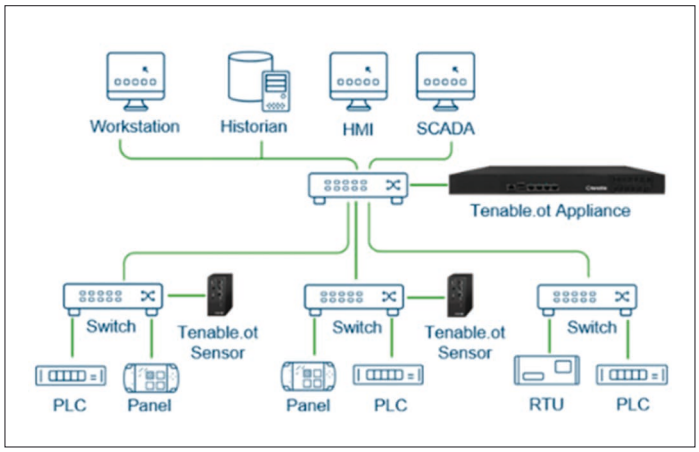
OT-Sicherheit weiterhin im Fokus

NIS2, vermehrter Einsatz von Sensoren und Vernetzung werden OT-Sicherheit in 2024 weiter in den Fokus rücken – Experten von Tenable erwarten vermehrte Angriffe auf IT/OT-Umgebungen



Vermehrte Cyberattacken auf Produktionsumgebungen (OT/Operational Technology) und deren Übergang zu IT-Umgebungen (IT/OT, IIoT) schärfen zunehmend das Bewusstsein für die Notwendigkeit hier die Sicherheitsvorkehrungen zu verschärfen. Zudem erhöhen rechtliche Vorgaben wie die NIS2 auch die Anforderungen seitens der Gesetzgeber.

Autoren:
Marty Edwards (li)
Deputy CTO of OT/IoT
Amir Hirsh (re)
Head of OT Security
www.tenable.com

„Angreifer verstehen das Ausmaß des Schadens, den sie OT-abhängigen Unternehmen, insbesondere in der Fertigungsindustrie, zufügen können. Daher werden sie im kommenden Jahr zunehmend diese lukrativen Ziele ins Visier nehmen – hauptsächlich mittels Ransomware. Das ist jedoch nicht die einzige Motivation. OT-Ziele verschaffen Angreifern auch ‚Markenbekanntheit' und Publicity, da diese Angriffe in der Regel öffentlichkeitswirksam sind.

Außerdem: Angesichts der zunehmenden Aufmerksamkeit und der steigenden Kosten und Strafen im Zusammenhang mit dem Energieverbrauch und den CO_2-Emissionen werden sich die Unternehmen einem intelligenteren Management ihrer Prozesse zuwenden, was den Einsatz von OT-basierten Sensoren und Kontrollen verstärken wird. Es werden immer mehr IoT- und OT-Geräte in intelligenten Gebäuden, im Fabrikmanagement und in Gebäudemanagementsystemen zum Einsatz kommen. Diese Trends werden Unternehmen weiteren Risiken aussetzen, da ihre Angriffsfläche größer wird und diese Umgebungen häufig mit dem Internet verbunden werden.

Alle Risiken betrachten

Erfolgreiche OT-Sicherheit erfordert die Betrachtung des gesamten Unternehmens, also aller Risiken, und das Herausfiltern derjenigen Risiken, die für die OT-Umgebung relevant und kritisch sind. Bei der OT-Sicherheit geht es nicht mehr nur um OT-Sicherheit. Unternehmen können ihre OT-Umgebung nicht sichern, wenn sie nur versuchen, OT-Daten zu schützen.

OT-Sicherheit wird weiterhin immer mehr IT-Sicherheitskonzepte umfassen und umgekehrt, während die Anbieter gängiger IT-Produkte OT-Sicherheitsfunktionen integrieren. Dies wird dazu führen, dass die Beziehung zwischen OT und IT in Zukunft weniger antagonistisch und mehr kooperativ sein wird."

Security-Hooks

OT-OEMs (z. B. Siemens, Honeywell, Rockwell Automation etc.) werden die Notwendigkeit erkennen, Security-Hooks in ihre Plattformen einzubauen, um die Abfrage von Sicherheitsinformationen von ihren Geräten zu erleichtern.

Beim OT-Schwachstellenmanagement wird man sich weniger um den Patch-Level oder die Firmware-Version des Geräts kümmern, sondern mehr um die kontextbezogene Nutzung des Geräts, um geeignete Maßnahmen zu ergreifen. Unternehmen werden nach ‚vorläufigen' Abhilfelösungen suchen, bis sie das betreffende geschäftskritische OT-Gerät patchen können.

Proaktive Sicherheit

Die erhöhte Sorgfaltspflicht, die von Cyberversicherungsanbietern verlangt wird, und die Veränderungen auf dem Cyberversicherungsmarkt werden den Druck auf Industrieunternehmen weiter erhöhen. Die Unternehmen sind aufgerufen, proaktiv mit ihrer Sicherheit umzugehen, anstatt reaktiv zu handeln und darauf zu warten, dass ein Vorfall eintritt, in der Hoffnung, dass die Versicherung ihn abdeckt. Cyberversicherer werden ihre Policen so einschränken, dass Zahlungen für Ransomware ausgeschlossen sind. Die Unternehmen werden gezwungen sein, andere Optionen für den Umgang mit diesem Risiko zu prüfen – sei es eine Selbstversicherung, ein proaktiver Ansatz, Systemredundanz oder anderes.

OT-Investitionen lohnen sich

CFOs und CISOs werden eine Kosten-Nutzen-Analyse der Investitionen in IT- und OT-Sicherheit durchführen und feststellen, dass sich Investitionen in OT im Jahr 2024 mehr lohnen als in IT. Für jeden Dollar, der in OT investiert wird, erhalten Unternehmen mehr, als wenn sie einen Dollar in IT-Sicherheit investieren würden. OT-Investitionen verringern das Risiko viel stärker als IT-Sicherheitsmaßnahmen.

Dienstleister für das OT-Segment

Mit dem zunehmenden Bewusstsein für OT-Sicherheit haben Dienstleister bereits begonnen, in dieses Geschäft einzusteigen und OT-Bewertungen und andere professionelle Dienstleistungen anzubieten. Dieser Trend wird sich 2024 noch verstärken, wenn ein wachsender Teil des OT-Geschäfts von globalen Systemintegratoren (GSI) und anderen Dienstleistern erbracht wird und das OT-Segment nicht nur als eigenständiges Produkt oder von kleinen Nischenanbietern bedient wird.

Mit der Notwendigkeit, immer mehr Vorschriften einzuhalten – und hier steht das Thema NIS2 im Fokus, dem Trend zu Cyberversicherungen, den Aktivitäten von Wirtschaftsprüfern und der Überwachung durch den Vorstand wird es eine Zunahme der Berichterstattung und Analyse des OT-Sicherheitsstatus geben. Dies wird nicht nur als Werkzeug zum Schutz der OT-Umgebung eingesetzt, sondern auch zur Berichterstattung über Status, Trends und Veränderungen im Laufe der Zeit."

Wer schreibt:

Tenable, Inc. ist spezialisiert auf Cyber Exposure-Lösungen. Als Erfinder von Nessus hat Tenable sein Fachwissen über Schwachstellen erweitert, um die weltweit erste Plattform zu liefern, die jedes digitale Asset auf jeder Computerplattform erkennen und schützen kann. ◄