OT-Security neu gedacht:

Kontextbezogenes Exposure Management für direkte Resultate

WHITEPAPER

sure[secure] X securance

Einleitung

Analog zu immer komplexeren IT-Umgebungen wachsen auch OT-Umgebungen in ihrer Komplexität an. Erschwerend kommt hinzu, dass diese Umgebungen häufig historisch gewachsen sind und somit ein heterogenes Bild von state-of-the-art und legacy Systemen abgeben. Das führt dazu, dass OT-Umgebungen aufgrund von Fehlkonfigurationen oder menschlichen Fehlern zu bevorzugten Zielen für Cyberangriffe werden. Denn Cyberkriminelle wissen, dass sie hier den größtmöglichen Schaden anrichten können.

Um die OT-Herausforderungen zu bewältigen, ist es entscheidend, den Fokus auf praktische, kosteneffiziente Maßnahmen zu verlagern. Durch die Implementierung von Maßnahmen, die auf die realistischen Bedrohungen und Risiken der jeweiligen Umgebung zugeschnitten sind, können Unternehmen ihre Resilienz steigern, Risiken minimieren und einen unmittelbaren Mehrwert für den Schutz kritischer Vermögenswerte und die Gewährleistung der Kontinuität ihrer Lieferkette erzielen. Wir sprechen von **kontextbezogenem Exposure Management.**

Exposure Management im Kontext der OT-Security (Operational Technology Security) bezieht sich auf die Identifizierung, Bewertung und Reduzierung von Risiken und Schwachstellen in industriellen Steuerungssystemen und anderen OT-Umgebungen. Dies umfasst das Erkennen von Schwachstellen, Risikobewertung sowie Risikominderung.

Ziel ist es, die Angriffsfläche zu verkleinern und die Resilienz der OT-Systeme gegen Cyberbedrohungen zu erhöhen.

In Unternehmen mit OT-Umgebungen ist es die gemeinsame Aufgabe von OT- und IT-Teams, die vorhandenen Unternehmensdaten zu nutzen und sie zugänglich und nutzbar zu machen. Es wird erwartet, dass diese Zusammenarbeit in den kommenden Jahren weiter ausgebaut wird und zu einer Erweiterung der Sicherheitskontrollen beiträgt, da Anforderungen wie NIS2 nicht isoliert betrachtet werden können, insbesondere im Hinblick auf die Reaktion auf Sicherheitsvorfälle.

Ein Blick auf den Status-Quo: Herausforderungen der traditionellen Cybersicherheit in OT-Umgebungen

Ein paar Herausforderungen haben wir bereits skizziert und wollen diese nun etwas näher betrachten.

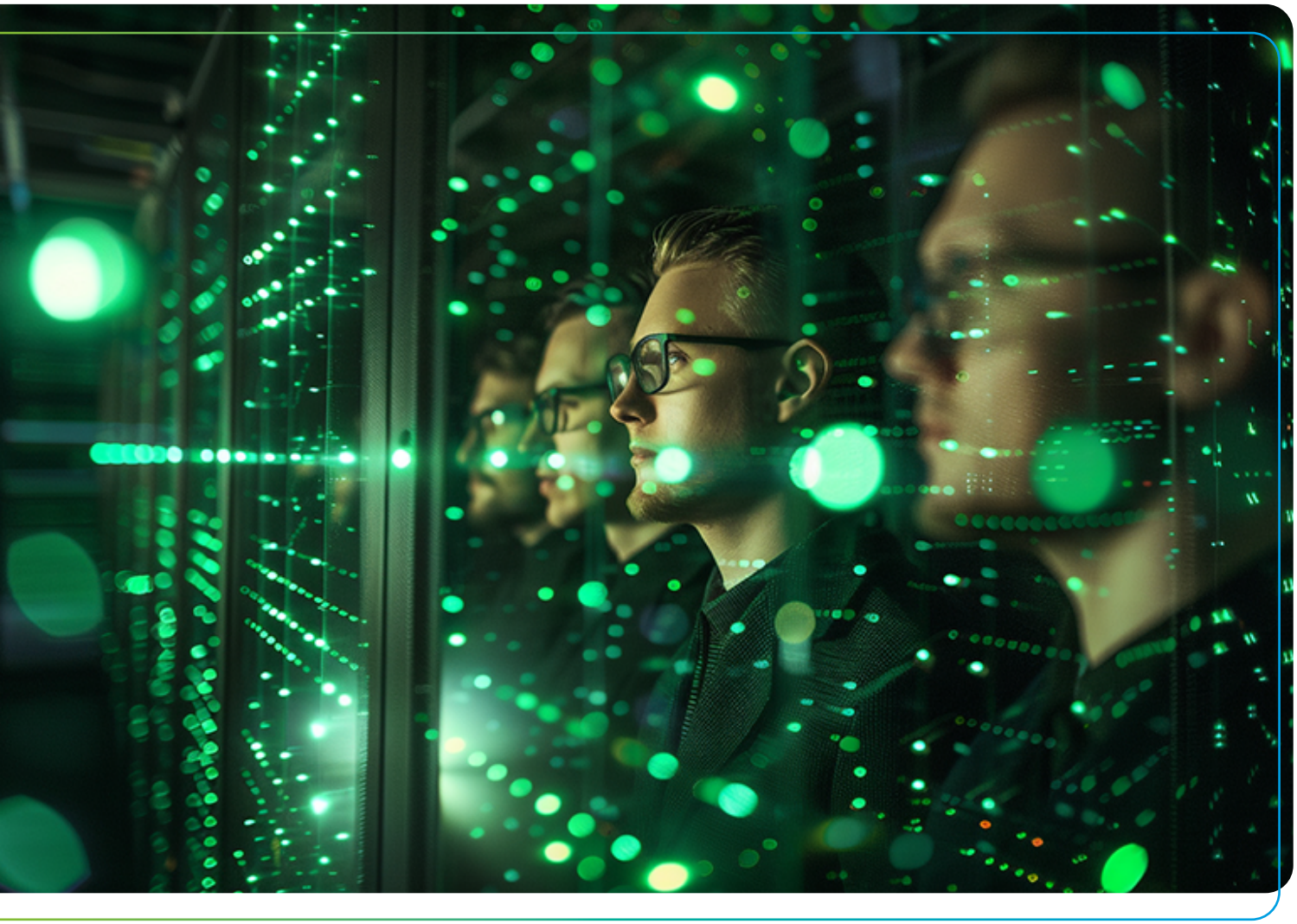
- **IT-Praktiken sind in OT-Umgebungen kaum anwendbar.**
  Das führt zu fehlender Visibilität.
  Ein Punkt, warum wir perspektivisch auch OTler benötigen. OT-Umgebungen zeichnen sich häufig durch Altsysteme, Echtzeit-Betriebsanforderungen und strenge Sicherheits- und Zuverlässigkeitsanforderungen aus, was maßgeschneiderte Sicherheitsansätze erforderlich macht. Herkömmliche Sichtbarkeitstools decken OT-Umgebungen nicht umfassend ab, was es schwierig macht, Schwachstellen zu identifizieren, zu priorisieren und wirksam zu beseitigen. Diese fehlende Visibilität macht es nahezu unmöglich, ein Monitoring aufzusetzen, da es immer bestehende Blind-Spots gibt.

- **Schwachstelle erkannt, Gefahr trotzdem nicht gebannt.**
  Die Behebung von Schwachstellen in OT-Systemen ist aufgrund von Bedenken hinsichtlich der Systemzuverlässigkeit und Betriebsunterbrechungen nahezu unmöglich, was die Schwachstellenschuld noch vergrößert. Denn kommt es in Produktionsstätten zu Ausfällen, entsteht schnell ein gigantischer Schaden. Die Implikationen sind selten klar, sodass lieber dem laufenden System – trotz erkannter Schwachstelle – vertraut wird.

Zwo, Eins, Risiko. Priorisierung und Quantifizierung:

Unternehmen haben Schwierigkeiten, Risiken effektiv zu quantifizieren und zu priorisieren. Der Kontext der betrieblichen Rolle einer Anlage und ihrer Konnektivität beeinflusst das Risiko erheblich, wird aber bei herkömmlichen Ansätzen oft übersehen. Denn es macht schon einen erheblichen Unterschied, welcher Alarm in welcher Region aufgerufen wird. So kann z. B. ein häufiger Log-in-Versuch entweder eine Brute-Force-Attacke oder aber ein User sein, der gerade sein Passwort vergessen hat. Ein Security-Alert, der anschlägt, weil ein bestimmtes Protokoll auf einem Server aktiviert wurde, kann harmlos sein – ist in einem Kontext aber vielleicht kritisch.

Das klingt super trivial – ist es in der Regel aber nicht. Denn die Skalierung von Cybersicherheitsmaßnahmen über verschiedene Infrastrukturen hinweg erfordert erhebliche Investitionen, Zeit und eben Ressourcen.



Und der Kontextbezug löst alle Probleme? Jein.

Gerade bei knappen Ressourcen ist ein effizienter Einsatz dieser wichtig. Wenn wir also von Kontextbezug sprechen, dann heißt das, dass Alarme nicht einfach Alarme sind, sondern immer im relevanten Kontext betrachtet werden sollten. Damit das gelingen kann, wird Technologie benötigt. Die Verwendung einer einheitlichen Plattformlösung verbessert den Schutz und die Resilienz von OT-Umgebungen. Diese Systeme ermöglichen es, auf spezielle Herausforderungen einzugehen und konzentrieren sich auf ganz spezifische Schwachstellen und Bedrohungen.

Der initiale Aufwand zur Konfiguration bildet dann die Basis für eine deutliche Reduzierung der Aufwände im weiteren Verlauf. Dafür ist es nämlich unter anderem essentiell, eine Bestandsaufnahme unter Kontextbezug durchzuführen. Das bildet die Basis, um z. B. Prioritäten und die Kritikalität bestimmter Events zu definieren. Zudem gibt es weitere Punkte, wo einheitliche Plattformlösungen unterstützen können.

- **Visibilität und Identifizierung:**
  Die automatisierte, kontextbezogene Erkennungstechnologie bietet einen umfassenden Einblick in OT-Umgebungen und identifiziert und bewertet Anlagen auf der Grundlage ihrer betrieblichen Rolle und potenziellen Auswirkungen auf das Geschäft.
- **Schwachstellenmanagement:**
  Modernste Tools für das Schwachstellenmanagement automatisieren die Identifizierung, Priorisierung und Behebung von Schwachstellen auf der Grundlage kontextbezogener Geschäftsauswirkungen und minimieren so das Cyberrisiko.
- **Verbesserte Risikominderung und Ressourcenoptimierung:**
  Hochentwickelte Methoden zur Risikoquantifizierung bewerten die potenziellen Auswirkungen von Cyber-Bedrohungen auf kritische Anlagen, so dass Unternehmen ihre Bemühungen zur Risikominderung effektiv priorisieren können.
- **Berücksichtigung von Betriebskontinuität, Sicherheit und Umweltaspekten:**
  Die Anpassung von Cybersicherheitsstrategien an die spezifischen Anforderungen der OT-Umgebung trägt zur Aufrechterhaltung der Betriebskontinuität, zur Minimierung von Ausfallzeiten und zur Gewährleistung eines sicheren und umweltfreundlichen Betriebs bei.
- **Einhaltung von Richtlinien und Vorschriften:**
  Ein automatisiertes Exposure Management hilft Unternehmen bei der Einhaltung spezifischer Cybersicherheitsvorschriften und -standards, um rechtliche Strafen zu vermeiden und ihren Ruf zu verbessern.

Strich drunter:

Dieser Ansatz zur OT-Cybersicherheit durch maßgeschneiderte Lösungen für das Exposure Management stellt einen grundlegenden Wandel dar, der in der heutigen dynamischen Bedrohungslandschaft notwendig ist. Durch die Festlegung von Prioritäten für umsetzbare Schutzmaßnahmen auf der Grundlage einer kontextbezogenen Bestandsaufnahme und eines automatisierten Exposure Managements können Unternehmen ihren Schutz vor Cyber-Bedrohungen effektiv verbessern.

Der Kontext ist entscheidend: Vorhandene Unternehmensinformationen werden genutzt, um sie für OT-Teams zugänglich und umsetzbar zu machen. Dieser Ansatz befasst sich mit den spezifischen Risiken und Schwachstellen, die jeder Betriebsumgebung innewohnen, wobei der Schwerpunkt auf der Verfügbarkeit liegt.

Kontextbezogenes Exposure Management bietet eine praktische und kosteneffiziente Lösung für die sich entwickelnden Herausforderungen der betrieblichen Cybersicherheit, die Absicherung kritischer Anlagen, den Schutz der Lieferkette und die Verbesserung der allgemeinen Cybersicherheitsresilienz in der heutigen dynamischen Welt der Betriebstechnologie.

Fragen? Uwe freut sich über deine Kontaktaufnahme.

LASS UNS GERNE SPRECHEN:

Uwe Grunwitz
Head Of OT-Security

Telefon: +49 (0) 2156 959 45 87
E-Mail: uwe.grunwitz@suresecure.de

suresecure GmbH
Dreischeibenhaus 1
40211 Düsseldorf

Telefon: +49 (0) 2156 974 90 60

E-Mail: kontakt@suresecure.de
www.suresecure.de