++++ PRESSEMITTEILUNG ++++

TAUCHA, 05.04.2018

Große und kleine Betriebe sind von Cyberangriffen und Netzwerkfehlern bedroht

Vernetzte Industrie steht im Fokus der diesjährigen HANNOVER MESSE Ende April / Digitalisierung in der Industrie braucht eine effektive Überwachung der Steuerungsnetze

Vernetzte Maschinen, die miteinander kommunizieren und aufeinander abgestimmt zusammenarbeiten und das selbstständig, reibungslos und schnell – in der Fabrik der Zukunft sind sämtliche Produktionsabläufe eng digital vernetzt und greifen fließend ineinander. Diese neue, digitalgesteuerte Art der Produktion wird unter dem Schlagwort Industrie 4.0 zusammengefasst. „Integrated Industry – Connect & Collaborate" nennt sich dies auf der internationalen, renommierten HANNOVER MESSE (23.-27.04.2018), die das Prinzip zum diesjährigen Leitthema macht. Doch die Digitalisierung und Vernetzung von Abläufen braucht verlässliche IT- und Operational Technology (OT)-Infrastrukturen. Und damit gewinnt ein Aspekt immer stärker an Bedeutung: Industrial Security.

„Industrie 4.0 revolutioniert die Produktion entscheidend, bietet aber auch zusätzliche Angriffsmöglichkeiten für Datenspione, die Schwachstellen und Sicherheitslücken in Prozessen gezielt suchen und aufdecken", erklärt Andreas Liefeith, Leiter des Arbeitskreises IT-Sicherheit im Cluster IT Mitteldeutschland e. V. und Leiter Marketing der procilon GROUP, „Unserer Erfahrung nach sind es dabei nicht nur die großen Wirtschaftsplayer, auf die sich die Angriffe von Hackern konzentrieren. Kleine und mittelständische Unternehmen stehen genauso im Fokus von Cyberkriminellen. IT-Sicherheit muss deshalb ein zentrales Thema für alle Unternehmen sein, um Produktions- und Kommunikationsprozessen bestmöglich abzusichern."

Dass das Gefahrenpotenzial vorhanden ist, zeigt zum Beispiel die jüngste Kriminalitätsstatistik des Sächsischen Staatsministeriums des Innern Ende März 2018. Demnach hat die Cyberkriminalität 2017 im Vergleich zum Vorjahr um fast neun Prozent (8,8 Prozent) zugenommen. Insgesamt registrierte die Polizei 11.173 Straftaten. Die Zahl der Angriffe auf Datennetze stieg sogar um fast ein Viertel (um 23,7 Prozent auf insgesamt 2.652 Fälle). Gleichzeitig rechnet die Polizei mit einer hohen Dunkelzahl.

Nach einer Befragung des Log Management-Lösungsanbieters Balabit unter rund 400 IT-Managern hatten im Vorjahr 79 Prozent einen Einbruch in ihre Unternehmens-IT verzeichnet. Allerdings glaubten viele Befragte, dass sie einen Angriff im Zweifelsfall nicht unbedingt bemerken würden. Nur 48 Prozent waren sich sicher, einen solchen auch aufzudecken.

Grundsätzlich gehen IT-Sicherheitsexperten davon aus, dass Unternehmen Angriffe auf ihre IT-Systeme häufig gar nicht bemerken. Daher ist es zunächst wichtig, einen stattfindenden Angriff aufzudecken und zu erkennen. Kristin Preßler, Mitglied im Arbeitskreis IT-Sicherheit des Clusters IT und Geschäftsführerin der Rhebo GmbH: „Der Ansatz ist, Anomalien innerhalb der Kommunikation von Steuerungsnetzen erkennen, denn jeglicher Störungsfaktor für die reibungslose Produktion spiegelt sich in der Netzwerkkommunikation wider. Die Kommunikationsstruktur in Steuerungsnetzen oder Industrial Control Systems ist stark deterministisch. Es gibt klare, sich wiederholende Muster und Befehle, nach denen sich zum Beispiel ein Roboterarm bewegt. Wird eine Manipulation versucht oder gibt es netzwerkinterne Probleme, zeigt sich das zuerst in der Kommunikation des Steuerungsnetzes. Diese Veränderung muss als Anomalie in Echtzeit an den Betreiber gemeldet werden, damit er umgehend darauf reagieren kann." Um diese Anomalien zu erkennen, müssen alle Netzwerkprozesse und der damit verbundene Datenverkehr transparent gemacht werden. Selbstlernende Programme speichern die regulären Kommunikationsvorgänge und erkennen, wenn es Abweichungen davon gibt. Auf diese Weise lassen sich in Echtzeit Sicherheitsrisiken und Netzwerkfehler aufdecken. Damit ermitteln Programme zur industriellen Anomalieerkennung auch fehlerhafte Einstellungen der Netzwerke, decken Potenziale zur Steigerung der Effizienz auf und reduzieren Ausfallzeiten.

Liegt der Verdacht für einen Angriff auf das Steuerungsnetz vor, ist es nötig, die Anomalie zu protokollieren und am besten rechtssicher zu belegen. „Für Betreiber so genannter Kritischer Infrastrukturen – wie Anbieter im Bereich Energie, Wasser oder Verkehr – ist es schon Pflicht, lückenlos IT-Sicherheitsverstöße zu dokumentieren und zu melden. Aber auch Unternehmen, die bisher per Gesetz nicht gebunden sind, sollten sich ernsthaft um bestmögliche Sicherheitsvorkehrungen bemühen. Die Techniken der Cyberkriminellen werden immer raffinierter und das Wissen aus der hiesigen Wirtschaft ist für Kriminelle weltweit interessant", so Liefeith, „Hier gilt es aus unserer Sicht, in der hierzulande überwiegend mittelständischen Unternehmerschaft deutlich nachzurüsten. Experten, die sich auf hocheffiziente, ausgeklügelte IT-Sicherheitsmechanismen spezialisiert haben, stehen in Mitteldeutschland zahlreich zur Verfügung."

Zum Cluster IT Mitteldeutschland e. V.

Der Cluster IT ist das Branchennetzwerk der IT-Wirtschaft in Sachsen, Sachsen-Anhalt und Thüringen mit der Zielsetzung, die Aktivitäten der Branche zu koordinieren und sichtbar zu machen. Gegründet wurde der Verein im Jahr 2009 und besitzt mittlerweile knapp 50 Mitglieder. www.it-mitteldeutschland.de.

Zur Rhebo GmbH

Rhebo ist ein deutsches Technologieunternehmen, das sich auf Ausfallsicherheit industrieller Steuerungssysteme und Kritischer Infrastrukturen mittels Detailüberwachung der Datenkommunikation spezialisiert hat. Das Unternehmen wird im internationalen „Marktführer für betriebstechnische Sicherheit 2017“ des IT-Marktanalysten Gartner Inc. als einziger deutscher Hersteller einer industriellen Anomalieerkennung unter den Top-30-Anbietern genannt. Rhebo ist u.a. auf der HANNOVER MESSE präsent und vergibt für interessierte Firmen Messetickets. www.rhebo.com

Zur procilon GROUP

Die Unternehmen der procilon Gruppe haben sich seit mehr als 15 Jahren auf die Entwicklung kryptologischer Software sowie die strategische Beratung zu Informationssicherheit und Datenschutz spezialisiert. Heute haben nahezu 1.400 Unternehmen, Organisationen und Behörden vorbeugende technische und organisatorische Maßnahmen zum Schutz ihrer Daten mit procilon Unterstützung ergriffen. www.procilon.de