Auf die Industrie zugeschnittene Cyber-Risikobewertung für sichere Digitalisierung

Die OTORIO-Risikobewertung ist ein umfassender und realistischer Ansatz zur Bewertung der Effektivität der digitalen Widerstandsfähigkeit der organisatorischen Produktion. Sie bewertet die Vorteile der Industrie 4.0 zusammen mit den Sicherheits- und Risikokosten. Das Ergebnis der Bewertung ist ein nach Prioritäten geordneter, potenziell auswirkungsreicher Reifeplan, der dazu dient, die Wahrscheinlichkeit, dass Angreifer in das OT-Netzwerk einbrechen und erfolgreiche Angriffe ausführen, erheblich zu verringern. Dadurch kann die Wahrscheinlichkeit für den Erfolg eines solchen Angriffes erheblich verringert werden.

Safe Industry 4.0 digitalization

Der Bewertungsbericht enthält einen maßgeschneiderten Aktionsplan, beginnend mit der kurzfristigen Verbesserung der organisatorischen und produktionstechnischen Sicherheitsvorkehrungen. Die OTORIO-Bewertungsteams entwerfen zusammen mit dem vom Kunden benannten operativen Kontaktpunkt auch einen langfristigen Cyber-Entwicklungsplan und unterstützen das Unternehmen auf seinem sicheren Weg zur Digitalisierung.

Der OTORIO-Prozess zur Bewertung industrieller Risiken ist auf die Anforderungen in der Produktion zugeschnitten, wobei die OT-Bedrohungsmodellierung, die Regulierungsanforderungen und die Risikobereitschaft des Managements in eine Cyber-Reife-Roadmap integriert werden. Unsere Bewertungsteams nutzen nationales Cyber-Fachwissen, um die Angriffsflächen der Organisation zu identifizieren und nach Angriffsvektoren, Bewertung der Bedrohungsmodellierung, einfacher Ausnutzung und potenziellen Auswirkungen auf Produktivität, Sicherheit und Zuverlässigkeit zu priorisieren.

OTORIOs IT-OT-Penetrationstest

In der heutigen, sich ständig verändernden digitalen Umgebung ist die traditionelle statische Modellierung einfach unwirksam. Praktische Penetrationstests (Hands-on Penetration Testing, PT) bieten einer Organisation einen “Realitätscheck” für Cyber-Bedrohungen, der zur Priorisierung von Abwehrmaßnahmen und zur Zuweisung von Ressourcen dient. Auf der Grundlage unübertroffener nationaler militärischer Erfahrungen beim Hacken missionskritischer Infrastrukturen haben die Teams von OTORIO einen maßgeschneiderten Ansatz für industrielle Penetrationstests entwickelt.

Die Testergebnisse werden in einem prägnanten Bericht präsentiert, der technische Angriffsvektoren im organisatorischen Sicherheitsprozess identifiziert und sie mit dem Geschäftsprozess in Beziehung setzt. Dadurch erhält der Endbenutzer einen effektiven Fahrplan zur Eindämmung von Angriffen

Vorteile

- Führt eine umfassende Bewertung der konvergierten IT-OT-Umgebung durch, einschließlich Netzwerk, Anlagen und Prozesse
- Erstellt einen maßgeschneiderten Entwicklungsplan für sicheres digitales Wachstum
- Erstellt einen Bewertungsbericht, der Lücken bei der Einhaltung von Vorschriften aufzeigt, mit einem klaren und präzisen Plan zur Erreichung der Einhaltung von Vorschriften (z.B. NIST, IEC 62443, NERC CIP, IMO)
- Setzt erstklassige, führende Hacker-Expertenteams ein, um realistische, rote Teambewertungen (Penetrationstests) durchzuführen, die die üblichen Bewertungsunterlagen ergänzen und eine Schätzung der tatsächlichen Sicherheitslage der Organisation erstellen.

Anwendungsfälle

- Identifizierung und Priorisierung von Cyber-Risiken in umsetzbare Elemente, um die Produktionskontinuität zu gewährleisten
- Durchführung von Lückenanalysen zur Einhaltung von Vorschriften als Teil der Unternehmensführung, des Risikomanagements und der Einhaltung von organisationsspezifischen und öffentlichen Vorschriften (GRC)
- Einsatz von Eindämmungskontrollen zur Verhinderung potenzieller Angriffe durch Vorwegnahme von Angriffsvektoren mit nicht-invasiven Angriffsszenarien
- Erstellung eines maßgeschneiderten Fahrplans für die Cyber-Entwicklung, um die Cyber-Resilienz der Organisation zu verbessern

Gefahrenquelle	Merkmale (Fähigkeit, Absicht und Zielrichtung, für feindliche Bedrohungen)
↓ Initiiert	
Bedrohungsereignis	Abfolge von Aktionen, Aktivitäten oder Szenarien
↓ nutz aus	
Schwachstellen	Schweregrad im Zusammenhang mit allgegenwärtigen prädisponierten Bedingungen und Sicherheitskontrollen
↓ verursachen	
Unerwünschte Auswirkungen	Bei Risiko eine Kombination von Auswirkung und Wahrscheinlichkeit
↓ erzeugen	
Risiko für Organisation	Auf organisatorische Operationen (Auftrag, Funktionen, Image, Ruf), Vermögenswerte, Personen, andere Organisationen und auf das Länderrisiko

Über OTORIO

OTORIO kombiniert die Berufserfahrung führender nationalstaatlicher Cyber-Sicherheitsexperten mit modernsten digitalen Risikomanagement-Technologien, um der Fertigungsindustrie ein Höchstmaß an Schutz zu bieten. OTORIOs automatisierte digitale risikobasierte Wartungslösung aggregiert die Analyse von Bedrohungsdaten, um tiefe Einblicke in industrielle Kontrollsysteme zu gewinnen, Risiken zu identifizieren und zu mindern, bevor sie Schaden verursachen. OTORIO versetzt Industrieunternehmen in die Lage, eine sichere Produktion zu implementieren, zu automatisieren und zu betreiben und so den Weg für eine sicherere, zuverlässigere und produktivere Industrie zu ebnen.

OTORIO - Anbieter von industrie-eigenen Cyber- und digitalen Risikomanagementlösungen

OTORIO kombiniert die Berufserfahrung führender nationalstaatlicher Cyber-Sicherheitsexperten mit modernsten digitalen Risikomanagement-Technologien, um der Fertigungsindustrie ein Höchstmaß an Schutz zu bieten. Die automatisierte digitale risikobasierte Wartungslösung von OTORIO aggregiert die Analyse von Bedrohungsdaten, um tiefe Einblicke in industrielle Kontrollsysteme zu gewinnen, Risiken zu identifizieren und zu mindern, bevor sie Schaden anrichten können. Unsere Cyber-Experten arbeiten eng mit den Cyber- und Betriebsteams unserer Kunden zusammen, um maßgeschneiderte Lösungen zu entwickeln, die ihren spezifischen industriellen Sicherheitsbedürfnissen entsprechend ihrem digitalen Reifegrad entsprechen. OTORIO versetzt Industrieunternehmen in die Lage, eine sichere Produktion zu implementieren, zu automatisieren und zu betreiben und so den Weg für eine sicherere, zuverlässigere und produktivere Industrie zu ebnen.