Sicherheitslücken – die Kehrseite der Digitalisierung

Industrielle Abläufe und Anlagen werden zunehmend digital miteinander vernetzt. Das bringt diverse Vorteile mit sich. Doch die digitale Transformation des Industriesektors birgt auch Risiken: Denn durch die Vernetzung werden Unternehmen auf völlig neue Art und Weise angreifbar. Das ist vor allem dann prekär, wenn Firmen nicht die notwendigen Vorkehrungen treffen.

TEXT **SMA**

Eine Industriemaschine generiert Gewinn – so lange sie reibungslos läuft und durchgehend produziert. Steht sie hingegen still und kommt es zu Produktionseinbussen, bringt sie dem Unternehmen schnell Verluste ein. Daher stellt die Verfügbarkeit der eigenen Produktionsstätten das wichtigste Gut für Industrieunternehmen dar, betonen Fachleute.

Die digitale Transformation des Industriesektors führt zu einer deutlichen Erhöhung dieser Verfügbarkeit: Dies, indem sämtliche Maschinen, Fertigungsschritte sowie die Logistik miteinander digital verbunden werden. Das Resultat ist eine durchgehende Produktionskette, die einen hohen Automatisierungsgrad aufweist und somit effizient und gleichzeitig kostengünstig operiert.

Nicht alles eitel Sonnenschein

Doch neben diesen klaren Vorteilen machen Branchenkenner immer wieder auch auf Gefahrenszenarien aufmerksam. Denn die Digitalisierung hat eine Kehrseite: Kommt es nämlich zu einem technischen Problem oder gar einem «Angriff von aussen», beschränkt sich der potenzielle Schadensradius nicht mehr nur auf eine einzelne Maschine oder Anlage – sondern kann im schlimmsten Fall die gesamte Fertigungskette betreffen. Stehen dann in der Folge die Maschinen still, bzw. kommt es zu einem länger andauernden Produktionsstopp, kann das gerade für KMU schnell existenzbedrohend werden. Dies nicht zuletzt deshalb, weil angesichts der zunehmenden technischen Komplexität die Behebung eines Sicherheitsvorfalls lange Zeit in Anspruch nehmen kann. Darum betonen Sicherheitsfachleute durchs Band: Es ist besser, einen Vorfall erst gar nicht entstehen zu lassen, anstatt sich im Nachhinein mit seinen Folgen herumschlagen zu müssen.

Doch wie unterbindet man Sicherheitsvorfälle präventiv? Und mit welchen konkreten Gefahrenszenarien hat man es zu tun? Expertinnen und Experten betonen, dass der erste Schritt in Richtung «mehr Sicherheit» nicht in den Fertigungshallen der Unternehmen geschehen muss – sondern in den Köpfen des Managements. Denn die Anlagenbetreiber müssten sich zuerst im Klaren darüber sein, dass sie neu zu den potenziellen Zielen von Hackern und Industriespionen gehören. Diese Angriffe, gezielt oder wahllos, häufen sich kontinuierlich und betreffen Unternehmen jeder Grösse.

Nun, da alles vernetzt ist, ändert sich das: Branchenkenner erzählen, dass sie quasi täglich beobachten können, wie Produktionsnetze «ans Netz» gehängt werden und sich bald darauf die ersten Probleme bemerkbar machen. Ein sehr reales Gefährdungsszenario ist bspw. ein Angriff mit sogenannter «Ransom Ware». Dabei handelt es sich um Schadprogramme, die ganze PCs sperren oder auch nur einzelne Datensätze verschlüsseln. Die Urheber dieser Programme erpressen die betroffenen Unternehmen dann und stellen quasi eine Lösegeldforderung: Nur wer bezahlt, kann seine Computeranlagen wieder nutzen. Insbesondere in einem digitalisierten Industrieumfeld kann Ransom Ware grossen Schaden anrichten, da die Programme von System zu System übergreifen können.

Fernwartung als Gefahr?

Einer der ganz grossen Vorteile der Digitalisierung im Industriebereich ist die Möglichkeit der «Predictive Maintenance» (vorausschauende Wartung). Zu diesem Zweck überwacht der Maschinenhersteller oder Betreiber das Gerät beim Kunden sozusagen live. Dank dieser ständigen Beobachtung kann etwa ein Ausfall einer Maschinenkomponente vorausgesagt und die Wartung präventiv angesetzt werden. Auf diese Weise lassen sich Stillstandzeiten minimieren und mit anderen Anlagen kompensieren. Doch die stetige Onlineüberwachung stellt laut Fachleuten eine potenzielle Gefährdung dar – denn schliesslich könne es sich um eine unsichere Verbindung handeln, womit Cyberkriminellen Tür und Tor geöffnet wird. Der Tenor: Viele Dienstleister, sprich Anlagenhersteller, würden dem Thema «Sicherheit» noch zu wenig Beachtung schenken.

Wie also lässt sich die Sicherheit erhöhen? Eine Möglichkeit besteht in der Segmentierung der Maschinen. Dies ist laut Sicherheitsfachleuten zwar eine wichtige Massnahme, sie kann aber allein noch nicht alle relevanten Felder abdecken. Darum sei ein flexibles IT-Sicherheitsmanagement ebenfalls essenziell. Dieses muss agil auf neue Gefahrenszenarien reagieren und im Idealfall neue potenzielle Sicherheitsvorfälle antizipieren können. Hierfür empfiehlt sich oft die Kooperation mit einem externen Sicherheitsdienstleister. Denn diese spezialisierten Unternehmen sind u.a. in der Lage, die IT-Umgebung eines Betriebs verschiedenen Stresstests zu unterziehen und so gezielt Schwachstellen aufzudecken. Ebenfalls eine Grundvoraussetzung: Die Sicherheit darf nicht einfach an die interne IT-Abteilung delegiert, sondern muss als zentrale Managementaufgabe wahrgenommen werden.

BRANDREPORT CLUE SECURITY SERVICES AG

«Ohne korrekte Einschätzung ist die Gefahr gross, dass man falsch vorgeht»

Schweizer Industrieunternehmen gehören in Sachen Innovation und Qualität zur Weltspitze. Doch durch die Digitalisierung werden sie mit neuen Sicherheitsproblemen konfrontiert. Um diese erfolgreich bewältigen und die Verfügbarkeit ihrer Anlagen gewährleisten zu können, müssen sie den richtigen Partner an der Hand haben. Wie die Expertinnen und Experten der Clue Security Services AG.

Johannes Raff
CEO Clue Security Services AG

Johannes Raff, wie unterstützen Sie Industrieunternehmen dabei, die Sicherheit ihrer Anlagen zu gewährleisten?

Wir setzen dafür auf zwei zentralen Ebenen an: Einerseits bieten wir unseren Kunden ein «Security-Consulting» an. Dabei geht es darum, zusammen mit ihnen eine nachhaltige und individuelle Security-Strategie zu entwickeln sowie passende Security-Lösungen zu implementieren und auszubauen. Dazu gehört auch ein «Security Awareness Training», also quasi eine Sicherheitsschulung für ihren Betrieb. Denn letztlich ist jede Sicherheitslösung nur so gut wie der Mitarbeiter, der sie bedient. Und andererseits bieten wir mit unseren «Managed Security Services» ein fokusiertes Portfolio an sicherheitsrelevanten Diensten an. Dies gelingt uns durch die konstante Weiterentwicklung der Abwehr-Mechanismen und dem Einsatz von speziellen Industrial Security Appliances, wie zum Beispiel von Barracuda Networks.

Können Sie Beispiele nennen?

Ein essenzielles Element ist etwa «Site Protection». Dafür kombinieren wir modernste Sicherheitsmechanismen mit dynamischen Standort-Anbindungen sowie dem unkomplizierten Zugang zu businessrelevanten Applikationen. Durch die Summe dieser und weiterer Massnahmen können wir die Sicherheit eines Unternehmens aber auch von Produktionsanlagen und Industrial IoT-Systemen deutlich erhöhen. Das von Clue betriebene Cyber Defence Center trägt zur kontinuierlichen Überwachung der Schutzmechanissmen bei und reagiert proaktiv auf Sicherheitsvorfälle, bevor diese Schaden anrichten können. Ein weiterer wichtiger «Managed Service» ist «Vulnerability Management». Dies ist für Industriefirmen in der Zeit zunehmender digitaler Vernetzung immer wichtiger.

Inwiefern?

Damit moderne IT-Infrastrukturen auf einem sicheren Stand sind, müssen Schwachstellen rechtzeitig als solche identifiziert werden. Zu diesem Zweck müssen Unternehmen verwundbare Systeme erkennen, aktualisieren und schützen. Doch ohne die korrekte Einschätzung der Risiken und Gefahren ist die Wahrscheinlichkeit gross, dass man falsch vorgeht. Genau hier setzt «Vulnerability Management» an: Wir überwachen die Kundensysteme kontinuierlich und decken Sicherheitslücken schnell auf – sodass diese direkt behoben werden können.

Wie läuft ein Mandat mit Clue Security typischerweise ab?

Am Anfang jeder Zusammenarbeit steht das persönliche Gespräch mit einem Spezialisten, um die individuellen Ansprüche und Herausforderungen des Kundenunternehmens zu erfassen. Unsere Dienstleistungen zeichnen sich aus durch Transparenz und Einfachheit: Die Clue Managed Security Services sind modular aufgebaut, sodass unsere Kunden sie genau in dem Umfang nutzen können, der für sie ideal ist. Darüber hinaus sind unsere Dienstleistungen als «Abo» konzipiert: Damit haben unsere Klienten zu jeder Zeit die absolute Übersicht und Kontrolle und profitieren von kürzeren Implementationszeiten.

Weitere Informationen sowie das volle Dienstleistungsportfolio der Clue Security Systems AG unter: **www.clue.ch**

SECURITY SERVICES AG CLUE Barracuda Your journey, secured.