Cyber Security in der industriellen Automation

Industrie 4.0 und das Industrial Internet of Things (IIoT) eröffnen Unternehmen immer neue, lukrative Geschäftsmodelle. Allerdings birgt der damit einhergehende Vernetzungsgrad auch einige Risiken. Das Thema IT-Sicherheit wird zum strategischen Faktor für den Unternehmenserfolg.

Unternehmen müssen Cyber-Kriminalität wirksam bekämpfen. **Foto** Shutterstock/Pasko Maksim

Immer intelligentere Malware, eine wachsende Anzahl mobiler Mitarbeiter und die zunehmende Adaption von Cloud-Services stellen Unternehmen vor völlig neue Sicherheitsanforderungen. Cyber-Kriminelle automatisieren ihre Angriffe, während viele Firmen noch mit einem unterbesetzten Sicherheitsteam, manuellen Prozessen und unterschiedlichen Systemen kämpfen. Die Unternehmen verstehen zwar, wie wichtig Automatisierung ist, um fehlende Cyber-Security-Kompetenz auszugleichen und eine bessere Sicherheit im Unternehmen zu erreichen. Mit der Entscheidung, wie, wann und wo sie automatisieren sollen, tun sie sich jedoch nach wie vor schwer. Zu diesem Ergebnis kommt im Sommer 2018 die Studie „The Challenge of Building the Right Security Automation Architecture", die Juniper Networks in Zusammenarbeit mit dem Ponemon Institut veröffentlicht hat.

Fehlende Security-Experten

Bis 2021 wird der Kampf gegen die Cyber-Kriminalität Unternehmen weltweit mehr als sechs Billionen US-Dollar pro Jahr kosten und es wird 3,5 Millionen offene Security-Jobs geben, prognostiziert eine Studie von Cybersecurity Ventures. Diese Ergebnisse spiegelt auch die Uniper Umfrage wider: 70 Prozent der Befragten halten Automatisierung für sehr wichtig, wenn es um erfolgreiche Sicherheit geht. Mehr als die Hälfte kämpft jedoch mit zu vielen Anbietern und fehlenden Security-Experten für die Implementierung. „Die Cybercrime-Landschaft ist unglaublich groß, organisiert und automatisiert. Cyber-Kriminelle verfügen über hohe Mittel und folgen keinen Regeln", erklärt Amy James, Security Marketing Leader bei Juniper Networks. „Unternehmen müssen sich anpassen und für gleiche Bedingungen sorgen. Sie können nicht über manuelle Sicherheitslösungen verfügen und erwarten, dass sie Cyber-Kriminelle damit erfolgreich bekämpfen."

Nachgefragt ....

... bei Sebastian Rohr, IT-Sicherheits-Experte

Sebastian Rohr

Foto dance-photos.de

Was raten Sie Unternehmen aus der Industrie 4.0?

Security by Design! Ohne eine gewisse Basis-Sicherheit sind alle Bemühungen um Industrie 4.0 von einem so hohen Risiko überschattet, dass es aus unternehmerischer Vorsicht gar keine Umsetzung geben dürfte.

Warum ist es so wichtig, jetzt die Produktionsanlagen vor Cyberattacken zu schützen?

Neben der Buchhaltung beziehungsweise dem Finanzwesen ist natürlich die Produktion der Stützpfeiler der Wertschöpfung. Wer die Sicherheit der Produktion durch vorschnelle „Öffnung" gegenüber der Industrie 4.0, dem Internet und der Cloud riskiert, bringt damit direkt den Fortbestand seines Unternehmens in Gefahr. Natürlich gilt es, die Chancen der Industrie 4.0 zu ergreifen, aber bitte nur mit einem guten Sicherheitskonzept.

Wie lässt sich eine wirksame Security-Automation-Architektur aufbauen?

Trennung ist das Stichwort! Eine gute Security-Automation-Architektur kann nur unter weitestgehender Abschottung der Produktion/Automation vom Rest des Netzes, vom Rest der Welt erfolgen. Es gilt, eine richtige Datenfluss-Analyse und eine Risikobetrachtung für diese Datenflüsse zu vollführen. Nur wer den Wert seiner Daten kennt, kann diese auch sinnvoll schützen. Es muss nicht alles verschlüsselt und überall vollständig geschützt werden. Es kommt auf die angemessene Umsetzung von Sicherheitsmaßnahmen an.

> „Nur wer den Wert seiner Daten kennt, kann diese auch sinnvoll schützen."

Ist der Fachkräftemangel ein Hindernis?

Auf jeden Fall! Nicht nur Automation-Experten und IT-Experten sind gefragt, sondern eben auch Experten für Automation und IT. Experten für IT-Sicherheit in der Automation sind ebenfalls Mangelware. Es hilft nur eines: Cross-Training. IT-Experten müssen Automation lernen und umgekehrt. Und beide Gruppen müssen ein Basiswissen an (IT-) Sicherheit aufbauen.

Das Gespräch führte Heike Reinhold.