STORMSHIELD

MEINUNGEN

OT UND CYBERSICHERHEIT: EIN BLICK IN DEN KERN OVPERATIVER INFORMATIONSSYSTEME

Stéphane Prevost
Product Marketing Manager, Stormshield

Operative Informationssysteme sind allgegenwärtig, von Fertigungsanlagen über Museen und Einkaufszentren bis hin zu öffentlichen Verkehrsmitteln. Fälschlicherweise werden sie oft industrielle Informationssysteme oder OT genannt. Sie begleiten uns im Alltag diskret auf Schritt und Tritt, um unseren Komfort und unsere Sicherheit unter allen Umständen zu gewährleisten. Ein wahrer Paradigmenwechsel, denn traditionelle IT-Informationssysteme fördern eher die Daten- als die Betriebssicherheit. Die Cybersicherheit industrieller Systeme darf jedoch nicht vernachlässigt werden, schließlich sind die mit Cyberangriffen verbundenen Risiken sehr präsent. Hier einige Erklärungen.

ALLGEGENWÄRTIGE OT

Viele Menschen meinen, die OT (Operational Technologie) betreffe nur Sektoren wie das verarbeitende Gewerbe, die Energie, das Gesundheitswesen oder den Verkehr. Aber das Ausmaß der OT-Anwendungen ist viel größer: **Operative Informationssysteme gibt es absolut überall.**

„Zum Beispiel gibt es in einem Flughafen einen sichtbaren Teil mit Beleuchtung, Brandmeldern, Videoüberwachung und Klimaanlage. Und einen weniger sichtbarer Teil mit Gepäcksortiersystemen, Zugangskontrollen für Sperrbereiche, Landebahnbefeuerung etc.", so **Jean-Christophe Mathieu,** Leiter industrielle Sicherheit bei Orange Cyberdefense. Beispiele dafür gibt es im Überfluss: Rolltreppen, Check-in-Automaten, U-Bahnen, Registrierkassen, Fahrkartenautomaten oder sogar Sicherheitsportale. Diese Instrumente erinnern zwar nicht an die Industrie, weil sie nichts produzieren, doch sind sie eigenständige operative Systeme. Und aus diesem Grund auch kritisch.

„Die Cybersicherheit für OT-Systeme ist von größter Bedeutung, da sie zur Betriebssicherheit beiträgt."

Vincent Nicaise, Industrial Partnership and Ecosystem Manager bei Stormshield

„Die operativen Informationssysteme steuern Geräte, die auf die physische Welt einwirken. Ein Angriff auf das Brandmeldesystem kann zum Beispiel die Sicherheit eines öffentlichen Gebäudes außer Kraft setzen", erklärt Vincent Nicaise, Industrial Partnership und Ecosystem Manager bei Stormshield. *„Nehmen wir ein Fußballstadion, das durch einen Cyberangriff auf die Beleuchtungsanlage in der Dunkelheit versinkt. Es ist nicht schwer, sich die mit der Panik verbundenen Massenbewegungen und ihre katastrophalen Folgen vorzustellen. Ebenso kann ein Angriff auf das dynamische Signalsystem, das die Fahrspurzuweisungssignale in einem Tunnel verändert, schwere Unfälle verursachen.* ***Cybersicherheit für OT-Systeme ist von größter Bedeutung, da sie zur Betriebssicherheit beiträgt.***"

SPEZIFISCHE ANFORDERUNGEN DER OT-SICHERHEIT

Die OT und die IT werden aufgrund ihrer Konvergenz oft verwechselt, doch handelt es sich um zwei Welten, die sich durch ihre operative Anforderungen deutlich unterscheiden. Trotz der IT/OT-Konvergenz sind die Ziele also nicht identisch: Während die IT Daten verarbeitet, steuert die OT sie, um über eine physische Aktion auf die Realität einzuwirken. Ein „klassisches" IT-System zu aktualisieren, ist relativ einfach, die Aktualisierung eines OT-Systems, d.h. der „industriellen" oder „operativen" IT, ist jedoch sehr komplex. So ist es zum Beispiel unmöglich, die Tätigkeit eines Abwasser- und Trinkwasserversorgungsnetzes ohne direkte Auswirkungen auf die Verteilung abzuschalten. Eine solche Maßnahme setzt eine fein abgestimmte Organisation und die genaue Planung der Aktualisierungen voraus.

Darüber hinaus werden Informationssysteme in industriellen Kontexten im Allgemeinen für längere Zeiträume (30 Jahre oder mehr) eingerichtet. Sie sind **veraltet und daher anfällig:** obsolete Komponenten, keine oder wenige integrierte Cybersicherheitsmechanismen, komplexe Management-Patches, die schwierig zu implementieren sind, usw.

Schließlich stellt die **Umgebung** mit ihren spezifischen Betriebsbedingungen (Staub, sehr niedrige oder hohe Temperaturen, Schwingungen, Elektromagnetismus, gefährliche Produkte in der Nähe usw.) und die Zugangsmöglichkeiten (Tunnel, Pumpwerke, Umspannwerke, abgelegene Orte usw.) **oft hohe Ansprüche.**

Daher sind die Schwerpunkte der OT-Sicherheit die Vermeidung physischer, ökologischer und materieller Schäden und die Aufrechterhaltung der industriellen Tätigkeit, auch unter schlechten Bedingungen. *„Es geht vor allem darum, Herausforderungen wie den Angriffsversuch auf das israelische Wassernetz im vergangenen April zu meistern, bei dem Chlor oder andere Chemikalien dem Wasser in falschen Proportionen beigemischt hätten werden können"*, meint Vincent Nicaise. Ein Anschlag nach dem Vorbild der Angriffe auf die französischen Werke von Fleury Michon im April 2019 oder auf die Anlagen von Honda im Juni 2020, wobei in beiden Fällen der Betrieb der Fertigungsstraßen eingestellt werden musste. Neben der Betriebssicherheit in der OT hat auch die Systemverfügbarkeit Vorrang vor der Datenintegrität und Vertraulichkeit. Ein großer Unterschied zur IT, die in erster Linie die Vertraulichkeit schützt. *„Es gibt Ausnahmen in einigen Branchen, in denen Vertraulichkeit noch wichtig ist. Beispielsweise in der Pharmakologie, die ihre Rezepturen sorgfältig geheim hält. Hier ist das geistige Eigentum ein echter Wettbewerbsvorteil. Aber für die meisten Werke ist der Schutz der Produktionsgeheimnisse keine Herausforderung an sich, auf jeden Fall viel weniger, als den Betrieb Hunderter von Maschinen mit Bedienernaufrechtzuerhalten, die nicht unbedingt vorsichtig sind"*, meint Jean-Christophe Mathieu.

OT UND CYBERRISIKEN

Infolge der IT/OT-Konvergenz und der Allgegenwart der digitalen Technologie werden traditionell isolierte operative Informationssysteme effizienter und agiler. Diese neue Flexibilität geht allerdings Hand in Hand mit neuen Cyberrisiken. Um sich davor zu schützen und die Cybersicherheit für OT-Systeme zu gewährleisten, müssen wir einige grundlegende Grundsätze der digitalen Hygiene berücksichtigen.

- **Netzwerksegmentierung:** Die IT/OT-Konvergenz und die Digitalisierung betrieblicher Informationssysteme führt zu einem Bruch in diesen früher hermetisch abgeriegelten kritischen Systemen. Die Netze müssen also unbedingt segmentiert werden, wie es die Norm IEC 62443 vorsieht, die sich mit der Cybersicherheit operativer Anlagen befasst. Sie sorgt für die Systemisolierung und begrenzt die Ausbreitung eines Cyberangriffs.

- **Sicherung der Prozesskommunikation**: Die kontrollierte Sicherheit setzt eine detaillierte Kenntnis des Austauschs auf der Prozessebene voraus. „*Es ist wichtig, die Kommunikationsflüsse zwischen den Automaten sowie den Austausch mit der Überwachung zu kennen*“, erklärt Vincent Nicaise. „*Sobald Sie das erreicht haben, müssen Sie in der Lage sein, die Grundlagen zu analysieren, und dürfen nur mehr legitime Kommunikationen zulassen. Auf diese Weise können unrechtmäßige Aufträge oder Austausche blockiert werden. Auf dieser Ebene des Informationssystems ist die Sicherung nur möglich, wenn die Sicherheitseinrichtungen in der Lage sind, die zur Prozesssteuerung verwendeten industriellen Protokolle zu analysieren.*“ Die Implementierung der Protokollanalyse geht noch einen Schritt weiter, weil sie die Legitimität des Nachrichtenaustauschs zwischen den Automaten gewährleistet.

- **Sicherstellung der Fernwartung und Fernsteuerung**: Im Rahmen der Anlagenwartung kann es erforderlich sein, dass der Systemintegrator eine Verbindung zum Produktionsnetzwerk herstellt. Es ist daher unerlässlich, den Dienstleister zu authentifizieren und die Kommunikationsflüsse zwischen dem Industriestandort und dem Instandhalter zu sichern – zum Beispiel durch die Verschlüsselung mit der Installation einer Firewall oder eines VPN. Andererseits wird empfohlen, den Bereich, in dem er agiert, zu definieren und seinen Zugang ausschließlich auf das unbedingt Notwendige zu beschränken. „*Dies ist umso wichtiger, als es viele externe Dienstleister geben kann, die wahrscheinlich an unterschiedlichen Bereichen der Industriesysteme arbeiten*“, betont Vincent Nicaise. Gleiches gilt für die Fernsteuerung verteilter Prozesse, um die Sicherheit der Kommunikation und damit die Datenintegrität zu gewährleisten.

- **Sicherung der Überwachungsstationen**: In dieser unflexiblen und alternden Umgebung kann sich Malware in kürzester Zeit verbreiten. Die Überwachungsstationen verwenden oft obsolete Betriebssysteme, was die Sicherung erschwert. „*In diesem Fall müssen Sie in der Lage sein, die Station zu schützen und eine Whitelist (oder Allowlist) der Anwendungen zu implementieren, die unbedingt notwendig sind*“, erläutert Vincent Nicaise. „*Auf diese Weise können wir verhindern, dass Schadprogramme und Schadprozesse starten. Wir dürfen nicht vergessen, dass die meisten Produktionsunterbrechungen in den letzten Jahren auf Ransomware zurückzuführen waren, die auf den Workstations der Werksüberwachung aufgetaucht sind. Der Schutz dieser Stationen ist daher von höchster Bedeutung.*“

- **Kontrolle der Anzahl der USB-Sticks:** ein nicht zu unterschätzender Punkt, da noch immer viele USB-Sticks im Betrieb verwendet werden, sowohl von Beschäftigten des Unternehmens als auch von Außenstehenden, die Daten über die Überwachungsstationen sammeln oder Automaten aktualisieren. In diesem Fall kann ebenfalls ein Listenprinzip eingesetzt werden. Alle Operationen aus einem nicht autorisierten Profil werden abgelehnt.

- **Datensicherung**: Datenschutz ist in der Pharma- oder der Lebensmittelindustrie unerlässlich, da alles, was produziert oder verarbeitet wird, rückverfolgbar sein muss. Aber im Allgemeinen muss ein Industrieunternehmen angesichts eines Cyberangriffs in der Lage sein, seine Daten jederzeit wiederherzustellen und sie wieder in das IS einzuspeisen. In diesem Fall sind ein Backup, eine Archivierung der speicherprogrammierbaren Steuerungen (PLC) sowie ein Plan für die Wiederaufnahme des Betriebs (PRA) notwendig.

„Alle diese Schichten der Sicherheit sind Elemente einer umfassenden Verteidigung", unterstreicht Vincent Nicaise. Dieser Ansatz wird insbesondere von der französischen Agentur für die Sicherheit von Informationssystemen (ANSSI) vertreten, deren 2004 veröffentlichtes Memento weiterhin uneingeschränkt relevant ist.

IT MUSS OT VERSTEHEN

Die IT-Welt hält die OT-Welt oft für zu standardisiert, weil viele Normen eingehalten werden müssen. Wenn die IT jedoch das OT-Ökosystem und dessen Probleme versteht, kann sie sich als echter Mehrwert für letzteres erweisen. *„Die zu schützenden Elemente befinden sich manchmal an geografisch abgelegenen, fast unzugänglichen Orten: Es fehlt daher an Personal, an echten Fachkräften. Die einzigen Wartungskräfte vor Ort sind mit der Verwaltung der Firewalls betraut. Dies ist an sich schon ein Problem, da sie nicht über die erforderlichen Kenntnisse betreffend Netzwerke und Cybersicherheit verfügen, um defekte Geräte zu ersetzen. Einer unserer Kunden hatte dieses Problem: Stormshield hat gemeinsam mit den Integratoren ein spezielles Verfahren entwickelt, das dieser Herausforderung gerecht wurde*", freut sich **Khobeib Ben Boubaker**, Leiter der Sparte Industrial Security bei Stormshield. *„Ein anderer unserer Kunden, der unsere Endpoint-Lösung übernommen hatte, fragte sich, wie er sie bei einer Wartung ohne Fachkräfte vor Ort abschalten könnte. Die Idee bestand darin, eine bestimmte Datei auf einem USB-Stick zu speichern, der nur von unserer Lösung erkannt und von Lösungen anderer Anbieter nicht gelesen werden konnte. Unsere Lösung wurde dadurch während der Wartung zugänglich. Kleinigkeiten dieser Art, die in der IT üblich sind, helfen der OT sehr*."

„Wenn die IT-/OT-Governance vereinheitlicht ist, verzeichnet man eine bessere Integration der Cybersicherheit für industrielle Systeme."

Jean-Christophe Mathieu, Leiter der industriellen Sicherheit bei Orange Cyberdefense

In einem Webinar, das Krankenhausgebäuden gewidmet war, stellten wir die Frage, **wer für das OT-Netzwerk verantwortlich ist**. Zwei Drittel der Befragten meinten, die IT-Abteilung werde dieses operationelle Netzwerk verwalten und sich so mit dem Thema allmählich vertraut machen. Die mangelnde Zusammenarbeit zwischen IT- und OT-Teams ist jedoch ein Hindernis für die globale Cybersicherheit von Unternehmen, die ihre Konvergenz voll ausnutzen wollen, um ihre Wettbewerbsfähigkeit zu steigern. Jean-Christophe Mathieu zufolge „*werden die IT-Teams sehr oft mit den Themen rund um die Industriesicherheit beauftragt. OT ist jedoch ein Umfeld, mit dem die IT immer vertrauter wird, das sie aber noch nicht ausreichend kennt, um einseitig über die zu implementierenden Lösungen zu entscheiden. Damit sich die Cybersicherheit harmonisch in industrielle Systeme integrieren kann, müssen IT- und OT-Teams zusammenarbeiten.*“

Ist die größte Herausforderung der betrieblichen und industriellen Cybersicherheit letztlich nicht der Mensch? Der Dialog zwischen den IT-Teams mit ihrer Erfahrung in der Cybersicherheit und den OT-Teams als Spezialisten ihres operativen Netzwerks ist wohl entscheidend für höhere Sicherheit in der globalen Infrastruktur. Einige Industrieunternehmen scheinen verstanden zu haben, dass die industrielle Cybersicherheit kompetentere Teams voraussetzen. Sie ermutigen ihre CISOs, umfassendere Kenntnisse bezüglich der OT sowie der betrieblichen und organisatorischen Anforderungen dieser Systeme zu erwerben. Diese Anforderung spiegelt sich in der Ernennung des ersten OT-Referenten unter den CISOs wider. **Was wäre, wenn IT/OT-Konvergenz auch Konvergenz der Teams bedeuten würde?**

STORMSHIELD

Weltweit müssen Unternehmen, Regierungsinstitutionen und Verteidigungsbehörden die Cybersicherheit ihrer kritischen Infrastrukturen, sensiblen Daten und Betriebsumgebungen gewährleisten. Die auf höchster europäischer Ebene zertifizierten Stormshield-Technologien sind die richtige Antwort auf IT- und OT-Risiken und erlauben den Schutz der Geschäftstätigkeit. Unsere Mission: Cybersorglosigkeit für unsere Kunden, damit diese sich auf ihre Kerntätigkeiten konzentrieren können, die für das reibungslose Funktionieren von Institutionen, Wirtschaft und Dienstleistungen für die Bevölkerung so wichtig sind. Die Entscheidung für Stormshield ist eine Entscheidung für eine vertrauenswürdige Cybersicherheit in Europa. Weitere Informationen finden Sie unter www.stormshield.com.