FORTINET

Komplexität der digitalen OT-Security verstehen

Vier Herausforderungen für Betreiber und Analysten von Netzwerken

Inhaltsverzeichnis

FORTINET

Zusammenfassung

Sicherheitslücken bei Betriebstechnologie (OT) entstehen durch die zunehmende Vernetzung mit IT-Systemen und stellen mittlerweile für OT-Unternehmen ein großes Problem dar. Als vermeintliche Lösung werden oft isolierte Einzelprodukte implementiert, die jedoch nur eine einzige Sicherheitslücke abdecken. Dieses „Security-Stückwerk“ erhöht nicht nur die Komplexität der betriebstechnologischen Infrastruktur, sondern stellt Betreiber und Analysten von Netzwerken auch vor neue Probleme bei manuellen Workflows, Compliance-Anforderungen und der Zugangskontrolle.

Konvergenz von OT und IT

Betriebstechnologie (OT) findet sich hauptsächlich in Energie-, Versorgungs-, Fertigungs- und Transportunternehmen. Ihr sicherer Betrieb ist oft entscheidend für die öffentliche Sicherheit, manchmal sogar für das nationale und globale wirtschaftliche Gleichgewicht. Betreiber und Analysten von Netzwerken kämpfen daher oft an mehreren Fronten und müssen gleichzeitig die allgemeine Sicherheit, die Betriebszeit und die Security von OT-Systemen aufrechterhalten. Angesichts erheblicher Änderungen der Art und Weise, wie diese Systeme heutzutage betrieben werden, sind jedoch neue Techniken für sichere und effiziente Umgebungen gefragt.

Früher wurde die Security durch das so genannte „Air-Gapping“ gewährleistet: Informationstechnologie (IT) und Betriebstechnologie (OT) waren strikt voneinander durch einen „Luftspalt“ getrennt. Diese Isolierung anfälliger, empfindlicher OT-Technologien bot Schutz vor den meisten Störungen von außen. Mittlerweile werden jedoch IT und OT zunehmend „unter ein Dach“ gebracht, um von mehr Effizienz und Geschäftsvorteilen zu profitieren. Fast drei Viertel der Unternehmen haben inzwischen nach eigenen Angaben zumindest grundlegende Verbindungen zwischen IT und OT geschaffen.[1] Damit fällt aber der schützende Luftspalt weg, wodurch Unternehmen mit Betriebstechnologie einer wachsenden Anzahl internetbasierter Angriffe ausgesetzt sind.

OT-Umgebungen können industrielle Steuerungssysteme (ICS) für den Betrieb von Anlagen und Maschinen sowie Subsysteme zur Überwachung und Datenerfassung (SCADA) umfassen, die eine grafische Benutzeroberfläche für Steuerungstechnik bereitstellen. Ein Absturz des SCADA- oder ICS-Systems in der Fertigung kann die Produktion stundenlang zum Erliegen bringen, empfindliche Fertigungsmaterialien im Wert von mehreren Millionen Euro ruinieren und Bußgelder wegen Compliance-Verstößen zur Folge haben. Bei Cyberangriffen auf kritische Infrastrukturen besteht zudem die Gefahr, dass die nationale Verteidigung lahmgelegt und der Zugang zu Ressourcen behindert wird – im schlimmsten Fall können sogar Bürgerinnen und Bürgern Schaden nehmen.

Fast Dreiviertel der OT-Unternehmen haben in den letzten 12 Monaten einen Malware-Angriff erlebt, der Schäden für Produktivität, Ertrag, Markenvertrauen, geistiges Eigentum und die physische Sicherheit nach sich zog.[2]

Probleme durch zu komplexe Security

Da OT und IT zunehmend ineinandergreifen, haben viele Unternehmen punktuelle Sicherheitslösungen implementiert, um die nun nicht mehr isolierte Betriebstechnologie zu schützen. Durch diese Einzellösungen wird die Security-Infrastruktur nicht nur komplexer, sondern auch fragmentierter – was zu neuen Schwachstellen und potenziellen Sicherheitsverletzungen führt. Das Problem: Security-Einzelprodukte arbeiten fast immer isoliert und decken jeweils nur eine einzige Schwachstelle oder Compliance-Anforderung ab. An Transparenz und den Austausch von Bedrohungsdaten ist nicht zu denken. Die Folge ist, das Betreiber und Analysten von Netzwerken im Blindflug arbeiten müssen – ohne aussagekräftige Echtzeit-Informationen über sicherheitsrelevante Vorgänge in der OT-Umgebung.

Im Durchschnitt werden in einem Unternehmen 75 verschiedene Sicherheitslösungen eingesetzt, von denen viele nur ein einziges Security- oder Compliance-Problem beheben.[3] Selbst wenn diese Zahl in OT-Umgebungen nicht so hoch sein mag, wird der vermehrte Einsatz von Security-Einzellösungen auch bei Betriebstechnologie zu einem wachsenden Problem: 31 % der OT-Fachkräfte gaben kürzlich in einem Webinar an, dass ihr aktueller Security-Ansatz für die OT-Architektur darin besteht, fragmentierte Einzellösungen einzusetzen. Weitere 24 % bekannten, gar keine Strategie für die OT-Security-Architektur zu verfolgen.[4] Security-Einzellösungen können in der Regel weder Bedrohungsdaten austauschen noch die Bedrohungsabwehr in einer zunehmend dezentralen Unternehmensinfrastruktur koordinieren. Dadurch steigt nicht nur die Reaktionszeit auf Sicherheitsvorfälle, sondern auch die Wahrscheinlichkeit, dass kritische OT-Systeme kompromittiert werden und ausfallen können.

64 % der OT-Unternehmen berichten von Schwierigkeiten, mit Neuerungen und Veränderungen Schritt zu halten.[5]

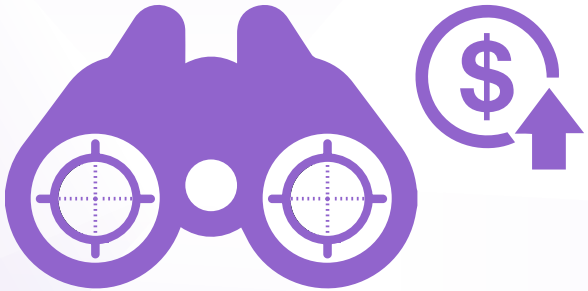
Eine komplexe Security für Betriebstechnologie führt zu unterschiedlichsten Problemen und hat Folgen für die Compliance, Audits und Mitarbeiter sowie für die Kosten und Effizienz. Diese Komplexitätsprobleme lassen sich in vier Hauptbereiche zusammenfassen, in denen Handlungsbedarf besteht:

1. Zuständigkeit und Aufgaben beim Compliance-Management

Viele Branchenvorschriften, wie der Schutz kritischer Infrastrukturen der North American Electric Reliability Corporation (NERC CIP), Industriestandards vom National Institute of Standards and Technology (NIST), oder Datenschutzgesetze wie die EU-Datenschutz-Grundverordnung (DSGVO) erfordern eine umfassende Überprüfung und Berichterstattung. In einigen Fällen drohen Bußgelder in Millionenhöhe für jeden Compliance-Verstoß – sowohl für dokumentierte Verstöße als auch für mangelnde Compliance-Nachweise.

Das Compliance-Management ist in der Regel ein stark manueller Prozess. Häufig sind hierfür mehrere Vollzeitmitarbeiter abgestellt und nicht selten dauert es Monate, bis alles regelkonform ist: Daten müssen aus unterschiedlichsten Security-Produkten aggregiert und normalisiert werden, damit sichergestellt ist, dass Regulierungsbehörden korrekte Meldungen erhalten. Vielen Netzwerk- und Security-Mitarbeitern bleibt nichts anderes übrig, als Sicherheitskontrollen mit den Audit-Tools jedes einzelnen Anbieters zu überwachen und deren Daten zu korrelieren, um die Konformität nachzuweisen. Ein derart komplexer, unpraktischer Auditprozess ist nicht nur ineffizient, sondern kann auch zu nicht erfassten oder widersprüchlichen Daten führen.

Die Komplexität fragmentierter Sicherheitslösungen wird durch Compliance-Änderungen noch verschärft. Ständig kommen neue Vorschriften, Standards und Normen hinzu, während gleichzeitig bestehende Regulierungswerke laufend überarbeitet werden. Ohne eine effektive Lösung, die automatisierte Funktionen für Nachverfolgung, Auditing und Reporting bietet, müssen Unternehmen viel Zeit in die manuelle Aggregation und Abstimmung von Daten investieren. Wer dagegen mit einem echtzeitfähigen Compliance-Management arbeitet, kann Sicherheitsfragen proaktiv angehen, Schwachstellen identifizieren und Risiken beheben, bevor Probleme überhaupt auftreten.



Compliance-Technologien, die zur besseren Visualisierung von Risiken beitragen, besitzen für Unternehmen höchste Priorität – sowohl in den kommenden zwölf Monaten (57 %) als auch innerhalb der nächsten drei Jahre (51 %).[6]

2. Aufrechterhaltung der Verfügbarkeit von sensiblen, ungepatchten Systemen

OT-Systeme, die 30 bis 40 Jahre lang betrieben werden können, lassen sich häufig nur mit veralteter und ungepatchter Firmware oder Software betreiben. Aber auch bei neueren Systemen wird oft absichtlich auf die Installation von Patches verzichtet. Da für Updates womöglich ganze Systeme heruntergefahren werden müssen, halten sich viele Betriebsleiter lieber an die Regel „Solange es funktioniert, muss auch nichts verändert werden“. Zeitdruck spielt dabei ebenfalls eine Rolle: In vielen Betrieben sind die Wartungsfenster derart knapp bemessen, dass die Anwendung von Patches und die Wartung auf die kritischsten Systeme beschränkt wird. Ohne regelmäßiges Patches und Wartungen können OT-Systeme jedoch extrem anfällig für viele IT-basierte Bedrohungen wie lang bekannte Malware-Angriffe werden. Erschwerend kommt hinzu, dass viele OT-Systeme aufgrund ihres Alters und des Verzicht auf Patches überraschend fragil sind: Selbst harmlose Sicherheitspraktiken wie das aktive Scannen von Geräten können zu einem Ausfall führen.

3. Belastung begrenzter Ressourcen durch manuelle Aufgaben

Für fast zwei Drittel der OT-Führungskräfte besteht die größte Herausforderung darin, mit Änderungen Schritt zu halten. Gleichzeitig klagt fast die Hälfte (45 %) über fehlende qualifizierte Arbeitskräfte.[7] Infolge des Fachkräftemangels im Bereich Cyber-Sicherheit sind heute weltweit fast 3 Millionen Security-Positionen unbesetzt.[8] Weitere Daten zeigen aber, dass OT-Unternehmen trotz knapper Personalressourcen entschlossen sind, ihr Sicherheitsprofil zu verbessern.[9]

Fragmentierte Security-Architekturen verhindern jedoch den Einsatz von Automatisierungsfunktionen, die personell begrenzte Teams von manuellen Aufgaben entlasten könnten. Diese Komplexität wird durch mangelnde Transparenz beim Security-Management noch verstärkt. Der Großteil der Unternehmen (78 %) verfügt nach eigenen Angaben nur teilweise über Transparenz bei der Cyber-Sicherheit von Betriebstechnologie.[10] Teams können so nur schwer ungewöhnliches Verhalten erkennen, schnell auf potenzielle Bedrohungen reagieren und Bedrohungsanalysen durchführen. Stattdessen geraten ohnehin unterbesetzte OT-Standorte durch das Management vieler isolierter Sicherheitslösungen zusätzlich unter Druck.

4. Kontrolle über das Zugangs-Management

Das Outsourcing von Teilbereichen des OT-Managements verursacht weitere Komplexität, die Betreiber und Analysten von Netzwerken in den Griff bekommen müssen. Drittanbieter und Partner erhalten mittlerweile per Remote-Access und vor Ort stärkeren Zugang zu OT-Umgebungen. Solche Zugriffsrechte für externe Benutzer setzen das Unternehmen jedoch weiteren Risiken aus. Vielen Unternehmen fehlt hierfür eine fein abgestimmte Zugangskontrolle, mit der unterschiedliche Rollen für diese Art von Benutzern definiert und der Zugriff eingeschränkt werden kann. Eine derart komplexe, uneinheitliche Security behindert nicht nur die Transparenz über Benutzer, sondern auch die Durchsetzung konsequenter, richtlinienbasierter Kontrollen in allen Teilen der Sicherheitsinfrastruktur.

Eine komplexe Security und mangelnde Transparenz führt oft auch zu Insider-Bedrohungen: Laut Verizon beginnen 81 % der Sicherheitsverletzungen mit verlorenen oder gestohlenen Anmeldedaten.[11] Viele illegale Zugriffe auf OT-Umgebungen gehen auf das sogenannte Spear-Phishing zurück, mit dem Anmeldedaten von Benutzern gestohlen werden, die in irgendeiner Form Zugriff auf die OT-Umgebung haben. Wie ernst dieses Problem ist, belegt ein Artikel im *Wall Street Journal*: Demnach erlitten schätzungsweise zwei Dutzend US-Stromversorger in den letzten zwei Jahren Angriffe, die durch Spear-Phishing und gestohlene Anmeldedaten erst möglich wurden.[12] Manchmal schleusen Angreifer dabei sogar Malware in OT-Umgebungen ein, um damit später den Betrieb zu sabotieren.

OT-Sicherheitsprobleme werden durch mangelnde Sicherheitskompetenz – sowohl bei internen Mitarbeitern (40 %) als auch bei beauftragten Security-Dienstleistern (41 %) – noch verstärkt.[13]

Wie Unternehmen die Sicherheit von Betriebstechnologie (OT) vereinfachen können

Komplexität ist der Feind der Sicherheit. Um die Betriebsintegrität von OT-Systemen zu gewährleisten, müssen Betreiber und Analysten von Netzwerken die vorhandene Security-Architektur neu bewerten. Durch die Reduzierung der Komplexität und der Fragmentierung isolierter Einzellösungen kann die Sicherheit auf ganzer Linie gestärkt werden. Davon profitieren alle Bereiche: das Compliance-Management, die verfügbare Betriebszeit, die Mitarbeiter (durch Entlastung von manuellen Arbeiten), das Zugangs-Management sowie die allgemeine Transparenz und der Schutz im gesamten Unternehmen.

[1] „Independent Study Pinpoints Significant SCADA/ICS Security Risks". Fortinet, 28. Juni 2019.

[2] „State of Operational Technology and Cybersecurity Report". Fortinet, März 2019.

[3] Kacy Zurkus: „Defense in depth: Stop spending, start consolidating". CSO, 14. März 2016.

[4] „Securing the Future of Industrial Control Systems".Fortinet-Webinar, 26. Juni 2019.

[5] „State of Operational Technology and Cybersecurity Report". Fortinet, März 2019.

[6] Samantha Regan, et al.: „Comply & Demand: 2018 Compliance Risk Study". Accenture, März 2018.

[7] „State of Operational Technology and Cybersecurity Report". Fortinet, März 2019.

[8] „Cybersecurity Skills Shortage Soars, Nearing 3 Million". (ISC)², 18. Oktober 2018.

[9] „State of Operational Technology and Cybersecurity Report". Fortinet, März 2019.

[10] Ebd.

[11] „2017 Data Breach Investigations Report". Verizon, abgerufen am 30. November 2018.

[12] Rebecca Smith und Rob Barry: „America's Electric Grid Has a Vulnerable Back Door – and Russia Walked Through It". The Wall Street Journal, 10. Januar 2019.

[13] John Maddison: „Is Converging Your IT and OT Networks Putting Your Organization at Risk?". CSO, 9. Mai 2018.

www.fortinet.com/de

391249-0-0-DE

5. Mai 2020, 14:18 Uhr