Risikomanagement in der Industrie

Systematischer Ansatz für effektive OT-Security

In zunehmend vernetzten industriellen Infrastrukturen stehen Unternehmen vor Herausforderungen bei der OT-Security. Betriebsunterbrechungen und Produktionsstillstände führen jedoch nicht nur zu finanziellen Einbußen, sondern wirken sich auch negativ auf die Reputation aus. Cyberangriffe auf diese kritischen Systeme bergen zudem das Risiko von Datendiebstahl und Sabotage, was langfristige Sicherheitsprobleme und Wettbewerbsnachteile nach sich ziehen kann.

Vor diesem Hintergrund gewinnen regulatorische Maßnahmen wie NIS2 oder der Cyber Resilience Act (CRA) an Bedeutung. Diese Regelwerke fordern umfassende Risikomanagementmaßnahmen, die explizit auch die OT-Security einschließen. Mehr noch: Unternehmen sind gezwungen, ihre Sicherheitsstrategien grundlegend zu analysieren und zu verbessern. Sie müssen in neue Technologien investieren, Prozesse anpassen und das Bewusstsein innerhalb ihrer Organisation schärfen. Gleichzeitig bieten die Gesetze Chancen, die Resilienz gegen Cyberangriffe zu erhöhen und das Vertrauen in digitale Technologien zu stärken.

Die OT-Security-Landschaft stellt die Industrie vor technische und organisatorische Aufgaben, wobei Inkompatibilität von Komponenten, Datensicherheit und veraltete Technologien zu den Hauptproblemen zählen. Mangelhafte Asset-Verwaltung und unzureichendes Wissensmanagement erhöhen Kosten und Risiken, während kontinuierliche Mitarbeiterschulungen essenziell für eine verbesserte IT-Sicherheit sind. Diese Komplexität erfordert einen systematischen Ansatz für effektive OT-Security-Strategien.

Maßnahme I: Transparenz

Das Asset-Management bildet das Fundament für eine umfassende OT-Security-Strategie und ermöglicht einen ganzheitlichen Ansatz zum Schutz kritischer Infrastrukturen. Um potenzielle Schwachstellen zu identifizieren und angemessen zu schützen, muss der Anwender wissen, welche Hard- und Software, Netzwerkgeräte und Steuerungssysteme sich im Netzwerk befinden. Da in OT-Umgebungen oftmals ältere Geräte mit Sicherheitsrisiken zum Einsatz kommen, hilft die Inventarisierung bei der Erkennung nicht mehr unterstützter Komponenten. Mit dem Wissen über alle Komponenten im Netzwerk kann eine Priorisierung hinsichtlich der potenziellen Bedrohung der einzelnen Assets vorgenommen werden, um so bei der Einführung von Sicherheitsmaßnahmen fundierte Entscheidungen zu treffen. Zudem unterstützt ein effektives Asset-Management bei der Einhaltung von Compliance-Anforderungen und ermöglicht

Das Asset-Management bildet das Fundament für eine umfassende OT-Security-Strategie.

Bild: ©stockbusters/stock.adobe.com

Bild: ©CandyRetriever/stock.adobe.com

Der ganzheitliche Sicherheitsansatz von Fortinet Security Fabric deckt sowohl IT- als auch OT-Systeme ab.

die gezielte, sichere und auf den Produktionsprozess abgestimmte Implementierung von Updates und Patches.

Wie eine ganzheitliche und umfassende Sichtbarkeit und Kontrolle in der gesamten Fertigungsumgebung im Sinne einer strengen Sicherheitsstrategie erreicht werden können, zeigt der Use Case des Asset-Intelligence-Spezialisten Armis und Colgate-Palmolive. Aufgrund von mangelnder Transparenz im Produktionsbereich waren die Verantwortlichen des Konsumgüterkonzerns auf der Suche nach einer Plattform, die alle Geräte im Netzwerk identifiziert, profiliert und klassifiziert, und es darüber hinaus ermöglicht, automatisiert Richtlinien durchzusetzen sowie die Netzwerksegmentierung zu erleichtern. Die einfache Verwaltung der Cloud-Infrastruktur stellt einen weiteren Vorteil dar. Damit bietet Armis mit seinen spezifischen Lösungsansätzen eine umfassende Asset-Erkennung, die Erstellung einer Risikobewertung und die Fokussierung auf die Behebung kritischer oder ausnutzbarer Schwachstellen zur schnellen Reduzierung der Angriffsfläche.

Maßnahme II: IT/OT-Konvergenz

Die Vernetzung von IT- und OT-Systemen erhöht potenzielle Cyberrisiken, indem isolierte OT-Systeme nun über Netzwerke erreichbar werden und neue Angriffsvektoren entstehen. Unterschiedliche Security-Standards zwischen ausgereiften IT-Systemen und älteren OT-Systemen, die oft nicht für Netzwerkverbindungen konzipiert sind, verschärfen dieses Problem. Die Integration von komplexen Systemen mit unterschiedlichen Protokollen, Datenformaten und Architekturen erschwert die Implementierung einheitlicher Maßnahmen. Strenge Verfügbarkeitsanforderungen von OT-Systemen stehen im Konflikt mit klassischen IT- Security-Maßnahmen, wie regelmäßigen Patches oder Neustarts. Fehlende Transparenz und Kontrolle über alle vernetzten Geräte in der konvergierten Umgebung behindern außerdem die effektive Erkennung von Cyberbedrohungen, während unterschiedliche Sicherheitskulturen und Prioritäten zwischen IT- und OT-Teams die Zusammenarbeit erschweren. Zudem lassen sich veraltete OT-Systeme mit langen Lebenszyklen meist nicht einfach aktualisieren, was sie anfällig für Sicherheitslücken macht. Schließlich können Vorfälle in konvergierten Umgebungen schwerwiegende Folgen für die physische Produktion und Sicherheit haben. Deshalb ist ein Ansatz erforderlich, der sowohl IT- als auch OT-spezifische Anforderungen berücksichtigt und eine enge Zusammenarbeit zwischen den Teams fördert.

Vor den Herausforderungen stand ein Kritis-Unternehmen im Bereich der erneuerbaren Energien. Dabei wurde nach einer skalierbaren und flexiblen Netzwerkinfrastruktur gesucht, die die laufenden Innovationen unterstützt und Sichtbarkeit sowie zentrale Kontrolle über alle Systeme bietet. Einen solchen integrierten Ansatz bietet Fortinet Security Fabric, dessen ganzheitlicher Sicherheitsansatz sowohl IT- als auch OT-Systeme abdeckt. Fortinets Cloud-kompatible Lösungen zahlen auf die Cloud-Strategie des Unternehmens ein, während die SD-Branch-Lösung eine flexible und skalierbare Netzwerkarchitektur ermöglicht. Die Fortinet-Plattform bietet zudem Transparenz und Kontrolle über alle Systeme sowie spezifische OT-Funktionen und Protokollunterstützung. Auf diese Weise konnte das Kritis-Unternehmen eine sichere, skalierbare und gut integrierte Netzwerkinfrastruktur aufbauen, die sowohl IT- als auch OT-Anforderungen erfüllt und gleichzeitig die Cloud-basierte digitale Strategie unterstützt.

Maßnahme III: Komplexität reduzieren

Eine sichere Koexistenz und Integration von Alt- und Neusystemen, ohne dabei die Betriebsabläufe negativ zu beeinflussen, ist für viele Unternehmen eine Mammutaufgabe. Denn Altsysteme verfügen häufig nicht über moderne Security-Funktionen und können daher nur schwer gepatcht werden, und auch die Integration beider Systemarten kann zu Kompatibilitätsproblemen führen. Wichtige Aspekte sind außerdem regulatorische und Verfügbarkeitsanforderungen.

Für das Getränkeunternehmen Krombacher stellte TXOne Networks ein passendes Lösungspaket im Sinne der IT/OT-Konvergenz bereit: Alt- und Neusysteme können durch virtuelle Segmentierung sicher getrennt und integriert werden, wobei die Sicherheitsmaßnahmen flexibel auf die unterschiedlichen Anforderungen angepasst sind. Die OT-nativen Lösungen berücksichtigen die Besonderheiten industrieller Umgebungen und gewährleisten umfassende Transparenz über alle Netzwerkgeräte. Für nicht direkt patchbare Systeme stellt TXOne virtuelle Patching-Optionen bereit und unterstützt bei der Einhaltung regulatorischer Vorgaben. Sämtliche Sicherheitsvorkehrungen lassen sich mit kleinen Betriebsunterbrechungen einführen. ■

Patrick Scholl
Head of OT
Infinigate Deutschland GmbH
www.infinigate.com

In seinem Secure Engineering Lab in Paderborn unterstützt das Fraunhofer IEM Unternehmen dabei, ihre Prozesse und Produkte den neuen EU-Richtlinien anzupassen.

Bild: Fraunhofer IEM

Cyber Resilience Act von der EU verabschiedet

Drei Sofortmaßnahmen für Unternehmen

Lange wurde er angekündigt, nun ist er offiziell verabschiedet worden: der Cyber Resilience Act, kurz CRA. Damit gelten ab dem November 2027 für eine Vielzahl vernetzter Geräte und deren Software EU-weite neue Mindestanforderungen in puncto Security – Schwachstellenmeldepflichten gelten sogar schon ab August 2026. Vor allem die Hersteller von Produkten werden in die Pflicht genommen: Sie müssen sicherstellen, dass ihre Produkte die Sicherheitskriterien für den europäischen Markt erfüllen, und zwar mit wenigen Ausnahmen, unabhängig der Branche. Das Fraunhofer IEM erarbeitet mit Unternehmen wie Adesso Mobile Solutions, Connext, Phoenix Contact und Kraft Maschinenbau seit vielen Jahren Security-Maßnahmen – und gibt Tipps, wie Unternehmen sich für den CRA rüsten können.

Für Dr. Matthias Meyer, Bereichsleiter Softwaretechnik und IT-Sicherheit am Fraunhofer IEM, drängt die Zeit: „Die Übergangsfrist, bis der CRA 2027 voll erfüllt werden muss ist kurz. Unternehmen müssen sich in vielen Bereichen neu aufstellen – angefangen von der Durchführung von Security-Risikoanalysen über kurzfristige Meldepflichten bei Bekanntwerden von Schwachstellen bis hin zu kostenfreien Security-Updates während der erwarte-

ten Lebensdauer des Produkts. Und Aufschieben gilt nicht, denn bei Nichteinhaltung des CRA drohen Strafzahlungen in Millionenhöhe."

Das Forschungsinstitut empfiehlt Unternehmen jetzt drei Maßnahmen zu ergreifen, um den Weg zur CRA-konformen Produktentwicklung zu beginnen. „Die schnelle Reaktion auf das Bekanntwerden von Schwachstellen und systematische Risikoanalysen sind essenzielle Maßnahmen zur Erfüllung der CRA-Anforderungen: Unternehmen, die diese Maßnahmen jetzt angehen, sind schon gut unterwegs. Zusätzlich bringt eine Ist-Stands-Analyse im Hinblick auf die Produkte und Prozesse Klarheit für das weitere Vorgehen", betont Dr. Meyer.

Aufbau eines Schnelleinsatzteams für den Ernstfall

Werden Hersteller gewahr, dass Schwachstellen in ihren Produkten ausgenutzt werden, müssen sie künftig die Agentur der Europäischen Union für Cybersicherheit (ENISA) umgehend informieren: Innerhalb von 24 Stunden müssen sie eine erste Warnung geben und innerhalb von 72 Stunden weitere Details zur Art der Schwachstelle, möglichen Gegenmaßnahmen und mehr liefern. Abgesehen davon müssen sie jederzeit ansprechbar sein für Personen, die Sicherheitslücken melden möchten, und im Blick behalten, ob Schwachstellen in einem zugelieferten Softwarebestandteil bekannt werden. Dies gehört zu den Aufgaben eines Product Security Incident Response Teams (PSIRT): Hersteller, die noch kein PSIRT etabliert haben, sollten sich dringend damit befassen, denn die genannten Pflichten sind bereits ab August 2026 zu erfüllen, und zwar für alle Produkte auf dem Markt, auch solche, die lange vor Inkrafttreten des CRA lanciert wurden.

Regelmäßige Bedrohungs- und Risikoanalysen

Im Kern verlangt der CRA, dass Hersteller ihre Produkte regelmäßig auf Sicherheitsrisiken analysieren und an diese Risiken angepasste Sicherheitsmaßnahmen integrieren. Unternehmen müssen das Durchführen von Bedrohungs- und Risikoanalysen für alle Produkte fest in den Entwicklungsprozess integrieren: So identifizieren sie systematisch Bedrohungen, bewerten das jeweilige Sicherheitsrisiko und leiten informiert und gezielt Schutz- und Gegenmaßnahmen ab. Das Sicherheitsniveau der Software kann somit kontinuierlich und vor allem angemessen erhöht werden. Entwickler:innen erlangen ein neues Sicherheitsbewusstsein und teure, aber eigentlich unnötige Maßnahmen werden sogar vermieden.

Überblick durch Ist-Stand-Analyse

Die ersten beiden Maßnahmen sind wichtig, werden aber nicht ausreichen: Unternehmen müssen sich ein Bild davon machen, welche Anforderungen des CRA sie erfüllen, und zwar sowohl bezüglich ihrer Prozesse im Produktlebenszyklus als auch der konkreten Produkte. Auch wenn noch keine harmonisierten Normen zum CRA vorliegen, ist einhellige Expertenmeinung, dass der bereits existierende Standard für industrielle Cybersicherheit IEC 62443 eine sehr gute Orientierung gibt. Unternehmen müssen also nicht warten, sondern können schon jetzt Ist-Stands-Analysen für ihre Prozesse und Produkte durchführen und Maßnahmen ableiten und somit wertvolle Zeit bei der Umsetzung des CRA gewinnen. ■

Informationen und Angebote zum Cyber Resilience Act stellt das Fraunhofer IEM hier zur Verfügung.

Fraunhofer IEM
www.iem.fraunhofer.de