FORTINET

Security für Betriebstechnologie-Netzwerke erfolgreich gestalten

Wie Sie Bedrohungen wirkungsvoll verhindern, erkennen und bekämpfen

Inhaltsverzeichnis

Zusammenfassung 3

Einleitung 4

Höhere Systemverfügbarkeit mit automatisierter Bedrohungserkennung und -abwehr 5

Identifizieren von OT-Gefahren mit Bedrohungs-informationen speziell für Betriebstechnologie 7

Erkennen hochkomplexer Bedrohungen mit Deception-Technologien 9

Isolieren und Eindämmen von Bedrohungen mit einer Netzwerk-Segmentierung 11

Fazit 13

Zusammenfassung

Ausgefeilte Cyber-Angriffe gefährden zunehmend Steuerungstechnik wie ICS- und SCADA-Systeme (Supervisory Control and Data Acquisition): Durch das Zusammenwachsen von Netzwerken der Betriebstechnologie (OT) und Informationstechnologie (IT) erweitert sich die Angriffsfläche und Betriebstechnologie wird anfälliger für hochkomplexe Cyber-Bedrohungen, die auf diese kritischen Systeme abzielen. Leider lassen sich ICS- und SCADA-Systeme in OT-Netzwerken wegen ihrer besonderen betrieblichen Anforderungen nicht einfach mit der gleichen Security wie IT-Netzwerke schützen, sondern erfordern andere Sicherheitsansätze und -lösungen, die speziell für Betriebstechnologie entwickelt wurden.

Automatisierte Sicherheitspraktiken und Deception-Technologien können dazu beitragen, erweiterte Bedrohungen in OT-Netzwerken besser zu erkennen. Auch lässt sich mit Security-Lösungen auf Netzwerk-Ebene die Ausbreitung von Cyber-Angriffen in einem OT-Netzwerk identifizieren und kontrollieren. Ein zentrales Element dieser Strategie sind Bedrohungsinformationen für Betriebstechnologie, die besonders die Threats schnell erkennen und eindämmen, die auf mehrere OT-Standorte abzielen oder eine globale Gefahr für die gesamte Industrie darstellen.

64 % der OT-Entscheidungsträger bezeichnen Cyber-Angriffe als große Herausforderung.[1]

Einleitung

OT-Systeme sind neuen Cyber-Bedrohungen ausgesetzt. In der Vergangenheit waren Betriebstechnologie-Netzwerke physisch von IT-Systemen durch einen „Air Gap“ – einen schützenden „Luftspalt“ – getrennt. Digitale Innovationen haben jedoch in vielen Unternehmen diese Trennung aufgehoben oder stark verringert und fördern das Zusammenwachsen von OT und IT. Dadurch entstehen neue Sicherheitslücken, über die Cyber-Kriminelle vom IT-Netzwerk aus in das OT-Netzwerk eindringen können.

OT-Systeme sind häufig langlebig und werden teilweise 20 Jahre oder länger genutzt. Dass im Laufe der Jahre bei Betriebstechnologie zahlreiche leicht ausnutzbare Sicherheitslücken entdeckt wurden, dürfte daher kaum überraschen. Doch zu diesen bekannten Bedrohungen kommen nun neue hinzu. Fieberhaft arbeiten Cyber-Kriminelle im Dark Web an neuartigen, hochkomplizierten Angriffsformen, die mehrere Stufen umfassen und speziell auf Betriebstechnologie und industrielle Netzwerke abzielen.

OT-Infrastrukturen haben einzigartige Anforderungen an die Verfügbarkeit. Sicherheitslösungen müssen deshalb sorgfältig entwickelt werden, damit sich die Security nur minimal auf den Betrieb auswirkt. Auch müssen OT-Netze spezielle Richtlinien für Betriebstechnologie erfüllen, wie z. B. die EU-Direktive zur Netz- und Informationssicherheit (NIS), den NIST-Industriestandard oder den Schutz kritischer Infrastrukturen gemäß NERC CIP.

Die automatische Erkennung und Abwehr von Bedrohungen, Deception-Technologien, Netzwerk-Segmentierung und Bedrohungsdaten speziell für Betriebstechnologie sind vier Kernelemente einer robusten OT-Security, um Sicherheitsprobleme in einer immer komplexeren Bedrohungslandschaft erfolgreich anzugehen.

In fast 75 % der Unternehmen mit Betriebstechnologie gibt es Verbindungen zwischen IT- und OT-Netzwerken.[2]

Höhere Systemverfügbarkeit mit automatisierter Bedrohungserkennung und -abwehr

Angreifer lernen ständig dazu. Mittlerweile verfügen Cyber-Kriminelle über die Ressourcen zur Entwicklung von Angriffsformen, die mit herkömmlichen Methoden nicht mehr erkannt werden können. Unternehmen benötigen daher eine tiefgehende Netzwerk-Transparenz und Lageerkennung, um tatsächliche Bedrohungen von Fehlalarmen zu unterscheiden und richtig einzuschätzen. Nur so lässt sich ein Angriffsverhalten erkennen und Angreifer können erfolgreich identifiziert werden.

Diese Transparenz und richtige situative Einschätzung ist für eine effektive, schnelle Reaktion auf Sicherheitsvorfälle notwendig. Realisieren lässt sich das nur mit einer Automatisierung: Werden Sicherheitsdaten automatisch erfasst, aggregiert und analysiert, können tatsächliche Bedrohungen treffsicher erkannt werden (ohne massive Fehlalarme). Zugleich ist der Kontext ersichtlich, der für eine erfolgreiche Abwehr und Behebung von Bedrohungen benötigt wird.

Automatisierung kann auch die Abwehr erkannter Bedrohungen beschleunigen. Mit Threat-Playbooks zu Vorgehensweisen für häufige Bedrohungen kann ein Unternehmen die Bedrohungserkennung und -abwehr teilweise automatisieren. Davon profitiert auch die Hochverfügbarkeit, die OT-Systeme erfordern: Hat ein Analyst eine aktive Bedrohung identifiziert, werden sofort einige oder alle Korrekturmaßnahmen ausgeführt, um die Folgen der Bedrohung für den Betrieb zu minimieren.

Eine bessere Lageerkennung und die automatisierte Bedrohungsabwehr tragen dazu bei, die Sicherheit und Verfügbarkeit von OT-Systemen zu gewährleisten. Durch gezielte Reaktionen, mit denen Bedrohungen auf Prozessebene identifiziert und behoben werden, werden die Auswirkungen der Incident Response auf die Systemverfügbarkeit minimiert.

78 % der Unternehmen verfügen nur teilweise über eine zentrale Transparenz der OT-Umgebungen.[3]

Automatisierung erhöht die Systemverfügbarkeit, da sie eine schnelle, gezielte Reaktion auf Cyber-Bedrohungen ermöglicht.

Identifizieren von OT-Gefahren mit Bedrohungsinformationen speziell für Betriebstechnologie

OT-Systeme sind wertvolle Ziele für Cyber-Kriminelle. Oft werden viel Zeit und Ressourcen in die Auslotung von Schwachstellen bei Betriebstechnologie investiert. Vor dem eigentlichen Angriff steht dabei meist eine „Testphase“, um die Anfälligkeit der OT-Systeme zu ermitteln. Da Betriebstechnologie benutzerdefinierte Netzwerk-Protokolle verwendet – die von Cyber-Security-Lösungen für IT-Netzwerke häufig nicht verstanden werden –, können Hacker oft ihre Aktivitäten leicht verschleiern.

Für das Management von Cyber-Bedrohungen in OT-Netzwerken ist nicht nur betriebstechnisches Fachwissen, sondern auch langjährige Erfahrung im Schutz von OT-Umgebungen notwendig. Auch Bedrohungsinformationen speziell für Betriebstechnologie sind ein wichtiger Teil der OT-Netzwerk-Security.

OT-Unternehmen integrieren Anlagen und Geräte unterschiedlicher Hersteller und müssen deren Schwachstellen kennen. Transparenz über diese heterogene Betriebstechnologie ist für die Sicherheit entscheidend: Anbieter von Betriebstechnologie können dann ihre Systeme gegen Exploits härten und virtuelle Patches bereitstellen, um anfällige Systeme bei langen Wartungsintervallen effektiv zu schützen.

Unternehmen müssen außerdem diese Bedrohungsinformationen innerhalb und außerhalb des Unternehmens weiterleiten und Bedrohungsdaten von Drittanbietern nutzen können. Nur dann kann schnell auf weitverbreitete Angriffskampagnen reagiert werden, die mit künstlicher Intelligenz (KI) und maschinellem Lernen (ML) speziell Betriebstechnologie im Visier haben.

85 % der OT-Bedrohungen zielen auf Computer ab, auf denen die Protokolle OPC Classic, BACnet und Modbus laufen.[4]

Cyber-Security-Lösungen für OT-Systeme müssen OT-spezifische Bedrohungen und Protokolle kennen und verstehen.

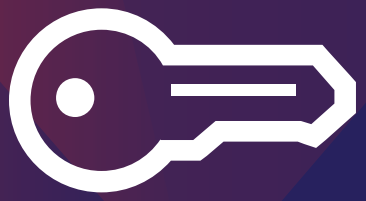
Erkennen hochkomplexer Bedrohungen mit Deception-Technologien

Besonders gefährlich für Betriebstechnologie sind langsame, schleichende Angriffe, bei denen Angreifer unentdeckt im Unternehmensnetzwerk verweilen. Eine herkömmliche Netzwerk-Sicherheit versagt bei solchen hochkomplexen Angriffsformen auf ganzer Linie.

Mit Deception-Technologien lassen sich allerdings solche verborgenen Bedrohungen aufdecken: Angreifern wird mit sogenannten Honeypots, die echte OT-Systeme nachbilden, ein Scheinziel für Malware oder andere bösartige Interaktionen präsentiert.

Wird dieses Fake-System angegriffen, deutet dies auf eine vorhandene Bedrohung im Schatten-Netzwerk hin, da diese Systeme sonst nicht verwendet werden. Des Weiteren kann das Studieren der Vorgehensweise des Angreifers wertvolle Bedrohungsinformationen über seine Tools, Techniken und Fähigkeiten liefern. Von diesen Erkenntnissen profitieren auch andere Systeme im OT-Netzwerk, auf denen Bedrohungen dann effizient gefunden und beseitigt werden können. Unternehmen erhalten mitunter sogar ein Mittel zur Identifizierung von Zero-Day-Angriffen, die sich mit herkömmlichen signaturbasierten Erkennungssystemen nicht entdecken lassen.

Auch Sandboxen, die OT-spezifische Systeme emulieren können, leisten wertvolle Dienste für die Sicherheit von Betriebstechnologie. Sie bieten eine automatisierte Instrumentierung und maschinelles Lernen, um unbekannte Bedrohungen in einer geschützten Emulation anhand anomaler oder verdächtiger Verhaltensweisen zu erkennen.



„Ein guter Decoy muss glaubwürdig sein und sich mit mäßigem Aufwand knacken lassen können. Wissen Angreifer, dass es sich um einen Köder handelt, werden sie ihn ignorieren. Deshalb darf sich der Köder in nichts vom restlichen Netzwerk unterscheiden.“[5]

Isolieren und Eindämmen von Bedrohungen mit einer Netzwerk-Segmentierung

OT-Umgebungen haben extrem hohe Anforderungen an die Verfügbarkeit, was sich auch auf die Cyber-Security von Betriebstechnologie auswirkt. Aufgrund enger Wartungsfenster und der Verfügbarkeitsanforderungen laufen auf vielen Geräten veraltete Betriebssysteme und Software. Oft kann auf älterer Hardware auch kein Virenschutz installiert werden. Dazu kommt, dass diese Systeme bei einem Sicherheitsvorfall nicht einfach heruntergefahren werden können.

All diese Faktoren bedeuten, dass die OT-Security häufig nicht auf dem Endgerät, sondern auf Netzwerk-Ebene erfolgen muss. Mit einer Netzwerk-Segmentierung und virtuellem Patching lässt sich das Risiko von ungepatchten, anfälligen Geräten verringern. Statt Updates auf dem Gerät zu installieren – was die Systemverfügbarkeit beeinträchtigen könnte –, verhindert der virtuelle Patch das Ausnutzen von Sicherheitslücken und blockiert schädlichen Traffic, bevor er das anfällige Gerät erreichen kann.

Die Netzwerk-Segmentierung kann auch die Folgen einer Sicherheitsverletzung in Grenzen halten, da sich der Angreifer dann nur eingeschränkt im Netzwerk bewegen kann – Stichwort „laterale Angriffe“. Eine Segmentierung stellt sicher, dass jede Kommunikation zwischen Geräten auf bösartige oder anomale Inhalte überprüft wird. Auch sorgt sie dafür, dass im gesamten Netzwerk eine starke Benutzerauthentifizierung und Zugriffskontrolle durchsetzbar ist.

Führende OT-Unternehmen haben mit 51 % höherer Wahrscheinlichkeit eine Netzwerk-Segmentierung als die Nachzügler der Branche.[6]

Eine Netzwerk-Segmentierung ist notwendig, damit sich hochkomplexe Bedrohungen nicht quer in OT-Netzwerken verbreiten können – Stichwort „laterale Angriffe“.

Fazit

OT-Netzwerke sind zunehmend ein Ziel hochkomplexer Cyber-Bedrohungen. Angreifer sind mit OT-Systemen bestens vertraut und entwickeln maßgeschneiderte Malware, um Schwachstellen in weitverbreiteten OT-Systemen auszunutzen.

Netzwerk-Verantwortliche müssen die ständig wachsende Angriffsfläche richtig einschätzen können. Auch sollten sie eine Automatisierung der Security, spezielle Deception-Technologien für Betriebstechnologie und eine Netzwerk-Segmentierung erwägen, um hochkomplexe Bedrohungen zu bekämpfen.

Grundsätzlich sollten sich Netzwerk-Verantwortliche folgende Fragen stellen:

- Können wir illegale Netzwerk-Zugriffe mit automatisierten Incident-Response-Workflows und einem Ereignis-Management eindämmen, bevor sich Angreifer im gesamten Netzwerk einnisten und größeren Schaden anrichten?
- Ist unsere Security-Infrastruktur so integriert, dass Bedrohungsinformationen in Echtzeit zwischen allen Sicherheitselementen geteilt werden können?
- Verfügen wir über erweiterte Funktionen zur Erkennung von Bedrohungen und Sicherheitsverstößen wie Sandboxing und Decoys?
- Haben wir Maßnahmen getroffen, um das Angriffsfenster zu verkleinern und den Zugriff auf Netzwerk-Ressourcen nach dem Eindringen zu blockieren?

[1] „Caught in the Crosshairs: Are Utilities Keeping Up with the Industrial Cyber Threat?“. Siemens und Ponemon Institute, 2019.

[2] „Independent Study Pinpoints Significant SCADA/ICS Cybersecurity Risks“. Fortinet, 28. Juni 2019.

[3] „Bericht zum Stand der operativen Technologie und der Cyber-Sicherheit“. Fortinet, 10. September 2020.

[4] „Fortinet 2019 Operational Technology Security Trends Report“. Fortinet, 8. Mai 2019.

[5] Kevin Townsend: „How Deception Technology Can Defend Networks and Disrupt Attackers“. SecurityWeek, 5. Juni 2019.

[6] „Bericht zum Stand der operativen Technologie und der Cyber-Sicherheit“. Fortinet, 10. September 2020.

www.fortinet.com/de

Copyright © 2020 Fortinet, Inc. Alle Rechte vorbehalten. Fortinet®, FortiGate®, FortiCare® und FortiGuard® sowie bestimmte andere Marken sind eingetragene Marken von Fortinet, Inc. Bei anderen hier aufgeführten Namen von Fortinet kann es sich ebenfalls um eingetragene und/oder Gewohnheitsmarken von Fortinet handeln. Alle weiteren Produkt- und Unternehmensnamen sind u. U. Marken ihrer jeweiligen Eigentümer. Leistungs- und andere hierin enthaltenen Kennzahlen stammen aus internen Labortests unter idealen Bedingungen. Die tatsächliche Leistung und andere Ergebnisse können davon abweichen. Keine der hierin enthaltenen Angaben stellt eine verbindliche Verpflichtung durch Fortinet dar und Fortinet lehnt alle ausdrücklichen oder implizierten Garantien ab. Ausnahme: Fortinet geht einen verbindlichen, schriftlichen Vertrag mit einem Käufer ein, der vom Leiter der Rechtsabteilung von Fortinet unterzeichnet wird und der eine ausdrückliche Garantie dafür gewährt, dass ein bestimmtes Produkt entsprechend den genau angegebenen Leistungskennzahlen bestimmungsgemäß funktioniert. In diesem Fall sind ausschließlich die in diesem verbindlichen, schriftlichen Vertrag aufgeführten spezifischen Leistungskennzahlen für Fortinet bindend. Jede diesbezügliche Garantie beschränkt sich einzig auf die Leistung unter den gleichen idealen Bedingungen wie bei den internen Labortests von Fortinet. Fortinet lehnt dementsprechend jegliche ausdrücklichen oder implizierten Verpflichtungen, Zusagen und Garantien ab. Fortinet behält sich das Recht vor, diese Veröffentlichung ohne Ankündigung zu ändern, zu bearbeiten, zu übertragen oder anderweitig zu überarbeiten. Es gilt die jeweils aktuellste Fassung der Veröffentlichung.

726519-0-0-DE

7. Dezember 2020, 14:06 Uhr