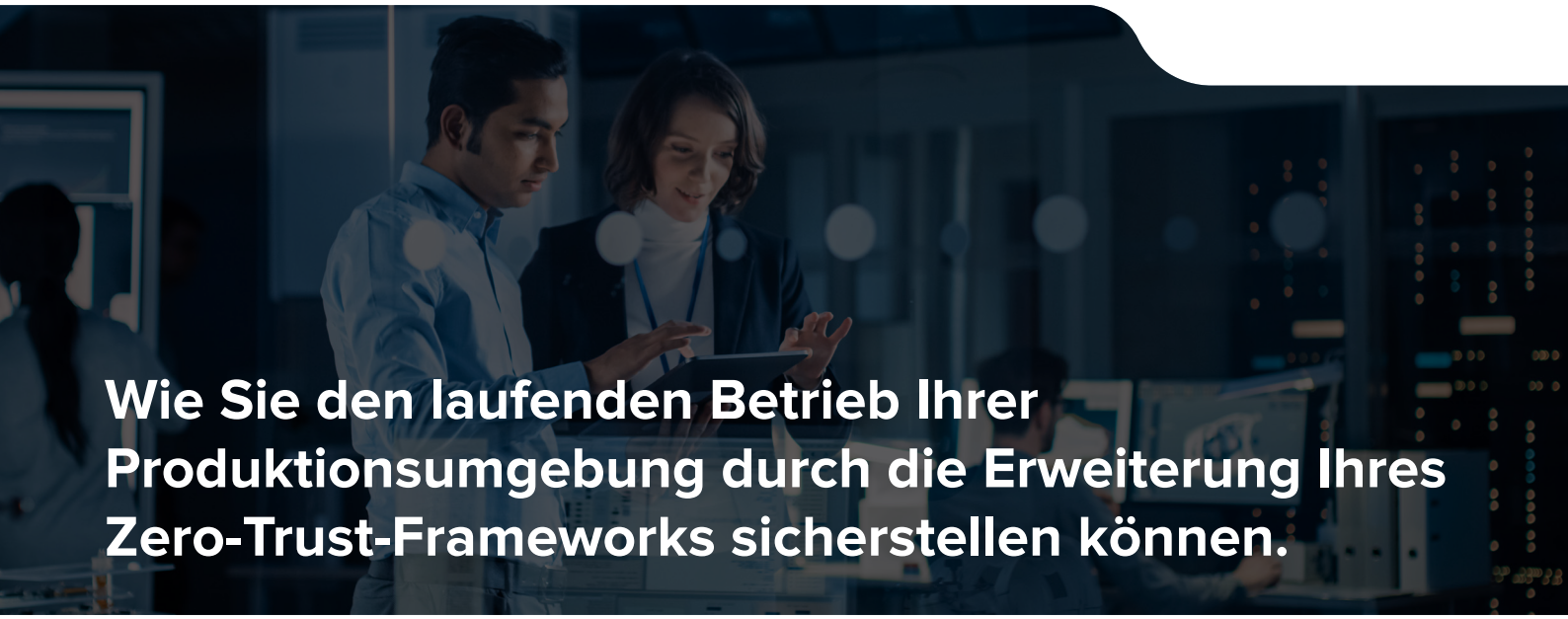

Wie Sie den laufenden Betrieb Ihrer Produktionsumgebung durch die Erweiterung Ihres Zero-Trust-Frameworks sicherstellen können.

Vernetzte Produktionsanlagen bieten eine riesige Angriffsfläche für lukrative Cyberangriffe. Die Erweiterung von Zero-Trust-Frameworks auf Ihre Produktionsumgebung ermöglicht sichere und widerstandsfähige automatisierte Abläufe.

Welche der folgenden Aussagen zu Zero-Trust treffen auf Ihr Unternehmen zu?

- Die Einführung von Zero-Trust-Prinzipien hat für uns höchste Priorität.
- Wir haben erkannt, dass es für Unternehmen vorteilhaft ist, Zero-Trust in Entwicklungen und Planungen zu integrieren.
- Wenn es die Umstände erfordern, ziehen wir Zero-Trust auf einer Ad-hoc-Basis in Betracht. Jedoch hat das für uns nicht die höchste Priorität.
- Nicht sicher/ weiß nicht

Quelle: IDC, Umfrage zur Sicherheit, 2022 (n = 700)

Wie schützt Ihr Unternehmen seine eingesetzten IIoT-Systeme (Industrial Internet of Things)?

64 %	52 %	47 %	43 %	42 %	40 %	33 %	29 %	1 %
Endpunkt-Security	Edge-Security-Gateway	Netzwerkzu-griffskontrolle (NAC)	PKI oder andere Lösungen für das Geräte-Identitäts-management	Firewall für industrielle Netzwerke	Integrierte Security im Gerät/ Sensor	Zero-Trust-Architektur	Intrusion detection and prevention	Sonstige; bitte angeben

Quelle: IDC, Umfrage zur Sicherheit, 2022 (n = 233)

Zero-Trust hat hohe Priorität. 41 Prozent der Unternehmen geben dem Einsatz von Zero-Trust-Prinzipien die oberste Priorität. Die Geschäftsleitung unterstützt neue Investitionen und Initiativen durch definierte Strategien und Zielvorgaben. Zero-Trust ist jedoch kein Produkt, keine Lösung oder ein bestimmtes Netzwerk, das erworben werden kann, sondern ein strategischer Sicherheitsansatz, der eine schwer zu implementierende Architektur darstellt. Nur ein Drittel der Unternehmen nutzt derzeit Zero-Trust, um IIoT-Bereitstellungen zu schützen.

Zero Trust

Die Zero-Trust-Architektur basiert auf dem Prinzip, den Zugriff standardmäßig für jeglichen Zugriff auf das Netzwerk zu verweigern. Dies erfordert eine ständige Überwachung von Unternehmensbedrohungen, eine kontinuierliche Umgebungswartung und – da es sich dabei um ein Framework handelt, das über eine technische Lösung hinausgeht – eine Abstimmung von Lösungen auf Governance- und Compliance-Anforderungen.

Zero-Trust ist für die meisten Unternehmen eine sehr wichtige Initiative, da sich Geschäftsmodelle ändern und Unternehmen ihre DX-Initiativen vorantreiben. Zero-Trust ist eine unternehmensweite Strategie, die das Gesamtrisiko für Unternehmen reduziert. Da immer mehr Unternehmensanwendungen in die Cloud verlagert werden und es immer mehr Geräte gibt, die sich mit dem Netzwerk verbinden (IoT- und OT-Anlagen), wird der herkömmliche Sicherheitsbereich der Infrastruktur kleiner. Für Unternehmen ist es eine Herausforderung, mit ständigen Unterbrechungen umzugehen und gleichzeitig Benutzer, Geräte, Anlagen und Anwendungen zu schützen. Das führt zu einer höheren Ineffizienz des Betriebs und steigert das Risiko von Sicherheitsverstößen.

Erweitern Sie Zero-Trust jetzt auf OT: Tipps für den Einstieg

- Zero-Trust muss über die herkömmlichen Definitionen von Benutzern und Identität hinausgehen, um alle Geräte und Ressourcen einzubeziehen.
- Sorgen Sie für einen umfassenden Einblick in das Netzwerk, um jedes Gerät zu identifizieren und zu überwachen (einschließlich der Kommunikation von Daten: wohin/ woher, von wem/ was).
- Automatisieren Sie die Durchsetzung von Richtlinien sowie die Erkennung und Blockierung von Bedrohungen.
- Teilen Sie das Netzwerk auf, um anhand von Bereichen Zero-Trust-Prinzipien in allen Umgebungen zu berücksichtigen. Unternehmen, IoT und OT könnten getrennt gehalten werden.
- Halten Sie bekannte anfällige, ungesicherte oder nicht reparierbare Geräte in weiter entfernten Bereichen, um die Angriffsfläche zu reduzieren.

Was bedeutet das für OT?

Vertraulichkeit in Sachen IT-Sicherheit hat im CIA-Dreieck (Vertraulichkeit, Integrität, Verfügbarkeit) höchste Priorität. Bei OT-Umgebungen ist jedoch die Verfügbarkeit der wichtigste Aspekt, wodurch Risikomanagement-Strategien sich anpassen müssen.

Die Erweiterung eines Zero-Trust-Frameworks auf OT-Bereitstellungen kann die Sicherheit verbessern und Risiken reduzieren, erfordert jedoch ein umfassendes Verständnis aller Anlagen im Netzwerk, über die herkömmlichen IT-Endpunkte hinaus. So können Unternehmen Entscheidungen zur Aufteilung treffen, um die Angriffsfläche zu verkleinern und das Gesamtrisiko zu reduzieren, ohne die Verfügbarkeit zu beeinträchtigen.

Miteinander verbundene Anlagen können in jedem Unternehmen sehr leicht eine Schwachstelle oder einen Einstiegspunkt darstellen. Die Erweiterung eines Zero-Trust-Frameworks auf OT-Bereitstellungen kann die Sicherheit verbessern und Risiken reduzieren, erfordert jedoch ein umfassendes Verständnis aller Anlagen im Netzwerk, über die herkömmlichen IT-Endpunkte hinaus. So können Unternehmen Entscheidungen zur Aufteilung treffen, um die Angriffsfläche zu verkleinern und das Gesamtrisiko zu reduzieren, ohne jedoch die Verfügbarkeit zu beeinträchtigen.

Die Herangehensweise von IDC

In den letzten Jahren sind sich IT und OT immer näher gekommen. Das bietet vielen Unternehmen die Chance, widerstandsfähigere Entscheidungsprozesse anzuwenden, um zukünftige Anforderungen im Betrieb zu erfüllen. IT und OT unterscheiden sich zwar fundamental, es gibt jedoch zwischen ihnen immer mehr Überschneidungen und eine zunehmende Integration, um die Betriebsleistung von Unternehmen zu verbessern und die historische Lücke zwischen betrieblichen und geschäftlichen Prozessen zu schließen, während OT äußerst breit gefächerten und fortgeschrittenen Cyberangriffen ausgesetzt ist.

Die Anwendung eines Zero-Trust-Ansatzes nicht nur für die herkömmliche IT-Infrastruktur, sondern auch für OT-Umgebungen mit präzisen Zugriffsberechtigungen auf Anwendungsebene sorgt für eine sicherere Konnektivität und Interoperabilität zwischen IT und OT und reduziert gleichzeitig die Risiken und Bedrohungen für den gesamten Betrieb.