Digitale Sicherheit von Produktionsanlagen: Achtung! Ihre Welt könnte plötzlich Kopf stehen!

Digitale Sicherheit von Produktionsanlagen:

ACHTUNG! IHRE WELT KÖNNTE PLÖTZLICH KOPF STEHEN!

Maschinen und Roboter, die rund um die Uhr produzieren, sind heute hochgradig vernetzt – sowohl untereinander als auch mit der Unternehmens-IT. Eingebettete Systeme kommunizieren selbständig miteinander, Anlagenführer überwachen und steuern aus der Ferne, Planungssysteme aus der Cloud berechnen Auftragsschritte und Maschinenbelegungen, Wartungspersonal greift weltweit zu und führt Konfigurationsänderungen durch.

Für Industrieunternehmen ist die Bedeutung von Schutzmechanismen für ihre „Operational Technology (OT)" deshalb heute zumindest gleich hoch wie die der physischen Schutzmaßnahmen für eine Fabrik. Über die Netzwerk-Verbindungen können Angreifer in die Systeme eindringen und sie manipulieren. Schadsoftware kann weite Bereiche vollständig lahmlegen und dabei auch immense physische Schäden sowie Gefahren für Leib und Leben verur-

Bild/Image: istock.com/gilaxia

Digital security of production facilities:

When your world is suddenly turned upside down!

Machines and robots, which operate around the clock in modern production facilities, are highly interconnected – both within OT (Operational Technology) and with IT. Embedded systems communicate independently with one another, plant operators monitor

sachen. Die Gefahr ist real: Die Ransomware Petya & NotPetya legten 2017 Markenhersteller für Schokolade und Kosmetik, Reederei, weitere multinationale Konzerne und Behörden lahm. Nicht erst seit diesen millionenteuren Produktionsausfällen ist klar, dass Fabriken und Anlagen Ziele für Cyber-Angriffe sind.

OT- und IT-Sicherheit in der industriellen Produktion unterliegt jedoch besonderen Rahmenbedingungen: Die Steuerung von Produktionsanlagen stellt Echtzeit-Anforderungen und ist 24/7 im Einsatz. Das macht Veränderungen auf den Systemen schwierig bis unmöglich. Das heißt zum Beispiel, dass Software-Patches auf den Systemen, Malware-Scannern und Antivirus-Programmen die Funktionsfähigkeit beeinträchtigen können. Hinzu kommt, dass sich der vergleichsweise lange Nutzungszeitraum von Hard- und Software in der Produktion erheblich von anderen Einsatzgebieten unterscheidet.

Für Produktionsumgebungen müssen also durchdachte Sicherheitskonzepte gefunden werden, um OT-Sicherheit – sowohl von neuen Systemen als auch von Altanlagen – in der Praxis umzusetzen. Die Konzentration liegt dabei immer auf der zeitnahen Erkennung von IT-Sicherheitsproblemen und Cyberangreifern. Die Sicherheitslage des Unternehmens muss auf Knopfdruck aktuell und auf einen Blick erfassbar sein. Angreifern werden so nahezu alle Einfallstore verschlossen.

Dazu braucht es Technologie, Experten und Prozesse. Softwareseitig stehen spezielle OT-Risikoerkennungsmodule zur Verfügung. Allem voran werden damit Protokolle und Applikationen im Netzwerkverkehr identifiziert, extrahierte Daten analysiert und Anomalien visualisiert. Stichwort: Industrial Network & Behaviour Analysis. Daneben werden sicherheitsrelevante Hinweise durch die Sammlung, Analyse und Korrelation von Logs aus verschiedenen Quellen – Industrial System Log Collection & Analysis – gewonnen. Schlussendlich führen Schwachstellen-Scans in ausgewählten Bereichen und Umgebungen – Selective Vulnerability Management & Assessment – zu wertvollen Informationen. Korreliert man die erkannten potentiell sicherheitsrelevanten Informationen aus allen drei Modulen erhält man qualitativ sehr hochwertige Informationen über den aktuellen „Gesundheitszustand" der OT.

Die Weiterverarbeitung der Ergebnisse ist aufgrund der Komplexität Sicherheitsspezialisten vorbehalten. Sie bewerten und priorisieren die automatisiert gewonnenen Erkenntnisse. Schlussendlich stellen sie alle Informationen übersichtlich in einem zentralen Portal zur Verfügung, auf das die relevanten Stakeholder – unter anderem IT & OT Operations Teams, aber auch das Unternehmensmanagement – Zugriff haben oder aus dem sie regelmäßig maßgeschneiderte und für sie verständliche und hilfreiche Berichte erhalten. Funktionieren die Prozesse von der eigentlichen automatisierten Erkennung bis hin zur zeitnahen Behebung von tatsächlichen Problemen, werden es Angreifer sehr schwer haben, Schaden an Produktionsanlagen anzurichten.

and control remotely, cloud planning systems calculate job steps and machine scheduling, maintenance personnel gain access and make changes to configurations from all over the world.

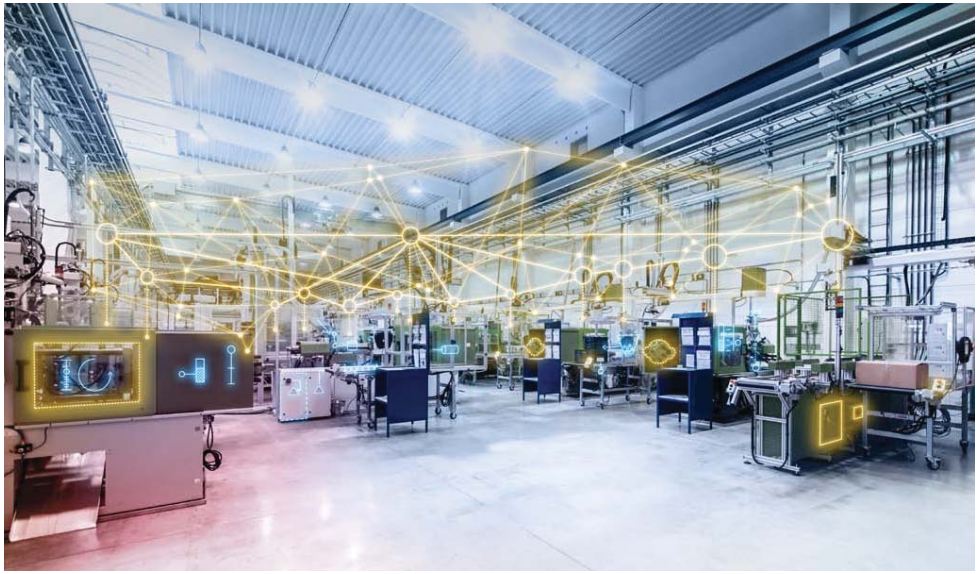
Nowadays, protective mechanisms for OT and IT are at least just as important as the physical measures taken to protect a factory. Threats can penetrate and manipulate systems via network connections. Malware can completely paralyse vast areas and also cause immense physical damage, as well as putting life in danger. It was clear that factories and plants were the targets of cyber attacks long before the numerous production failures experienced by the multinationals in 2017.

Particular constraints are applicable to OT and IT security in industrial production. Production plant control technology has real-time requirements that make it difficult if not impossible to modify the systems. This means, for instance, that software patches on the systems, malware scanners and antivirus programs can impair functionality. There is also the fact that hardware and software are used for comparably long periods in production, in stark contrast to other applications.

Sophisticated security concepts have to be found for the production environments so that OT and IT security can be put into practice both for new systems and old equipment. The focus here is always on the timely detection of IT security problems and cyber attackers. It must be possible to determine the current security situation of the company at a glance at the touch of a button, thereby ensuring that almost all entry gates are closed to attackers.

This requires technology, experts and processes. In terms of software, special OT risk detection modules are available. First and foremost, such software identifies protocols and applications in network traffic, analyses extracted data and visualises anomalies. Keyword: Industrial Network & Behaviour Analysis. In addition, security-relevant information is gained through the collection, analysis and correlation of logs from various sources – Industrial System Log Collection & Analysis. Finally, vulnerability scans in selected areas and environments – Selective Vulnerability Management & Assessment – provide valuable information. If the identified potentially security-relevant information from all three modules is correlated, this delivers very high-quality information about the current "health status" of the OT.

The further processing of the results is reserved for security specialists due to the level of complexity. They evaluate and prioritise the automatically generated findings. Finally, they provide all the information in a single, easy-to-understand portal that is accessible by the relevant stakeholders – including IT & OT operations teams and the company management – or from which they receive regular, customised and helpful reports. If the processes work, from the actual automated detection to the timely resolution of actual problems, attackers will have a very hard time causing damage to production facilities.



Maschinen und Roboter sind ständig vernetzt. / Machines and robots are highly interconnected.

Bild/Image: istock.com/yoth4nn