Fachartikel

Operational Technology (OT) Security heute und morgen:

Fertigungs- und Industrieanlagen müssen jetzt gegen Cyberangriffe gewappnet sein!

Zwar sind sich Unternehmen ihrer Verwundbarkeit hinsichtlich Cyberangriffen bewusst. Dennoch fokussieren sie dabei häufig nicht die Sicherheit ihrer operativen Technologie (OT), also ihrer Fertigungsanlagen oder Infrastruktureinrichtungen. Dabei kann gerade hier das Schadenspotenzial enorm sein – und sogar zu Gefahren für Leib und Leben führen. Operational Technology (OT) Security muss also einen essenziellen Bestandteil des IT-Sicherheitskonzepts eines Unternehmens darstellen, aber auch die besonderen Herausforderungen wie veraltete Systeme oder raue, industrielle Betriebsumgebungen beachten – etwa durch die Belastung mit hohen Temperaturen oder Staub. Unternehmen sollten für eine Einführung ein schrittweises Vorgehen wählen und auf zeitgemäße Security Verfahren setzen.

Berichte über Cyberangriffe auf Unternehmen sind in den Medien allgegenwärtig – betroffen sind Unternehmen wie z.B. große Elektronikketten genauso wie öffentliche Verwaltungen. Angreifer(-gruppen) zeichnet eine hohe kriminelle Energie aus – sie sind hochmotiviert in ihrem Handeln, gut vernetzt und haben kommerzielle oder politische Interessen, ihr Zielunternehmen auszuspionieren, zu erpressen und ihm finanziell oder hinsichtlich seiner Reputation zu schaden.

Ein Großteil von Unternehmen sind deswegen bemüht, für ihre IT Security ein angemessenes Niveau zu erreichen und zu halten. Begrenzte IT Security-Budgets und mangelnde Zeit- sowie Personal-Ressourcen limitieren aber oft ihre Möglichkeiten. Hinzu kommt: Die Operational Technology (OT) Security – also die Sicherung von operativer Technologie wie Fertigungs- und Industrieanlagen oder Infrastruktureinrichtungen – steht häufig noch gar nicht im Fokus der Security Konzepte in Unternehmen. Dabei können die Schäden immens sein: Folgen von Fehlfunktionen und Ausfällen können von Umsatzeinbußen bis zur Gefährdung von Leib und Leben oder auch der Umwelt reichen.

Unternehmen sind jedoch häufig nicht in der Lage, potenzielle Bedrohungen für ihre OT rechtzeitig zu erkennen oder verdächtigen Datenverkehr durchgehend zu überwachen. Es fehlen Kontrollfunktionen, um die Sicherheit und die Risiken, die der Bereich IoT (Internet of Things)

mit sich bringt, zu verwalten und zu überwachen. Dabei steht die Integration von IoT mit künstlicher Intelligenz, maschinellem Lernen, automatisierten Prozessen und Cloudtechnologien noch ganz am Anfang. Gleichzeitig findet zu häufig noch das Paradigma „Never change a running system“ Anwendung. Das ist fatal, denn im dynamischen Zeitalter der Digitalisierung sollten nicht nur die eigene IT-Strategie und -Infrastruktur regelmäßig in Hinblick auf ihre Sicherheit hinterfragt, sondern auch grundlegende Systementscheidungen auf den Prüfstand gestellt werden.

Trotz einiger Überschneidungen von OT und IT, wie z.B. dem Einsatz identischer Betriebssysteme, Infrastruktur- oder Netzwerkkomponenten, gibt es fundamentale Aspekte in der OT, die berücksichtigt werden müssen:

- Safety First: Ein OT System muss sicher und stabil laufen, denn bei Störungen kann es im schlimmsten Falle zu Gefährdungen von Leib und Leben kommen.
- Keine Unterbrechungen des Regelbetriebes: Das Herunter- und Herauffahren der Anlage ist mit großem Aufwand verbunden.
- In der OT befindet sich oft noch alte Hardware mit Betriebssystemen im Einsatz, die keinen herstellerseitigen Support und Sicherheitspatches mehr erhalten.
- Verbreitet ist häufig ebenfalls noch der Einsatz von Lösungen IT-fremder, oft mittelständischer Systemhersteller.
- Vielen Komponenten und Geräten steht nur wenig Personal gegenüber.
- Es werden andere Protokolle als in der IT verwendet (ICCP, Modbus oder DNP3).
- Die Betriebsumgebungen der Industrieanlagen sind herausfordernd und rau, etwa hinsichtlich der herrschenden Temperaturen, mechanischen Einwirkungen wie Vibrationen oder Staub- und Schmutzbelastungen.

Für die Operational Technology (OT) Security müssen also Systeme aus zwei Welten miteinander verbunden werden; diese Systeme können aber teilweise schon über Jahrzehnte in Betrieb und wenig dokumentiert sein. OT Security ist auch deshalb kein Quick Win, sondern komplex und mühsam. Deswegen empfiehlt sich ein schrittweises Vorgehen, um das Sicherheitslevel auf OT Ebene langfristig und nachhaltig zu heben.

1. **Bestandsaufnahme der Anlagen**

   Hier wird das Inventar an Vermögenswerten erfasst (Asset Inventory). Das heißt, es wird recherchiert und analysiert, wie die OT Systemlandschaft aussieht, wie sie im Netzwerk integriert ist und welche Daten, Software, Systeme, Geräte und Prozesse geschützt werden müssen. Es erfolgt eine Schwachstellenanalyse in Verbindung mit

möglichen Patches. Dabei ist es entscheidend, keine blinden Flecken zu übersehen, die Angreifer ausnutzen können.

2. **Risikoanalyse**

   Bestandsaufnahme und Schwachstellenanalyse liefern die notwendigen Informationen für die Risikoanalyse. Manchmal kann es zum Beispiel sicherer sein, mit einer älteren Systemversion ohne Patches zu arbeiten und ein potenzielles Sicherheitsproblem durch gezielte Überwachung zu mindern: Man akzeptiert dann ein Risiko oder schwächt es ab, anstatt das System durch Änderungen, deren Komplexität und Abhängigkeiten nicht in ihrem ganzen Umfang vorhersehbar sind, möglicherweise zum Absturz zu bringen. Für die Risikoanalyse bietet das MITRE ATT&CK Framework für Industrial Control Systems (ICS) eine geeignete Hilfestellung.

3. **Zentrales Logging**

   Cyberangriffe, oder auch nur eine Fehlfunktion eines Systems oder einer Komponente hinterlassen ihre Spuren in Logfiles. Die zentrale Sammlung dieser Logfiles ist deswegen die Grundvoraussetzung für Analyse, Alerting und automatisierte Eindämmung eines Angriffs. Es ist entscheidend, dass die Protokolldaten der unterschiedlichsten, teilweise alten Subsysteme in einem normalisierten Format abgelegt werden: Performante Analysemethoden und Machine Learning benötigen saubere Daten.

Die OT Security nimmt die Arbeit auf

Sind diese Grundlagen geschaffen, kann die Arbeit zur Herstellung der OT Security beginnen. Sie besteht vor allem in der fortlaufenden Analyse von Logdaten, um Angriffe rechtzeitig zu erkennen und abzuwehren. Dabei kommen zwei Verfahren, die sich in der IT Security bewährt haben, zum Einsatz: Realtime Correlation und User and Entity Behaviour Analytics (UEBA), also sogenanntes unsupervised Machine Learning.

Beim Verfahren Realtime Correlation werden die Logdaten mit Hilfe von definierten Korrelationsregeln analysiert. Entscheidend für die Wirksamkeit ist die Performance der Analyse. Ziel ist die Reduktion der „Detection Time“ und der „Reaction Time“. Um sicherzustellen, dass das relevante Spektrum von möglichen Angriffen abgedeckt wird, bietet auch hier das MITRE&ATT&CK Framework für ICS einen sinnvollen Rahmen. Es erlaubt, mögliche Angriffsvektoren strukturiert in die Security Analyse aufzunehmen.

Das Verfahren UEBA hingegen setzt, anders als Realtime Correlation, darauf, eine Baseline zu bilden. Diese Baseline besteht in einer statistisch ermittelten Abbildung des OT Systems, des Verhaltens und der Interaktion der Komponenten im Normalbetrieb. Sie ist wichtig, um

Abweichungen vom Regelbetrieb zu erkennen. UEBA hat zwei Vorteile: Zum einen lernt das System selbständig und kann daher auch auf Angriffe reagieren, die noch nicht in Korrelationsregeln hinterlegt sind. Zum anderen können bei Angriffen auf OT Systeme auch Systeminteraktionen zum Einsatz kommen, die für sich gesehen unproblematisch sind. UEBA erkennt diese in ihrer Zeit bzw. Häufigkeit als eine Abweichung von der Baseline. UEBA ist in der IT Security ein relativ neuer Ansatz, den Unternehmen oft als nächsten Evolutionsschritt nach der Realtime Analyse in Angriff nehmen. Für OT Security empfiehlt sich aber der umgekehrte Weg: OT Systeme sind darauf angelegt, Tätigkeiten, Fertigungs- oder Prozessschritte zu wiederholen. Auffälligkeiten, also Abweichungen von der Baseline, sind so einfacher zu finden. Grundvoraussetzung für UEBA – basierend auf Machine Learning – sind bereinigte Daten.

Lösungen für das OT-Security-Monitoring

Um Cyberattacken in Echtzeit zu erkennen, bedarf es einer Sicherheitssoftware, die durch starke Sicherheitsanalysen unterstützt wird: ArcSight beispielsweise verfügt über die Konnektoren, um OT Systeme anzubinden – sowohl moderne Logquellen, als auch betagte Subsysteme. Alle Konnektoren bringen die Daten auf ein einheitliches Format als Grundlage für die weitere Analyse. Logdaten werden in einer Logdatenbank mit eingebauten Analytics gespeichert; sowohl Forensik als auch Realtime Correlation und UEBA können dann auf einer gemeinsamen, konsistenten Datenbasis erfolgen. Eine Lösung wie ArcSight Intelligence ermöglicht durch den Einsatz von Machine Learning die Erkennung von Abweichungen vom Regelbetrieb und somit eine Sicherung der OT bereits nach wenigen Tagen des selbständigen Lernens. Die gezielte Analyse von Angriffsvektoren kann mit ArcSight Detect erfolgen; hier finden die im MITRE&ATT&CK-ICS Framework dokumentierten Taktiken und Methoden Anwendung.

Damit ist das OT System gegen Cyberangriffe nachhaltig geschützt. Da die Daten nun in konsistenter und bereinigter Form vorliegen, können sie auch für andere Zwecke genutzt werden, etwa für Predictive Maintenance oder die Optimierung des Gesamtsystems. Denn nicht jede Abweichung weist auf einen Cyberangriff hin; gegebenenfalls handelt es sich in vereinzelten Fällen auch um Hinweise auf das Versagen von einzelnen Komponenten. Wer nicht die Kapazitäten hat, ein OT Security-Monitoring in Eigenregie zu managen, kann hierzu auch eine SaaS Lösung einsetzen oder OT Security als Managed Service erbringen lassen.

Fazit

OT Security wird durch neue Technologien, Internet 4.0 und Machine Learning stetig komplexer. Das macht es erforderlich, Systeme, die aus unterschiedlichen Zeiten stammen, zu vernetzen und Daten zu vereinheitlichen, um eine systematische Überwachung leisten zu können.

Die Voraussetzung sind Asset Inventory, Risikoanalyse und zentrales Logging. Dann können Verfahren wie Realtime Correlation und UEBA eingesetzt werden, um ein höchstmögliches OT Security Niveau für z.B. Fertigungsanlagen und Infrastrukturkomponenten sicherzustellen.

Autoren: Felix Gutjahr, Cyber Defense Consultant SECUINFRA

Marcel Röhrl, Portfolio Sales Specialist - NextGen Security Operations, MicroFocus

Weitere Informationen: https://www.secuinfra.com/de/techtalk/ot-security-heute-und-in-zukunft-wie-gelingt-die-absicherung-von-kritis/

Pressekontakt: SECUINFRA GmbH

Svenja Koch

Stefan-Heym-Platz 1

10367 Berlin

Deutschland

Tel. +49 (0) 160 921 633 44

svenja.koch@secuinfra.com