OT und IT in Harmonie

IT (Information Technology) und OT (Operational Technology) sind bisher losgelöst voneinander betrachtet worden. Das lässt sich ändern.

In friedlicher Koexistenz erledigen IT (Information Technology) und OT (Operational Technology) ihre jeweiligen Aufgaben, doch Anknüpfungspunkte gibt es wenig. In einer zunehmend vernetzten Welt im Zuge von Industrie 4.0 und Internet of Things (IOT) wachsen die beiden Welten allerdings immer mehr zusammen. Erfahren Sie nachfolgend, wie ein gemeinsamer Security Ansatz geschaffen werden kann.

IT versus OT

IT (Informationstechnologie) beschreibt alle Technologien zur Datenverarbeitung mittels Software. Laut Gartner ist Operational Technology (OT) „Hardware und Software, die eine Änderung durch die direkte Überwachung und/oder Kontrolle von physikalischen Geräten, Prozessen und Ereignissen im Unternehmen erkennen oder verursachen."

Der Bereich OT kann dabei noch in weitere unterschiedliche Bereiche eingeteilt werden. So kann zum Beispiel zwischen den Bereichen Gebäudesteuerung oder -automatisierung (Zutrittskontrolle, Videoüberwachung, Einbruchmeldeanlagen, Brandmeldeanlagen, etc.) oder Produktionsanlagen (Fertigungsstraßen, Abfüllanlagen, etc.) unterschieden werden.

Während in der OT beim Thema Sicherheit in erster Linie von Verfügbarkeit gesprochen wird, spricht man in der IT eher von Begriffen wie Vertraulichkeit und Integrität. Aus der unterschiedlichen Schwerpunktsetzung entsteht häufig ein Spannungsfeld bei den definierten Zielen und wie man diese umsetzen möchte.

Darüber hinaus gibt es einen gravierenden Unterschied bei den Planungs- und Lebenszyklen der eingesetzten Technologien. Während in der IT üblicherweise mit einem Planungszyklus von drei bis fünf Jahren gearbeitet wird, wird in der Gebäudesteuerung oder in Produktionsumgebungen mit einen Lebenszyklus von zehn und deutlich mehr Jahren geplant. Das betrifft auch die eingesetzte Steuerungstechnologie (OT).

„In der OT geht es vor allem um Verfügbarkeit, in der IT eher um Begriffe wie Vertraulichkeit und Integrität."

IT und OT stellen Unternehmen vor komplexe Security-Herausforderungen

Während lange Zeit Bereiche wie Gebäudeautomatisierung oder Produktion (OT) gekapselte Systemlandschaften waren, wachsen diese mit der zunehmenden Digitalisierung immer weiter mit der klassischen Information Technology (IT) zusammen. Die zunehmende Vernetzung der Geräte und Maschinen mit der Infrastruktur und dem Internet erfordert die Konvergenz zwischen IT und OT, besonders im Hinblick auf das Thema IT-Sicherheit. Um Digitalisierungsprojekte erfolgreich umzusetzen, sind nicht nur technische Maßnahmen, sondern auch die Veränderung der Organisationsstruktur und klare Definitionen und Verantwortlichkeiten wichtig.

Einheitlicher Sicherheitsansatz für IT- und OT-Infrastrukturen

Mit einem Security Information and Event Management (SIEM) ist es möglich, die beiden Welten mit Blick auf eine ganzheitliche Sicherheitsbetrachtung im Auge zu behalten. Mit einem SIEM ist ein Unternehmen oder eine Organisation in der Lage, Gefährdungen und Angriffe auf ihre IT-Systeme zu entdecken und abwehren zu können, auch wenn technisch keine präventiven Maßnahmen möglich sind. Und das bevor ein Schaden die Geschäftstätigkeit nachhaltig beeinträchtigen oder zum Erliegen bringen kann. Darüber hinaus verbessert ein SIEM im laufenden Betrieb kontinuierlich die Sicherheit, Compliance und Qualität der IT-Systeme. Mithilfe eines SIEM erfolgt eine ständige, automatisierte Log- und Eventüberwachung der Systeme auf sicherheitsrelevante Vorfälle.

Security Use Cases als Basis für ein erfolgreiches SIEM

Ein wesentlicher Pfeiler eines SIEM sind die Security Use Cases (Sicherheits- oder Risikoszenarien), die mittels einer SIEM-Lösung gemonitort werden sollen. Denn so unterschiedlich IT-Infrastrukturen

Foto: Adobe Stock

sind, so unterschiedlich sind auch die Compliance-Anforderungen wie auch das Risikomanagement der einzelnen Unternehmen. Dieses bedeutet, dass die Use Cases immer auf die jeweilige Umgebung und Infrastruktur angepasst werden müssen. Beispiele für Use Cases aus dem IT-Umfeld sind:

- Direktes Auslesen von großen Datenmengen aus einer Datenbank unter Umgehung des Anwendungsservers,
- verdächtige Kommunikation mit bekannten infizierten IP-Adressen,
- unerwartete Konfigurationsänderung an sicherheitsrelevanten Systemen,
- Nutzung privilegierter Accounts.

Informationsquelle für ein SIEM können selbstverständlich auch Ereignisse aus der OT sein. Bestimmte Ereignisse oder Kombinationen von Ereignissen können auch hier auf ein Sicherheitsvorfall hinweisen. Im Rahmen einer Risikoanalyse werden die für ein SIEM zu überwachenden Risikoszenarien entwickelt.

Beispiele für Use Cases aus dem OT Umfeld Gebäudesteuerung/Automatisierung sind:

- Mehrfaches Betreten des Gebäudes/Geländes mit derselben Zutrittskarte, ohne dass vorher das Gebäude/Gelände mit dieser Zutrittskarte wieder verlassen wird.
- Mehrfacher Zutrittsversuch von einem ungewöhnlichen Ort,
- Verstoß gegen das „Mehr-Augen-Prinzip“,
- Kontrolle der Datenflüsse.

„Für die Auslagerung von IT-Sicherheit sprechen viele Gründe. IT-Landschaften werden immer komplexer, sodass den meisten Unternehmen weder das Know-how noch die personellen Ressourcen zur Verfügung stehen.“

Über Consecur

Die Consecur GmbH, gegründet 1999 mit Sitz in Meppen, ist eine Unternehmensberatung für Informationssicherheit: Consecur entwickelt, analysiert und realisiert Sicherheitskonzepte für die Informationsverarbeitung. Darüber hinaus bewertet und verbessert Consecur bestehende Sicherheitskonzepte, schult Anwender und Experten und berät seine Kunden herstellerneutral bei der Auswahl von IT-Sicherheitskomponenten.

Weitere Informationen: www.consecur.de

Über Corewillsoft

Die Corewillsoft GmbH, gegründet 2017 mit Sitz im Bonn, bringt Produkt- und Sicherheitsinnovationen in die Branche der Zutritts- und Betriebstechnologie. Unternehmensvision ist es, komplexe Sicherheitslösungen jedem Nutzer unabhängig von seinem Alter und IT-Affinität leicht bedienbar zur Verfügung zu stellen.

Weitere Informationen:
www.corewillsoft.com

Wird eines dieser Szenarien im SIEM in den gesammelten Daten identifiziert, erfolgt ein Alarm, und ein Security Analyst kümmert sich unverzüglich um diesen Vorfall.

Als Erweiterung zur SIEM-Lösung bieten SOAR (Security Orchestration, Automation and Response)-Lösungen entscheidende Vorteile für die betriebliche Effizienz. SOAR beschreibt Software und Verfahren, um das Bedrohungs- und Schwachstellenmanagement in einem Unternehmen zu verbessern. Durch Automatisierung und Orchestrierung auf priorisierte Bedrohungen mit hohem Risiko kann mit SOAR entscheidende Zeit gewonnen werden.

Managed Security Services

Für die Auslagerung von IT-Sicherheit (Managed Security Services) sprechen viele Gründe. IT-Landschaften werden immer komplexer, sodass den meisten Unternehmen weder das Know-how noch die personellen Ressourcen zur Verfügung stehen. Zudem werden Kosten kalkulierbar, entsprechend wiederkehrende Schulungen sind nicht mehr erforderlich, und es bleibt mehr Zeit für Unternehmenswachstum. ■

ConSecur GmbH:
www.consecur.de

CoreWillSoft GmbH:
www.corewillsoft.com