute Grundlage der Schlüssel zur Bewältigung von Komplexität und Vielfalt ist.
* Meghna Subramani, EMEA Commercial Product Manager, und Ian Murgatroyd, EMEA Product Manager, Safety Components, erörtern die engen [Verbindungen zwischen Sicherheit und Schutz](https://www.rockwellautomation.com/en-gb/company/news/presentations/rokstudios/safety-and-security-two-sides-of-the-coin.html?utm_source=Marketing&utm_medium=Public_Relations&utm_campaign=MultiInitiative_MultiIndustry_EMEA_CMP-05431-R0T3R4&utm_content=news_wire) und wie sich neue Vorschriften entwickeln, um beide abzudecken.
* Cesar Delgado Villalba von Rockwell Automation Cybersecurity Services erklärt [die unterschiedlichen Rollen, die OT und IT einnehmen](https://www.rockwellautomation.com/en-gb/company/news/presentations/rokstudios/how-to-secure-your-ot-network-from-the-inside-out.html?utm_source=Marketing&utm_medium=Public_Relations&utm_campaign=MultiInitiative_MultiIndustry_EMEA_CMP-05431-R0T3R4&utm_content=news_wire), dass die Bedrohungslandschaft tatsächlich sehr ähnlich ist und wie die Ergebnisse eng miteinander verbunden sind.
* Helena Taribó Gómez, Leiterin des globalen Security Operations Center (SOC), und Sergio Sánchez Palma, Leiter des Cybersecurity-Teams, erklären, warum [Transparenz sowohl für die Erkennung als auch für die Prävention von entscheidender Bedeutung ist](https://www.rockwellautomation.com/en-gb/company/news/presentations/rokstudios/the-benefits-security-operations-center-offers-manufacturers.html?utm_source=Marketing&utm_medium=Public_Relations&utm_campaign=MultiInitiative_MultiIndustry_EMEA_CMP-05431-R0T3R4&utm_content=news_wire) und gleichzeitig einen Prüfpfad für die Einhaltung von Vorschriften bietet. Helena schließt mit dem weisen Rat, dass die Kosten eines Cybervorfalls die Kosten der proaktiven Präventivmaßnahmen oft bei weitem übersteigen.

„Cybersicherheit ist ein sich ständig veränderndes Ziel“, erklärt Partha Seshadri, Regional VP, Lifecycle Services, EMEA bei Rockwell Automation. „Nicht nur im Hinblick auf neue Angriffe und Bedrohungsvektoren, sondern auch auf die sich ständig ändernden Standards und Gesetze, die präventive, proaktive und reaktive Verfahren vorschreiben. Dank unserer engagierten Cybersecurity-Teams, unseres PartnerNetwork™-Ökosystems und unserer branchenerprobten Hardware- und Software-Plattformen können wir vollständig optimierte Lösungen für die IT/OT-Konvergenz und für lokale, nationale und globale Digitalisierungskampagnen in verschiedenen Branchen und für eine breite Palette kritischer Infrastrukturanwendungen anbieten.“

Um herauszufinden, ob Ihr Unternehmen auf einen Cyberangriff vorbereitet ist, können Sie das [Cybersecurity Preparedness Assessment](https://www.rockwellautomation.com/en-gb/capabilities/industrial-cybersecurity/services/cybersecurity-preparedness-assessment.html?utm_source=Marketing&utm_medium=Public_Relations&utm_campaign=MultiInitiative_MultiIndustry_EMEA_CMP-05431-R0T3R4&utm_content=news_wire" \t "_blank) von Rockwell Automation nutzen.

**Über Rockwell Automation**
Rockwell Automation, Inc. (NYSE: ROK), ist ein weltweit führender Anbieter für industrielle Automatisierung und digitale Transformation. Wir verbinden die Kreativität von Menschen mit der Leistungsfähigkeit der Technik, um die Grenzen des menschlich Möglichen zu erweitern und die Welt produktiver und nachhaltiger zu gestalten. Der Firmensitz von Rockwell Automation befindet sich in Milwaukee, Wisconsin, USA. Rockwell Automation beschäftigt etwa 29 000 Mitarbeitende, die Kunden in mehr als 100 Ländern zur Seite stehen. Weitere Informationen darüber, wie wir Unternehmen der verschiedensten Branchen auf dem Weg zum Connected Enterprise® begleiten, finden Sie auf [http://www.rockwellautomation.com](https://www.rockwellautomation.com/).

**Pressekontakt**

Burson

Felix Brecht

Felix.Brecht@bursonglobal.com