INTERVIEW MIT CHRISTIAN GÄBEL

„Gerade der deutsche Mittelstand hat viel zu verlieren. Wir sind weltweit noch immer Know-how-Träger Nummer 1. Wir laufen Gefahr, unser digitales Gold zu verlieren.“

Christian Gäbel, Business Development Manager Information Security, pco GmbH & Co. KG

Herr Gäbel, Stichwort: IoT-Gefahren. Wie unterscheiden wir IoT-Gefahren in privaten Haushalten und gewerblichen Unternehmen?

Die SmartHome-Vernetzung schreitet ebenso voran wie die Vernetzung von Maschinen und IoT-Endgeräten (Internet der Dinge) in Unternehmen. Schauen wir uns das Beispiel einer smarten Vernetzung von Dingen in Häusern an, das könnten Waschmaschinen, Fernseher und Kaffeemaschinen sein. Wenn ein Angreifer sich hier einen Zugriff verschafft, dann hat das zwar hohe Auswirkungen auf die Sicherheit in der Privatsphäre, aber vermutlich einen geringeren finanziellen Schaden, als dies in der Produktion eines Unternehmens der Fall ist.

Stehen hingegen Maschinen in einem Unternehmen still, fallen logistische Prozesse und Produktionsprozesse aus. Das hat Auswirkungen auf die gesamte Wertschöpfungskette und mindert die Reputation von Unternehmen in der Außenwirkung. Kommt es zu Stillständen, kann ein Unternehmen Ausfälle in Millionenhöhe erzeugen und erleidet dadurch einen großen finanziellen Schaden. Vernetzte Maschinen müssen daher geschützt werden.

Und was unterscheidet produktionsspezifische IoT-Sicherheitslücken von Sicherheitslücken in der Verwaltungs-IT?

In der Produktion werden spezifische technische Protokolle und Systemkomponenten eingesetzt, die sich von IT-Systemen und Anwendungen in der Verwaltungs-IT unterscheiden. Teilweise werden auch sehr alte Systeme und Anwendungen eingesetzt, die nicht erneuert werden. Es ist nicht unüblich, dass Maschinen und Anwendungen eingesetzt werden, die deutlich älter als 10 Jahre sind. Angreifer spezialisieren sich zunehmend auf Schwachstellen dieser Maschinen und bringen sie gezielt zum Stillstand.

Es ist notwendig, auf aktuelle Standards zu achten und diese einzuhalten, und dazu muss man nicht sehr weit schauen. Die Produktions-IT könnte von der Verwaltungs-IT sehr viel lernen, wenn Standards aus der Verwaltung ebenfalls in der Produktion verwendet werden würden.

Worin liegen die Unterschiede möglicher Gefahren in den Bereichen IoT-Systeme/ -Geräte/-Installationen?

Fertigungsnetze bergen ein höheres Risiko für Angriffe: Mehr Dienstleister und Hersteller greifen aufgrund von Wartungsarbeiten oder Einspielung von Updates remote auf die Maschinen oder Dinge zu, ohne Sicherheitsvorgaben zu berücksichtigen. Wer darauf zugreift, wie lange das passiert und was getan wurde, wird nicht erfasst und kontrolliert. Ebenso finden keine Überprüfungen statt, ob diese Zugriffe aus sicheren Wartungsnetzen durchgeführt werden. Im Gegensatz dazu blicken die IT-Abteilungen in Verwaltungsbereichen auf langjährige Erfahrungen zurück und haben meistens definierte technische Abläufe aufgebaut und notwendige Policies dazu entwickelt. Hiermit sind sie signifikant besser aufgestellt als die Fertigungsbereiche in Unternehmen.

Wie ist IoT-Sicherheit im Rahmen einer Gesamtlösung zu sehen? Was bedeutet das für die IT-Strukturen?

Es gilt, gute Erfahrungen aus dem Verwaltungsbereich auf die Produktion zu übertragen, zu standardisieren und kompatibel zu machen. Hierfür gibt es sinnvolle Leitfäden (z. B. ISO 27001), die dazu dienen, sichere Prozesse für die Produktions- und Verwaltungs-IT umzusetzen.

Welche gravierenden Fehler können Mitarbeiter bei IoT machen?

Stellen Sie sich einen Hersteller von Kunststoffprodukten vor. Er hat große Maschinen, die mit Kunststoffgranulat befüllt werden, um die Produkte zu fertigen. Um Zeit zu sparen und Ablesefehler zu vermeiden, soll die manuelle Erfassung der Füllbestände von Mitarbeitern durch IoT-Komponenten zur automatisierten Messung der Füllbestände eingesetzt werden. Die IoT-Endprodukte senden von nun an automatisiert an den Lieferanten, wenn die Füllbestände leer sind. So weit, so gut. Aber die Produktions- und Einkaufsleiter haben eigenständig mit dem Lieferanten der Maschine einen Server und eine Internetverbindung ohne eine Absicherung eingerichtet. Die Meldedaten der Füllstände fließen ohne Abstimmung mit der IT-Abteilung an den Lieferanten. Es besteht das Risiko, dass Daten bei Wettbewerbern landen oder die Schwachstellen von Angreifern leicht gefunden werden können, da der Zugang frei im Internet sichtbar ist. Hier wäre eine Zusammenarbeit der Fachbereiche IT und Produktion ratsam und angebracht, um derartige Szenarien zu vermeiden.

Wer haftet bei erfolgreichen Angriffen durch Hacker oder kriminelle Vereinigungen?

Wenn durch Ausfälle und lange Stillstandszeiten Produkte nicht geliefert werden können, wird auf die vertragliche Vereinbarung geschaut. Kommt es zu einer Haftung, sind immer zuerst die Geschäftsführer in der Verantwortung.

So weit sollte es nicht kommen. Hersteller wie Cisco oder auch Verbände wie die VDMA stellen Leitfäden zur Orientierung zur Verfügung und erklären darin, wie Sicherheit besser gewährleistet wird und welche Standards einzuhalten sind.

Des Weiteren ist zu bedenken, wenn durch einen Cyber-Angriff auch personenbezogene Daten verloren gehen, so muss der Verlust der Daten binnen 72 Stunden bei der Datenschutzbehörde gemeldet werden. Ist das nicht der Fall, drohen hohe Geldstrafen.

Wie groß ist die Akzeptanz von besonderen IoT-Sicherheitssystemen im Mittelstand?

Die Verantwortlichen, die sich mit IoT auseinandersetzen, sehen meist die Vorteile der Wirtschaftlichkeit und Automatisierung. Hingegen wird der Aspekt Sicherheit oftmals nicht ausreichend berücksichtigt. Daher ist es unbedingt erforderlich, ihnen zu erklären, welche Folgen Sicherheitslücken haben können. Und natürlich, welcher Schutz effizient ist. Daher ist es unbedingt nötig, Kunden zu erklären, welche Folgen Sicherheitslücken haben können. Und natürlich, welcher Schutz effizient ist.

Was sollten gerade Mittelständler unbedingt bei der Wahl ihres Sicherheitsdienstleisters beachten? Was sind Ausschlusskriterien? Oder besser gefragt: Wie sieht der ideale Sicherheitsdienstleister aus?

Nicht jeder Anbieter setzt sich mit der industriellen Sicherheit auseinander. Viele wissen nicht, dass Produktions- und Logistikprozesse stark digitalisiert werden und kennen die Abläufe nicht. Da empfiehlt sich ein Anbieter wie die Innovation Alliance, der die Mittelstandskunden kennt und mit den spezifischen Sicherheitsrisiken vertraut ist. Die Innovation Alliance bietet hier gezielte Lösungen.

Wie können Mittelständler ihre IoT-Sicherheit konstant auf hohem Niveau halten?

Neue Gefahren müssen auf jeden Fall schnellstmöglich erkannt und behoben werden. Bei der Innovation Alliance sind alle Partner optimal aufgestellt. Jeder Partner verfügt über ein großes Portfolio von Lösungen und Managed-Security-Services. Für Kunden bedeutet das: Sie werden umgehend über neue Gefahren informiert. Und wir bieten an, diese Sicherheitslücken schnell zu schließen.

Was kann pco im Rahmen der Innovation Alliance für die Informations- und Datensicherheit bei IoT leisten?

IoT- und Information-Security-Lösungen haben viele Facetten. pco hilft mit seinem Know-how dabei, dass wir im Netzwerk der Innovation-Alliance-Mitglieder ein Gesamtkonzept für Informationssicherheit und Digitalisierung anbieten können. Der Gewinner ist der Endkunde, der von dem Gesamtportfolio profitiert.

Fazit

Unternehmer müssen in ihrem Managementsystem für Informationssicherheit die Industriesicherheit einbeziehen, sonst laufen sie Gefahr, ihr „digitales Gold“ (Informationen wie Entwicklungsdaten, Rezepturen etc.) zu verlieren, und auch das Risiko eines Ausfalls der Wertschöpfungsketten steigt massiv an.