

CYBERSECURITY-KANAL ZWISCHEN IT & OT

Die steigenden Cyber-Angriffe auf den Maschinenbau erfordern eine proaktive Herangehensweise an die Sicherheit. Die neue NIS-2 Richtlinie und Maschinenverordnung unterstreichen die Dringlichkeit dieser Aufgabe. Die TG alpha GmbH, Schwesterfirma der T&G Automation GmbH, bietet dazu mit alphaWatch und alphaShark benutzerfreundliche und hochwirksame Lösungen für Intrusion Detection – zu erfahren auf der SPS.

In einer zunehmend vernetzten Welt sehen sich Maschinenbauunternehmen mit einer wachsenden Bedrohung konfrontiert: Cyberangriffen. In diesem Kontext gewinnt die NIS-2 der EU große Bedeutung. Sie stellt sicher, dass kritische Infrastrukturen, einschließlich der Maschinenbauindustrie, angemessen gegen Cyber-Bedrohungen geschützt sind und verpflichtet Unternehmen dazu per Gesetz, robuste Cyber-Sicherheitsmaßnahmen zu implementieren und Sicherheitsvorfälle zu melden. Zieht man weitere Regularien, Richtlinien und Gesetze in Betracht, so kommen jedoch nicht nur auf die Betreiber von Anlagen erweiterte und zum Teil neue Vorgaben zu, sondern auch als Lieferant sind Nachweise über die eigene Absicherung gegenüber Cyber-Angriffen nachzuweisen. So betrachtet die neue Maschinenverordnung 2023/1230 nun auch den Aspekt der Cyber-Sicherheit und ist somit zwingend für die CE-Kennzeichnung.

Herausforderungen im Maschinenbau

Die Herausforderungen, denen sich der Maschinenbau in Bezug auf Cyber-Sicherheit gegenüberstellt, sind vielfältig. Erstens haben viele Produktionsanlagen eine lange Lebensdauer, was bedeutet, dass ältere Maschinen oft nicht von Haus aus mit modernen Sicherheitsprotokollen ausgestattet sind. Zweitens ist die Integration von IoT-Geräten in industrielle Netzwerke zwar vorteilhaft, erweitert jedoch auch die Angriffsfläche. Drittens sind Cyber-Angriffe immer raffinierter und entwickeln fortgeschrittene Techniken, um Schwachstellen auszunutzen.

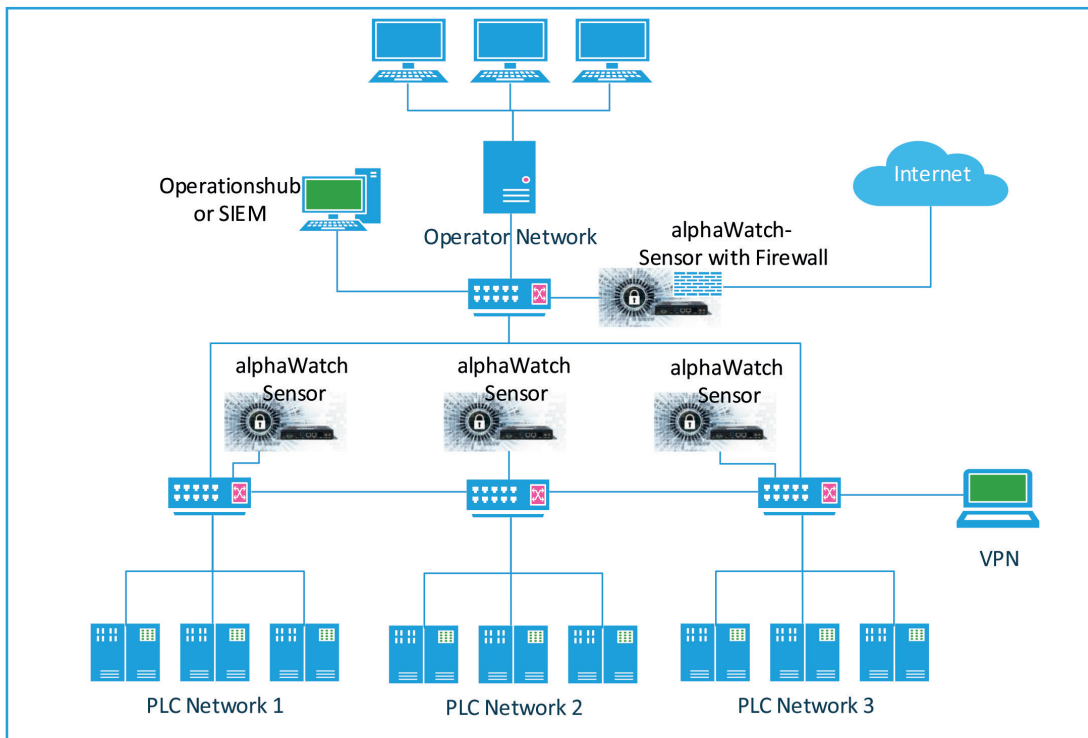
Mit alphaShark bietet TG alpha eine Lösung für das umfassende Assetmanagement im Bereich der Cyber-Sicherheit. Es bietet die Möglichkeit, alle Netzwerkteilnehmer zu inventarisieren und übersichtlich in einer Liste oder einem Netzwerkgraphen darzustellen. Dies beinhaltet nicht nur Endgeräte wie PLCs und Server, sondern auch Router, Switches und andere Netzwerkgeräte sowie IoT-Komponenten. Und das Hersteller- und Maschinenaufbau-unabhängig. Die grafische Netzwerkübersicht von alphaShark visualisiert die Verbindungen zwischen den Geräten und erleichtert so das Verständnis der Netzwerkstruktur. Tagesaktuelle Auswertungen für verschie-

dene Anwendergruppen, ob Shopfloor, Leitungsebene oder Geschäftsführung werden automatisiert und nach individuellen Wünschen konfiguriert. Darüber hinaus können Exportmöglichkeiten der generierten Auswertungen bequem als PDF-Datei oder im JSON-Format exportiert werden. Dies ermöglicht eine nahtlose Integration der Daten in bestehende Security Information- und Event Management (SIEM)-Systeme sowie die weitere Verwendung für gezielte Sicherheitsanalysen. Damit bietet alphaShark eine zuverlässige Lösung, um proaktiv auf potenzielle Sicherheitsbedrohungen reagieren zu können und die Netzwerk-Integrität zu schützen und stellt damit ein sich in jedem Fall rechnendes Investment dar, das eigene Unternehmen sowie dessen Maschinen und Anlagen vor Cyber-Gefahren zu schützen.

Echtzeit-Absicherung der Maschine per alphaWatch

alphaWatch ist eine hochmoderne Lösung von TG alpha für Intrusion Detection (IDS), die speziell auf die Bedürfnisse des Maschinenbaus zugeschnitten ist. Sie unterstützt dabei den vorgenannten Herausforderungen zu begegnen und bietet die Möglichkeit, Angriffe auf industrielle Netzwerke von Stunde null an zu erkennen und unverzüglich zu melden. Ein entscheidender Vorteil von alphaWatch ist seine Flexibilität und Benutzerfreundlichkeit. Das System kann sowohl als Hardware- als auch als Softwarelösung bereitgestellt werden, je nach den individuellen Unternehmensanforderungen. Die Installation und Konfiguration sind einfach umzusetzen und erfordern keine speziellen Cyber-Sicherheitskenntnisse.

alphaWatch überwacht ein Netzwerk kontinuierlich und erkennt Anomalien automatisch. Das System erstellt ein detailliertes Profil des normalen Netzwerkverhaltens und warnt sofort, wenn es Abweichungen feststellt. Dies ermöglicht eine schnelle Reaktion auf potenzielle Bedrohungen, bevor diese Schaden anrichten können. Diese Anomalie-Erkennung beruht auf dem White-Listing Ansatz, der besonders in stationären Netzwerken, wie sie in der Industrie und Produktion verwendet werden, effizient ist. Hierbei wird im System sowohl automatisch als auch individuell vermerkt, welche Netzwerkteilnehmer „erlaubt“ sind und welche Kommunikationsparameter – wie



Möglicher Aufbau eines alphaWatch-Systems, das Angriffe von Stunde null an erkennt und meldet.

z. B. Kommunikationsrichtung oder Protokoll-Paketgröße – die entsprechenden Verbindungen definieren. Als eine weitere Option kann das alphaWatch-System durch ein Black-Listing erweitert werden. Durch dieses Verfahren kann das Netzwerk auf bekannte Vulnerabilities und bekannte Risikofaktoren überprüft werden. Die schnelle Erkennung von Angriffen ist entscheidend. alphaWatch benachrichtigt Sicherheitsteams in Echtzeit über mögliche Bedrohungen, sodass sie sofortige Maßnahmen ergreifen können, um den Angriff zu stoppen und Schäden zu minimieren.

Investment

Die steigenden Cyber-Angriffe auf den Maschinenbau erfordern eine proaktive Herangehensweise. Die neue NIS-2 Richtlinie und Maschinenverordnung unterstreichen die Dringlichkeit. alphaWatch bietet eine benutzerfreundliche und hochwirksame Lösung für Intrusion Detection, die es Maschinenbauern ermöglicht, sich vor Cyber-Bedrohungen zu schützen und sicherzustellen, dass ihre Produktion reibungslos verläuft.

www.tug.at • Halle 5, Stand 158