Industrial Cyber Defence

ERHÖHEN SIE DIE WIDER-STANDSFÄHIGKEIT IHRER PRODUKTION – MIT DETEKTION UND REAKTION

DIGITAL Trust.

Im Zuge der Digitalisierung werden Cloud-, IT- und OT-Umgebungen (Operational Technology) von Industrie- und Produktionsanlagen zunehmend vernetzt – und eröffnen damit neben zahlreichen Vorteilen für die Unternehmen gleichzeitig auch Cyberkriminellen völlig neue Angriffsvektoren. Mit einem Basisschutz allein ist es nicht mehr getan.

Damit Angriffe schnell erkannt und eingedämmt werden können, noch bevor hoher Schaden entsteht, sollten existierende Schutzmaßnahmen um Visibility-, Detektions- und Reaktionsfunktionen erweitert werden. Effektiven Schutz bieten beispielsweise Monitoring- und Managementlösungen aus dem IT-Umfeld, die auf OT-Umgebungen adaptiert wurden.

Ein willkommener Nebeneffekt: Die Monitoring-Systeme verschaffen nicht nur in Echtzeit einen Überblick über die Informationssicherheit der Produktionsumgebung, sondern unterstützen zudem Betriebsprozesse wie zum Beispiel die Anreicherung und automatisierte Pflege des Asset Managements.

NETZWERKZUGANGSKONTROLLE IN DER PRODUKTION – STUFENWEISE VON DER TRANSPARENZ BIS HIN ZU AUTORISIERTEN ZUGRIFFEN

Computacenter stellt mit einem eigens für die Produktion entwickelten Lösungsdesign eine Basis für ein stufenweises Implementierungsmodell für Netzwerkzugangskontrolle und -transparenz bereit. Da sich häufig beim Thema Netzwerkzugangskontrolle die beiden Anforderungen Security und Verfügbarkeit auszuschließen scheinen, empfiehlt es sich, nach und nach Workflows zu implementieren, die sich an spezifischen Anwendungsfällen orientieren. So lässt sich sukzessive Vertrauen in die Schutzmaßnahme gewinnen und erkennen, dass beides geht: Verfügbarkeit erhalten und gleichzeitig die Sicherheit erhöhen.

So sind Produktionsleiter:innen und deren Teams in der Lage, Veränderungen (z. B. neuer Teilnehmer, Austausch oder Umzug eines Teilnehmers, Wartungstechniker:innen) zu erkennen und mit geeigneten Maßnahmen zu reagieren. Bei Bedarf können weitere Sicherheitsmaßnahmen wie eine gezielte Überwachung bestimmter Netzwerkbereiche oder Teilnehmer sowie eine aktive Zugriffssteuerung implementiert werden. Die als „Nebenprodukt" gesammelten Daten lassen sich zudem einem Asset-Management-System zur Verfügung stellen.

OT VULNERABILITY MANAGEMENT

Schwachstellenmanagement in der OT stellt aufgrund der funktionalen und technologischen Heterogenität der Umgebungen meist eine größere Herausforderung dar als in der IT. Bei Bedarf können Unternehmen

Prävention ist gut, aber nur durch die Detektion von Security-Vorfällen lassen sich langfristige Schäden vermeiden. Um Cyberkriminelle dauerhaft auszuschließen, bedarf es einer Response-Strategie, die nicht nur auf der Wiederherstellung von Systemen basiert!

Rainer Leisen
Solution Manager Industrial Security

daher bei Computacenter auf ein dediziertes Team von erfahrenen Industrial-Security-Fachleuten zurückgreifen, das die Komplexität über alle Domänen hinweg managen kann und die verschiedenen Phasen eines Schwachstellen-Management-Programms begleiten sowie durchführen kann:

- Bewertung von Assets auf bekannte Schwachstellen
- Priorisierung von Schwachstellen basierend auf Risiko und Auswirkung
- Ableitung von einem Maßnahmenkatalog: Behebung von Schwachstellen oder mitigierende Maßnahmen

Computacenter unterstützt Unternehmen anschließend auf Wunsch bei der Umsetzung der unternehmensindividuell sinnvollen Maßnahmen und kann auch hier wieder auf die Breite und Tiefe seines Portfolios zurückgreifen. So profitieren Sie von einem ganzheitlichen Security-Ansatz, bei dem alles aus einer Hand kommt – von Planung über Umsetzung bis hin zum Betrieb.

ICS-MONITORING

Visibilität und Detektion lassen sich mit der Einführung eines ICS-Monitoring-Systems (Industrial Control System) herstellen: Die zumeist passiven erhobenen Daten werden nicht nur für den Betrieb eines Asset Managements gewonnen, sondern auch für die Schwachstellenanalyse Ihrer Infrastruktur genutzt. Darüber hinaus können die Detektionsfunktionen auch gewollte, aber ungeplante Änderungen – beispielsweise beim Instandhaltungsprozess – erkennen und dokumentieren. Auf diese Weise hilft ein ICS-Monitoring nicht nur bei der Security, sondern auch, die betrieblichen Prozesse zu optimieren.

Doch gerade der Markt im ICS-Monitoring-Bereich ist zurzeit sehr dynamisch, sodass die Produktauswahl für unsere Kunden sehr herausfordernd ist. Umso wichtiger ist es, den Anforderungskatalog an die Produkte nicht nur anhand des Funktionsumfangs zu bestimmen, sondern auch die betrieblichen Aspekte wie zum Beispiel die Analyse der Sicherheitslage zu berücksichtigen. Dabei sollten die für den Anwendungsbereich von den Cyberkriminellen verwendeten Angriffstechniken beziehungsweise deren Ausnutzung von Schwachstellen im Vordergrund stehen.

SIEM SOC

Um Angriffspfade zu verschleiern und unbemerkt ins Unternehmen einzudringen, führen Cyberkriminelle Attacken oft über verschiedene Ebenen der IT und OT aus. Daher ist es für Industrieunternehmen umso wichtiger, über beide Welten eine durchgängige Transparenz zu erhalten.

Eine Ausrichtung des SIEM (Security Information and Event Management) an dem neuesten MITRE ATT&CK Framework für industrielle Steuerungen ist hierbei unablässig, um unternehmens- und branchenspezifische Angriffsmuster effizient und effektiv zu erkennen. Zudem verschafft das zusätzliche Mapping unserer eigenen Use-Case-Datenbank mit MITRE den von uns betreuten Unternehmen einen Vorsprung, indem Angriffserkennungen noch schneller und passgenauer implementiert werden können.

Ein weiterer Vorteil der Use-Case-Datenbank: Neben dem klassischen Fokus auf Security sind auch Anwendungsfälle aus dem Produktionsbetrieb enthalten. So kann mit den gewonnen Prozessdaten eine vorausschauende Wartung (Predicitive Maintenance) realisiert oder auch die Produktivität gesteigert werden, indem sich die Ursachen für Verfügbarkeitsverluste analysieren lassen. Mit Einführung dieser Sicherheitsmaßnahmen können Sie deutlich das Level Ihrer Security erhöhen und proaktiv der aktuellen Bedrohungslage begegnen.

Sie möchten mehr erfahren?
Sprechen Sie gern Ihr Account Management an oder kontaktieren Sie uns über
www.computacenter.com/de

Computacenter

Computacenter AG & Co. oHG
Computacenter Park 1, 50170 Kerpen