CHECKLISTE

Betriebstechnologie effektiv schützen

Schutz vor erweiterten Bedrohungen erfordert Automatisierung und Integration in Sicherheitslösungen

Die Folgen von Angriffen auf Betriebstechnologie (OT) sind schwerwiegend. In Unternehmen, die auf betriebliche und industrielle Produktionssysteme angewiesen sind, muss der Chief Information Security Officer (CISO) daher sicherstellen, dass Security-Teams über die richtige Architektur und die richtigen Lösungen verfügen.

7 Punkte, die jeder für Betriebstechnologie zuständige CISO bedenken sollte

Fortinet unterstützt CISOs dabei, die Komplexität der Netzwerk-Security zu verringern und zugleich die Kosten zu senken, die durch das ständige Hinzufügen isolierter Einzelprodukte bei neuen Bedrohungen oder Risiken verursacht werden.

☑ OT- und IT-Security integrieren

Um sowohl IT- als auch OT-Netzwerke vor komplexen Bedrohungen zu schützen, muss der CISO einen mehrstufigen Ansatz verfolgen. Das bedeutet nicht, dass Security-Lösungen unabhängig voneinander arbeiten sollten. Stattdessen sollten alle Lösungen zum Schutz von OT- und IT-Netzwerken eng integriert sein und Informationen in Echtzeit austauschen können. Werden dann Bedrohungen in einem Bereich erkannt, kann eine koordinierte Bedrohungsabwehr für die gesamte Sicherheitsinfrastruktur des Unternehmens aktiviert werden.

Die Fortinet Security Fabric bietet eine solche Infrastruktur. Gemeinsam sorgen eng integrierte Security-Fabric-Lösungen für einen gut abgestimmten Schutz, der alles abdeckt – bis hin zum Randbereich von OT- und IT-Netzwerken. Fortinet-Lösungen bieten außerdem eine umfassende Transparenz über die gesamte digitale Angriffsfläche und ermöglichen automatisierte Workflows, um Security-Abläufe und Gegenmaßnahmen effizienter und schneller zu gestalten.

☑ Effektive Zugriffskontrolle für OT-Ressourcen

Immer mehr Unternehmen arbeiten mit Outsourcing und nehmen Prozessänderungen vor, die einen Netzwerk-Zugang für Gäste, Vertragspartner, Auftragnehmer und Drittanbieter erfordern. In vielen Fällen sind WLAN- und Remote-Access-Funktionen für Mitarbeiter und alle Besucher notwendig, die das Netzwerk nutzen müssen. Solche Umgebungen erfordern eine genaue Zugriffskontrolle, um unbefugte Verbindungen zu Netzwerk-Ressourcen zu blockieren.

Unternehmen können mit der Fortinet Security Fabric intelligente Lösungen zur Erkennung und Verwaltung der Benutzeridentität bereitstellen. FortiAuthenticator unterstützt beispielsweise rollenbasierte Zugriffsrichtlinien und eine Multi-Faktor-Authentifizierung (MFA) für alle Benutzer von OT- und IT-Systemen.

FortiAP und FortiSwitch bieten einen sicheren WLAN-Zugang bzw. einen sicheren Wechsel zwischen Netzwerken (Network Switching). Beide wurden speziell für betriebliche und industrielle Produktionsumgebungen entwickelt. Dank ihres robusten Designs können sie problemlos unter extremen Bedingungen – z. B. in Außenstellen, Fertigungsstandorten oder Lagern – eingesetzt werden.

☑ Seitliche Bewegungen zwischen IT und OT mit Netzwerk-Segmentierungen kontrollieren

Next-Generation-Firewalls (NGFWs), die zwischen OT- und IT-Netzwerk-Segmenten platziert werden, können den Verkehrsfluss steuern und einen „Air Gap“ nachbilden – den schützenden „Luftspalt“, durch den früher OT-Ressourcen in vielen Unternehmen von IT-Systemen getrennt wurden. FortiGate NGFWs sind in dieser Umgebung besonders leistungsfähig: Sie bieten ein Whitelisting speziell für OT-Anwendungen und können so konfiguriert werden, dass nur bestimmte OT-Protokolle im OT-Unternehmensnetzwerk zulässig sind und der gesamte andere Datenverkehr abgewiesen wird.

Eine weitere wichtige Überlegung bei der Auswahl von FortiGate NGFWs für die Netzwerk-Segmentierung oder die Edge-Sicherheit ist der Durchsatz. Bei einigen Firewalls wird der Durchsatz bei der Aktivierung erweiterter Sicherheitsfunktionen stark gedrosselt. Nicht bei FortiGate NGFWs: Sie wurden speziell für minimale Latenzzeiten entwickelt – auch dann, wenn das Intrusion Prevention System (IPS) und andere erweiterte Funktionen aktiviert sind.

☑ Threat Intelligence integrieren

Um vor neuen, unbekannten Malware-Formen geschützt zu sein, müssen lokale und globale Bedrohungsdaten in nahezu Echtzeit im gesamten Netzwerk verbreitet werden können. Die Lösungen in der Fortinet Security Fabric integrieren KI-gesteuerte Daten-Feeds von den FortiGuard Labs Threat Intelligence Services. Mit einem der branchenweit größten Teams von Security-Experten überwachen und analysieren die FortiGuard Labs kontinuierlich die Bedrohungslandschaft, um Zero-Day-Threats zu identifizieren, die nicht nur IT-Systeme, sondern auch die häufigsten OT-Protokolle und Schwachstellen von OT-Anwendungen betreffen.

☑ Sandbox- und Deception-Technologien speziell für Betriebstechnologie einsetzen

Kein Threat Intelligence Service kann jede Bedrohung erkennen, bevor sie das Unternehmensnetzwerk erreicht. Unternehmen müssen daher auch Lösungen implementieren, die verhindern, dass eingeschleuste, unbekannte Bedrohungen bis zu den OT-Systemen vordringen können. Bei der Fortinet Security Fabric senden alle Elemente dieser Sicherheitsstruktur verdächtige Pakete an die FortiSandbox, die dann deren Code in einer Quarantäne-Umgebung überprüft. In Betriebsumgebungen kann die FortiSandbox auch OT-Plattformen emulieren und so Dateien öffnen, die für bestimmte OT-Betriebssysteme einzigartig sind.

Täuschungstechnologien – Stichwort „Deception" – sind ein weiterer wichtiger Bestandteil einer umfassenden Security-Infrastruktur. Mit FortiDeceptor lassen sich Deception-VMs, Decoys und Anwendungen speziell für Betriebstechnologie implementieren, die mit Täuschungsmanövern Angreifer „in die Falle locken". Da sich komplexe Bedrohungen ständig weiterentwickeln, müssen CISOs das Problem der Zero-Day-Bedrohungen aus mehreren Richtungen gleichzeitig angehen.

☑ Schutz vor Insider-Bedrohungen implementieren

Bösartige und vorsätzliche Angriffe von Insidern stellen sowohl für OT- als auch für IT-Umgebungen eine Bedrohung dar. Es kann aber auch vorkommen, dass Mitarbeiter in gutem Glauben oder unbeabsichtigt Angreifern den Zugriff auf das Netzwerk oder auf Daten ermöglichen. FortiInsight User and Entity Behavior Analytics (UEBA) ist eine Lösung, die Benutzer und Endgeräte kontinuierlich überwacht. Sie nutzt maschinelles Lernen (ML) und Analysen, um gefährdete Konten anhand von verdächtigen, regelwidrigen oder sonst wie anomalen Verhaltensweisen automatisch zu identifizieren.

☑ Priorität auf eine effektive Kontrolle der Security-Infrastruktur

Security-Teams müssen Richtlinien auf Grundlage von Sicherheitsstandards wie NIST (National Institute of Standards and Technologies) oder CIS (Center for Internet Security) zentral verwalten und effizient auf Sicherheitslösungen anwenden können. Sie brauchen außerdem Zugriff auf zentrale, automatisierte Berichte zur Bedrohungserkennung und -abwehr von Sicherheitslösungen. Das Fortinet Security Fabric Management Center bietet genau das: Verwaltung, Reporting und Analysen erfolgen von einer einzigen, zentralen Konsole mit automatisierten Workflows. Security-Teams erhalten so einen umfassenden Überblick über die Sicherheitslage und können genau die OT-Sicherheitsdaten erfassen, die für branchenspezifische und behördliche Audits benötigt werden.

Fazit

Sicherheitsverletzungen bei OT-Netzwerken können katastrophale Folgen haben. CISOs in Sektoren, die Betriebstechnologie einsetzen, müssen Security-Lösungen implementieren, die eine zeitgemäße, erstklassige Bedrohungserkennung, mehr Transparenz dank einer engen Integration und eine automatisierte Bedrohungsabwehr bieten.

Die Fortinet Security Fabric erfüllt diese Anforderungen: Sie ermöglicht eine enge Integration von Fortinet- und Drittlösungen, wird von führenden Testinstituten wie den NSS Labs empfohlen und ist – dank dem reibungslosen Zusammenspiel erstklassiger Fortinet-Lösungen – ideal für Unternehmen mit Betriebstechnologie geeignet.

FORTINET

www.fortinet.com/de

31. August 2020, 8:34 Uhr

448524-0-1-DE