IT&Production E-PAPER

SONDERTEILE, BRANCHENSPECIALS, THEMENSCHWERPUNKTE



Bild: ©Ayse/stock.adobe.com

SONDERTEIL

Cybersecurity

Software - Konzepte - Prävention

25 JAHRE IT&Production



Die erste Plattform, um Ideen sichtbar zu machen

25 Jahre IT&Production – in einer Branche, die sich rasanter entwickelt als kaum eine andere, ist das eine beeindruckende Wegmarke. In dieser Zeit haben wir technologisch viel erlebt: von den Anfängen, als Planungsentscheidungen oft lange dauerten und endgültig galten, bis hin zu heute, wo Vernetzung, Echtzeitzugriff auf viele Devices, Automation auf mehreren Ebenen und KI eine neue Flexibilität ermöglichen.

IT&Production war dabei stets mittendrin: ein Medium, das früh die richtigen Themen aufgegriffen hat – selbst als virtuelle Inbetriebnahme noch wie Science-Fiction klang. Für uns war es oft die erste Plattform, auf der wir unsere Ideen sichtbar machen konnten. Vielen Dank für die tolle Zusammenarbeit! Wir wünschen IT&Production weiterhin die richtige Mischung aus technischer Tiefe, journalistischem Gespür und dem Mut, auch unbequeme Fragen zu stellen – und natürlich ein glückliches Händchen für die nächsten 25 Jahre!

Beate Maria Freyer
CEO

Machineering GmbH & Co.KG



Security Operations Center: Ansätze im Vergleich

Eine Kommandozentrale für die Cybersicherheit

Die Integration von Soft- und Hardware der Informationstechnologie (IT) in Umgebungen der Operational Technology (OT) schafft neue Angriffsvektoren für Hacker. Die Einbindung von Produktionssystemen in die IT-Infrastruktur von Unternehmen bringt spezifische Herausforderungen mit sich, die mit traditionellen Sicherheitsansätzen oft nicht adäquat adressiert werden können. Security Operations Center unterstützen hier.

Der Schutz von Anlagen, Systemen, Maschinen und Netzwerken gegen Cyber-Bedrohungen ist komplex, da verschiedene Sicherheitsebenen koordiniert werden müssen – von Management-Level IT über die Produktionsplanung und Steuerung bis hin zu OT-Systemen auf Feldebene. Diese mehrstufige Architektur erfordert spezialisiertes Knowhow.

Jedoch fehlt es an qualifizierten Fachkräften mit kombinierter IT-, OT- und Cybersecurity-Expertise. Dieser Skill-Gap gilt als Haupttreiber für die Nachfrage nach externen Sicherheitslösungen. Darüber hinaus verschärft sich die regulatorische Landschaft kontinuierlich. Die NIS-2 Richtlinie und nationale Verordnungen zum Schutz kritischer Infrastruktur wie NERC, CIP oder KRITIS in Deutschland erweitern die Compliance-Anforderungen erheblich und gehen weit über traditionelle IT-Security hinaus.

Security Operations Center

Um diesen Herausforderungen zu begegnen sind Security Operations Center (SOC) ein Ansatz. Ein SOC fungiert als Kommandozentrale für die kontinuierliche Überwachung, Analyse und Reaktion auf Sicherheitsereignisse. Zu den Kernfunktionen gehören das Security-Monitoring, also die kontinuierliche Überwachung der IT/OT-

Bilder der Doppelseite: Siemens AG

Umgebung zur Aufdeckung verdächtiger Aktivitäten, Threat Detection durch Korrelation multipler Indikatoren, Triage sowie Incident Response. Darüber hinaus unterstützen SOCs Unternehmen bei der Compliance mit Sicherheitsregulierungen.

Für ein SOC für die OT bieten sich zwei Ansätze an:

- Auf die OT fokussierte SOC-Services: Dieser Ansatz konzentriert sich primär auf die Cybersecurity von OT-Umgebungen und IT-Systemen im OT-Bereich. Das Servicemodell bietet konfigurierbare Standard-Service-Verträge mit definierten Service Level Agreements, Compliance-Beratung und Support durch spezialisierte Dienstleister.

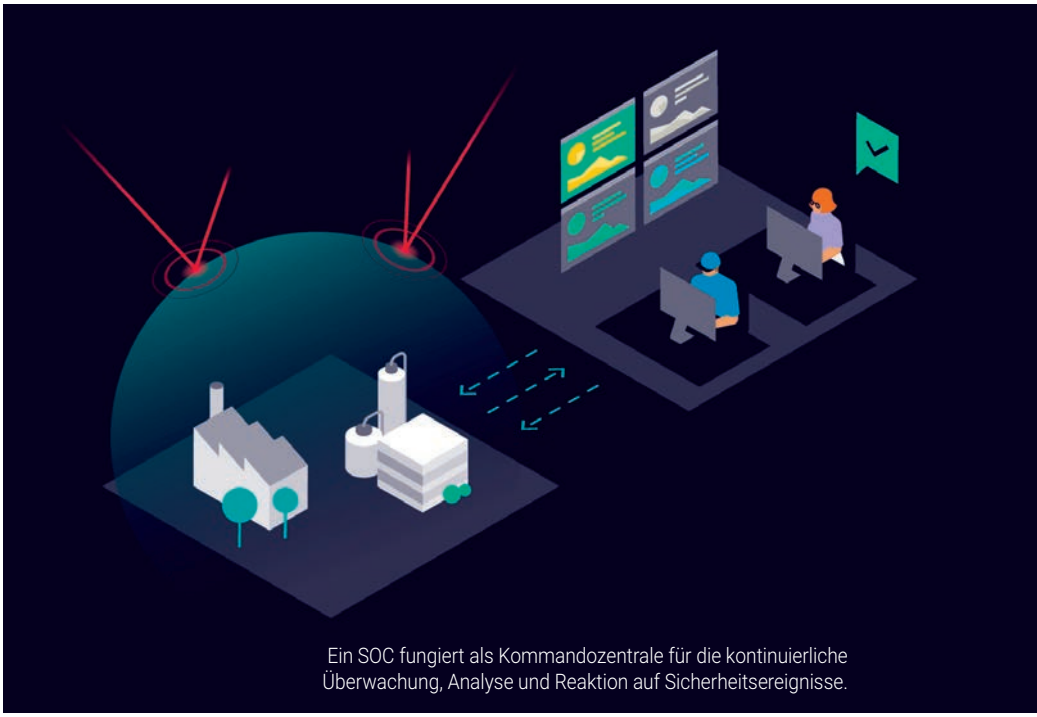
- Konvergierte IT und OT-SOC-Services: Diese umfangreichere Variante beschreibt die Integration des Sicherheitsmanagements der IT und OT vom Sensor in der Fabrik bis zum Konzernrechenzentrum und der Office IT in ein SOC. Das Modell bietet IT/OT-Sicherheits-Operations, Compliance-Unterstützung und ein einheitliches Reporting.

Anstatt interne Teams für Rund-um-die-Uhr-Überwachung aufzubauen, können Unternehmen ein ausgelagertes IT/OT SOC nutzen und auf skalierbare Expertise zugreifen.

Technische Architektur und Implementierung

Grundlegende Systemarchitektur: Beide SOC-Servicemodelle basieren auf einer einheitlichen technischen Architektur. Eine skalierbare, cloudbasierte CMDB (Configuration Management Database) und SIEM-Plattform (Security Information and Event Management) bildet das Rückgrat für die Sammlung der Daten der OT-Geräte in Produktionsnetzwerken, das Event Processing, Incident Response und Reporting.

Spezialisierte OT-Überwachung: Herzstück der OT-Sicherheit sind industrielle Intrusion-Detection-Systeme. Diese erfassen industrielle Kommunikationsprotokolle passiv und analysieren sie, ohne Produktionsprozesse zu beeinträchtigen. Die Systeme erkennen Anomalien in der OT-Kommunikation und melden verdächtige Aktivitäten an das übergeordnete SOC.



Ein SOC fungiert als Kommandozentrale für die kontinuierliche Überwachung, Analyse und Reaktion auf Sicherheitsereignisse.

Strukturierter Implementierungsprozess: Die Einführung erfolgt in definierten Phasen. Zunächst werden IT/OT-Diagnose-Checks und Asset-Identifikationen durchgeführt. Anschließend erfolgt das Deployment von OT-Sensoren in den Netzwerksegmenten. Parallel werden Backup- und Restore-Verfahren etabliert sowie Vulnerability-Management implementiert.

Incident Response: Im Ernstfall analysieren spezialisierte SOC-Teams kritische Vorfälle, während Experten in den Kundenregionen lokale Unterstützung und, wenn gewünscht, Incident Response und Recovery bereitstellen. Dieser hybride Ansatz verbindet globale Security-Expertise mit lokalem Industrial Operations-Knowhow.

SOC-Services von Siemens

Siemens bietet sowohl ein auf die OT fokussiertes Security Operations Center as a Service (SOCaaS) als auch einen umfassenderen, konvergierten IT/OT SOC-Ansatz in Kooperation mit Accenture an.

Das Siemens OT SOCaaS konzentriert sich auf das Sicherheitsmanagement von OT-Systemen und IT-Komponenten in der OT-Umgebung mit flexiblen, standardisierten Serviceverträgen und wird durch Remote Industrial Operations Services als zentrale Anlaufstelle bereitgestellt. Der IT/OT-SOC-Ansatz ermöglicht vollständige IT/OT-Konvergenz mit flexibler Vertragsgestaltung und umfassender Compliance-Unterstützung.

Durch die Kombination von OT-Domainexpertise und IT-Security-Knowhow entstehen Servicemodelle, die die spezifischen Anforderungen der digitalen Transformation adressieren. Die steigenden Zahlen von IoT-Endpunkten und Cyber-Angriffen, kombiniert mit verschärften Compliance-Anforderungen bringen traditionelle Sicherheitsansätze an ihre Grenzen. SOC-Services bieten hier eine Möglichkeit, die bewährte IT-Security-Prinzipien mit spezialisierter OT-Expertise kombiniert. ■

Daniel Leese
Product Portfolio Manager
Digital Maintenance and Operations
Siemens AG
www.siemens.com

Identitäten werden 2025 zum zentralen Angriffsvektor

Wenn 2024 als Jahr des Comebacks der Ransomware galt, dann war 2025 das Jahr, in dem Angriffe gezielt auf Identitäten gerichtet waren. Das schreibt OpenText in der Pressemitteilung zur Veröffentlichung des jährlichen Nastiest Malware Report. Demnach drangen Cyberkriminelle nicht mehr nur in Netzwerke ein, sondern griffen gezielt Identitäten an. Social Engineering, Deepfakes und KI-gestützte Chattools verwandelten alltägliche Kommunikation in Angriffsvektoren. Gestohlene Passwörter oder abgefangene Anrufe reichten oft für den Zugriff auf interne Systeme. Mit künstlicher Intelligenz, die Phishing, Stimmklonen und gefälschte Vorstellungsgespräche ermöglicht, wurde Cyberkriminalität zu einem Instrument der Identitätsmanipulation. Angreifer verwendeten legitime Zugangsdaten und umgingen damit klassische Sicherheitsmechanismen. Ransomware erzielte keine neuen Rekorde, der Markt blieb aber auf hohem Niveau stabil.



Bild: ©MK-Photo/stock.adobe.com

Die Erpressungsökonomie setzte weniger auf Brute-Force-Verschlüsselung, sondern auf gestohlene Daten und Druckmittel. Als besonders auffällige Angreifer nennt der Bericht Qilin (Agenda). Die Gruppe verursachte über 200 bestätigte Angriffe auf Krankenhäuser, Labore und kommunale Einrichtungen. In einem Fall führte der Ausfall von Diagnosediensten zum Tod eines Patienten. Als ebenfalls besonders aktiv schätzt OpenText Akira ein. Deren Angriffe fokussierten sich auf Unternehmen und Managed Service Provider. Sie war für nahezu jeden fünften Ransomware-Vorfall weltweit verantwortlich. Scattered Spider gehörte 2025 ebenfalls zu den einflussreichsten Gruppen. Durch Social Engineering, SIM-Swapping und Deepfake-Stimmen kompromittierte die Gruppe Unternehmen und umging Zugriffssysteme.

www.opentext.com

Wie Cyberkriminelle KI einsetzen

Die Google Threat Intelligence Group (GTIG) gibt in ihrem aktuellen AI Threat Tracker einen Überblick darüber, wie Cyberkriminelle künstliche Intelligenz (KI) einsetzen. Der Analyse zufolge haben sich die KI-gestützten Fähigkeiten von Bedrohungsakteuren deutlich weiterentwickelt. Laut GTIG-Analyse nutzen Angreifer künstliche Intelligenz nicht mehr nur zur Steigerung ihrer Produktivität, sondern experimentieren mit neuen Funktionen und Szenarien. Sie setzen in aktiven Kampagnen neuartige, KI-gestützte Malware ein, die in der Lage ist, das Angriffsverhalten während der Ausführung dynamisch zu verändern. Diese Veränderung hat sich nach Angaben der GTIG in den letzten Monaten vollzogen.


Bild: ©DC Studio/stock.adobe.com

cloud.google.com

BSI-Lagebericht zur Cybersicherheit

Die Widerstandsfähigkeit kritischer Infrastrukturen nimmt zu, Deutschland ist im digitalen Raum jedoch weiterhin verwundbar. Bundesinnenminister Alexander Dobrindt und die Präsidentin des Bundesamtes für Sicherheit in der Informationstechnik (BSI), Claudia Plattner, haben dies bei der Vorstellung des BSI-Jahreslageberichts zur Cybersicherheit deutlich gemacht. Dieser kommt zu dem Schluss, dass viele digitale Systeme, Server und Online-Dienste weiterhin unzureichend geschützt sind. Webanwendungen sind laut Bericht besonders häufig schlecht geschützt, auch Server sind oft falsch konfiguriert oder ungeschützt, und bekannte Sicherheitslücken werden oft zu spät oder gar nicht behoben. So ist die Zahl der täglich neu entdeckten Schwachstellen zwischen Juli 2024 und Juni 2025 um 24 Prozent gestiegen. Im Durchschnitt bedeutet das 119 weltweit bekannt gewordene Schwachstellen pro Tag. Ein Grund dafür: durch die Digitalisierung kommen neue internetbasierte Anwendungen und Systeme hinzu.



Bild: ©InfiniteFlow/stock.adobe.com

www.bsi.bund.de



WISSENS-VORSPRUNG NUTZEN

WIE OT-SECURITY IN KMUS GELINGEN KANN

Neue Gesetze, mehr Angriffe, weniger Schutz: Mit dem Whitepaper zum Thema „OT-Security in Produktionsanlagen" bringen produzierende KMUs Ihr Security-Wissen auf den aktuellen Stand – inklusive Vorgehensmodell! So kommen sie vom Wissen ins Handeln!

Rotkäppchen-Mumm setzt auf Tenable OT Security

Schwachstellen risikobasiert gemanagt

Jetzt anhören!



- Symbolbild -

Der Sekt- und Spirituosen-Hersteller Rotkäppchen-Mumm setzt auf Tenable OT Security, um Schwachstellen in der hochkomplexen Produktionsumgebung zu identifizieren. Die gemeinsam mit dem Leipziger Tenable Partner WBS IT-Service (WBS) implementierte Software priorisiert das Schwachstellen-Management risikobasiert und unterstützt so einen sicheren, performanten und NIS-2-konformen Betrieb.

Der Schutz der Produktivsysteme vor externen Angriffen nimmt bei Rotkäppchen-Mumm von Beginn an einen hohen Stellenwert ein. Mit der NIS-2, die ursprünglich bereits im Oktober 2024 umgesetzt werden sollte und deren Allgefahrenansatz klar die Operational Technology (OT) einschließt, hat das Thema aber ein neues Maß an Brisanz erhalten: „Als Hersteller von Nahrungsmitteln und Roh-Alkohol sind wir gleich doppelt von der NIS-2 betroffen. Um der risikobasierten Ausrichtung der Richtlinie gerecht zu werden, entschieden wir uns, im ersten Schritt die unternehmensweite Schwachstellen-Analyse in den Fokus zu rücken - und evaluierten die auf dem Markt verfügbaren Produkte", erklärt CISO Max Gutberlet. „Dabei suchten wir eine zuverlässige, skalierbare und ganzheitliche Plattform, die Schwachstellen nicht nur identifizieren, sondern auch fundiert nach ihrem Business Impact priorisieren sollte."

Detaillierte Inventarisierung im ersten Anlauf

Im ersten Proof-of-Concept evaluierte Rotkäppchen-Mumm zunächst eine Reihe nativer OT-Security-Anbieter. Weil sich deren auf passives Scanning von OT-Netzwerken ausgelegte Systeme aber bereits bei der Inventarisierung schwer taten, wurde kurzfristig Tenable eingeladen und setzte die Teststellung binnen zwei Wochen am Standort Nordhausen auf Anhieb um. Das Werk betreibt den breitesten Maschinenpark aller Standorte und hat neben Hightech-Anlagen auch Legacy-Systeme aus den 1980er-Jahren im Einsatz. Tenable OT Security lieferte bereits nach kurzer Feinjustierung ein detailliertes Inventar. Dieses enthielt neben der Liste der Systeme viele Detailinformationen zur Software, den Versionen und den Schwachstellen des Equipments und legte damit ein robustes Fundament für die Absicherung der Umgebung.

„Als wir die ersten Ergebnisse der Tenable Analyse erhielten, sahen wir sofort, dass die Lösung eine um ein Vielfaches höhere

Bild ©Dmitry/stockadobe.com

Informationsmenge lieferte als die vorher getesteten Systeme", so Max Gutberlet. „Es war faszinierend, was wir schon in dieser frühen Phase an Informationen aus dem System extrahieren konnten."

Weitere Standorte angebunden

Rotkäppchen-Mumm entschied sich, den Proof-of-Concept zeitnah in den Echtbetrieb zu überführen und zog den langjährigen Tenable Partner WBS hinzu, um den Rollout zu begleiten. Die Leipziger Netzwerk- und Security-Experten entwickelten anschließend in enger Zusammenarbeit mit Rotkäppchen-Mumm und Tenable ein detailliertes Deployment-Konzept. Maik Oettler, Technical Sales Manager bei WBS IT-Service, erinnert sich: „Insgesamt galt es, eine Vielzahl von Sensoren sowie mehrere hundert Assets zu implementieren. Besonders spannend war dabei der Einsatz von Sensorik mit 10-GBit-Interfaces – eine Herausforderung, für die wir gemeinsam mit dem Kunden eine passende Lösung finden konnten." Mit den Automatisierungsfeatures der Tenable OT Security ließ sich die Umsetzung anschließend zügig realisieren. So konnte Rotkäppchen-Mumm innerhalb weniger Monate alle deutschen Standorte – und mit der Prosecco-Manufaktur Ruggeri die erste internationale Produktionsstätte – anbinden. Flankierend dazu unterstützte WBS das Team von Rotkäppchen-Mumm bei der kaufmännischen Projektabwicklung und der vergleichsweise komplexen Lizenzierung.

Einsatz in der Praxis

Der Nutzen von Tenable OT Security zeigte sich etwa als Rotkäppchen-Mumm in Freyburg eine fabrikneue Dosieranlage für Chemikalien in Betrieb nahm. Obwohl das System frisch vom Hersteller geliefert worden war, schlug Tenable OT Security bereits während der Erstinstallation Alarm – mit kritischen Warnmeldungen an den CISO und den OT-Verantwortlichen. Ein kurzer Check belegte, dass ein Teil der Steuersysteme massive Sicherheitslücken aufwies, für die seit Jahren Patches verfügbar sind. Die Schwachstellen konnten durch das Aufspielen aller erforderlichen Updates behoben werden. Ohne Tenable OT Security wäre die Produktionsumgebung aber unweigerlich angreifbar geworden.

Positive Projektbilanz

Die erste Bilanz von Max Gutberlet fällt positiv aus: „Als Mittelständler mit einer hochkomplexen IT, aber äußerst begrenzten Personalressourcen, achten wir bei der Auswahl unserer Systeme akribisch auf einen hohen Grad an Automatisierung und Autarkie. Die Systeme müssen zuverlässig für sich selbst laufen, ohne dass wir täglich manuell eingreifen müssen. Und genau das hat Tenable OT Security geschafft." ■

Tenable Inc.
de.tenable.com

- Anzeige -

ECOS Technology GmbH

Vernetzte Industrie – aber sicher!



Bild: ©Pugun & Photo Studio/stock.adobe.com

IoT- und OT-Infrastrukturen absichern: Für Industrieunternehmen eine wichtige Herausforderung. Unterschiedlichste Geräte, Smart Devices, Dienste, Prozesse und Sensoren müssen sicher und geschützt kommunizieren können. Und auch KI-Agenten müssen authentifizierbar sein und zuverlässig in Zero Trust-Architekturen eingebunden werden – Stichwort „Industrial AI".

Digitale Maschinenidentitäten für Industrial Cybersecurity

Mit der ECOS TrustManagementAppliance (TMA) steht eine hochintegrierte PKI- und Key-Management Lösung zur Verfügung, die digitale Zertifikate und Schlüssel automatisiert erstellt, verteilt und verwaltet. Sie eignet sich für klassische OT-Umgebungen ebenso wie für den hochskalierenden IoT-Bereich. Unternehmen schaffen damit die Basis für vertrauenswürdige Infrastrukturen – und können gleichzeitig das Fundament legen, um regulatorische Anforderungen wie NIS-2 und CRA zu erfüllen.

Zertifikate direkt im Produktionsumfeld ausrollen

Für (verteilte) Produktionsumgebungen, Auftragsfertiger und Standorte mit eingeschränkter Netzverfügbarkeit ist die Erweiterung TMA Edge Gateway konzipiert. Die kompakte Softwarelösung für das Ausrollen und Verwalten von digitalen Zertifikaten kann direkt auf Edge Devices eingesetzt werden und bietet breite Protokoll- und Schnittstellenunterstützung (OPC UA/GDS, MQTT/HTTPS/TLS, SCEP/EST/ACME/CMP, REST-API).

ecos

Kontakt

ECOS Technology GmbH
Sant' Ambrogio-Ring 13A-b • 55276 Oppenheim
Tel.: +49 6133 939-222
info@ecos.de
www.ecos.de/iot

Nachrüstbare Sicherheits-Kits für Embedded-Systeme

Sicherheitsupdate per Retrofit

Artikel anhören!



Embedded-Systeme erfordern beim Thema Cybersicherheit eine spezielle und oft aufwendigere Herangehensweise. Ihr Schutz ist aber nicht weniger wichtig und teils auch vorgeschrieben. Hier können Security-Upgrade-Kits auf MicroSD-Karten unterstützen.

Embedded-Systeme sind Hard- und Software-Komponenten, die in andere technische Geräte, Maschinen oder Systeme integriert sind, um innerhalb dieser bestimmte Aufgaben zu erfüllen, wie etwa die Steuerung von Robotern. In ihren Aufgaben unterscheiden sie sich wenig von klassischen IT-Systemen. Im Gegensatz zu diesen erfordern Embedded-Systeme jedoch spezielle Sicherheitsmaßnahmen. Denn sie können sowohl digital als auch physisch angegriffen werden, was die Angriffsfläche signifikant erhöht. Beispielswiese muss ein effektiver Schutz in diesem Fall auch Zugangskontrollen umfassen. Außerdem ist der Produktlebenszyklus von Embedded-Systemen im Vergleich zu ähnlichen Technologien sehr lang – oft mehrere Jahrzehnte – während die Weiterentwicklung von Angriffsmethoden wie auch Schutzmaßnahmen gegen diese neuen Angriffsvektoren viel schneller und dynamischer abläuft. Dies lässt sich oft nur schwer in Einklang bringen. Daher werden Embedded-Systeme in manchen Fällen nie aktualisiert und mit effektiven Schutzmaßnahmen ausgestattet.

Nicht zuletzt gestaltet sich der eigentliche Update-Prozess von Embedded-Systemen in vielen Fällen aufwendig, da diese Systeme oft nur schwer zugänglich und über viele einzelne Standorte verteilt sind. Außerdem sind sie oft aufgrund ihres Alters, ihren spezifischen Architekturen und Betriebssystemen sowie der begrenzten Speicher- und Rechenleistung der eingebetteten Hardware wenig anpassungsfähig. Dies schränkt die Updates und Sicherheitsfunktionen ein, die nachträglich hinzugefügt werden können.

Gesetzliche Regularien

Aufgrund ihrer Bedeutung für die Kontinuität wichtiger Prozesse in Industrie, Produktion und kritischen Infrastrukturen existieren für Embedded-Systeme zahlreiche gesetzliche Regularien, die ihren Schutz vorschreiben. In der EU umfassen die Regularien etwa die Radio Equipment Directive (RED), die zweite EU-Richtlinie zur Netzwerk- und Informationssicherheit (NIS2) sowie den Cyber Resilience Act (CRA), der Ende 2024 in Kraft trat. Ein oft gefordertes zentrales Prinzip im Rahmen verschiedener Cybersicherheits- und Compliance-Regelwerke sowie Industrienormen und Standards ist 'Security by Design'. Dies bedeutet, dass Sicherheit von Anfang an in die Architektur eines Systems eingebettet sein muss.

Update per MicroSD-Karte

Für im Einsatz befindliche Embedded-Systeme ist 'Security by Design' aus verschiedenen Gründen schwierig umzusetzen. Ein Komplettaustausch dieser Systeme ist jedoch ebenfalls oft nicht wirtschaftlich und führt fast immer zu Systembrüchen. Eine Möglichkeit ist die Nachrüstung mit einem Security Upgrade-Kit etwa in Form einer MicroSD-Karte, die in Bestandssystemen die vorhandene, oft unsichere Speicherkarte ersetzt. Die MicroSD-Karte des Security Upgrade-Kits nutzt einen speziellen Security Flash-Controller. Mit diesem lassen sich auch ältere Embedded-Systeme ohne größeren Aufwand mit modernen Sicherheitsfunktionen ausstatten. Dazu zählen etwa Hardware-basierte Zugriffskontrolle, Echtzeit-Datenverschlüsselung mit AES 256, individuelle Entwicklung von Schutzprofilen, Kopierschutz für sensible Daten, sicheres Löschen sensibler Informationen, Schutz der Systemintegrität sowie Secure Boot. Der integrierte Controller übernimmt dabei sämtliche Aufgaben, die das Host-System nicht selbst ausführen kann.

Eine zusätzliche Sicherheitsebene bieten Upgrade-Kits mit integriertem Sicherheitselement (Secure Element), das als Kryptografie-Controller fungiert und Aufgaben übernimmt, die sonst ein Trusted Platform Module (TPM) bereitstellen würde, wie etwa die Verschlüsselung von ein- und ausgehendem Datenverkehr. Gleichzeitig dient es als fälschungssicherer digitaler Ausweis des Systems im Netzwerk zur eindeutigen Identifikation. Da diese sicherheitskritischen Funktionen auf einer jederzeit austauschbaren Speicherkarte hinterlegt sind, lassen sie sich flexibel weiter nachrüsten, um neuen Cyberbedrohungen und regulatorischen Anforderungen gerecht zu werden. ■

Roland Marx
Senior Product Manager für Embedded IoT Solutions
Swissbit AG
www.swissbit.com

Bild ©Veronika/stock.adobe.com

Cybersecurity in der Produktions-IT: Ganzheitliche Sicherheit als Schlüssel zur resilienten Fabrik

Die Digitalisierung der industriellen Fertigung bringt enorme Effizienz, aber auch neue Risiken. Produktionssysteme, Maschinen und IT-Landschaften wachsen immer stärker zusammen. Damit wächst auch die Angriffsfläche für Cyberkriminelle. Spätestens seit den gezielten Angriffen auf industrielle Steuerungen wissen Unternehmen: Ohne eine ganzheitliche Sicherheitsarchitektur ist die Smart Factory verwundbar.



Bild: SPIRIT/21 GmbH

Viele Produktionsumgebungen (OT) wurden ohne Fokus auf IT-Sicherheit entwickelt. Steuerungen, SPS-Systeme oder SCADA-Komponenten basieren häufig auf älteren Betriebssystemen, die keine Sicherheitsupdates mehr erhalten. Gleichzeitig bestehen vielfältige Schnittstellen zu ERP-Systemen, Lieferantenportalen oder Cloud-Plattformen – und genau hier entstehen Einfallstore für Angreifer. Besonders kritisch: In der OT zählt Verfügbarkeit oft mehr als Sicherheit. Updates lassen sich im laufenden Betrieb kaum einspielen, da jeder Stillstand Kosten verursacht. Zudem erschwert die organisatorische Trennung von IT und OT eine durchgängige Sicherheitsstrategie. Das Ergebnis: fehlende Transparenz und hohe Risiken für Produktion und Lieferkette.

Zero Trust, SIEM und SOC – Bausteine moderner Security

Ein zeitgemäßer Schutzansatz muss IT und OT gemeinsam betrachten. Bewährt hat sich hier das Zero-Trust-Modell: „Never trust, always verify". Es setzt auf kontinuierliche Prüfung aller Zugriffe – ob durch Mitarbeitende, Maschinen oder externe Partner. Identitäten, Geräte und Berechtigungen werden dynamisch bewertet, bevor eine Verbindung zugelassen wird. Ergänzend sammelt und korreliert ein Security Information and Event Management (SIEM) Log- und Sicherheitsdaten zentral, um verdächtige Aktivitäten frühzeitig zu erkennen. Im Security Operations Center (SOC) analysieren Spezialisten diese Daten in Echtzeit, reagieren auf Vorfälle und sorgen mit Hilfe automatisierter Alarme und klar definierter Response-Prozesse für proaktiven Schutz.

Wie der IT-Dienstleister zum Sicherheitsfaktor wird

Ein erfahrener IT-Dienstleister kann Unternehmen gezielt entlasten – besonders bei fehlenden internen Ressourcen. Der Einstieg erfolgt meist über eine umfassende Security-Analyse der gesamten Produktionsumgebung. Diese zeigt auf, wo Risiken bestehen, welche Systeme priorisiert werden müssen und wie Zero Trust, SIEM und SOC sinnvoll integriert werden können. Ein Managed SOC übernimmt anschließend 24/7-Monitoring, Incident Response und kontinuierliche Optimierung. So erhalten Unternehmen Transparenz über ihre IT- und OT-Sicherheitslage, ohne eigene Expertenteams aufbauen zu müssen.

Sicherheit als Basis für digitale Wettbewerbsfähigkeit

Cybersecurity ist heute kein isoliertes IT-Thema mehr, sondern integraler Bestandteil der digitalen Produktion. Nur wer IT und OT ganzheitlich schützt – idealerweise mit einem erfahrenen Partner – schafft die Grundlage für resiliente Prozesse, planbare Sicherheit und nachhaltigen Erfolg in der vernetzten Industrie.

SPIRIT/21
IT that works.

Kontakt

SPIRIT/21 GmbH
Otto-Lilienthal-Straße 36 • 71034 Böblingen
Tel.: +49 7031-209-3333
info@spirit21.com
www.spirit21.com/de

25 JAHRE IT&Production



Früher unterschätzt, heute unverzichtbar

In den vergangenen 25 Jahren hat sich die industrielle IT von einem Nischenthema zu einem entscheidenden Innovationstreiber entwickelt. Was früher oft unterschätzt wurde, ist heute unverzichtbar für die Wettbewerbsfähigkeit der gesamten Industrie. Lösungen wie MES, ERP oder PLM sind längst zu einem integrierten digitalen Ökosystem zusammengewachsen. Zukunftstechnologien wie künstliche Intelligenz und virtuelle Zwillinge stehen sinnbildlich für diesen Wandel. Sie unterstützen Unternehmen dabei, Prozesse digital durchzuspielen, fundierte Entscheidungen zu treffen und die Wettbewerbsfähigkeit nachhaltig zu sichern – nicht nur einzelner Unternehmen, sondern der gesamten Branche.

IT&Production hat diesen Wandel nicht nur begleitet, sondern maßgeblich mit Orientierung, Weitblick und dem frühzeitigen Aufgreifen von Trends geprägt. Damit leistet das Magazin einen wertvollen Beitrag für eine Industrie, die heute weit mehr betrifft als die reine Produktion: Sie liefert Antworten auf die großen Herausforderungen unserer Zeit.

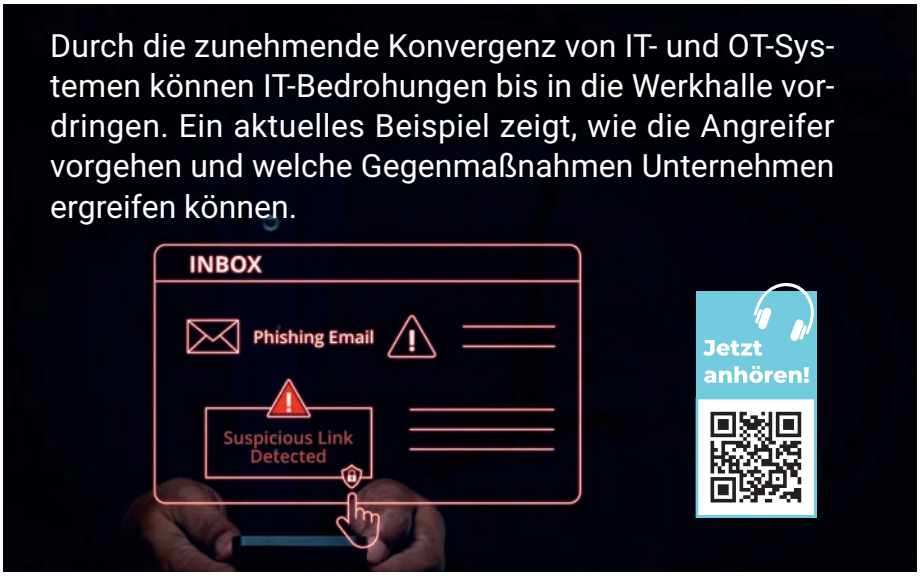
Jeroen Buring
Senior Director

Dassault Systèmes Deutschland GmbH

Angriffsmethoden und Schutzmechanismen

WENN SOCIAL ENGINEERING DIE PRODUKTION GEFÄHRDET

Durch die zunehmende Konvergenz von IT- und OT-Systemen können IT-Bedrohungen bis in die Werkhalle vordringen. Ein aktuelles Beispiel zeigt, wie die Angreifer vorgehen und welche Gegenmaßnahmen Unternehmen ergreifen können.



Im August traf einen europäischen Industriekonzern in Asien ein Angriff, der harmlos wirkte: Eine Chat-Nachricht über WhatsApp, getarnt als Stellenbeschreibung mit ZIP-Archiv, entfaltete beim Öffnen eine perfide Kette. Ein PDF-Viewer lud zusammen mit einer manipulierten Bibliothek Schadcode nach – das sogenannte DLL-Sideloading. So entstand eine Hintertür ins Unternehmensnetz. Von dort aus spionierten die Angreifer, weiteten Rechte aus und stahlen Daten. Hinter dem Angriff steht mutmaßlich die nordkoreanische Gruppe 'Lazarus'. Der Fall zeigt typische Schwachstellen moderner Produktionsbetriebe: die enge Verknüpfung von IT und OT sowie die Abhängigkeit von Standardsoftware, die sich leicht missbrauchen lässt.

Warum Produktionsbetriebe betroffen sind

Angriffe beginnen selten in der Werkhalle, enden aber oft dort. Angreifer nutzen Menschen, Kommunikations-Apps und alltägliche Dokumente, um in wertschöpfende Bereiche vorzudringen. Wer die Schnittstelle zwischen IT und OT kontrolliert, beeinflusst Taktzeiten, Rezepturen und Qualitätsdaten. Genau hier setzen Angreifer an – und genau hier braucht es Schutz.

Legitime Tools, illegitime Zwecke

Im geschilderten Fall wurde nicht die PDF-Datei selbst, sondern ein präpariertes Viewer-Paket (legitimer Reader plus manipulierte Bibliothek) ausgeführt und lud unbemerkt Schadcode nach. Betriebssysteme vertrauen signierten Programmen, und viele Unternehmen schränken das Nachladen von Bibliotheken nicht ein. Der Schadcode etablierte eine Verbindung zu C2-Servern (Command-and-Control) und folgte einem bekannten Muster: Nutzer ausspähen, Systeme analysieren, Daten und Zugänge sichern. In schlecht segmentierten Netzen reichen bereits wenige Schritte, um OT-nahe Systeme wie Historian-Server oder Wartungsgateways zu erreichen.

Wechselnde Werkzeuge, bleibende Muster

Gruppen wie Lazarus nutzen verschiedene Loader und RATs (Remote-Access-Trojaner), die über legitime Web-Dienste kommunizieren,

Bild ©LAONG/stock.adobe.com

Dateien verschieben, Befehle empfangen und Spuren verwischen. So nutzte der auf Windows-Servern entdeckte RAT 'Kaolin' kompromittierte SharePoint- oder WordPress-Instanzen als Zwischenstation. Andere Tools erscheinen in neuen Varianten, ändern aber nur die Oberfläche und Datenübertragung, um unentdeckt zu bleiben. Entscheidend bei der Abwehr ist nicht der Name, sondern die Prozesskette: Social Engineering, Initialausführung in vertrauenswürdigen Prozessen, unauffällige C2-Kommunikation, schrittweise Rechteausweitung, laterale Bewegung und zielgerichtete Exfiltration.

Ein falscher Klick kann ausreichen

In der Fertigung verstärkt die OT/IT-Konvergenz das Risiko. Produktionsanlagen sind oft länger im Dienst als Bürorechner, Patches lassen sich nicht jederzeit einspielen, und Fernwartungen sind unverzichtbar. Wird ein Office-Client zum Einfallstor, laufen Angriffe entlang identitätsbasierter Vertrauensbeziehungen weiter: Ein Domain-Admin mit Zugriff auf Dateiserver besitzt oft auch administrative Rechte auf Maschinen, die historisch ins Active Directory eingebunden wurden. Wenn hier strikte Zonen- und Conduits-Konzepte nach IEC62443 fehlen, reicht ein falscher Klick, damit ein Office-Vorfall die Prozess-IT berührt.

Mögliche Schutzmechanismen

Eine Schutzkette muss den Angriffsfluss an mehreren Stellen unterbrechen, ohne den Betrieb zu stören. Der erste Schritt: Angriffe an den üblichen Kommunikationskanälen verhindern. So sollten Chat- und Mail-Gateways Dateien grundsätzlich in isolierten Umgebungen prüfen. Ebenso sinkt die Trefferquote von Ködern, wenn neu aufbereitete, potenziell gefährliche Inhalte in sichere Formate überführt werden (Content Disarm & Reconstruction). Wo immer möglich, sollten ausführbare Anhänge aus kollaborativen Kanälen gesperrt oder mit manuellen Freigabeschritten versehen werden. Parallel begrenzen AppLocker- und WDAC-Profile (Windows Defender Application Control) die Möglichkeit, fremde Bibliotheken in legitime Prozesse einzuschleusen. Mit einer streng selektierten Positivliste samt sauber dokumentierten Ausnahmen lässt sich DLL-Sideloading auf breiter Front verhindern.

Der zweite Schutzwall betrifft Identitäten und Berechtigungen. In vielen Industrienetzen existieren noch immer gemeinsame Admin-Konten oder technische Benutzer mit Rechten über Office und OT hinweg. Eine Trennung der Identitäten, dedizierte Jump-Hosts (abgesicherte Übergabepunkte zwischen Netzwerkzonen) und 'Tiering-Modelle' für Administratoren erschweren laterale Angriffe. Multifaktor-Authentifizierung hilft wenig, wenn ein kompromittierter Prozess ohnehin lokal mit hohen Rechten läuft. Deshalb sind Just-in-Time-Privilegien, kurzlebige Tokens und eine strikte Sitzungsüberwachung entscheidend. Eine gehärtete Softwareverteilung und kontrollierte Skriptausführung verhindern zudem, dass Angreifer Standard-Tools für ihre Zwecke missbrauchen.

Der dritte Schutzriegel liegt in der Sichtbarkeit. Ein modernes SOC benötigt Messdaten aus der Nähe kritischer Prozesse. Während Prozessdaten tabu bleiben, liefern Anmelde-, Prozess-, DNS-, Proxy- und PowerShell-Logs aus OT-nahen Zonen, wertvolle Hinweise zur Identifikation typischer Muster. IOA und IOC (Indicators of Attack/Compromise) für verdächtige Viewer/DLL-Kombinationen, ungewöhnliche Verbindungen zu Cloud-Diensten oder auffällige ZIP-/PDF-Kaskaden sollten kontinuierlich überwacht werden. Ein Incident-Response-Playbook (IR-Playbook) muss zudem die Realitäten des Schichtbetriebs abbilden: Wer darf wann welche Anlage in welchen Zustand versetzen? Wie koordiniert man Lieferanten? Welche Notfallmaßnahmen halten die Produktion im Degradationsmodus stabil?

Nachweisbar sicher und auditfest handeln

Regulatorische Vorgaben helfen, den Aufwand zu rechtfertigen. Der Ende Juli vom Bundeskabinett vorgelegte Entwurf des NIS2-Umsetzungsgesetzes (NIS2UmsuCG) verlangt etwa nachweisbare Sicherheitsmaßnahmen und ein belastbares Incident-Management. Zudem nimmt der ab Dezember 2027 vollständig geltende Cyber Resilience Act (EU-Verordnung zur Produktsicherheit) Hersteller und Betreiber in die Pflicht, Sicherheitsprozesse, wie Software-Bill-of-Materials (SBOM) und Patch-Prozesse nachvollziehbar zu führen. IEC62443 bietet den Rahmen, um Zonen, Übergänge, Rollen und technische Kontrollen zu definieren. Unternehmen, die den beschriebenen Fall als Blaupause für ihre Gefährdungsanalyse nutzen, können Maßnahmen direkt auf Governance-Pflichten abstimmen und so Budget, Prioritäten und Messpunkte festlegen.

Klare Regeln

Der wichtigste Hebel ist die Kultur im Unternehmen. Statt aus dem Bauch heraus auf Links und Anhänge zu reagieren, müssen Mitarbeitende einfachen und verbindlichen Spielregeln folgen. Empfehlenswert sind realistische Übungen mit Chat- und Meeting-Ködern, um den Blick zu schärfen, denn dadurch werden Auffälligkeiten früher erkannt und sofort gemeldet. Für Dateien, Links und Bewerbungsunterlagen in Chat-Kanälen gelten klare Do's and Don'ts, damit niemand unter Zeitdruck allein entscheiden muss. Die Technik ist dabei so eingestellt, dass riskante Aktionen standardmäßig gebremst werden ohne den Arbeitsfluss aufzuhalten, etwa durch das Öffnen von Anhängen in einer sicheren Umgebung oder zusätzliche Bestätigungen. Das macht Angriffe langsamer und teurer für die Angreifer.

Social-Engineering-Ketten schwächen

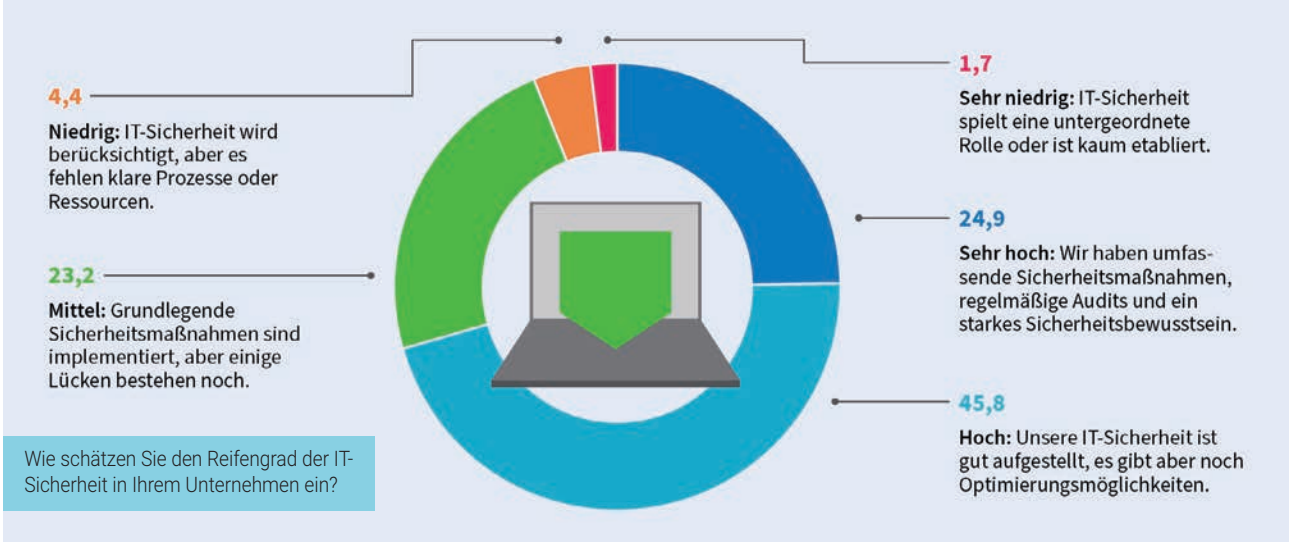
Gruppen wie Lazarus arbeiten arbeitsteilig, iterieren schnell und nutzen alltägliche Prozesse: Kommunikation, Kollaboration und Standardsoftware. Fertigungsunternehmen, die das erkennen und ihre Netze so gestalten, dass Fehler nicht eskalieren, senken ihre Risiken erheblich. Wer die drei Schutzwälle – Content-Härtung an der Peripherie, strikte Identitäts- und Zonen-Trennung, OT-nahe Sichtbarkeit mit eingeübten Reaktionsabläufen – konsequent umsetzt, schwächt Social-Engineering-Ketten. ■

Markus Neumaier
Head of CyberSoc Central EU
Orange Cyberdefense Germany GmbH
www.orangecyberdefense.com/de

Cybersicherheit in Deutschland

Vorlesen lassen!

Wie bereit sind Unternehmen?



Digitale Sicherheit ist längst ein strategisches Thema. Wie die aktuelle Lage ist, zeichnet die Umfrage 'Cybersicherheit in Zahlen' von G Data CyberDefense, Statista und Brand Eins nach. Diese stellt zunehmende Risiken durch den Missbrauch von KI, unzureichendes Sicherheitsbewusstsein bei Mitarbeitenden und Defizite auf Organisationsebene fest.

Der Einsatz von KI-Technologien verspricht Produktivitäts- und Qualitätssteigerungen. Doch dieselben Technologien werden inzwischen auch von Angreifern missbraucht. So lassen sich etwa täuschend echte Phishing-E-Mails automatisiert erzeugen, die kaum noch als Fälschung erkennbar sind. Die aktuelle Ausgabe 'Cybersicherheit in Zahlen' von G Data CyberDefense, Brand Eins und Statista zeigt, dass zwei Drittel der Befragten erwarten, dass KI die Bedrohungslage weiter verschärft. Ein kritischer Schwachpunkt liegt bei den Angestellten selbst: Nur 16,5 Prozent der Befragten trauen sich zu, betrügerische Mails zuverlässig zu erkennen. Mehr als vier von fünf Mitarbeitenden sind hingegen unsicher – ein Risiko für alle, die auf digitale Kommunikation im täglichen Betrieb angewiesen sind. Sicherheitsbewusstsein muss deshalb in allen Abteilungen verankert sein. Von der Geschäftsführung über die IT bis hin zu Angestellten in den Bereichen Konstruktion, Instandhaltung und Logistik oder Personal und Marketing.

Struktuelle Mängel rächen sich

Weitere Defizite zeigen sich auf Prozessebene: Nur ein Viertel der Befragten schätzt den Reifegrad der IT-Sicherheitsmaßnahmen im eigenen Unternehmen als 'sehr hoch' ein, inklusive klar definierter Prozesse, regelmäßiger Audits und etablierter Schutzmechanismen. Während 46 Prozent zumindest eine solide Ausgangslage mit Verbesserungspotenzial sehen, berichtet fast ein Drittel von gravierenden Lücken wie fehlenden Zuständigkeiten oder Ressourcen. Besonders kritisch ist dies in vernetzten Lieferketten: Angreifergruppen wählen gezielt das schwächste Glied in dieser Kette. Nicht selten ist das eigentliche Ziel ein Zulieferer, Partner oder Kunde.

Umfassend relevant

Cybersicherheit ist kein reines IT-Thema, sondern betrifft alle Fachbereiche und sollte von der Führung vorangetrieben werden. Während auf Geschäftsleitungsebene 77 Prozent der Befragten eine hohe Sensibilität zeigen, ist diese in nachgelagerten Hierarchieebenen deutlich geringer (23 Prozent). Dabei sind auch Fachabteilungen wie Entwicklung oder Einkauf potenzielle Angriffspunkte. Mehr als 30 Prozent der befragten Unternehmen waren im letzten Jahr von mindestens einem Cybervorfall betroffen, jeder Zehnte sogar mehrfach. Eine kontinuierliche Überwachung der IT-Systeme ist eine Voraussetzung für effektive IT-Sicherheit. Zwei von fünf Unternehmen verfügen intern über die Ressourcen für eine dauerhafte Kontrolle. Ein Großteil der Befragten setzt auf externe Spezialisten für diese Aufgabe. Ob durch regulatorische Vorgaben wie NIS-2 und den Cyber Resilience Act, den Fachkräftemangel oder die steigende Komplexität moderner Angriffe: Der Handlungsdruck auf IT-Verantwortliche steigt. ■

Stefan Karpenstein
PR-Manager
G Data CyberDefense AG
www.gdata.de

Bild: G Data CyberDefense AG



Security-Schwachstellen in der Industrie

Warum Backups unverzichtbar sind

Viele Industrieunternehmen sind unzureichend gegen Cyberangriffe geschützt. Und Schwachstellen finden sich hier häufig in der OT. Das Zero-Trust-Modell zielt darauf ab, alle IT- und OT-Komponenten unabhängig von ihrem Standort zu überprüfen. Die dazugehörige Sicherheitsstrategie berücksichtigt alle Phasen eines möglichen Angriffs und basiert auf einem herstellerunabhängigen Anlagenmanagement mit zentraler Überwachung und Backup-Software.

Um die Netzwerk- und Informationssicherheit in Deutschland zu verbessern, hat die Europäische Union (EU) die NIS-2-Richtlinie ins Leben gerufen. Durch diese sind deutlich mehr Akteure dazu verpflichtet nachweislich höhere Sicherheitsstandards zu etablieren – Schätzungen gehen hier von ca. 30.000 Unternehmen aus. Insbesondere Unternehmen aus dem produzierenden Gewerbe schließt die Regelung mit ein. (siehe Kasten). Die EU macht damit deutlich, wie wichtig die Resilienz der Produktion und deren Lieferketten als Teil der kritischen Infrastruktur ist. In der Realität lassen es viele Industrieunternehmen allerdings an den Grundlagen, sprich dem Erstellen von wiederherstellbaren Backups, vermissen. Dabei sind Datensicherungen die Grundvoraussetzung dafür, betriebliche Abläufe nach einem disruptiven Ereignis, wie etwa einem Cyberangriff, schnellstmöglich wiederherzustellen.

Einfallstor: Operational Technology

Als Eintrittstor für Hackerangriffe dienen häufig OT-Komponenten, die für die Steuerung und Überwachung von Maschinen zuständig sind. Während IT-Systeme oft durch standardisierte Backup-Systeme geschützt werden, wurden OT-Sicherheitssysteme in diesem Bereich lange Zeit vernachlässigt. Die Konsequenz: Schwachstellen können beispielsweise mit Hilfe legaler Suchmaschinen ausfindig gemacht und Produktionsanlagen so mit einfachsten Mitteln angegriffen werden.

NIS-2-Betroffenheitscheck des BSI

Unter dem Motto 'NIS2know' hat das Bundesamt für Sicherheit in der Informationstechnik eine Informationskampagne zur NIS-2-Regulierung gestartet. Unternehmen können mittels einer Betroffenheitsprüfung eruieren, ob sie von der Richtlinie betroffen sein werden und welche Vorbereitungen in dieser Hinsicht zu treffen sind. Mehr als 100.000 Zugriffe auf das digitale Tool konnte das BSI bereits verzeichnen.

https://tedo.link/aNaPv4



Bild: ©Gorodenkoff/stock.adobe.com

Zero Trust: vertraue niemandem

Mit dem Sicherheitsmodell Zero Trust hat sich ein Paradigmenwechsel in der Informationstechnologie vollzogen. Es basiert auf dem Prinzip, zunächst keiner IT-Einheit zu vertrauen. Jeder Benutzer, jedes Gerät und jede Netzwerktransaktion wird unabhängig von ihrem Standort als potenziell gefährlich betrachtet. Deswegen sollte auch jede Anfrage, egal, ob sie von außen oder innen erfolgt, vor dem Zugriff verifiziert werden. Der Zero Trust-Ansatz berücksichtigt nicht nur die IT-Ressourcen, sondern auch die komplette Industrieanlage und gleichzeitig die gesamte OT-Landschaft. Auch wenn dieses Sicherheitsmodell kein fest umrissener oder normierter Industriestandard ist, stellt es einen proaktiven Ansatz zur Vermeidung von Cyberattacken dar.

Zero Trust basiert auf dem Prinzip, keiner IT-Einheit zu vertrauen. Jeder Benutzer, jedes Gerät und jede Netzwerktransaktion wird unabhängig von ihrem Standort als potenziell gefährlich betrachtet.

Stefan Jesse, AMDT

Den Überblick in komplexen IT/OT-Umgebungen behalten

Um der heterogenen und komplexen IT/OT-Umgebung Herr zu werden, ist ein herstellerunabhängiges Anlagenmanagement Grundvoraussetzung. Eine Backup- und Versionierungsoftware wie etwa das Tool Octoplant von AMDT ermöglicht beispielsweise die Überwachung der gesamten Produktion. Mit dem System können Unternehmen alle Assets, Geräte und Dokumente zentral verwalten. Die Produktionsdaten bleiben sicher am Standort, während über die Metadaten ein zentraler Überblick über den Status der Produktionsanlagen eingerichtet werden kann. Ergänzt wird sie durch eine Cybersicherheitsstrategie, die alle Phasen eines möglichen Angriffs berücksichtigt: Prävention, Erkennung von unautorisierten Änderungen sowie Schadensminimierung durch schnelle Wiederherstellung im Schadensfall. ■

Stefan Jesse
Group CEO
Auvesy GmbH
amdt.com



Octoplant von AMDT überwacht und verwaltet Assets, Geräte und Dokumente.

Bild: ©Gorodenkoff/stock.adobe.com

Angriffsrisiken und Verteidigungsmethoden

KI mit KI bekämpfen


Bild: ©Gorodenkoff/stock.adobe.com

Social Engineering, Phishing und KI-gesteuerte Attacken – Cyberangriffe werden immer raffinierter und stellen die Fertigungsindustrie vor Herausforderungen. Marc Meckel, Manager Domain Consulting bei Palo Alto Networks, gibt einen Überblick über aktuelle Risiken und die Rolle von künstlicher Intelligenz (KI) für Verteidigungsstrategien.


Bild: Palo Alto Networks

Marc Meckel ist Manager Domain Consulting bei Palo Alto Networks.

Ein aktueller Report von ABI Research und Palo Alto Networks zeigt: Mehr als 76 Prozent der befragten Unternehmen waren bereits Opfer von Cyberangriffen, wobei etwa 75 Prozent von regelmäßigen Attacken berichten – monatlich, wöchentlich oder sogar täglich. Und gerade die zunehmende Vernetzung von IT (Informationstechnologie) und OT (Operative Technologie) schafft neue Angriffsflächen für Cyberkriminelle. 72 Prozent der Angriffe auf den OT-Bereich kommen aus der IT-Umgebung. Diese Angriffe lassen sich in zwei Kategorien einteilen: breit angelegte Angriffe auf möglichst viele Opfer und gezielte Attacken auf spezifische Unternehmen oder Branchen. Gerade letztere werden durch den Einsatz künstlicher Intelligenz zu einer immer größeren Gefahr.

Häufige Angriffsvektoren

Zu den häufigsten Einfallstoren für Cyberangriffe in der fertigenden Industrie zählen weiterhin Phishing und Social Engineering. Mitarbeiter werden hier zur Preisgabe sensibler Informationen verleitet. Als weiteren Angriffsvektor nutzen Cyberkriminelle Schwachstellen in der IT-Infrastruktur aus. Sie zielen vor allem auf bereits bekannte Sicherheitslücken in Softwaresystemen ab. Ein Problem sind auch veraltete Systeme, die in vielen Fertigungshallen als sogenannte Legacy-Systeme im Einsatz sind. Eine weitere Gefahr stellt die Verbreitung von Remote-Zugriffen auf Unternehmenssysteme dar. Sowohl eigene Mitarbeiter als auch Zulieferer können dadurch unwissentlich ein Einfallstor für Schadcode bieten. Der Einsatz von IoT-Geräten und die BYOD-Praxis (Bring Your Own Device) erhöhen die Angriffsfläche. Hier hat sich insbesondere seit der COVID-19-Pandemie die Nutzung privater Geräte im beruflichen Kontext verstärkt, aber oft ohne ausreichende Sicherheitsmaßnahmen im Gegenzug.

Gezielte Angriffe

In der Vergangenheit waren es oft gezielte Kampagnen, die Aufmerksamkeit erregten: Im Februar 2021 wurde etwa versucht, das Trinkwasser der Stadt Oldsmar in Florida mittels Fernzugriff auf die Steuerung der Zufuhr von Natriumhydroxid von 100 ppm auf 11.100 ppm zu vergiften. Im Mai 2021 ereignete sich ein Ransomware Angriff auf Colonial Pipeline in den USA, bei dem die Daten des Unternehmens verschlüsselt und ein Lösegeld von 4,4 Millionen Dollar gefordert wurden.

Aktuell werden im OT-Umfeld der fertigenden Industrie überwiegend gezielte Angriffe beobachtet. Die Vorgehensweise lässt sich dabei oft in mehrere Phasen unterteilen. Zunächst sammeln Angreifer Informationen über das Zielunternehmen, seine Mitarbeiter und Systeme. Darauf folgt die soziale Manipulation, bei der Methoden wie Phishing oder sogar Spearphishing gegen Schlüsselpersonal eingesetzt werden. Die eigentliche Kompromittierung erfolgt letztendlich durch Ausnutzung von entdeckten Schwachstellen oder Social Engineering. Nach der erfolg-

reichen Kompromittierung eines Accounts können sich die Angreifer lateral im Netzwerk bewegen, um wertvolle Assets zu erreichen. Je nach Ziel und Motivation des Angriffs werden dann Daten gestohlen oder Systeme manipuliert.

Angreifer nutzen oft einen Zugang über externe Lieferanten, die als unbeabsichtigte Eintrittspunkte dienen. Hierauf haben die Unternehmen selbst selten einen direkten Einfluss. Umso mehr müssen sie aber die Sicherheit ihrer gesamten Lieferkette im Blick haben. Die Komplexität und Verflechtung moderner Lieferketten machen dies zu einer besonderen Herausforderung, da jeder Zulieferer eine potenzielle Schwachstelle darstellen kann. Als Reaktion darauf implementieren immer mehr Unternehmen das 'Zero Trust'-Prinzip. Der Report zeigt, dass 87 Prozent der Unternehmen diesen Ansatz mittlerweile als essenziell für den Schutz ihrer Produktionsumgebungen betrachten.

KI in der Cybersicherheit

Immer mehr Angreifer nutzen KI, um ihre Angriffe zu automatisieren, zu skalieren und zu optimieren. Phishing-Kampagnen lassen sich etwa durch KI-generierte Inhalte unterstützen, um täuschend echt wirkende Mails oder sogar Deepfake-Video-Konferenzen zu erstellen. Ebenso können Kriminelle durch KI-gestützte Tools schneller Schwachstellen identifizieren. Doch auch in der Verteidigung kann KI unterstützen. Die Technologie erkennt Bedrohungen und kann darauf reagieren. Automatisierte Analysen erlauben eine schnellere Bearbeitung selbst großer Datenmengen, um Anomalien zu identifizieren.

Ein Blick in die Zukunft

Ein Schlüsselfaktor in der nächsten Zeit ist die Verkürzung der Zeitspanne zwischen Angriffserkennung und -abwehr. Auch die Vernetzung von IT und OT wird weiter zunehmen und neue Sicherheitsstrategien erfordern. Angreifer wie auch Verteidiger nutzen vermehrt KI-basierte Tools. Somit steigt die Notwendigkeit für schnelle, automatisierte Reaktionen auf Bedrohungen. Für Fertigungsunternehmen ist es ratsam, in moderne Sicherheitstechnologien und KI-basierte Lösungen zu investieren.

Zudem sind regelmäßige Schulungen und Sensibilisierung der Mitarbeiter für Cybersicherheit sind unerlässlich, da der Mensch oft das schwächste Glied in der Sicherheitskette ist. Es empfiehlt sich auch eine enge Zusammenarbeit zwischen IT- und OT-Teams, um gemeinsam ganzheitliche Sicherheitsstrategien zu entwickeln und umzusetzen. Außerdem empfiehlt es sich, Standards für Zulieferer zu definieren und deren Einhaltung zu überwachen. Berücksichtigen Unternehmen diese Elemente, können sie den Gefahren erfolgreich begegnen ■

Marc Meckel
Manager Domain Consulting
Palo Alto Networks
www.paloaltonetworks.de

- Anzeige -

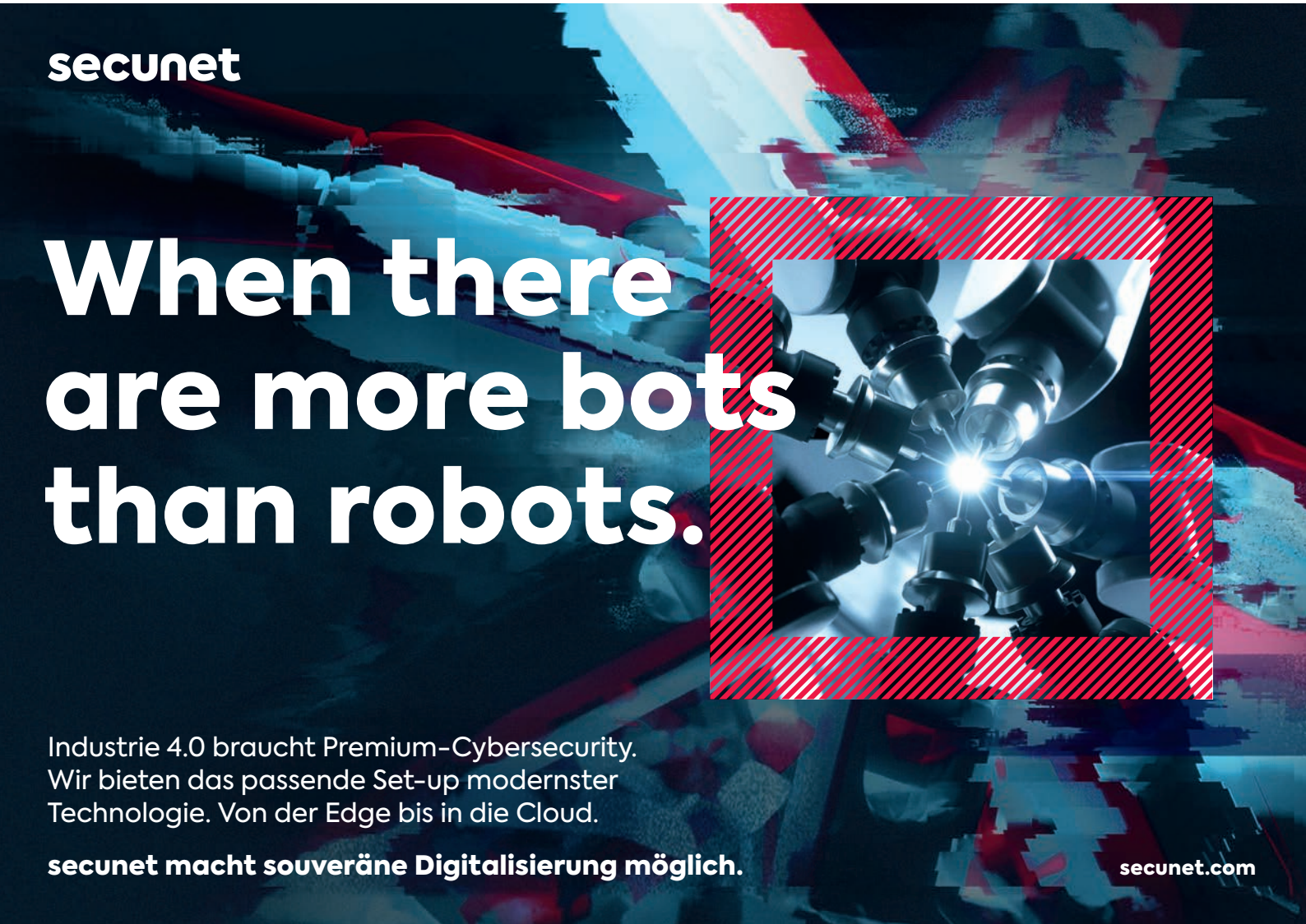




Bild: ©gorodenkoff/stock.adobe.com

IT-Sicherheit in der Prozessindustrie

Sensibilisierung und Technik stärken die Cybersicherheit

Cybersicherheit war lange nur in der IT-Abteilung verortet. Mit der Vernetzung wird der Schutz vor Cyberattacken aber auch für OT-Umgebungen und -Teams wichtiger. Falk Plonus, Technical Key Account Manager bei Copa-Data Deutschland, erläutert, worauf es bei einer erfolgreichen Sicherheitsstrategie insbesondere in der Prozessindustrie ankommt und wie Software dabei unterstützen kann.

Im Kontext der fortschreitenden Digitalisierung und Vernetzung von Anlagen und Systemen durchläuft auch die Prozessindustrie eine Transformation. Neben den daraus resultierenden Möglichkeiten sieht sich die Branche jedoch mit bislang ungekannten Herausforderungen im Bereich der Cybersicherheit konfrontiert. Die erweiterte Konnektivität der Informationsräume führt zu einer exponentiellen Zunahme des Risikos von Cyber-Angriffen. Laut Statista galten im Jahr 2023 weltweit 25,7 Prozent aller Cyberattacken der Fertigungsindustrie. Durch gezielte Sicherheitsmaßnahmen kann die Prozessindustrie jedoch Risiken reduzieren

Von der Planung bis zur Wartung

Konzepte zur Resilienzsteigerung sollten in sämtlichen Phasen des Lebenszyklus einer technischen Anlage umgesetzt werden, von der Planung über die Implementierung bis hin zur Wartung. Entlang dieser Wertschöpfungskette empfiehlt es sich, dass Anlagenbetreiber, Hersteller von Automatisierungs- und Steuerungskomponenten sowie Systemintegratoren themenspezifisch eine systemische Einheit bilden und miteinander kooperieren, um ein optimales und nachhaltiges Ergebnis zu erzielen.

Risiken von Cyber-Angriffen in Zeiten von Industrie 4.0

Industrieanlagen galten lange als weitgehend resistent gegenüber Cyber-Angriffen. Ihre Isolation von anderen Netzwerken sowie der proprietäre Charakter der eingesetzten Hardware und Kommunikationsprotokollen boten einen natürlichen Schutz. Die zunehmende Vernetzung zwischen Industriesystemen und dem Inter-


Bild: ©goodluz/stock.adobe.com

net erhöht jedoch die Angriffsvektoren. Insbesondere ältere Systeme weisen Schwachstellen auf. Oft wurden bei der Konzeption dieser Systeme keine hinlänglichen Sicherheitsvorkehrungen berücksichtigt, waren sie doch lange Zeit nicht vernetzt. Solche Legacy-Systeme können in Verbindung mit IoT-Technologien zu gravierenden Sicherheitslücken führen.

Prozessleitsysteme und SCADA-Anwendungen überwachen, steuern und automatisieren teils komplexe Produktionsprozesse. Aufgrund ihrer zentralen Rolle innerhalb der vernetzten Infrastruktur sind sie daher ebenfalls ein attraktives Ziel für Cyber-Angriffe.

Security by Design und modulare Out-of-the-Box-Sicherheitsfeatures bieten in diesem Zusammenhang besonderen Nutzen. Die Integration von Sicherheitsfunktionen sollte inealerweise bereits durch den Hersteller erfolgen, sodass keine aufwendige Nachrüstung erforderlich ist.

IEC62443 und NIS-2

Die Normenreihe IEC62443 bietet einen Rahmen für die Cybersicherheit von industriellen Automatisierungs- und Steuerungssystemen. Sie umfasst Aspekte wie das Systemdesign, die Implementierung, den Betrieb und die Wartung und unterstützt Unternehmen bei der Umsetzung von Sicherheitsmaßnahmen. Die von Copa-Data entwickelte Softwareplattform Zenon ist gemäß der Norm IEC62443 zertifiziert. Die modular aufgebaute Software kann an individuelle Sicherheitsanforderungen angepasst werden und bringt und unterschiedlichste Disziplinen in Einklang. Dies zahlt auf die Absicherung von Industrieanlagen ein. Zudem unterstützt die Einhaltung der Anforderungen aus der IEC62443 die Umsetzung der EU-Richtlinie NIS-2 Richtlinie.

Mit der NIS-2-Richtlinie erhöht die EU die Anforderungen an die Cyber-Sicherheit und erweitert den Kreis der betroffenen Unternehmen. Die wesentlichen Anforderungen der Richtlinie umfassen die Entwicklung von Konzepten für Risikoanalysen entlang der gesamten Lieferkette und die Sicherheit von Informationssystemen, um potenzielle Bedrohungen frühzeitig zu identifizieren. Das Management von Sicherheitsvorfällen sowie die Aufrechterhaltung des Betriebs durch solide Backup- und Notfallpläne sind hier von essenzieller Bedeutung. Awareness-Trainings zur Steigerung des Sicherheitsbewusstseins der Mitarbeitenden ist ebenfalls als Anforderung genannt, genauso der Einsatz von Kryptographie und Verschlüsselung, um die Vertraulichkeit und Integrität sensibler Daten zu gewährleisten.

Mitarbeiter sensibilisieren

Da Cyber-Security in der Vergangenheit der Verantwortung der IT-Abteilung zugewiesen wurde, herrscht bei Akteuren aus dem Bereich der Operational Technology oft noch ein Mangel an Bewusstsein und Wissen in diesem Bereich. Schulungen bieten sich an, um Mitarbeiterinnen und Mitarbeitern die Basics rund um das Thema Cybersicherheit beizubringen, wie etwa die Verwendung solider Passwörter.

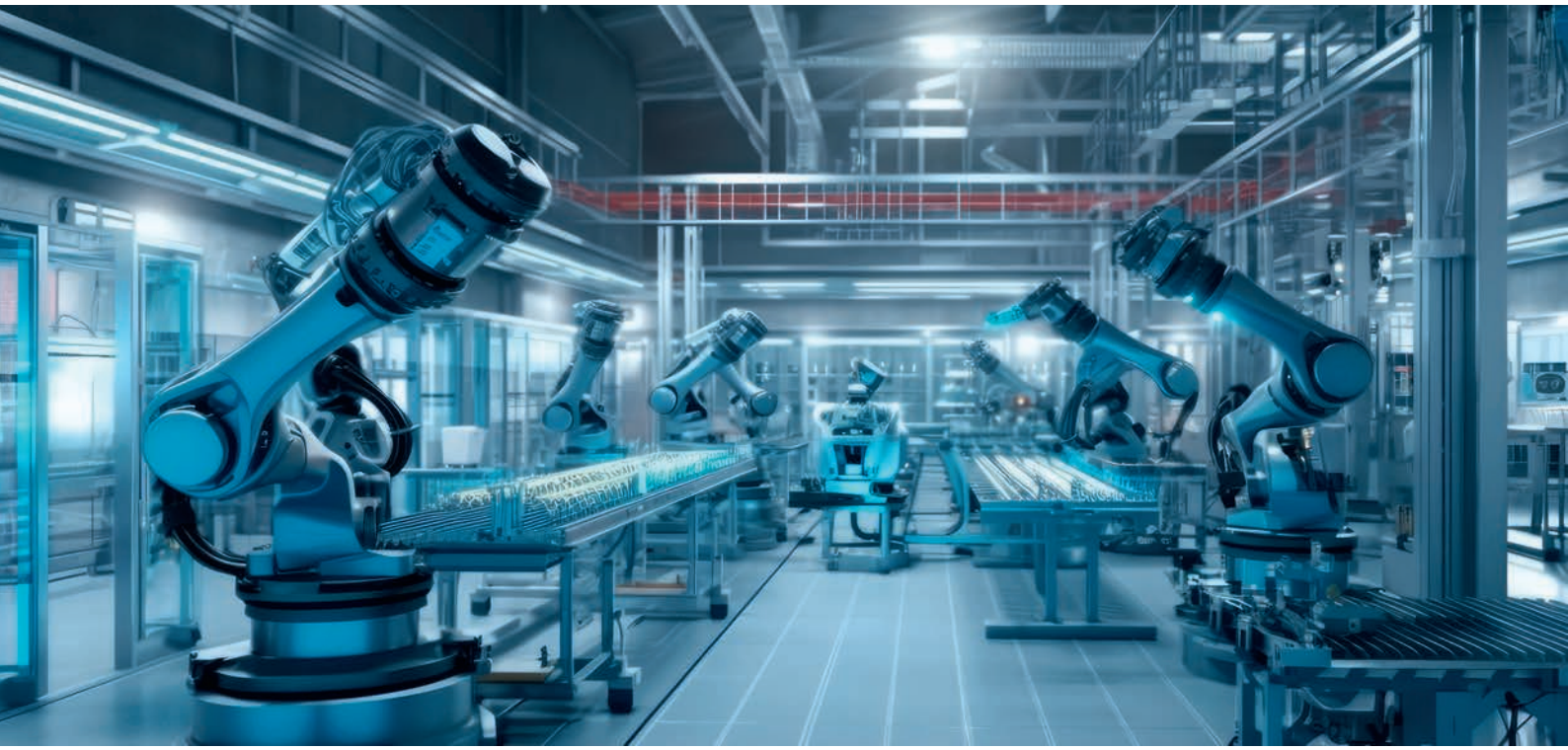
Für eine möglichst sichere Produktionslandschaft, die den Prinzipien des Zero-Trust-Ansatzes folgt, ist es wichtig, nicht allein auf die Vertrauenswürdigkeit der Benutzer und Geräte innerhalb ihres Netzwerks zu vertrauen. Es gilt, sämtliche Zugriffe auf Assets vor und hinter der Firewall zu kontrollieren. Jeder Zugriff sollte individuell authentifiziert und autorisiert werden.

Software unterstützt

Traditionelle Methoden der IT-Sicherheit erweisen sich oft als unzureichend, um industrielle Umgebungen angemessen zu schützen. Es Bedarf also spezifischer Sicherheitsstrategien. Interdisziplinäre Plattformen wie Zenon bieten durch Security by Design und Zero-Trust-Ansatz Schutz vor Datenverlust und unautorisierten Zugriffen vom OT-Bereich bis in die Cloud. Eine weitere Komponente hierbei ist die integrierte SIEM-Funktion (Security Information and Event Management), die sicherheitsrelevante Ereignisse in Echtzeit überwacht, analysiert und zentral verwaltet.

Eine Kombination aus Technologie sowie der Sensibilisierung der Mitarbeitenden bildet die Grundlage für eine zukunftssichere OT/IT-Security. Software unterstützt Unternehmen aus der Prozessindustrie dabei, die Möglichkeiten von Industrie 4.0 zu nutzen und gleichzeitig die Resilienz gegenüber Cyber-Bedrohungen zu stärken. ■

Falk Plonus
Technical Key Account Manager
Copa-Data Deutschland.
www.copadata.com



Cybersicherheit in der Automatisierungsindustrie

Dem Cyber Resilience Act und der IEC62443 begegnen

Der Cyber Resilience Act verlangt von Herstellern, Integratoren und Betreibern digitaler Produkte umfangreiche Cybersicherheitsmaßnahmen über den gesamten Lebenszyklus hinweg. Bei deren Umsetzung und bei der Vernetzung von IoT-Geräten hilft eine Public Key-Infrastruktur (PKI) sowie ein Secure Development Lifecycle für alle Produkte mit digitalen Elementen.

2023 wurden die Cybersicherheitsvorschriften der EU durch die NIS2-Richtlinie aktualisiert, und auch das EU-Gesetz über Cyberresilienz, der Cyber Resilience Act (CRA), wurde vom Europäischen Parlament verabschiedet. Nach der Verabschiedung durch den Europäischen Rat – eine reine Formsache – haben Hersteller 36 Monate Zeit, die Vorgaben umzusetzen. Er gilt für Produkte, Software und Hardware, mit digitalen Elementen und damit ist auch die Industrie angesichts von vernetzter Fertigung im Industrial Internet of Things (IIoT) voll im Fokus: Geräte, Maschinen und Komponenten in der Produktion sammeln und erzeugen Daten mit Sensoren und Aktoren und tauschen sie aus, industrielle Steuerungssysteme (Industrial Control Systems, ICS) arbeiten damit. Sicherheitskritische Produkte mit digitalen Elementen werden im Anhang III des CRA sogar als kritische Hard- und Softwareprodukte gelistet: Dazu zählen u.a. Firewalls, Angriffserkennungs- und -präventionssysteme, Router, Modems und Switches, auch im industriellen Kontext.

Für all diese Produkte legt der CRA einen **umfangreichen Anforderungskatalog** fest. Demnach benötigen sie:

- einen sicheren Produkt- und Entwicklungslebenszyklus (Security by Design), der Cybersicherheit im gesamten Lebenszyklus berücksichtigt.
- ein kontinuierliches Schwachstellen-Management: Cybersicherheitsrisiken müssen dokumentiert werden und die Hersteller aktiv ausgenutzte Schwachstellen und Zwischenfälle melden.
- ein sicheres Software-Update-Management: Die Hersteller müssen nach dem Verkauf weiterhin sicherstellen, dass für die Dauer des Supportzeitraums Schwachstellen ihrer Produkte wirksam behandelt werden. Außerdem sind Sicherheitsaktualisierungen und Patches für die voraus-

Bild ©AKA-RA /stock.adobe.com



IT-Sicherheit ist Teamplay

Viele IT-Verantwortliche in Unternehmen sind mit der Aufgabe, für Cybersicherheit zu sorgen, überfordert. Es mangelt sowohl an Zeit und Personal als auch an tiefgreifendem Fachwissen. IT-Sicherheit ist komplex und unter diesen Bedingungen kaum zu gewährleisten. Eine Lösung für das Problem sind umfassende Dienstleistungen wie G DATA 365 | MXDR.

Cybercrime wird heutzutage sehr professionell betrieben. Einige Angreifer versuchen zum Beispiel, den initialen Zugang zu einem Netzwerk zu erlangen. Dann verkaufen sie den Zugang an andere Gruppen, die sich mit der Ausbreitung und Absicherung verstehen. Diese wiederum übergeben an solche, die auf Datenverschlüsselung und Lösegelderpressung spezialisiert sind. Die Angreifer gehen dabei sehr behutsam und mitunter langsam vor, um nicht aufzufallen. Daher kann es sein, dass ein Unternehmen schon lange, bevor es dies bemerkt, betroffen ist.

Verteidigung rund um die Uhr

Dinge, die verdächtig wirken, wie zum Beispiel das Anlegen neuer Admin-User oder das Hinzufügen von Autostart-Einträgen bleiben oft für lange Zeit unbemerkt. Das liegt zum einen daran, dass Kriminelle bewusst in den Nacht- oder Wochenendzeiten arbeiten. Zum anderen daran, dass IT-Abteilungen oft überlastet sind und ihnen die Zeit fehlt, um in Logdaten nach Auffälligkeiten zu suchen. Dies durch die Einstellung zusätzlicher Mitarbeiter zu kompensieren, ist aufgrund des Fachkräftemangels ebenfalls keine Option.

Das Risiko ist hoch und ein 24/7-Schutz der IT-Infrastruktur unerlässlich. Als Ausweg aus dem Dilemma bieten sich Dienstleistungen wie MXDR (Managed Extended Detection and Response) an. Dabei überwachen IT-Sicherheitsexperten eines spezialisierten Anbieters alle Vorgänge im Netzwerk und intervenieren bei Cyberangriffen zu jeder Tages- und Nachtzeit. Unternehmen müssen sich dem Risiko durch Ransomware also nicht allein stellen.

Verlässlicher Partner

Durch die Nutzung von G DATA 365 | MXDR profitieren IT-Verantwortliche von der fast 40-jährigen Erfahrung des Cyber-Defense-Unternehmens. Kunden stehen direkte Ansprechpartner zur Seite, unterstützt von einem preisgekrönten 24/7-Support in deutscher Sprache. G DATA setzt auf persönliche und individuelle Betreuung statt auf Call Center.

Damit IT-Verantwortliche weiterhin die Kontrolle behalten, werden sie natürlich über Vorfälle informiert – in dringenden Fällen auch telefonisch. Eine Webkonsole ermöglicht es darüber hinaus, detaillierte Einsicht in Vorfälle und ergriffene Maßnahmen zu nehmen. Dort erhält man leicht verständliche Handlungsempfehlungen, sofern erforderlich.

Die Datenverarbeitung im Rahmen von G DATA 365 | MXDR geschieht ausschließlich auf Servern in Deutschland. Damit unterliegt sie den strengen deutschen Datenschutzrichtlinien. Der Schutz der Kundendaten sowie der Schutz vor Cyberbedrohungen stehen für G DATA CyberDefense an erster Stelle.

G DATA CyberDefense

Kontakt

G DATA CyberDefense AG
Königsallee 178 a • 44799 Bochum
Tel.: +49 234 9762-0
info@gdata.de
www.gdata.de/mxdr

sichtliche Nutzungsdauer des Produkts vorgeschrieben.

- eine sicherheitsbezogene Dokumentation mit klaren und verständlichen Anweisungen.

- Vorgaben zur Konformitätsbewertung bzw. der Produktkonformität und der Risikobewertung.

Die Anforderungen

Die konkreten Cybersicherheitsanforderungen stehen in Anhang I des CRA: Produkte mit digitalen Elementen benötigen auf Grundlage ihrer Risikobewertung geeignete Kontrollmechanismen, die Schutz vor unbefugtem Zugriff bieten. Genannt werden hier Authentifizierungs-, Identitäts- oder Zugangsverwaltungssysteme. Sie müssen die Integrität gespeicherter, übermittelter oder anderweitig verarbeiteter Daten, ob personenbezogener oder sonstiger Daten, Befehle, Programme und Konfigurationen vor einer Manipulation schützen. Ihre Beschädigung muss gemeldet werden. Außerdem muss sichergestellt werden, dass Schwachstellen durch (automatische) Sicherheitsaktualisierungen behoben werden können. Die normativen Anforderungen legt die IEC62443 fest, die wichtigste Sicherheitsnorm der Automatisierungsindustrie.

Die Sicherheitsanforderungen des CRA zu erfüllen und die IEC62443 umzusetzen, ist weder für Hersteller noch für Integratoren und Betreiber eine einfache Aufgabe. Nicht nur, dass die speziellen Anforderungen an die Vernetzung mit Routern und smarten Geräten oft nicht im Fokus liegen. Viele Unternehmen sind per se keine IT-Sicherheitsspezialisten und verfügen nur über limitierte IT-Sicherheitskapazitäten in einem allgemeinen Sicherheitsumfeld wie IT Security Management Systems (EN/ISO270001). Zudem sind Verantwortlichkeiten oft nicht klar definiert.

Public-Key-Infrastruktur

Mit elektronischen Zertifikaten können die wichtigsten Sicherheitsanforderungen des CRA realisiert werden: Sie werden über eine Public Key Infrastruktur (PKI) bereitgestellt. Eine PKI gilt bis dato als das sicherste Verfahren für die Vernetzung von IoT-Geräten und industriellen Steuerungssystemen. Sie ist eine asymmetrische Kryptographietechnologie, die mit öffentlichen und privaten Schlüsseln einen vertraulichen Datenaustausch ermöglicht. Die Daten werden dafür signiert und verschlüsselt. Digitale Zertifikate erzeugen einen Zertifizierungspfad und stellen die Authentizität der Schlüssel sicher.

Über die Zertifikate der PKI greifen **vier Schutzmechanismen:** Die initiale Geräteidentität in der Produktion beim Hersteller wird durch eine zertifikatsbasierte Authentifizierung im Netzwerk sichergestellt – ein Geburtszertifikat identifiziert und authentifiziert das jeweilige Gerät, so dass ein sicherer Kommunikationskanal ins Internet aufgebaut werden kann. Elektronische Zertifikate sichern auch das Update Management ab: Die PKI prüft darüber die Authentizität der Software, so dass keine Malware eingeschleust oder unerlaubte Änderungen vorgenommen werden können. Die Firmware-Updates durch den Hersteller sind signiert. Auch kann über Zertifikate die Autorisierung von Updates von Drittanbietern gesteuert werden. Dritter Anwendungsfall ist der sichere Gerätestart, das Secure Boot. Hierbei wird gewährleistet, dass die Firmware der Geräte vor jedem Start authentifiziert ist und sie über einen sicheren Integritätscode verfügen. Eine PKI sichert auch die Inbetriebnahme eines Geräts bei seinem Betreiber ab – nach einer Authentisierung wird eine lokale Geräteidentität generiert.

Secure Development Lifecycle

Bei der CRA-konformen Entwicklung von Steuergeräten und Systemen unter Berücksichtigung industrieller Sicherheitsstandards gemäß IEC62443 hilft ein Secure-Development-Lifecycle-Ansatz (SDL). Eine Bestandsaufnahme des Produkts mit Gap-Analyse zu CRA-Anforderungen macht hier den Anfang. Dem schließt sich im Rahmen von Security Requirements Engineering/TARA eine Bedrohungs- und Schwachstellenanalyse und Risikobewertung an, um Sicherheitsanforderungen spezifizieren zu können. Danach werden im Security Architecture Engineering Prozess Sicherheitskonzeption und -architektur entwickelt. Auch die Update- und Boot-Prozesse der ICS-Komponenten müssen sicher sein – hier greift das Embedded Security Engineering, bei dem kryptographische Funktionen implementiert werden. Unternehmen benötigen nun leistungsfähige Testwerkzeuge, um ihre ICS- Produkte herstellerunabhängig auf Sicherheit und Konformität mit der IEC62443 und individuellen Sicherheitsanforderungen zu testen – u.a. in Form von Robustheitstests, Code-Analysen oder Penetrationstests. Danach sind zudem Produkt-Evaluierungen nach IEC62443 sinnvoll.

Hilfe bei der Umsetzung

Bei der Umsetzung der Anforderungen des CRA und der IEC können externe Partner helfen. Unternehmen erhalten so Unterstützung bei der Systemplanung, der Bereitstellung und beim Betrieb. Das Systemhaus Achelos begleitet Unternehmen etwa beim Aufbau bzw. der Migration von PKI-Systemen. Nach der Risikoabschätzung wird definiert, welche Prozesse aufgesetzt werden müssen, und ein Betriebskonzept erstellt. Die Sicherheit der PKI wird konzeptioniert, bestimmt, welche Komponenten und welche Sicherheitsebenen notwendig sind und die geeignete Software ausgewählt. Audits werden integriert und Notfallpläne erstellt. Auch der Secure Development Lifecycle wird abgedeckt und der Entwicklungsprozess von Produkten unterstützt.

Für die Zukunft gerüstet

Industrieunternehmen müssen bei der Entwicklung ihrer Steuerungen den CRA berücksichtigen, einen sicheren Produktlebenszyklus, Konformität und Schwachstellenmanagement gewährleisten und dabei die Industrienorm IEC62443 umsetzen. Eine PKI mit Signatur-Services für Firm- und Software bzw. elektronischen Zertifikaten ermöglicht Datensicherheit in der Kommunikation der Infrastruktur und ein Secure-Development-Lifecycle-Ansatz die CRA konforme Entwicklung von Steuergeräten und Systemen. ■

Michael Jahnich
Director Business Development
Achelos GmbH
www.achelos.de

Die unterschätzte Gefahr: Cyber-Security in der OT

Je weiter Digitalisierung und Vernetzung in produzierenden Unternehmen voranschreiten, desto drängender wird das Thema Cyber-Security. Falk Plonus, Technical Key Account Manager bei COPA-DATA, benennt die größten Herausforderungen in der OT-Sicherheit und erläutert, was Unternehmen jetzt tun sollten.

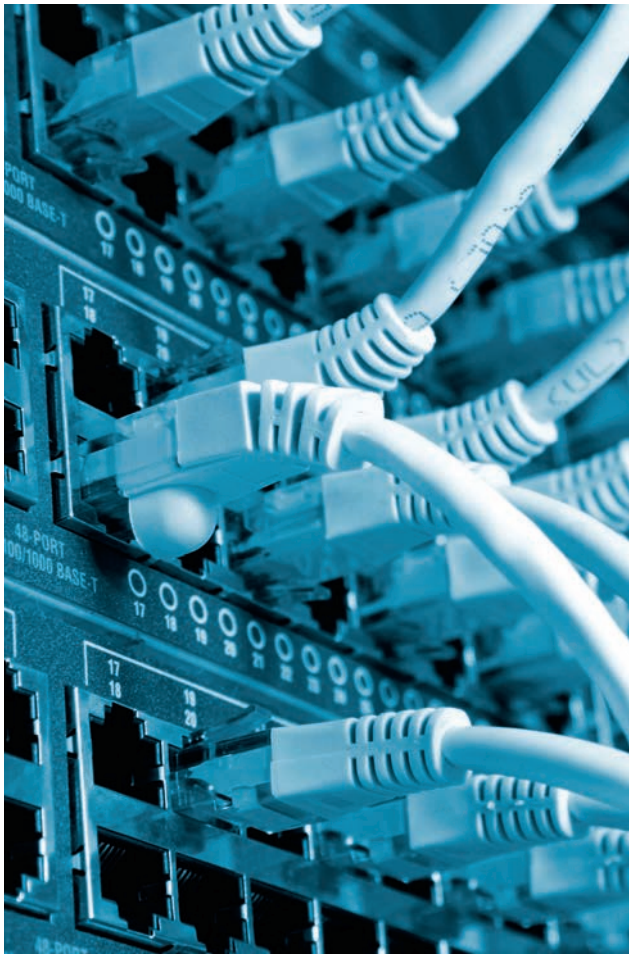


Bild: Ing. Punzenberger Copa-Data GmbH / ©macka/Shutterstock.com

Was sehen Sie als größte Herausforderung im Bereich Cyber-Security in der OT?

Cyber-Angriffe werden zu einer immer größeren Bedrohung für produzierende Unternehmen. Studien belegen, dass mittlerweile rund ein Viertel der Cyber-Attacken auf die Fertigungsindustrie abzielen. Gleichzeitig sehen wir, dass viele Unternehmen diesen Herausforderungen noch nicht gewachsen sind. Eine große Schwachstelle für Cyber-Bedrohungen sind veraltete Systeme. Sie sind häufig mit unzureichenden Sicherheitsmaßnahmen ausgestattet. Bleiben sie ungeschützt, können in Verbindung mit IoT-Technologien große Sicherheitslücken entstehen. Eine weitere Herausforderung sehe ich im Faktor Mensch. Lange Zeit galt das Thema Cyber-Security als ein typisches IT-Thema. In der OT fehlen deshalb oftmals noch heute das Bewusstsein für die Gefahren und das Wissen, sich dagegen zu schützen.

Wie können diese Herausforderungen zukünftig bewältigt werden?

Neben der Abwehr von externen Einflüssen bzw. Hackerangriffen sollte die IT-Sicherheit weitere Maßnahmen ergreifen, die auf drei Grundwerten basieren: A und O ist die Datensicherheit. Dazu gehören Backup-Mechanismen, manipulationsgeschützte Datenablage oder die Validitätsprüfung von Daten. Außerdem müssen die Daten vor unbefugten Gebrauch geschützt werden (Datenintegrität). Als Drittes muss die Verfügbarkeit sichergestellt werden – ein Zugriff auf Dienste, Dateien und Informationen zu jeder Zeit. Normen und Standards definieren diese Aspekte und geben Unternehmen damit einen Leitfaden an die Hand. Wer diese nicht als lästige Pflicht sieht, kann die Chancen erkennen, die sie bieten, um den Herausforderungen gerecht zu werden.

Gibt es Quick-Wins, die Unternehmen schnell und einfach umsetzen können?

Grundsätzlich können Unternehmen dieser gewachsenen Herausforderung nur mit langfristigen und nachhaltigen Strategien gerecht werden. Es lassen sich aber auch kurzfristig umsetzbare Maßnahmen identifizieren, welche die Sicherheit der Produktion erhöhen: Unternehmen sollten sich Hilfe von außen holen und Anlagen sowie Systeme durch umfassende Systemanalysen, Penetrationstests oder gar Schwachstellen-Scans auf den Prüfstand stellen. Ebenso wichtig ist es, auf mögliche Angriffe vorbereitet zu sein und sogenannte Notfallpläne zu entwickeln. Außerdem sollten Unternehmen in das Know-How zu Cyber-Sicherheit investieren, beispielsweise mittels Schulungen des eigenen Personals oder dem Beitritt in Verbände oder Vereinigungen, beispielsweise der Allianz für Cyber-Security. Es gibt Software, wie beispielsweise zenon von COPA-DATA, die ohne großen Aufwand in jede IT/OT-Sicherheitsarchitektur eingebunden werden kann und damit auch die Sicherheit bestehender Systeme erhöht.

COPA-DATA

Kontakt

Ing. Punzenberger COPA-DATA GmbH
Haidgraben 2
85521 Ottobrunn
Tel.: +49 89 660 298 90
info@copadata.de • www.copadata.com

- Anzeige -

PKI- und Lifecycle-Management für IoT/OT

Zertifikate und Schlüssel effizient verwalten – auch direkt im Produktionsumfeld

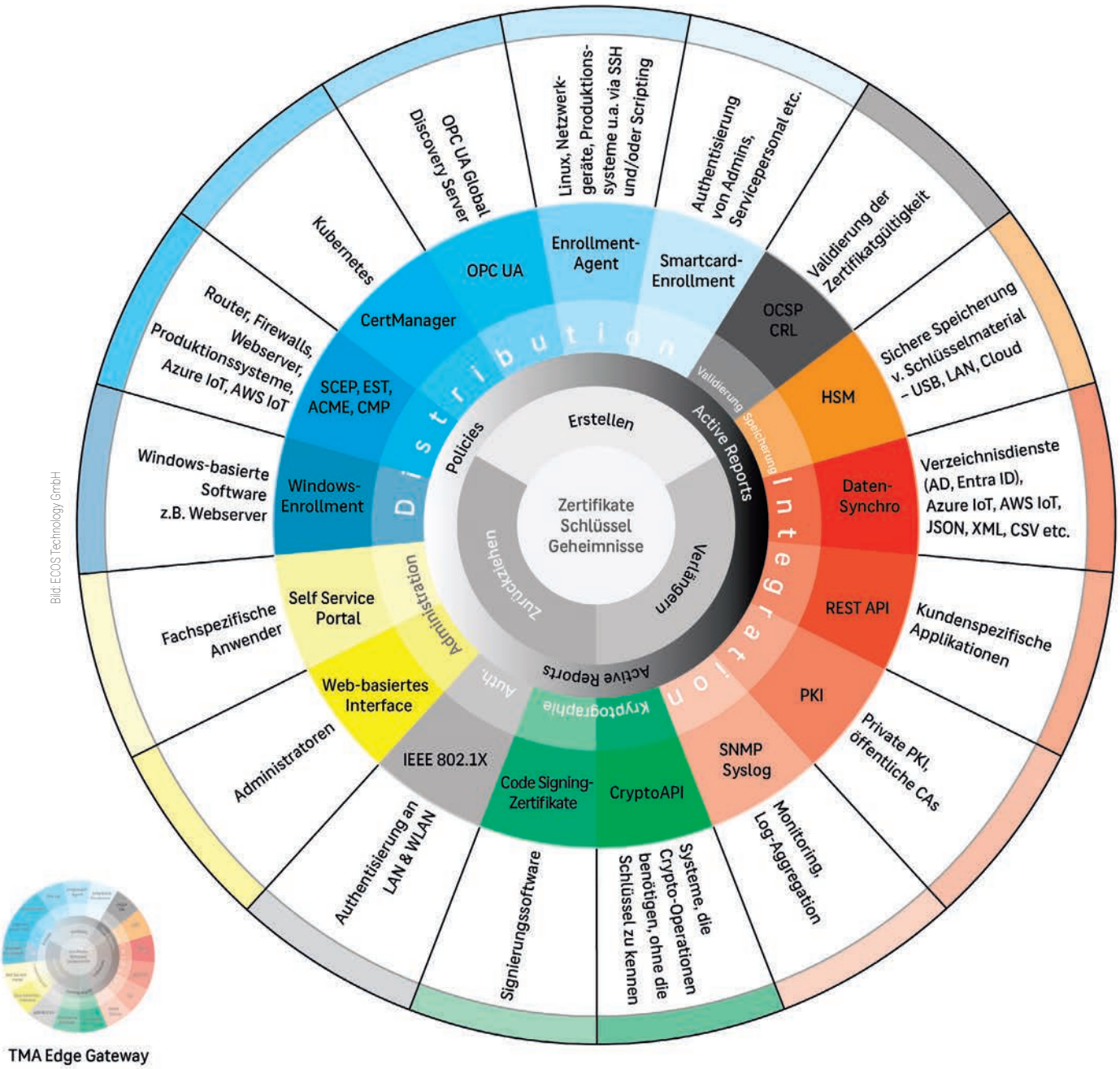


Bild: ECOS Technology GmbH

TMA Edge Gateway

In modernen Produktionsumgebungen spielt die Vernetzung verschiedenster Geräte eine entscheidende Rolle. Neu ist dabei vor allem: Längst kommunizieren nicht mehr nur PCs und Server miteinander. Industrie 4.0 bedeutet ganz konkret stattdessen oft eine Vervielfachung von Geräten mit Internetverbindung – von komplexen Steuerungs- und Produktionsanlagen bis hinab auf die Ebene einzelner Aktoren und Sensoren.

Unternehmen müssen NIS-2 und CRA umsetzen

Für viele Industrieunternehmen ist diese Entwicklung aber auch mit neuen Herausforderungen mit Blick auf die Cybersicherheit verbunden. Denn klar ist: All diese Geräte und Dienste müssen sicher und geschützt miteinander kommunizieren können. Dies ergibt sich nicht nur aus praktischen Sicherheitserwägungen, sondern auch aus regulatorischen

Vorschriften. Dazu zählen beispielsweise die EU-Richtlinie NIS-2 oder der Cyber Resilience Act (CRA) – Regelungen, deren dringliche Umsetzung bei vielen Unternehmen derzeit hoch auf der Agenda steht. In beiden Regelwerken wird explizit eine Absicherung nach dem Stand der Technik und Entwicklung mit dem Grundsatz „Security by Design" gefordert.

Sichere Maschinenidentitäten als Basis

Die Grundvoraussetzung für eine sichere Kommunikation von OT- und IoT-Geräten ist eine eindeutige Identifizierung. Über digitale Schlüssel und Zertifikate erhalten selbst kleinste Geräte und Elemente sichere Maschinenidentitäten. Meist finden hier X509-Zertifikate Anwendung. Eine mögliche Grundlage bietet beispielsweise die Industrienorm IEEE 802.1AR, welche sichere Maschinenidentitäten (Secure Device Identities) beschreibt. Die Norm definiert einen Secure Device Identifier (DevID), der sich aus einem Schlüsselpaar mit Zertifikat und Zertifikatkette zusammensetzt. Das Zertifikat soll dabei z.B. im Subject Informationen enthalten, die das Gerät eindeutig identifizieren kann, etwa die Geräteseriennummer. Zusätzlich werden ein oder mehrere CA-Zertifikate auf dem Gerät gespeichert. Diese dienen als Vertrauensanker, damit das Gerät bei einer Kommunikation sein Gegenüber ebenfalls sicher identifizieren kann.

Effizientes Management von Schlüsseln und Zertifikaten

Als besondere Herausforderung erweist sich in vielen Unternehmen jedoch das effiziente Management dieser Schlüssel und Zertifikate. Schließlich müssen diese erstellt bzw. erzeugt, ausgerollt und verteilt, validiert und über ihren gesamten Lebenszyklus hinweg verwaltet und gegebenenfalls erneuert (oder auch zurückgezogen) werden. Sinnvoll ist, dabei von Beginn an ein soweit wie möglich automatisiertes Lifecycle-Management der Zertifikate und Schlüssel umzusetzen.

Die ECOS TrustManagementAppliance (TMA) ist als Lösung für das sichere und einfache PKI- und Lifecycle-Management von Zertifikaten und Schlüsseln für IoT/OT konzipiert. Dabei werden sämtliche Funktionen rund um die Erzeugung, das Ausrollen und die Validierung von Zertifikaten abgedeckt. Auf diese Weise lassen sich Schlüssel und Zertifikate komfortabel erstellen, verwalten, verteilen und verifizieren. Eine weitgehende Automatisierung sorgt dabei für zusätzliche Effizienzsteigerung. Die TMA verfügt zusätzlich über entsprechende Schnittstellen und lässt sich flexibel an unterschiedlichste Bestandssysteme anbinden. Dabei kann es sich z.B. um Produktionssysteme, IoT-Management-Lösungen oder IAM-Systeme (Identity & Access Management) handeln.

Auf Edge Devices direkt im Produktionsumfeld einsetzbar

In der Praxis gibt es in produzierenden Unternehmen und Industriebetrieben oft auch das Szenario, dass ein Ausrollen und Verwalten von Zertifikaten direkt vor Ort wünschenswert oder erforderlich ist – neben Produktionsanlagen z.B. auch in Außenstellen oder bei Auftragsfertigern im In- und Ausland. Nicht immer ist am jeweiligen Standort allerdings der Betrieb einer umfassenden PKI-Lösung möglich. Dies kann beispielsweise am fehlenden IT-Fachpersonal an einem reinen Produktionsstandort liegen. Und auch bei der Zusammenarbeit mit Auftragsfertigern ist häufig eine besonders einfach nutzbare und auf den spezifischen Anwendungszweck begrenzte Lösung gefragt.

In diesen und ähnlichen Szenarien kann ergänzend das TMA Edge Gateway von ECOS zum Einsatz kommen. Dabei handelt es sich um eine kompakte Softwarelösung für das Ausrollen und Verwalten von Zertifikaten, die auf Edge Devices verwendet werden kann. Zusätzlicher Administrationsaufwand fällt nicht an. Das Edge Gateway kann wahlweise als virtuelle Maschine, in einer Container-Infrastruktur oder auf eigener Hardware betrieben werden. Zertifikate für Maschinenidentitäten lassen sich direkt im Produktionsprozess sicher aufbringen. Bei der Validierung von Zertifikaten per OCSP (Online Certificate Status Protocol) kann die Lösung zudem direkt dort verwendet werden, wo die Zertifikate zum Einsatz kommen. Das TMA Edge Gateway sorgt darüber hinaus für 24/7-Verfügbarkeit: Durch die „Plug&Play"-Auslegung ist bei etwaigen Ausfällen nach dem Start eines neuen Systems ein einfacher Weiterbetrieb möglich – die Funktionalität steht sofort nahtlos wieder zur Verfügung.

Fazit

Die zunehmende Vernetzung im Produktionsumfeld stellt Unternehmen vor neue Cybersicherheits-Herausforderungen. Eine fundamentale Rolle spielt dabei die geschützte Kommunikation von IoT- und OT-Geräten. Dabei können Maschinenidentitäten die Basis schaffen, sichere IT-/OT-/IoT-/IIoT-Infrastrukturen aufzubauen und zu betreiben. Smartes und automatisiertes PKI- und Key-Management rund um die erforderlichen Zertifikate und Schlüssel kann nicht nur für deutlich mehr Effizienz sorgen, sondern auch die Sicherheit erheblich steigern.

Weitere Informationen:

https://www.ecos.de/iot

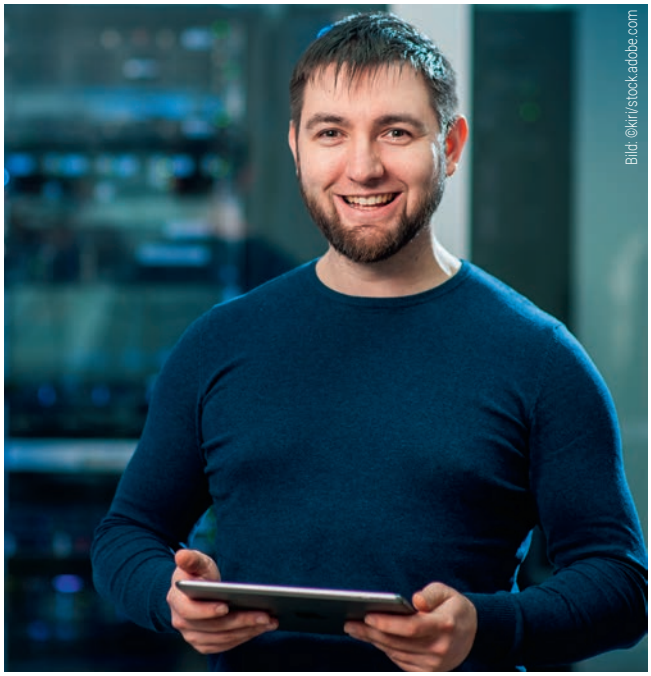
ecos

Kontakt

ECOS Technology GmbH
Sant' Ambrogio-Ring 13 a-b
55276 Oppenheim
Tel: +49 6133 939-222 • Fax: +49 6133 939-333
info@ecos.de • www.ecos.de

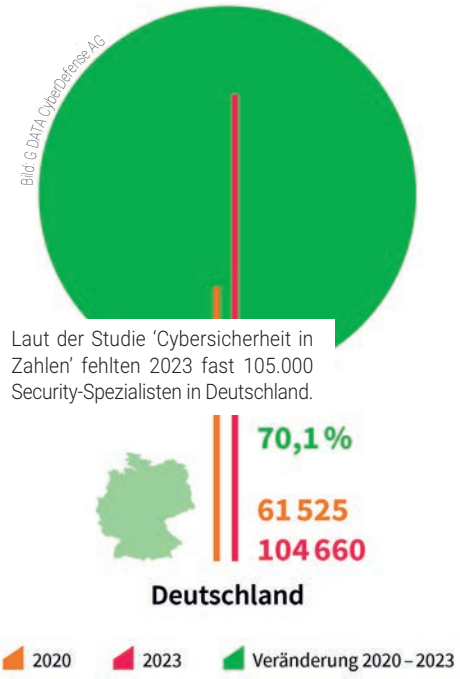
Managed Extended Detection and Response

IT-Security ausgelagert


Bild: ©kiri/stock.adobe.com

IT-Abteilungen in Unternehmen fehlt es oft an Zeit und Fachkräften, wenn es um das Thema IT-Security geht. Die Cyberbedrohungslage macht davor nicht halt und auch neue Auflagen wie etwa die NIS-2-Richtlinie setzen Unternehmen unter Zugzwang. Warum also nicht einen Teil der IT-Sicherheit an Dritte übergeben?

Im Bereich IT-Sicherheit wird es immer schwieriger, mit den Entwicklungen Schritt zu halten. Das liegt unter anderem am Katz-und-Maus-Spiel zwischen Cyberkriminellen und Anbietern von IT-Security-Systemen. Für Unternehmen ist das eine schwierige Situation, denn IT-Abteilungen haben oft nicht die Zeit, um sich mit den aktuellen Möglichkeiten der Abwehr von Cyberangriffen zu beschäftigen. Teamleiter kämpfen etwa mit Fachkräftemangel: Im Jahr 2023 fehlten laut der Studie 'Cybersicherheit in Zahlen' von G Data CyberDefense, Statista und Brand Eins fast 105.000 Security-Spezialisten in Deutschland. Von 2020 bis 2023 vergrößerte sich diese Lücke um 70 Prozent.



Laut der Studie 'Cybersicherheit in Zahlen' fehlten 2023 fast 105.000 Security-Spezialisten in Deutschland.

NIS-2-konform werden

Für zusätzliches Kopfzerbrechen bei IT-Verantwortlichen könnte die Network-and-Information-Security Directive 2 (NIS-2) der Europäischen Union sorgen. Sie setzt neue Standards für die Cybersicherheit kritischer Infrastrukturen und erweitert den Anwendungsbereich der Sicherheitsanforderungen auf eine größere Anzahl von Unternehmen. Das Ziel: „Verhütung, Erkennung, Analyse und Eindämmung von Sicherheitsvorfällen oder die Reaktion darauf und die Erholung davon". Betroffen sind Firmen, die einem der 18 Sektoren angehören oder unter Sonderregelungen fallen.

Response-Team ausgelagert

Eine Möglichkeit, diesen Einflussfaktoren zu begegnen, ist Managed Extended Detection and Response (MXDR). MXDR überwacht die IT-Systeme und reagiert auf erkannte Cyberattacken. Im Hintergrund steht möglichst rund um die Uhr ein Analystenteam zur Verfügung. Bestätigt sich der Verdacht eines Angriffs, kann das Team schnell reagieren.

Augen auf bei der Auswahl

IT-Verantwortliche erhalten oft einen persönlichen Ansprechpartner. Für Anwender kann es zudem bedeutsam sein, ob die Anbieter die verwendete Schutztechnologie selbst entwickeln oder mit eingekaufter Software arbeiten. Dies kann beeinflussen, wie Dienstleister die Systemmeldungen interpretieren. Auch ergeben sich so Unterschiede bezüglich der individuellen Anpassbarkeit. Das Thema Datenschutz ist bei Managed-Security-Dienstleistungen ebenfalls wichtig. Immerhin bekommen Anbieter Einblick in Unternehmensdaten. Werden zu viele Daten gesammelt, kann dies das Vertrauensverhältnis gefährden. Je nach Sitz des Anbieters gelten hier unterschiedliche Gesetze zum Datenschutz und auch zur Datensparsamkeit.

Spielraum für das Personal

MXDR unterstützt Unternehmen, ihren Sicherheitsanforderungen nachzukommen. Für IT-Verantwortliche ist ein Managed-Extended-Detection-and-Response-System eine Möglichkeit, ein höheres IT-Sicherheitsniveau zu erlangen, auch ohne zusätzliches Fachpersonal. Zudem wird eventuell Zeit für Aufgaben neben der IT-Security frei. ■

G DATA CyberDefense AG
www.gdata.de