Rockwell Automation

ERGEBNISSE DER UMFRAGE VON 2022

Vorkehrungen zur Cybersicherheit in kritischen Infrastrukturen: Vermeidung des „großen Shutdowns“

Inhaltsverzeichnis

Einleitung	3
Zusammenfassung	4
Identifizieren von Risiken und Sicherheitslücken	5
Schützen kritischer Ressourcen	7
Frühzeitiges Erkennen von Bedrohungen	10
Schnelle Reaktion auf Vorfälle	13
Wiederherstellung nach Plan	14
Vorbereitung auf die Zukunft	15
Anhang: Alle Umfrageergebnisse	16

EINLEITUNG

Die Sektoren der kritischen Infrastrukturen stehen im Bereich der Cybersicherheit vor einem perfekten Sturm. OT-Organisationen sehen sich mit wachsenden Schwachstellen, neuen und bestehenden Cybersicherheitslücken, einer wachsenden Angriffsfläche und zunehmenden globalen Bedrohungen konfrontiert.

Gut ausgerüstete, raffinierte Akteure wie Ransomware-Banden und nationalstaatliche Hacker haben es auf Organisationen mit kritischen Infrastrukturen abgesehen. 2021 gaben in einer Umfrage 83 % der befragten Organisationen mit kritischen Infrastrukturen an, dass sie von Verletzungen der Cybersicherheit betroffen waren.[1]. Da die Angriffe immer weiter eskalieren und die Schwachstellen in den kritischen Infrastrukturen nicht behoben werden, rückt der „große Shutdown" – eine groß angelegte Katastrophe mit weitreichenden, gefährlichen Auswirkungen – immer näher an die Realität heran. Organisationen mit kritischen Infrastrukturen können nicht länger unvorbereitet zusehen.

Um den Stand der Cybersicherheit für kritische Infrastrukturen zu verstehen und Einblicke in die Bereitschaft und die bewährten Verfahren von Unternehmen zu erhalten, wurde ISMG von Rockwell Automation beauftragt, eine Umfrage unter Verantwortlichen für IT und Cybersicherheit in verschiedenen Branchen für kritische Infrastrukturen durchzuführen. In diesem Bericht stellen wir unsere Erkenntnisse sowie die daraus gezogenen Lehren und Empfehlungen vor.

Wir haben diesen Bericht in fünf Kernthemen gegliedert, die sich am NIST Cybersecurity Framework orientieren (Identifizieren, Schützen, Erkennen, Reagieren und Wiederherstellen). Dieses Framework wird auch von Rockwell Automation als grundlegende Roadmap für die Beurteilung und Stärkung der Cybersicherheit kritischer Infrastrukturen verwendet.

[1] Skybox Security (über Yahoo! Finance): 83 % of Critical Infrastructure organizations suffered breaches, 2021 cybersecurity research reveals, 11. November 2021

ZUSAMMENFASSUNG

Bedrohungsakteure, die Schaden anrichten möchten oder auf schnellen Profit aus sind, haben in Organisationen mit kritischen Infrastrukturen ein attraktives Ziel gefunden. Ransomware-Banden haben es beispielsweise oft auf Versorgungs-, Energie-, Öl- und Gasunternehmen abgesehen. Sie sind von allen Branchen am ehesten bereit, Lösegeld zu zahlen[2], weil sie keine Ausfallzeiten riskieren können.

Aufgrund der Komplexität der IT- und OT-Umgebung erholen sich diese Organisationen nur schwer, und der Schaden durch Ausfälle kann immens sein, z. B. durch Ausfallzeiten, finanzielle Verluste und die Gefährdung von öffentlicher Sicherheit und des Gemeinwohls.

Die ISMG-Umfrage zeigt, dass die Organisationen mit kritischen Infrastrukturen auf dem richtigen Weg sind. Sie ergreifen Maßnahmen, um die Bereitschaft und Widerstandsfähigkeit im Bereich der Cybersicherheit zu verbessern. Die Umfrage zeigt jedoch auch, dass die Fortschritte im Vergleich zur Dringlichkeit eher langsam sind. Viele kämpfen damit, Hürden zu überwinden, wie z. B. knappe Budgets und Fachkräftemangel, unzureichende Festlegung von Prioritäten durch das Management und fehlendes Wissen dazu, wie sich die Abwehrmaßnahmen jetzt am besten stärken lassen.

In den meisten Fällen werden grundlegende Schritte wie Bestandsbeurteilungen, Netzwerksegmentierung und Bedrohungsüberwachung überhaupt nicht oder viel zu langsam durchgeführt. Folglich bestehen weiterhin weit verbreitete Schwachstellen in kritischen Infrastrukturen.

Zu den wichtigsten Erkenntnissen für Unternehmensleiter und Sicherheitsverantwortliche gehören:

1. **Organisationen mit kritischen Infrastrukturen bleiben weitgehend anfällig für Cyberangriffe.** Die Umfrage ergab erhebliche Lücken in Bereichen mit hoher Priorität wie Bestandsüberwachung, Management des dezentralen Zugriffs, Patch Management, Endpunktsicherheit, Netzwerksegmentierung, Reaktions- und Wiederherstellungsplanung bei Zwischenfällen, Sicherheitsbewertung der Lieferkette und Sicherheitsbewusstsein der Mitarbeiter. So führen beispielsweise weniger als 20 % der befragten Unternehmen Bestandsprüfungen in angemessener Häufigkeit durch. Nur ein Drittel verfügt über effektive Verfahren für das OT Patch Management. Darüber hinaus ist die kontinuierliche Bedrohungserkennung ein Schwachpunkt in allen Bereichen: 60 % der Unternehmen verfügen über keine Echtzeit-Bedrohungserkennung. Besonders auffällig ist die Situation im verarbeitenden Gewerbe und im Maschinenbausektor, wo nur 37 % der Befragten angaben, in allen abgefragten Bereichen Maßnahmen getroffen zu haben. Erstaunlich ist, dass die anderen 63 % überhaupt nichts unternehmen – und es ist nur eine Frage der Zeit, bis dies katastrophale Folgen hat.
2. **Der Schließung der Lücken muss oberste Priorität eingeräumt werden.** Kürzlich publik gewordene Angriffe haben deutlich gemacht, welch hohe Kosten durch Ausfallzeiten aufgrund von Cyberangriffen entstehen, und wie groß die Gefahr ist, dass nicht nur der Betrieb lahmgelegt, sondern auch das tägliche Leben gestört wird. Angriffe auf OT-Netzwerke (Operational Technology) und Netzwerke mit Industriesteuerungssystemen in Branchen, bei denen ein Ausfall die öffentliche Sicherheit gefährden kann, wie z. B. die Wasser-, Lebensmittel-, Öl- und Gasindustrie, das Gesundheitswesen und das Transportwesen, nehmen an Umfang und Intensität zu. So können heute nur 56 % der Befragten auftretende Bedrohungen analysieren, eindämmen und entschärfen.
3. **Eine unzureichende Budgetierung erhöht das Risiko und behindert den Fortschritt.** Sicherheitsverantwortliche gaben an, dass fehlende finanzielle Mittel sie daran hindern, bekannte Tools und Verfahren zur Risikominderung, wie Bestandsbeurteilungen und Patch Management, anzuwenden. In Anbetracht der Bedrohungslage und des potenziellen Schadens eines Cyberangriffs müssen Unternehmen erkennen, dass die Kosten des Untätigseins (oder des zu langsamen Handelns) drastische Auswirkungen auf die Betriebszeit haben, die Systeme gefährden und letztlich Endkunden, die Wirtschaft und sogar die nationale Sicherheit beeinträchtigen können.
4. **Organisationen fehlt es an Weitsicht.** Die US-Regierung konzentriert sich immer weniger auf die Cybersicherheit, insbesondere weil die geopolitischen Risiken zunehmen. Die Bundesregierung plant, Zuschüsse in Höhe von 1 Milliarde USD für die Cybersicherheit von Organisationen mit kritischen Infrastrukturen bereitzustellen, aber weniger als 30 % der Befragten verfügen über einen Cybersicherheitsplan, der dabei hilft, kritische Cybersicherheitslücken zu ermitteln und einen Fördermittelantrag zu erstellen, der zur Schließung dieser Lücken beitragen könnte.
5. **Organisationen mit kritischen Infrastrukturen müssen schnell handeln.** Auf der Grundlage dieser Erkenntnisse empfehlen die Cybersicherheitsexperten von Rockwell Automation die folgenden wichtigen Schritte:
   - Durchführung präziser Risiko- und Schwachstellenbeurteilungen, um die Bereiche mit den größten Sicherheitslücken zu bestimmen.
   - Entwicklung eines Cybersicherheitsplans auf der Grundlage der Beurteilungsergebnisse.
   - Segmentierung und Absicherung von Netzwerken mit IDMZs (industriellen Demilitarized Zones) und Firewalls.
   - Implementieren einer Bedrohungsüberwachung.
   - Ausarbeitung und Erprobung von Plänen zur Reaktion auf Vorfälle.

DEMOGRAFISCHE DATEN DER FORSCHUNGSSTUDIE

Die Umfrage wurde im Januar 2022 durchgeführt und lieferte 122 Antworten. ISMG bat um Antworten von Führungskräften aus dem Bereich der industriellen Sicherheit, deren Rollen vom CISO und Sicherheitsbeauftragten bis zum Betriebsingenieur und Geschäftsleiter reichten. CISOs und Direktoren oder Leiter der Sicherheitsabteilung bildeten mit fast 25 % bzw. 19 % die beiden größten Gruppen.

Die Teilnehmer der Umfrage waren in fast 20 vertikalen OT-Branchen tätig, 57 % davon in der kritischen Infrastruktur, darunter Öl und Gas, Energie, Chemie und Wasser/Abwasser. Unter den Fertigungsunternehmen war die Zahl der Antworten aus einer einzigen vertikalen Branche mit 18 % am höchsten.

[2] Sophos, „The State of Ransomware 2021", April 2021

ABSCHNITT 1

Identifizieren und Beurteilen von Risiken

Die Sicherheit kritischer Infrastrukturen ist in den letzten Jahren immer komplexer geworden. Bedrohungsakteure setzen enorme Ressourcen ein, um zu verstehen, wie die neuen, miteinander verbundenen Systeme und Netzwerke kritischer Infrastrukturen funktionieren, und um Schwachstellen zu finden, die sie ausnutzen können. Die Betreiber kritischer Infrastrukturen allerdings sind noch nicht in der Lage, sich diesen Überblick zu verschaffen, um ihre Risiken zu erkennen und Prioritäten für ihre Abwehrstrategien festzulegen.

Um den „großen Shutdown" zu vermeiden, müssen Organisationen mit kritischen Infrastrukturen sofortige und dringende Maßnahmen ergreifen, um Risiken zu verstehen und Lücken zu schließen.

Bestandsbeurteilungen

Die Überprüfung des Anlagenbestands ist ein wichtiger erster Schritt bei der Risikobeurteilung. Es ist auch ein Bereich, in dem Unternehmen Schwierigkeiten haben, die richtigen Erkenntnisse zu gewinnen und Berichte in der erforderlichen Regelmäßigkeit zu erstellen. Einer der Befragten sagte: „Es ist wirklich schwer, eine Bestandsliste zu führen. Eine virtuelle Maschine kann eingerichtet und abgeschaltet werden, bevor das Governance-Team überhaupt weiß, dass sie jemals vorhanden war.

Unter den Umfrageteilnehmern war der häufigste Turnus für die Bestandsbeurteilung der installierten Basis weniger als vierteljährlich, wobei fast 30 % der Befragten diesen Zeitraum angaben. Dieser Zeitraum war auch in drei sehr kritischen Branchen am weitesten verbreitet: in der Fertigungsindustrie und im Maschinenbau, im Gesundheitswesen, im öffentlichen Gesundheitssektor und bei Rettungsdiensten sowie in der pharmazeutischen und chemischen Industrie.

Insgesamt überwachen 45 % der Unternehmen ihre Bestände vierteljährlich, und weniger als 1 von 5 führt die Überprüfungen täglich durch – dies ist die von Rockwell Automation empfohlene Mindestpraxis.

Warum ist das so wichtig?

Jedes nicht berücksichtigte Gerät stellt eine Schwachstelle für den Zugriff auf Ihr Netzwerk dar. Vor einigen Jahren reichten vierteljährliche oder sogar monatliche Beurteilungen vielleicht noch aus. Angesichts der Geschwindigkeit der heutigen Angriffe sind tägliche Überprüfungen in den meisten Fällen unerlässlich, und einige der Befragten gaben an, dass sie zu Echtzeitbeurteilungen übergehen, was mit dem richtigen Netzwerkdesign und den richtigen Überwachungstools möglich ist.

Wir haben auch festgestellt, dass das Bewusstsein der Unternehmen für Bestandsbeurteilungen auf der Grundlage installierter Systeme nicht immer vorhanden ist. Die befragten Führungskräfte der C-Ebene (z. B. CIOs, CEOs, COOs) waren eher der Auffassung, dass Beurteilungen stündlich, täglich oder wöchentlich durchgeführt würden. Die Technologen, die einen besseren Überblick über die täglichen Sicherheitsabläufe haben (z. B. Sicherheitsbeauftragte, IT-Manager und -Architekten oder Ingenieure), zeichneten jedoch ein weniger positives Bild und gaben für die Häufigkeit durchweg „monatlich", „vierteljährlich" oder seltener an.

EMPFEHLUNGEN

Durch automatisierte Bestandsaufnahmen lassen sich Angriffe, die auf mangelnde Transparenz zurückzuführen sind, besser verhindern oder stoppen. Es gibt eine Reihe von automatisierten Tools und Services, die das Bestandsaufnahmeverfahren sowohl für die IT als auch für die OT vereinfachen, und zwar in einer Häufigkeit, die innerhalb Ihrer Risikotoleranzschwelle liegt. Für Organisationen mit kritischen Infrastrukturen, bei denen das Risiko übermäßiger Auswirkungen auf die Bevölkerung besteht, ist eine Bestandsaufnahme in Echtzeit eine vernünftige Strategie, die einen vollständigen Einblick in ihre Netzwerkressourcen ermöglicht.

Geschäftskritische Systeme

Unsere Umfrage ergab, dass nur 56 % der Unternehmen geschäftskritische Systeme identifiziert und mit Prioritäten versehen haben, was zeigt, dass dies ein Bereich mit hoher Dringlichkeit ist (Abbildung 1). Zudem zeigt die Erfahrung von Rockwell Automation, dass einige Unternehmen die Effektivität ihrer Schutzmaßnahmen für geschäftskritische Systeme unterschätzen. In den Kommentaren zu den Umfragen spiegelt sich diese Unklarheit zum Teil wider: Ein Befragter gab an, dass er diesen Schritt mit einer zuverlässigen Sicherheitssoftware gelöst hat.

In der Praxis kann es vorkommen, dass allgemeine Kontrollen der Cybersicherheit nicht ausreichen, um hochkritische Systeme im erforderlichen Umfang zu schützen. Die betrieblichen und geschäftlichen Systeme mit der höchsten Kritikalität müssen in der Regel durch zusätzliche Netzwerksegmentierung, Identitäts- und Zugangskontrollen, wie z. B. Multi-Faktor-Authentifizierung und ähnliche Maßnahmen, gesichert werden. Wenn zunächst die Kritikalität identifiziert und priorisiert wird, lässt sich sicherstellen, dass die richtigen zusätzlichen Sicherheitsstrategien angewandt werden, um das Risiko System für System anzugehen.

Zero Trust ist ein bewährtes Sicherheitsverfahren, das sich in allen Sektoren durchsetzt. Es steht auch auf dem Plan der US-Bundesregierung für Organisationen mit kritischen Infrastrukturen und spielt eine wichtige Rolle bei diesem Schritt der Identifizierung geschäftskritischer Systeme.

Zero Trust ist kein „Alles-oder-Nichts"-Sicherheitsmodell – vielmehr kann es aus vielen Blickwinkeln angegangen und schrittweise, auch in kleinen Schritten, eingeführt werden. Die Identifizierung und Priorisierung der für das Unternehmen wichtigsten Punkte ist ein wichtiger Schritt auf dieser progressiven Reise, der Einblicke liefert, anhand derer Zero Trust-Kontrollen dort eingesetzt werden können, wo sie am dringendsten erforderlich sind.

Wurden geschäftskritische Systeme identifiziert und mit Prioritäten versehen?

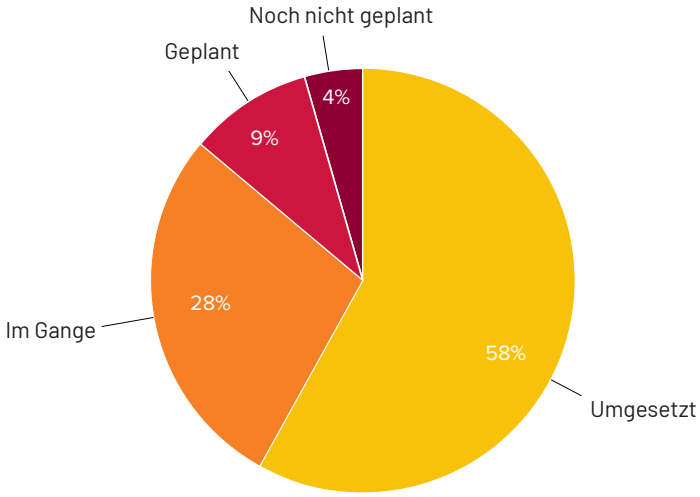


Abbildung 1

EMPFEHLUNGEN

In Anlehnung an die Zero Trust-Strategie sollten alle DAAS-Elemente des Unternehmens – Daten, Anlagen, Anwendungen und Services – überprüft und nach ihrer Kritikalität mit Prioritäten versehen werden. Dies sind die „Schutzflächen" des Unternehmens, auf die jeweils die richtigen Cybersicherheitskontrollen mit der richtigen Priorität angewendet werden.

Im Bereich der kritischen Infrastrukturen sind Industriesteuerungs- und Produktionslinienanwendungen sowie -daten Beispiele für möglicherweise geschäftskritische Systeme. Fragen Sie Ihre Geschäfts-, Betriebs-, IT- und Sicherheitsteams, was geschieht, wenn diese Systeme durch einen Ransomware-Angriff lahmgelegt werden. Fragen Sie, welche Systeme den Produktionsbetrieb, die Datensicherheit oder -integrität, die Kommunikation, die Kontinuität der Lieferkette oder einfach die Erbringung von Dienstleistungen für Kunden ermöglichen, um die Festlegung von Prioritäten zu erleichtern.

ABSCHNITT 2

Schützen und Implementieren von Schutzmaßnahmen

Digitale Transformation, Digitalisierung von Prozessen und IoT-Technologie sowie die daraus resultierende Konvergenz von OT und IT haben die Effizienz und Zuverlässigkeit kritischer Infrastrukturen verbessert und ermöglichen es den Anbietern, die Öffentlichkeit besser zu bedienen und Dienstleistungen kostengünstiger zu erbringen.

Diese Entwicklungen sind zwar positiv, aber sie setzen Organisationen mit kritischen Infrastrukturen neuen Bedrohungen und Sicherheitslücken aus, da sie durch Sensoren und Geräte, dezentrale Mitarbeiter, APIs von Drittanbietern und ungesicherte speicherprogrammierbare Steuerungen, Gateways, Aktoren und viele andere Komponenten verstärkt mit dem Internet verbunden sind.

Die Sicherheitskontrollen für OT-Systeme unterscheiden sich von den IT-Praktiken, da viele OT-Komponenten in der Regel nicht mit grundlegenden Schutzmaßnahmen ausgerüstet sind. Altsysteme, die die Produktion steuern, können oft entweder nicht oder nicht mit der Geschwindigkeit der normalen IT-Patching-Verfahren gepatcht werden.

Darüber hinaus wird die OT-Sicherheit zunehmend in den Verantwortungsbereich der CISOs verlagert, doch viele CISOs verstehen die Auswirkungen des Managements der OT- und damit auch der IoT-Sicherheit nicht in vollem Umfang. Auf der anderen Seite müssen die Verantwortlichen für das Anlagen-Engineering die Betriebszeit zuverlässig aufrechterhalten und können es sich einfach nicht leisten, OT-Netzwerke für längere Zeit auszuschalten, um Sicherheitslücken zu schließen – vor allem nicht im laufenden Betrieb.

Vielleicht ist dies der Grund für die Umfrageergebnisse, die zeigen, dass nur 28 % der Befragten heute eine Roadmap für konvergierte IT/OT-Sicherheit haben, während weitere 35 % angeben, dass dieser Schritt in Arbeit ist. Unternehmen mit kritischen Infrastrukturen sollten dem Beispiel der Fertigungs- und Maschinenbauindustrie folgen, in der 84 % der Befragten angaben, dass sie diese Konvergenz bereits erreicht haben oder sie auf ihrer Roadmap haben. Die anderen Sektoren müssen zweifellos einen großen Rückstand aufholen.

Doch der Vorstoß zur Konvergenz wird fortgesetzt. Zum Erstellen einer soliden Roadmap für die Konvergenz müssen IT- und- OT-Führungskräfte einen echten gemeinsamen Planungsprozess einleiten. Rockwell Automation empfiehlt seinen Kunden in der Regel, eine ganze Woche einzuplanen, in der ein erfahrener Prozesstechniker die beiden Teams bei der Identifizierung aller Sicherheitselemente, Barrieren und Anforderungen unterstützen kann. Auf diese Weise wird bei wichtigen Entscheidungen die Akzeptanz aller Beteiligten erreicht.

Einige Kunden richten auch ein Cybersecurity Center of Excellence (COE) ein, in dem Interessengruppen aus IT, OT und Unternehmen ständig zusammenarbeiten, um funktionierende Systeme zu schaffen und Fehler gemeinsam zu beheben, wenn neue Probleme auftreten.

Sicherer dezentraler Zugriff

Bedrohungsakteure werden jede Möglichkeit ausnutzen, um in einer Organisation Fuß zu fassen. Mit der Umstellung während der Pandemie auf rein dezentrale Arbeitsplätze oder Hybrid-Arbeitsplätze und der insgesamt gestiegenen Mobilität der Mitarbeiter ist der ungesicherte dezentrale Zugriff zu einem leichten Ziel geworden.

Systeme für den dezentralen Zugriff verwenden häufig veraltete Sicherheitssysteme, die sich oft nur auf Kennwörter verlassen und keine Multi-Faktor-Authentifizierung (MFA) bieten. In den Sektoren Versorgungsunternehmen, Öl-/Gasförderung und Bergbau sind Anmeldeinformationen die Art von Daten, die bei Sicherheitsverletzungen am häufigsten offengelegt werden[3], und die große Menge an gestohlenen und geleakten Anmeldeinformationen im Dark Web macht es skrupellosen Hackern leicht, in Systeme mit dezentralem Zugriff einzudringen. Zwar geben 69 % der Befragten an, über einen sicheren dezentralen Zugriff zu verfügen, doch ist dieses Ergebnis im Hinblick auf einen angemessenen Schutz für den dezentralen Zugriff möglicherweise irreführend.

Die COVID-19-Pandemie war in dieser Hinsicht sowohl eine Herausforderung als auch ein Glücksfall. Einer der Umfrageteilnehmer wies darauf hin, dass Hybrid-Arbeitsmodelle einen konsolidierten dezentralen Zugriff erschweren, während ein anderer anmerkte, dass das Modell des „ortsunabhängigen Arbeitens", das während der Pandemie zum Standard wurde, die Unternehmen zu erhöhter Aufmerksamkeit zwingt.

EMPFEHLUNGEN

Ein zuverlässiges Programm zur Identitäts- und Zugriffsverwaltung (Identity and Access Management, IAM) ist für eine Zero Trust-Strategie unerlässlich. IAM bietet Einblicke dazu, wer von wo aus, mit welchem Gerät, zu welcher Zeit Zugriff auf welche Anwendungen und Daten anfordert, und stellt Kontrollfunktionen für andere genehmigte Verhaltensnormen zur Verfügung. Dies ermöglicht die Überwachung und Durchsetzung von Zugangsrichtlinien und -kontrollen. Eine IAM-Lösung mit integrierter MFA kann die Bedrohung durch kompromittierte Kennwörter erheblich verringern.

Industrielle Demilitarized Zone (IDMZ)

Die Einrichtung einer Luftstrecke („Air Gap") zwischen Industriesteuerungs- und OT-Systemen und der IT mithilfe einer industriellen Demilitarized Zone ist eine Grundvoraussetzung für die Cybersicherheit im Netzwerk, die sicherstellt, dass Bedrohungsakteure nicht lateral in OT-Netzwerke und -Steuerungen eindringen können, wenn sie Zugang zu IT-Systemen erhalten – und umgekehrt. Den Umfrageergebnissen zufolge haben etwa 50 % der Unternehmen innerhalb ihrer OT-Architektur eine IDMZ eingerichtet, und weitere 25 % arbeiten daran (Abbildung 2).

Die medizinische Versorgung, das Gesundheitswesen und die Rettungsdienste sind besonders rückständig – 38 % der Befragten haben noch keine IDMZ geplant, verglichen mit 16,5 % in allen Branchen. Diese Ergebnisse decken sich mit den Erkenntnissen, die Rockwell Automation aus dem Gesamtmarkt gewinnt.

Luftstrecken („Air Gaps") einer IDMZ sind nicht das entscheidende Kriterium für die Cybersicherheit, zumal sich OT-Systeme und IoT-Geräte über IT-Netzwerke direkt mit dem Internet verbinden können. Für eine solide Verteidigung müssen zusätzliche Maßnahmen ergriffen werden.

Wie ist der Status der Umsetzung einer industriellen Demilitarized Zone (IDMZ) innerhalb der OT-Sicherheitsarchitektur?

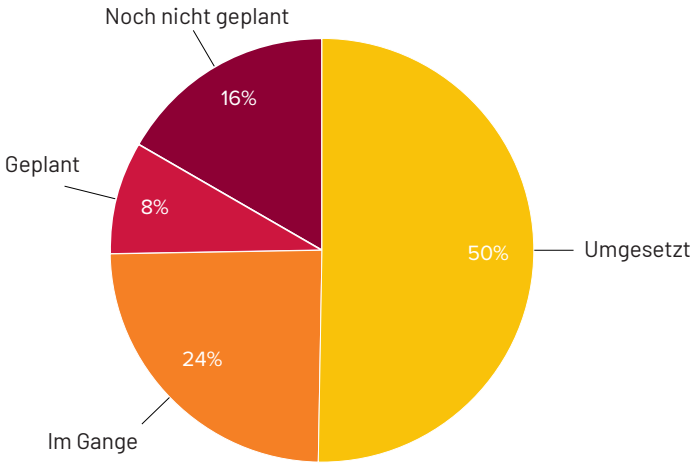


Abbildung 2

EMPFEHLUNGEN

Für eine sichere Architektur sollte eine IDMZ als grundlegende Best Practice implementiert werden. Durch die Trennung von IT- und OT-Netzwerken und -Anlagen ist sichergestellt, dass sich Bedrohungsakteure nicht zwischen den beiden Systemen bewegen können. Denken Sie jedoch daran, dass eine moderne Sicherheitsarchitektur für kritische Infrastrukturen zusätzliche Schutzmaßnahmen umfassen sollte, insbesondere im Bereich der geschäftskritischen Schutzflächen und für alle internetfähigen Ressourcen.

[3] Verizon, „2021 Data Breach Investigations Report", Mai 2021

Patch Management

OT-Patching ist eine bedeutende Fehlerquelle. Die Umfrage bestätigte, was in der Praxis immer wieder beobachtet wird: Patch Management wird entweder nicht als wichtige Maßnahme angesehen, nicht finanziert oder ist einfach zu kompliziert in der Durchführung. Von unseren Teilnehmern haben nur 37 % ein effektives OT Patch Management implementiert, und 13 % haben noch nicht einmal ein Patching-Konzept geplant (Abbildung 3).

In der vertikalen Fertigungs- und Maschinenbaubranche gibt es bei 42 % der befragten Unternehmen kein effektives Patch Management oder es wird es wird noch nicht einmal daran gearbeitet. Die wichtigsten Branchen mit den größten Fortschritten sind die verarbeitende Industrie in den USA und im Vereinigten Königreich/Irland sowie der Finanzsektor im Nahen Osten und im asiatisch-pazifischen Raum (APAC).

Diese Ergebnisse sind in Anbetracht der Häufigkeit der erkannten Schwachstellen und des Risikos, dass verdeckte Malware im Verborgenen lauert, in jeder Hinsicht alarmierend.

Viele OT-Systeme können nicht normal gepatcht werden, da sie nur über eine begrenzte, minimale Funktionalität verfügen und/oder veraltete Strukturen die Einbettung von Sicherheitskomponenten nicht zulassen. Bei Dutzenden oder Hunderten von Netzwerkservern kann das Patchen [jeweils] einen ganzen Tag in Anspruch nehmen, was aufgrund der Ausfallzeiten unglaublich kostspielig ist, sodass sich die Anlagenbetreiber in der Vergangenheit gegen IT-Konzepte für das Patchen gewehrt haben.

Wie ist der Status des effektiven OT Patch Managements?

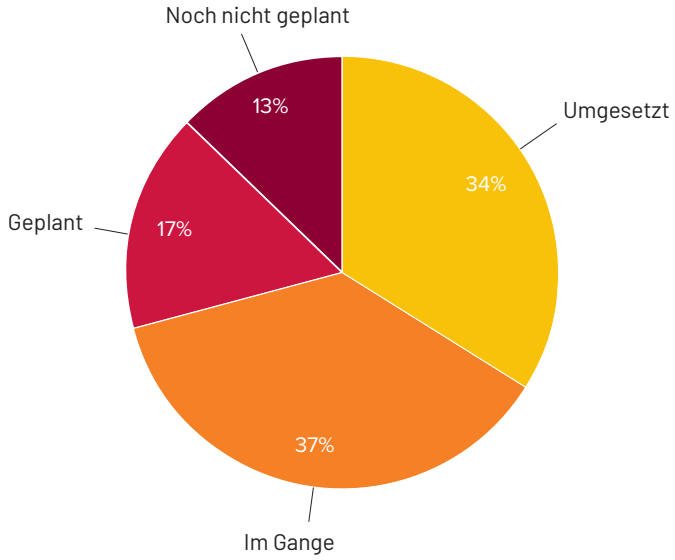


Abbildung 3

Zusätzliche Sicherheitslücken

- **Wechselmedien.** Nur etwas mehr als die Hälfte der Unternehmen nannte wirksame Sicherheitsverfahren für Wechseldatenträger. Bei den anderen Befragten kann jeder jederzeit Daten mitnehmen oder in Systeme eindringen und möglicherweise Malware in die Netzwerke einschleusen. Anhand der Insiderfälle Snowden und Manning lassen sich die potenziellen Auswirkungen gut nachvollziehen. Einer der Befragten, dessen Organisation an einer Lösung arbeitet, äußerte folgende hervorragende Erkenntnis: „Konfigurieren Sie Ihre nächste Generation von Endpoint Detection and Response(EDR)-Tools so, dass Speichersticks unzulässig sind."
- **Netzwerksegmentierung.** Ebenso haben nur 49 % der Unternehmen eine Segmentierung oder Mikrosegmentierung implementiert, um geschäftskritische Systeme zu schützen. Dies gehört zu den wesentlichen Best Practices, die von vielen staatlichen Stellen gefordert werden, und es ist eine Kernkomponente von Zero Trust. In Anbetracht der Wirksamkeit des Zero Trust-Ansatzes werden von den Anbietern kritischer Infrastrukturen wahrscheinlich mehr Verpflichtungen zur wirksamen Segmentierung der Netze verlangt werden.
- **Sensibilisierung der Mitarbeiter.** 69 % der Unternehmen haben Programme zur Sensibilisierung, Schulung und Prüfung der Mitarbeiter in Sachen Sicherheit eingeführt. Der Finanz- und Bankensektor in der APAC-Region und im Nahen Osten ist hier führend, während die US-amerikanische Reise- und Transportindustrie überhaupt keine Schulungen anführte. Fast ein Drittel der Unternehmen hat keine Sicherheitsschulungen durchgeführt, die zu den Best Practices des NIST Frameworks gehören und dringend empfohlen werden. Sensibilisierungsschulungen sind eine bewährte Schutzmaßnahme zur Verhinderung und Unterbindung von Angriffen, die mit Phishing beginnen (beachtliche 86 % der bestätigten Sicherheitsverletzungen). Unabhängig davon, ob für Ihr Programm die Personalabteilung oder die IT-Abteilung zuständig ist, sollten Sie sicherstellen, dass es Cybersicherheitsbedrohungen und Best Practices speziell für die OT abdeckt. Zudem empfehlen wir Penetrationstests, um herauszufinden, in welchen Bereichen die Mitarbeiter mehr Schulungen benötigen.

EMPFEHLUNGEN

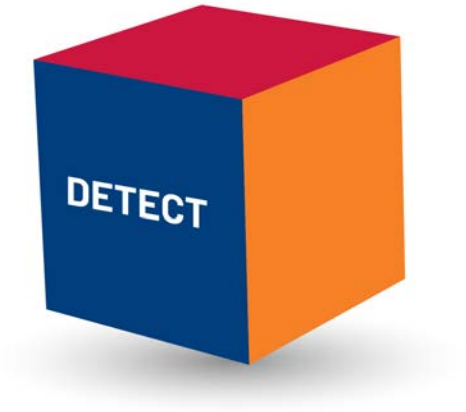
Bedrohungsakteure sind ständig auf der Suche nach Schwachstellen. Keine Organisation, vor allem nicht im Bereich der kritischen Infrastrukturen, kann so weitermachen, wie bisher. Da das Risiko von Ausfallzeiten aufgrund von Cyberangriffen zunimmt, sollte das Risiko-Nutzen-Verhältnis zwischen Untätigkeit und der endgültigen Auseinandersetzung mit der Komplexität von OT-Patches angesichts des hohen Verlust- und Schadenspotenzials natürlich in Richtung Prävention tendieren.

Effizientes und effektives OT Patch Management beginnt mit umfassender industrieller Erfahrung und Know-how im Bereich der OT-Cybersicherheit. Dieses Know-how trägt dazu bei, häufige Fehler zu vermeiden und Best Practices aus mehreren erfolgreichen Implementierungen zu nutzen. Die Zusammenarbeit mit einem Partner, der die Dynamik von Produktionsumgebungen und die akuten Auswirkungen von Ausfallzeiten aufgrund von Cybervorfällen kennt, kann diesen komplexen, aber erforderlichen Prozess rationalisieren und OT-Patches mit minimalen Unterbrechungen durchführen.

[4] Verizon, „2021 Data Breach Investigations Report", Mai 2021

ABSCHNITT 3

Erkennen von Bedrohungen und Identifizieren von Cybersicherheitsvorfällen



Ein zentraler Grundsatz der Zero Trust-Sicherheit ist die Annahme, dass bereits eine Verletzung erfolgt ist. Keiner Verbindung und keiner Zugriffsanfrage darf vertraut werden, bevor diese nicht jedes einzelne Mal dynamisch überprüft und authentifiziert wurde. Dieses Prinzip basiert auf der kontinuierlichen Echtzeitüberwachung von Aktivitäten durch Black Hat Hacker, um Bedrohungen zu erkennen und einzudämmen.

Leider zeigen die Umfrageergebnisse, dass die Erkennung von Bedrohungen eine Schwachstelle bei Unternehmen mit kritischen Infrastrukturen darstellt. Dies bedeutet, dass Angriffe auf OT-Systeme unbemerkt bleiben können und Unternehmen sich nicht mit gängigen Angriffsrisiken befassen, wie z. B. Ransomware, die den Betrieb lahmlegen könnte, Akteure aus Nationalstaaten, die langfristige Spionageaktivitäten durchführen, und Angreifer, die sich durch Systeme und Lieferketten bewegen, um einen groß angelegten Angriff vorzubereiten.

Erkennung von Bedrohungen und Anomalien durch ein OT-SOC

Ein OT-SOC (Security Operations Center) bündelt die Technologien, Tools, Fachkräfte und anderen Ressourcen für die Überwachung und Reaktion auf Bedrohungen rund um die Uhr. Ein OT-SOC ist unverzichtbar, um Bedrohungen und Anomalien schnell zu erkennen und die Auswirkungen auf geschäftskritische Systeme zu minimieren. Unsere Umfrage ergab, dass 43 % der Unternehmen derzeit nicht über ein OT-SOC zur Erkennung von Bedrohungen und Anomalien in Echtzeit verfügen (Abbildung 4) – ein großes Defizit bei den Maßnahmen zur Verstärkung der Cybersicherheit.

Vor allem in der Region APAC, Australien und Neuseeland steht die Antwort „noch nicht geplant" auf die Frage nach der Implementierung von OT-SOCs an erster Stelle. Von den Befragten in dieser Region planen 31 % kein OT-SOC, verglichen mit 16 % weltweit. Bei näherer Betrachtung der Daten fanden wir in der Energie-, Kraftwerks- und Nuklearindustrie der Region keine Organisation, die über ein SOC verfügt oder ein solches wenigstens plant. Zum Vergleich: 74 % der Unternehmen im Nahen Osten und in Afrika haben ein automatisiertes SOC realisiert oder arbeiten daran, wobei zwei Branchen den Weg weisen: der Finanz- und Bankensektor sowie der Energie-, Strom- und Kernkraftsektor.

Darüber hinaus haben 47 % der Befragten keine SIEM-Plattform (Security Information and Event Management) zur Analyse von Sicherheitswarnungen aus Anwendungen und Netzwerkhardware eingerichtet. Zwar generieren die meisten SIEM-Systeme keine Alarme in tatsächlicher „Echtzeit", aber einige kommen dem sehr nahe, was sie zu einem wichtigen Bestandteil Ihre SOC-Tools und zu einer entscheidenden Komponente für die effektive Verteidigung kritischer Infrastrukturen macht.

Wie ist der Status der Umsetzung von Echtzeit-Bedrohungs- und Anomalieerkennung durch ein OT-SOC (eigene oder Managed Servics) für Malware, Ransomware und Schwachstellen?

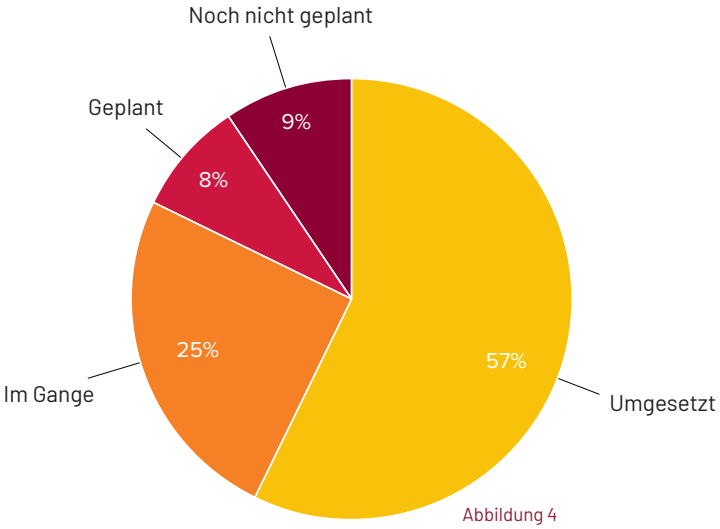


Abbildung 4

EMPFEHLUNGEN

Ressourcenengpässe, wie z. B. ein Mangel an internen Fachkräften, können für viele Unternehmen unüberwindbare Hindernisse für die Überwachung und Erkennung von Bedrohungen darstellen, obwohl dies in der sich wandelnden OT-Bedrohungsumgebung von heute eine Grundvoraussetzung ist. Nutzen Sie die Vorteile der OT-SOC-Lösungen von Drittanbietern, die Services wie die kontinuierliche Überwachung von Bedrohungen und die Reaktion auf Vorfälle umfassen.

Wenn Sie mit einem zuverlässigen OT-SOC-Partner zusammenarbeiten, steht Ihnen nicht nur das Know-how eines hochqualifizierten Sicherheitsteams vor Ort zur Verfügung, sondern Sie erhalten auch Echtzeiteinblicke von allen Kunden, die das SOC betreut. Mit einem verwalteten OT-SOC lassen sich außerdem hohe Investitionskosten vermeiden und es wird sichergestellt, dass die neuesten Tools, Techniken und Erkenntnisse über Bedrohungen für Sie genutzt werden – ein Vorteil angesichts des weltweiten Mangels an schätzungsweise 2,72 Millionen geschulten Sicherheitsexperten ((ISC)^2 2021 Cybersecurity Workforce Study).

Sicherung von Endgeräten

Von industriellen IoT-Sensoren über persönliche Mitarbeitergeräte bis hin zu Steuerungen – die Verbreitung von Endgeräten vergrößert die OT-Angriffsfläche enorm. Der Schutz von Abläufen in dieser Umgebung stellt ein wachsendes Problem dar. Von den befragten Sicherheitsverantwortlichen gaben 46 % an, dass sie die Endgeräte heute nicht rund um die Uhr in Echtzeit überwachen und kontrollieren (Abbildung 5). Dies bedeutet, dass ein großer Teil der an OT-Systeme angeschlossenen Geräte nicht richtig konfiguriert ist oder Sicherheitslücken aufweist. Vielleicht haben Organisationen Glück, aber in den meisten Fällen ist es nur eine Frage der Zeit, bis Bedrohungsakteure diese ungesicherten und unüberwachten Endgeräte für Cyberangriffe nutzen.

Wie ist der Status der Zugangskontrollen und Echtzeitüberwachung aller Endgeräte rund um die Uhr?

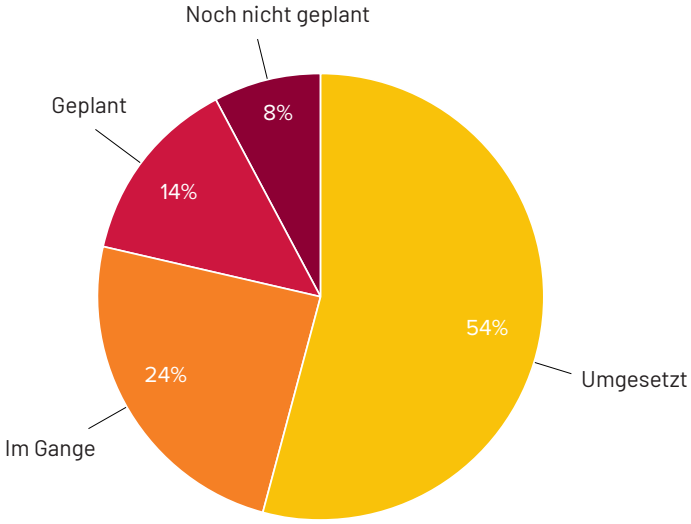


Abbildung 5

EMPFEHLUNGEN

Endgeräte sind ein Bereich, der umgehend verbessert werden muss. Beginnen Sie mit der bereits angesprochenen Bestandsaufnahme der Netzwerkressourcen, um alle mit Ihrem Netzwerk verbundenen Endgeräte zu identifizieren. Sobald Sie die Sicherheitsrisiken identifiziert und bewertet haben, können Sie auf der Grundlage der von Ihnen bestimmten geschäftskritischen Systeme und Sicherheitsprioritäten einen Plan für die Tools, Mitarbeiter und Services entwickeln, die erforderlich sind, um diese Zugangspunkte zu schützen.

ABSCHNITT 4

Reaktion auf Cybervorfälle

Die Planung und Vorbereitung der Reaktion auf Vorfälle ist von entscheidender Bedeutung. Mit den richtigen Vorbereitungen lassen sich Ausfallzeiten, finanzielle Verluste, Unterbrechungen der Kundenbeziehungen und andere negative Auswirkungen von Cybersicherheitsvorfällen minimieren. Für Anbieter kritischer Infrastrukturen ist eine schnelle Reaktion besonders wichtig, da das Ausmaß der möglichen Schäden, einschließlich öffentlicher Dienstleistungen und Sicherheitsprobleme, in einigen Fällen unter Umständen Millionen von Menschen betreffen kann.

Organisationen, die sich mit kritischen Infrastrukturen befassen, verzeichnen Fortschritte: 57 % gaben an, dass sie in der Lage sind, Cyberbedrohungen zu analysieren, einzudämmen und zu entschärfen (Abbildung 6). Wir haben jedoch auch festgestellt, dass dieses Thema Ängste auslöst, vielleicht aufgrund der ständigen und schnellen Veränderungen in der Bedrohungslandschaft. Einer der Befragten merkte an: „Kennt sich denn überhaupt irgendwer damit aus?" Ein anderer Umfrageteilnehmer fragt: „Wie können Anbieter kritischer Infrastrukturen, die Fortführung des Geschäftsbetriebs und die Ausfallsicherheit planen, während sie noch dabei sind, eine grundlegende Strategie für die Reaktion auf Vorfälle zu entwickeln?"

Wie ist der Status der Fähigkeiten zur Analyse von Cyberbedrohungen, zur Eindämmung von Bedrohungen und zur Gefahrenabwehr?

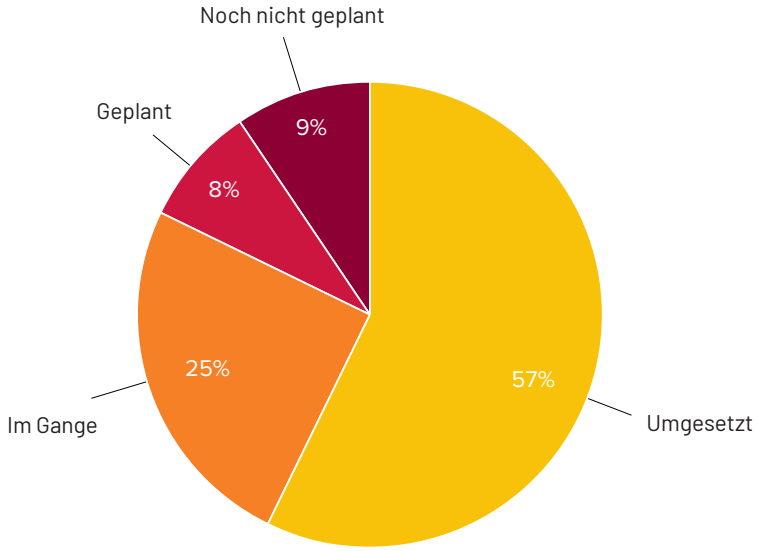


Abbildung 6

EMPFEHLUNGEN

Wenn Ressourcen und Know-how bei der Entwicklung Ihrer Strategie zur Reaktion auf Vorfälle ein Problem darstellen, sollten Sie einen Anbieter von Managed Services in Betracht ziehen – z. B. einen OT-SOC-Partner –, um schnell voranzukommen und angesichts des weltweiten Personalmangels zu vermeiden, dass Sie bei Ihren Bemühungen zur Anwerbung erfahrener Fachkräfte für Cybersicherheit an Ihre Grenzen stoßen. Ein erfahrener OT-SOC-Partner mit fundierten Branchenkenntnissen, wie Rockwell Automation, kann sicherstellen, dass Sie über einen effektiven Plan für die Reaktion auf Vorfälle verfügen, und kann bei Bedarf auch in Ihrem Namen tätig werden, um Angriffe abzuwehren und zu einzudämmen. Expertenteams führen außerdem laufend Schulungen und Szenariotests durch, um die Fähigkeit zur schnellen Reaktion zu überprüfen. Darüber hinaus besitzt ein hochqualifizierter OT-SOC-Partner ein umfassendes Verständnis der OT-Compliance-Anforderungen und der Berichterstellung.

ABSCHNITT 5

Wiederherstellung nach einem Vorfall

46 % der Umfrageteilnehmer gaben an, dass sie heute über Wiederherstellungsprozesse verfügen, d. h. über Systeme, Daten und Betriebsverfahren, die eine schnelle Wiederherstellung des Betriebs nach einem Cyberangriff ermöglichen.

Was bedeutet „schnell" im Hinblick auf die Wiederherstellung nach einem Cyberangriff? In manchen Fällen kann eine Woche als ausreichend erachtet werden. In anderen Fällen dagegen zählt jede Minute.

Als es beispielsweise im Jahr 2021 während des großen Schneesturms in Texas zu Ausfällen bei den Stromversorgern kam, kostete eine Woche Ausfallzeit Hunderte Menschenleben. Im Fall des Ransomware-Angriffs auf Colonial Pipeline führten selbst 24 Stunden ohne Wiederherstellung zu Kosten in Millionenhöhe und ungeahnte wirtschaftliche Auswirkungen durch den Ausfall der Gaslieferungen an der Ostküste der USA.

Die Rückkehr zum normalen Betrieb ist zwar das Hauptziel der Wiederherstellungsphase, sie bietet aber auch die Gelegenheit, verbesserungsbedürftige Bereiche zu bestimmen. Die Umsetzung sinnvoller Änderungen auf der Grundlage der Erkenntnisse, die aus Vorfällen gewonnen werden, schafft eine Kultur der kontinuierlichen Verbesserung der Cybersicherheit, die zu immer belastbareren und besser geschützten Systemen führt.

Nutzung staatlicher Fördermittel

Im November 2021 verabschiedete der US-Kongress ein Infrastrukturgesetz (H.R. 3684, Infrastructure Investment and Job Act), in dem rund 2 Milliarden USD für die Erhöhung der Cybersicherheit und die Verbesserung kritischer Infrastrukturen vorgesehen sind. 1 Milliarde USD des Betrags ist für die Finanzierung von Fördermitteln für staatliche, kommunale, stammesbezogene und bestimmte gemeinnützige Organisationen vorgesehen. Die Richtlinien für die Beantragung von Fördermitteln stehen noch aus. Rockwell Automation erwartet jedoch, dass sich die Fördermittel an den Fähigkeiten des NIST Cybersecurity Framework orientieren, da das Framework von der Bundesbehörde für Cybersicherheit und Infrastruktursicherheit (Cybersecurity and Infrastructure Security Agency, CISA) verwendet wird.

Etwa ein Drittel der Umfrageteilnehmer (29 %) verfügt über einen Cybersicherheitsplan, der für die Beantragung von Fördermitteln angepasst werden kann. Weitere 25 % sind dabei, einen Plan zu entwickeln. Dies bedeutet, dass etwa 40 % der Organisationen nicht entsprechend vorbereitet sind.

Mit einem Cybersicherheitsplan können die Mitarbeiter in den Zielorganisationen nicht nur schnell Fördermittel beantragen, sobald diese zur Verfügung stehen, sondern auch das richtige systematische Cybersicherheitsprogramm auf den Weg bringen, das Lücken aufdeckt, Risiken verringert und dazu beiträgt, Prioritäten für den Schutz der Organisation und ihrer Kunden vor schädlichen Auswirkungen zu setzen.

Rockwell Automation empfiehlt allen Verantwortlichen für kritische Infrastrukturen, sich mit dieser Gesetzgebung vertraut zu machen, einen Basisplan zu erstellen und sich um finanzielle Unterstützung zu bemühen, wenn die Fördermittel für ihr Unternehmen in Frage kommen. Warten Sie nicht, bis die Fördermittelanforderungen veröffentlicht werden, sondern beginnen Sie schon jetzt mit der Vorbereitung und der Ausarbeitung Ihres Plans. Rockwell Automation hat eine Vorlage und eine Checkliste für die Cybersicherheitsplanung auf der Grundlage des NIST Frameworks erstellt: **Planungsvorlage herunterladen**

EMPFEHLUNGEN

Die Planung für die Wiederherstellung und die Wiederinbetriebnahme sollte eine ebenso gängige betriebliche Praxis sein wie die Instandhaltung von Anlagen, die für eine zuverlässige Betriebszeit von zentraler Bedeutung ist. Die finanziellen und personellen Kosten von Ausfallzeiten eskalieren immer weiter, und Sie können sich nicht darauf verlassen, dass Sie das Risiko auf Ihre Versicherungsgesellschaft abwälzen können. Mit zunehmender Haftung und eingeschränkter Versicherbarkeit wird die Last wieder auf die Versicherten zurückfallen, die den Großteil der Schäden und Wiederherstellungskosten tragen müssen.

NÄCHSTE SCHRITTE

Vorbereitung auf die Zukunft

Jeder Anbieter kritischer Infrastrukturen muss jetzt handeln, um den großen Shutdown zu vermeiden. Leben, Wohlergehen, Sicherheit und Lebensgrundlagen hängen davon ab.

OT-Cybersicherheit ist nicht einfach. Andererseits gibt es für die meisten Sicherheitsverletzungen auch bekannte Schutzmaßnahmen. Organisationen mit kritischen Infrastrukturen haben dank der digitalen Transformation und Automatisierung große Fortschritte hinsichtlich Effizienz und Zuverlässigkeit gemacht. Doch nun müssen sie das Thema Cybersicherheit mit der gleichen Beharrlichkeit angehen. Die Ergebnisse der Umfrage zeigen, dass in diesem Sektor die Notwendigkeit einer modernen, zielgerichteten Cybersicherheit erkannt wurde, wenn auch nur langsam – und noch immer mit großen Lücken, schlecht definierten Prioritäten und mangelnder Klarheit in Bezug auf Risiken und Best Practices.

Doch Führungskräfte im Bereich der kritischen Infrastrukturen werden langsam aufmerksam. Viele der Befragten gaben an, dass sie wichtige Schutzmaßnahmen planen oder bereits in die Wege geleitet haben. Der Sektor bewegt sich von einer geringen Sensibilisierung über die Reaktionsbereitschaft nach Meldungen schwerer Angriffe in den Nachrichten und die entsprechende Reaktion der Regierung hin zu der Frage, wie sie die Cybersicherheit in ihren Unternehmen schneller voranbringen können.

Rockwell Automation: Sichern, worauf die Welt angewiesen ist

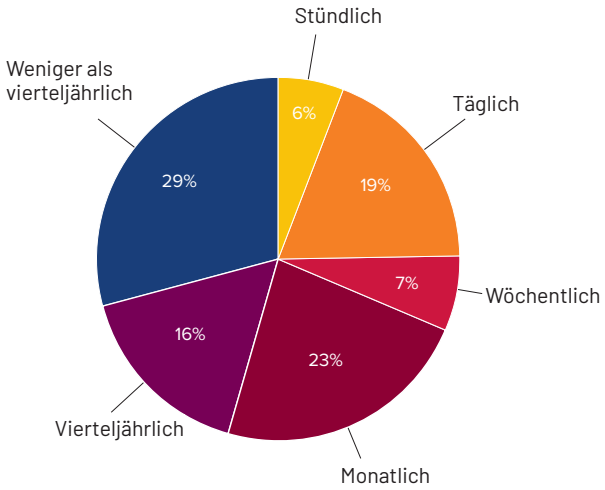
Rockwell Automation bietet eine Vielzahl von Sicherheitslösungen und -services für die Industrie, die Sie bei der Abwehr von Bedrohungen unterstützen und die Widerstandsfähigkeit Ihres OT- und IT-Ökosystems verbessern können. Unsere Experten unterstützen Sie beim Aufbau einer stabilen und sicheren Netzwerkinfrastruktur und helfen Ihnen, sich gegen Bedrohungen zu schützen und schnell auf Vorfälle zu reagieren. Wir verfügen nicht nur über fundiertes Know-how und über Kenntnisse zu den neuesten Best Practices, sondern auch über die Erfahrung aus mehr als 100 Jahren industrieller Automatisierung. Unsere Standorte auf der ganzen Welt ermöglichen es unseren Kunden, Cybersicherheitsschutz auf globaler Ebene über mehrere Standorte hinweg umzusetzen – und dies mit einer Logistik, die so fein abgestimmt ist, wie Sie es vom Branchenführer der industriellen Automatisierung erwarten.

EMPFEHLUNGEN

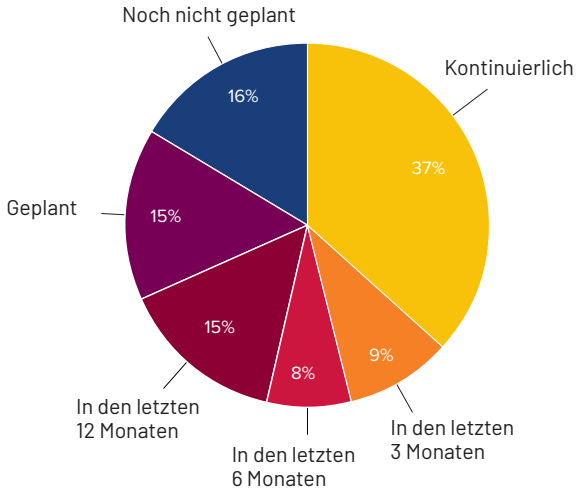
- Melden Sie sich für die **Rockwell Automation Cybersecurity Preparedness Assessment (Beurteilung der Cybersicherheitsbereitschaft)** an und erhalten Sie einen individuellen Bericht, der sich an den ursprünglichen Umfrageteilnehmern orientiert. Informieren Sie sich, wie Ihr Unternehmen im Vergleich zu anderen Unternehmen abschneidet – abhängig von Branche, Unternehmensgröße und Region.
- Laden Sie unsere **Vorlage für einen OT-Cybersicherheitsplan** herunter, um sich vorab einen Überblick über Tools, Services und personelle Voraussetzungen für einen wirksamen Schutz Ihres Betriebs zu verschaffen. US-Organisationen mit kritischen Infrastrukturen: Verwenden Sie die Planungsvorlage, um sich auf die Beantragung von Fördermitteln vorzubereiten, die die Schließung von Cybersicherheitslücken unterstützen können.
- **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.

ANHANG

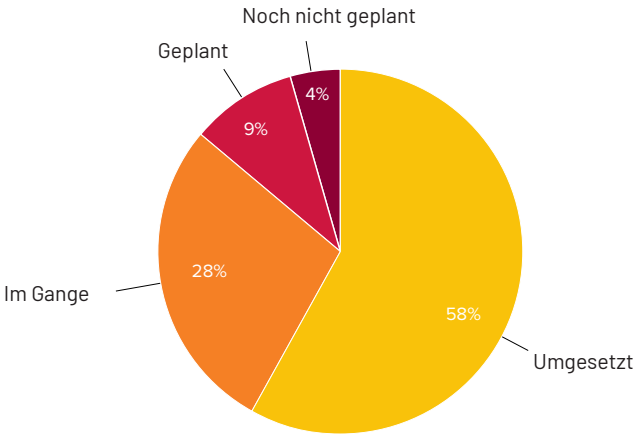
Wie oft wird der Bestand der installierten Basis beurteilt?



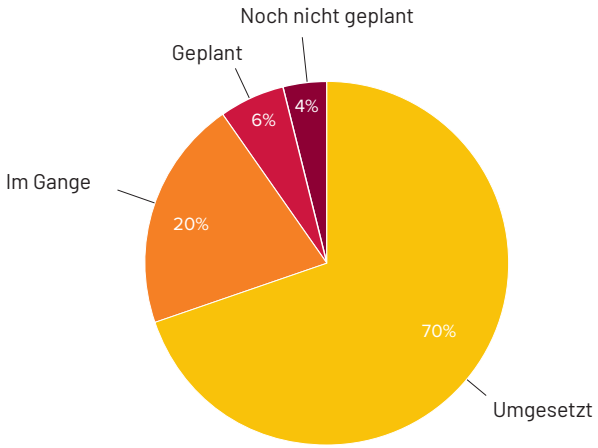
Wie oft wird eine Risikobeurteilung für die Lieferkette durchgeführt?



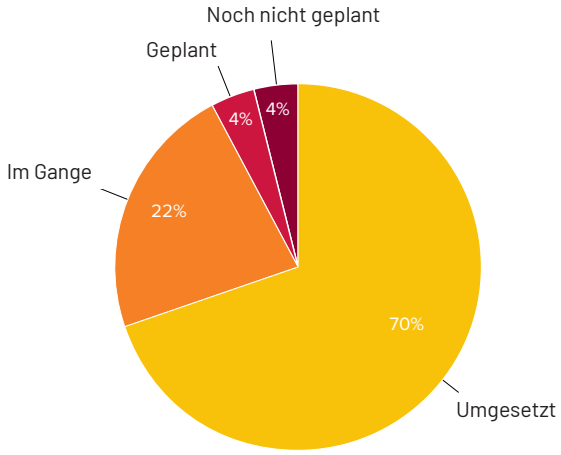
Wurden geschäftskritische Systeme identifiziert und mit Prioritäten versehen?



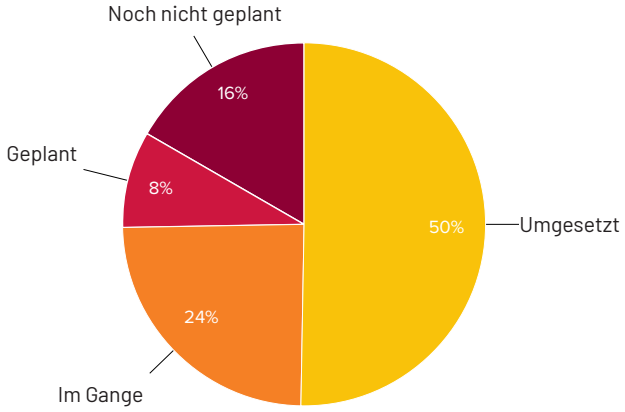
Wie ist der Status der Kontrollen des dezentralen Zugriffs für die sichere Anmeldung von außerhalb des Unternehmens?



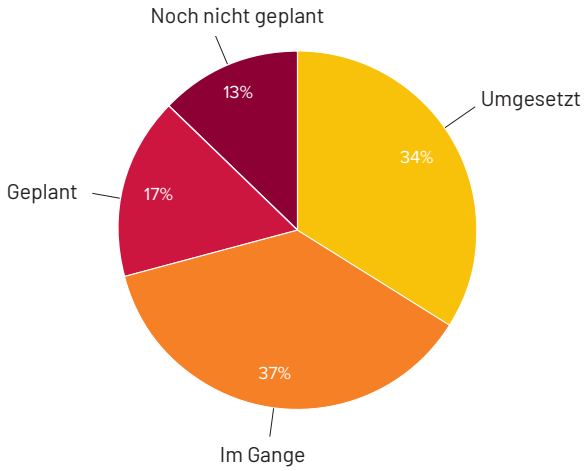
Wie ist der Status der Kontrollen des physischen Zugangs, die den nicht autorisierten Zugang zum System erkennen und verhindern?



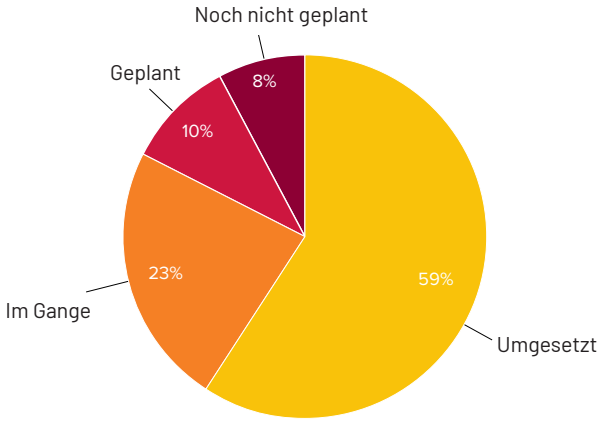
Wie ist der Status der Umsetzung einer industriellen Demilitarized Zone (IDMZ) innerhalb der OT-Sicherheitsarchitektur?



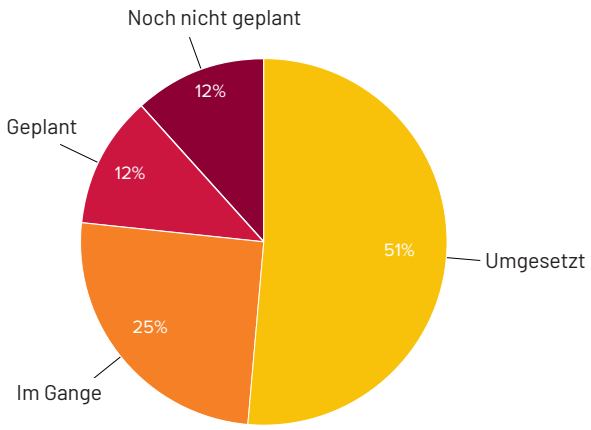
Wie ist der Status des effektiven OT Patch Managements?



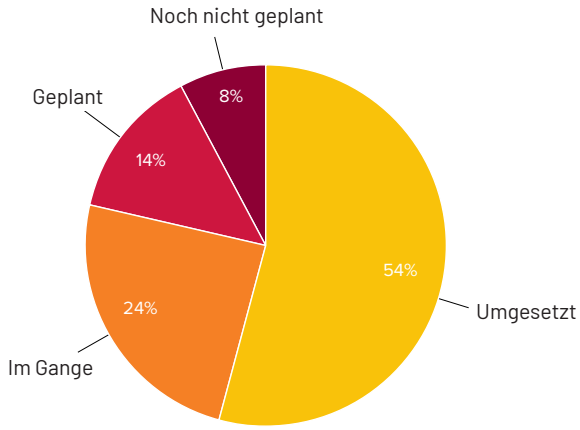
Werden die Datensicherungsprozesse für die betrieblichen Systeme regelmäßig durchgeführt?



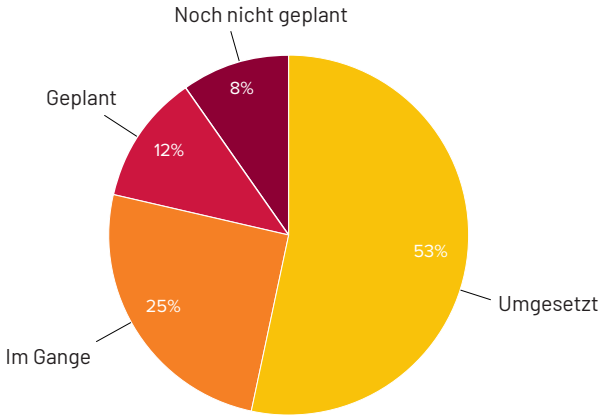
Sicherheitsrelevante Technologie: Wie ist der Status effektiver Sicherheitsmaßnahmen für Wechselmedien?



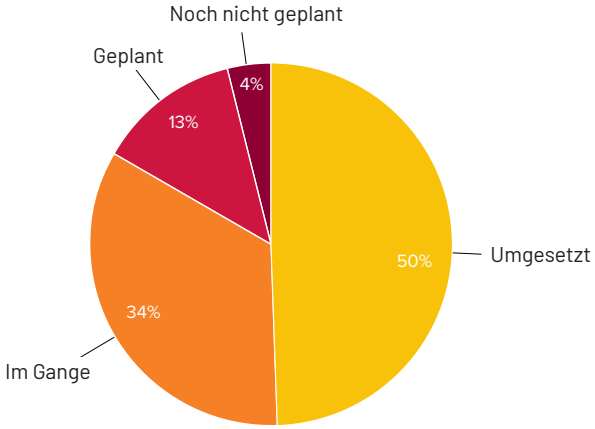
Wie ist der Status der Zugangskontrollen und Echtzeitüberwachung aller Endgeräte rund um die Uhr?



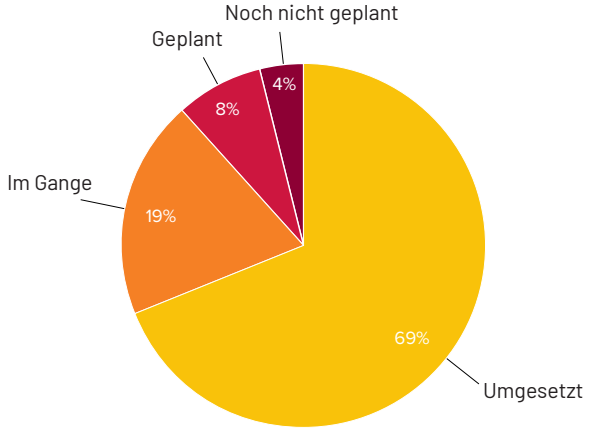
Wie ist der Status eines SIEM-Systems (Security Event Information Management), das Echtzeitanalysen der von Anwendungen und Netzwerkhardware generierten Sicherheitsalarme bereitstellt?



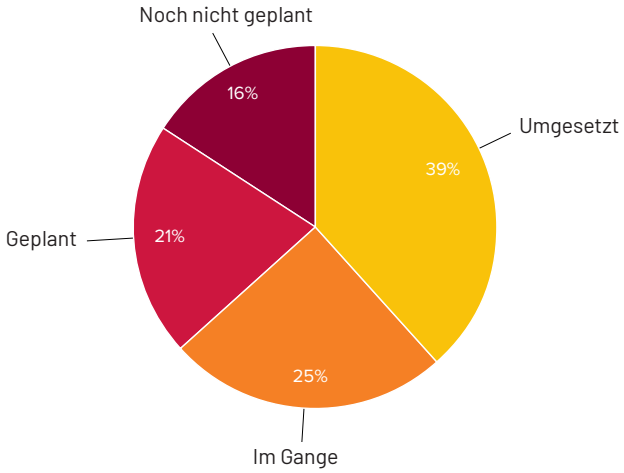
Wie ist der Status der Umsetzung einer Architektur für die Netzsegmentierung/ Mikrosegmentierung, mit der geschäftskritische Systeme durch Sicherheitsperimeter geschützt werden?



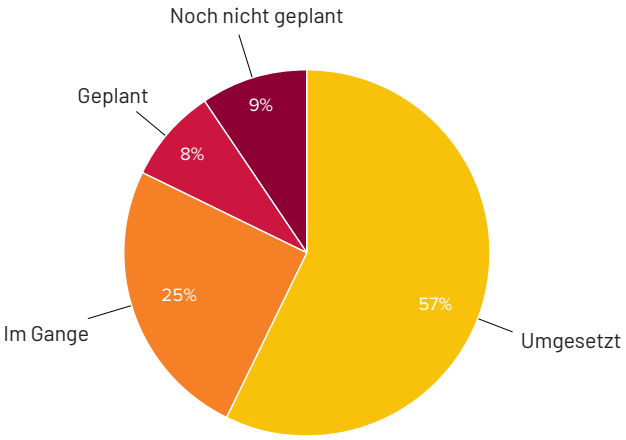
Gibt es Schulungen und Prüfungen zum Sicherheitsbewusstsein der Mitarbeiter?



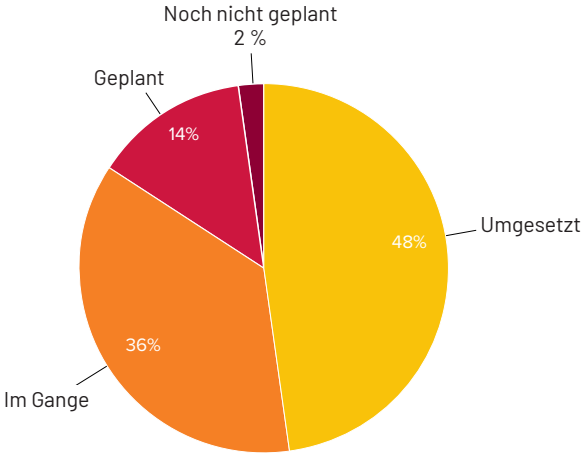
Wie ist der Status der Umsetzung von Echtzeit-Bedrohungs- und Anomalieerkennung durch ein eigenes oder Managed-Services-OT-SOC für Malware, Ransomware und Schwachstellen?



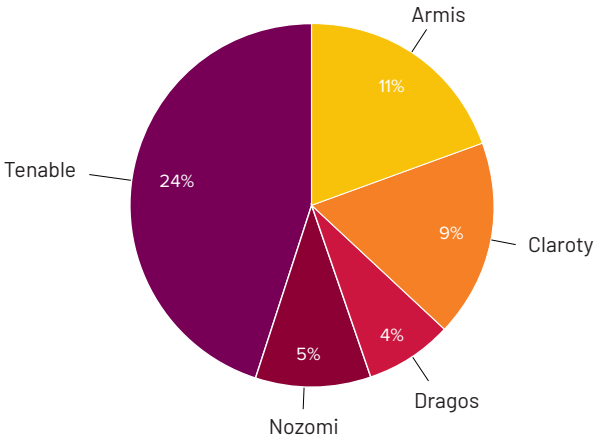
Wie ist der Status der Fähigkeiten zur Analyse von Cyberbedrohungen, zur Eindämmung von Bedrohungen und zur Gefahrenabwehr?



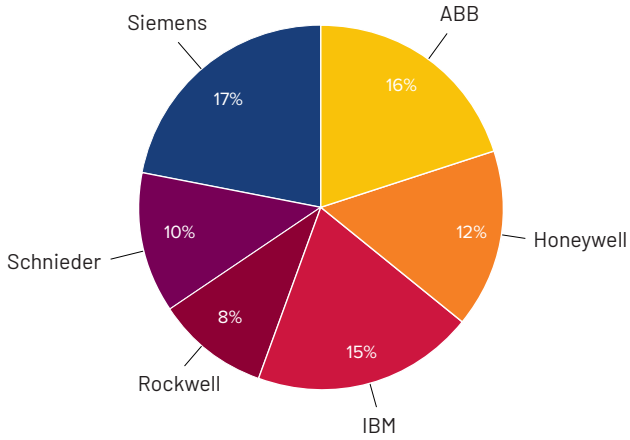
Wie ist der Status der Systeme, Daten und betrieblichen Verfahren zur schnellen Wiederherstellung des Betriebs im Falle eines Cyberangriffs?



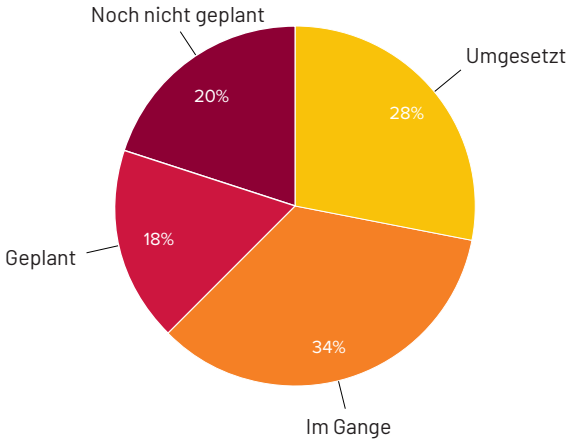
Werden Plattformen oder Services zur Erkennung von Bedrohungen eingesetzt?



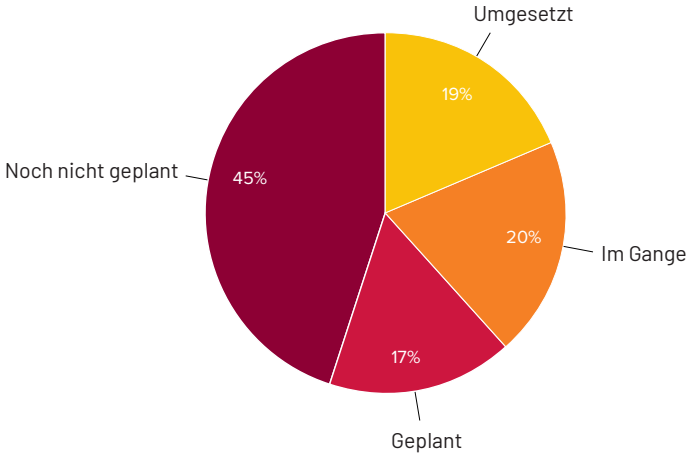
Wird auf Dienstanbieter für industrielle Automatisierung zurückgegriffen?



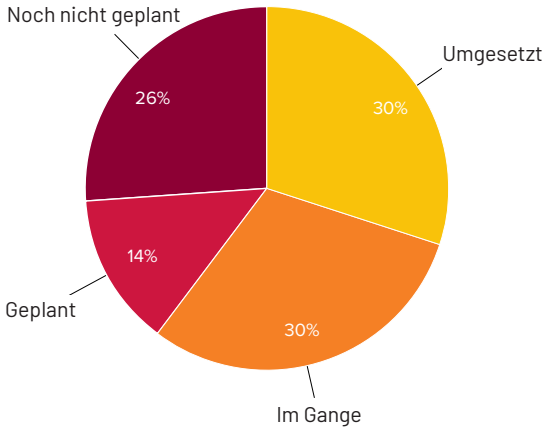
Wie ist der Status der Umsetzung einer Roadmap für die konvertierte IT/OT-Cybersicherheit?



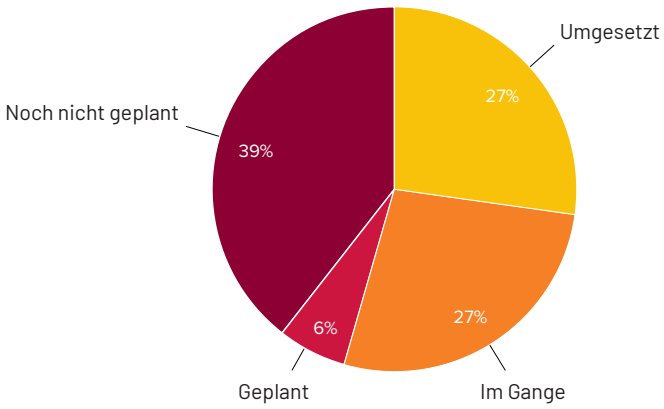
Wie ist der Status der Verwendung von CIP-zertifizierten (Common Industrial Protocol) Produkten zur Sicherung und Verschlüsselung von Ethernet-Kommunikation?



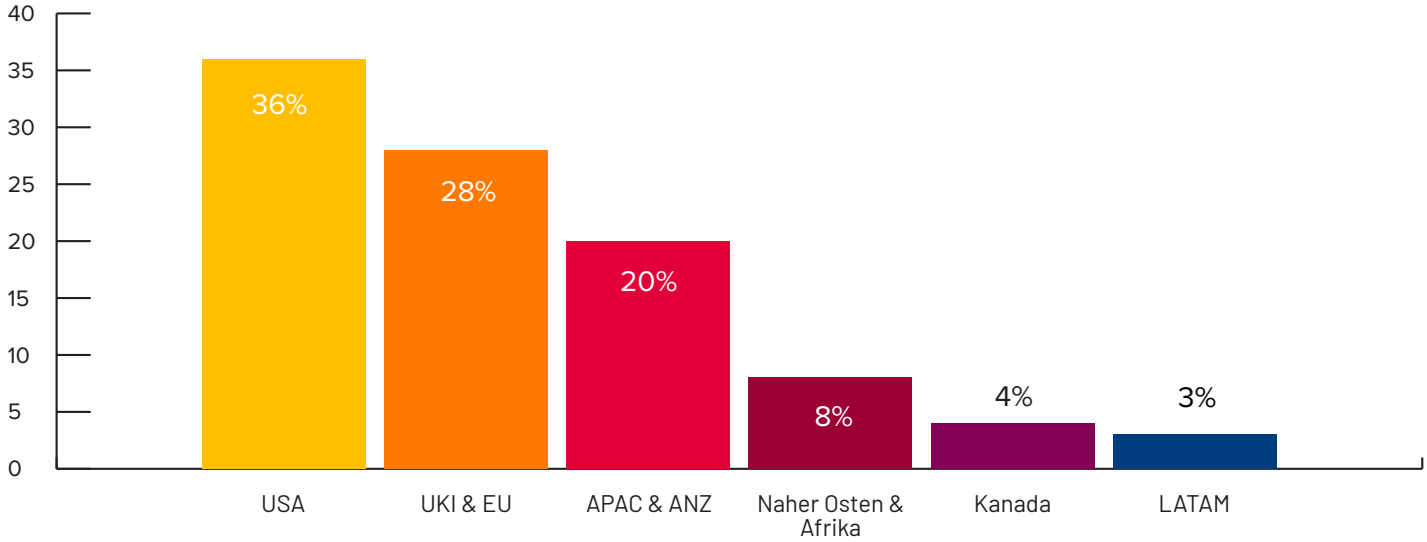
Arbeitet Ihre Organisation mit einem oder mehreren etablierten Cybersicherheitspartnern zusammen, die dynamisch aktualisierte und skalierbare SOC-Services für OT anbieten?



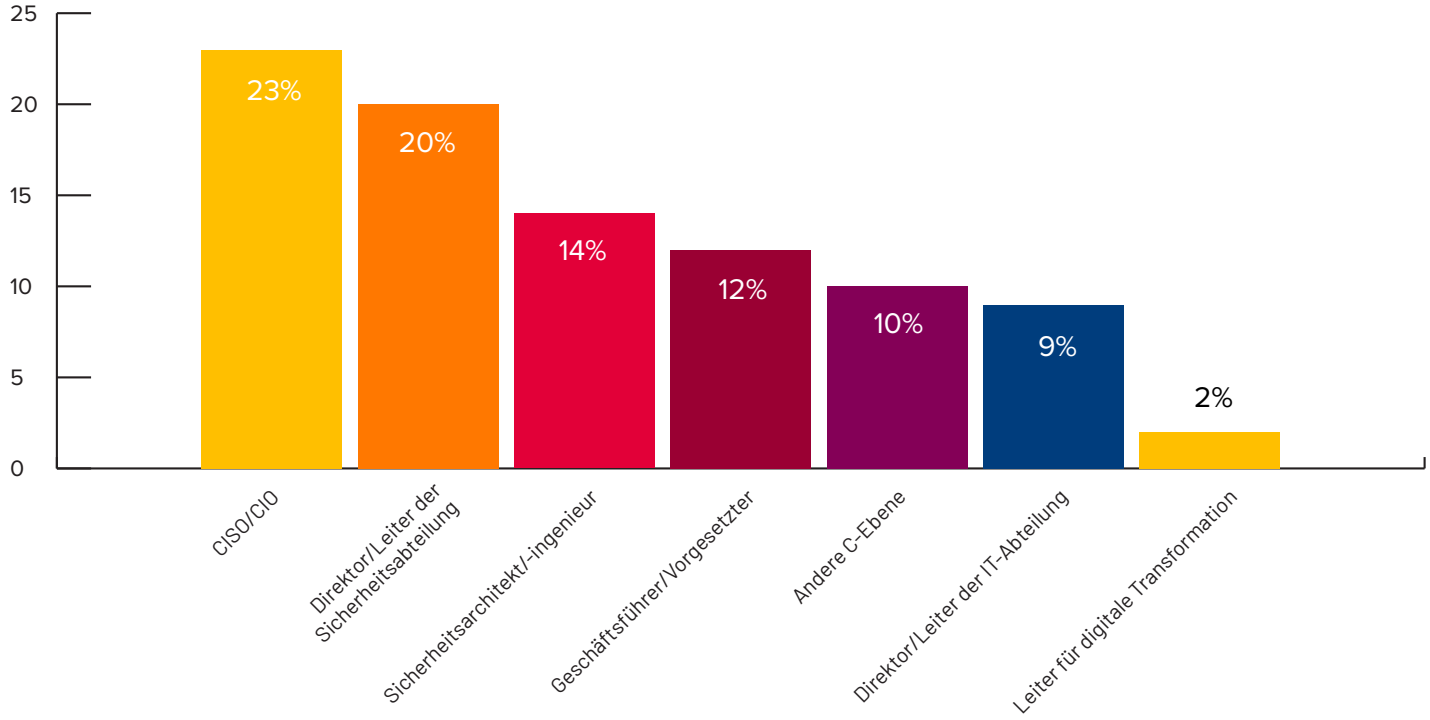
Verfügt Ihre Organisation über einen Cybersicherheitsplan, der sich für die Beantragung von Fördermitteln im Rahmen des US-amerikanischen Infrastrukturgesetzes eignet?



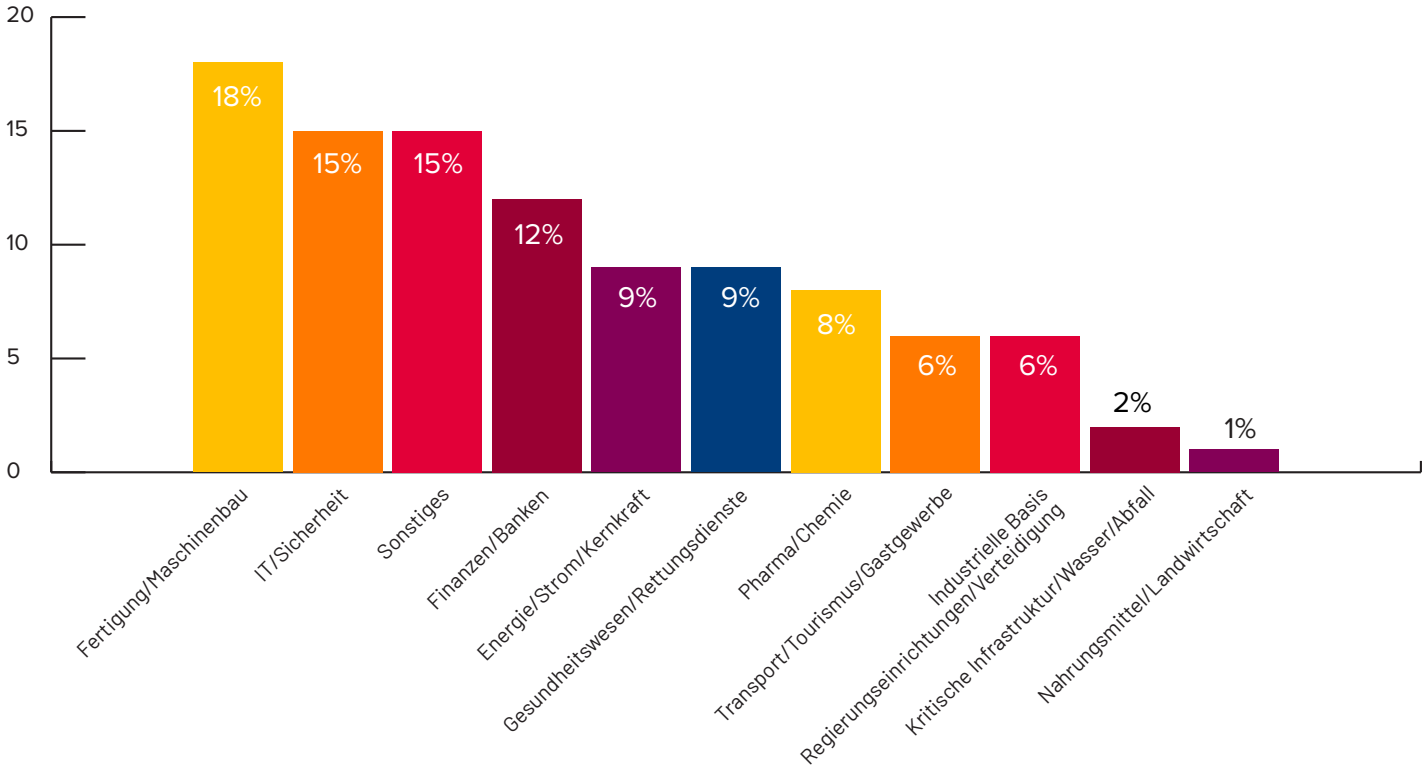
Umfrageteilnehmer nach Region



Umfrageteilnehmer nach Rolle



Umfrageteilnehmer nach Industriezweig



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-SP016A-DE-P – Juni 2022
Copyright © 2022 Rockwell Automation, Inc. Alle Rechte vorbehalten. Printed in USA.