Sicherheitsrisiken im Internet der Dinge

Crime as a Service

IT automatisiert vieles: in der industriellen Produktion, zu Hause, auf der Strasse und im Fitnessstudio – aber auch in der Cyberkriminalität. Wie gehen wir damit um? **Von Thomas Zweifel**

Die IT hat die Industrie in den letzten zwanzig Jahren grundlegend verändert. Fabriken wurden umgerüstet, Logistiknetzwerke aufgebaut und übergreifende Wertschöpfungsketten etabliert. Wo früher in Massenfertigung an einem Standort und mit grosser Lagerhaltung produziert wurde, können nun in geschickter Kombination von globaler und lokaler Fertigung (glokale Produktion) zeitnah individualisierte Produkte bereitgestellt werden. Augmented Reality weist im Hochregallager den Weg zum Ersatzteil, cyber-physische Systeme wirken mittels Sensoren und Aktoren in Produktionsprozessen mit und überwachen diese. Dadurch bieten Smart Factories jedoch auch mehr Angriffsflächen für Attacken: vom Diebstahl materieller und immaterieller Assets wie Daten und Prozesse über Werkspionage bis zur handfesten Sabotage.

Derselbe Trend schlägt auch bei der Betriebstechnik durch. Technologiewandel und Kostendruck führen dazu, dass weniger Arbeiten vor Ort ausgeführt werden. Fernzugriffe bergen jedoch Risiken, etwa bei kritischen Infrastrukturen wie Kraft- oder Wasserwerken. Die Lebenszyklen der eingesetzten Technologien sind dort um ein Mehrfaches länger als in der IT. Die zentrale Verwaltung muss also mit verschiedensten Komponenten aus dem letzten Jahrtausend umgehen können – und mit deren nicht auf heutige Bedrohungen ausgerichteten Sicherheitsstandards. Zudem braucht es bei kritischen Infrastrukturen eine Vielzahl von Sensoren, um den Betrieb zu gewährleisten. Auch die neueren Sensoren sind jedoch nicht risikolos. Sie haben deutlich mehr Funktionen und viele verfügen über einen Funk- oder Netzwerkanschluss sowie genügend CPU- und Speicherreserven, um auch in zehn Jahren noch ihren Dienst erledigen zu können. Wird die Sicherheit vernachlässigt, mutieren solche Geräte schnell zu kleinen schlagkräftigen Soldaten in einer Armee von Bots.

Smart Homes, Health & Fahrzeuge

Auch innerhalb der eigenen vier Wände gibt es zahlreiche Veränderungen: Kleine digitale Helfer messen alles Mögliche und erleichtern uns den Alltag, indem sie Daten sammeln. Die Sensormodelle werden in immer kürzeren Zeitabständen durch neue Modelle mit noch mehr Funktionen ersetzt. Dabei bleibt die Sicherheit oft auf der Strecke. Selbst auf der Strasse werden Daten gesammelt: Assistenzsysteme in intelligenten Fahrzeugen gleichen ihre Daten oft direkt mit dem Hersteller ab. Als Benutzer wissen wir nicht, ob unsere Nutzerdaten dafür genügend anonymisiert wurden. Meist ist auch ungeklärt, wem die Daten gehören, welcher Rechtsprechung sie unterstehen, wer sie auswerten darf und wer dafür haftet, wenn sie gestohlen werden.

Bild: iStockphoto/Chombosan

Organisierte Kriminalität

Abgesehen von der Bedrohung des Datenschutzes sind auch die direkten Gefahren nicht zu unterschätzen. So gibt es zum Beispiel bereits Wege, intelligente Schliesssysteme zu knacken, um fremde Fahrzeuge zu öffnen. Sowohl im privaten Umfeld als auch in den Unternehmen spielt die organisierte Kriminalität eine immer grössere Rolle. Auch sie setzt vermehrt auf Arbeitsteilung, Automatisierung und Modularisierung. Dabei nutzen die Cyberkriminellen standardisierte Services wie Plattformen und Botnetze, Frameworks für Trojaner oder Money Mules zur Geldwäsche. Mittlerweile werden schon Gesamtpakete angeboten, zum Beispiel für Ransomware, sozusagen Crime as a Service. Diese Professionalisierung macht einzelne Aufgabenbereiche ersetzbarer und die Bekämpfung schwieriger. Ausserdem ermöglicht die Automatisierung grossflächige Angriffe, wodurch schon eine sehr tiefe Erfolgsquote genügend Ertrag bringt.

Was also tun?

Die Herausforderungen für die Sicherheit sind vielschichtig und müssen auf verschiedenen Wegen angegangen werden. Dazu gehören technische Anpassungen an der Infrastruktur des Endbenutzers ebenso wie Massnahmen bei den Herstellern von Soft- und Hardware sowie regulatorische Vorgaben.

Als Privatperson bleiben einem nur wenige Optionen, zum Beispiel die klassische Abwägung von Vor- und Nachteilen bei der Beschaffung eines Produkts. Dabei ist der offerierte Support essenziell. Bietet der Hersteller wohl in zwei Jahren noch Sicherheits-Updates? Werden die Patches automatisch installiert oder muss der Nutzer das selbst erledigen? Daneben stellen sich Fragen des Datenschutzes und der Eigentümerschaft, gerade bei Fitnesstrackern oder bei einem vernetzten Eigenheim. Weiter kann die private Infrastruktur segmentiert werden, etwa durch die Abkapselung des smarten Hauses, des Autos oder des Backup-Systems in einem eigenen Netz, analog zu den Perimetern in Firmen. Kombiniert mit einem besseren Authentisierungsschutz, beispielsweise mittels eines zweiten Faktors, erhöht dies die Barrieren gegen einen erfolgreichen Angriff oder erlaubt zumindest eine angemessene Wiederherstellung im Schadensfall.

Unternehmen stehen mehr Optionen offen, die Absicherung gestaltet sich aber auch schwieriger. Wer darf in der Industrie 4.0 was machen, wann und wo? Wie werden Schnittstellen geschützt, wer regelt Berechtigungen, wer trägt die Verantwortung und wer haftet? Auch bei der Betriebstechnik muss geklärt werden, wie mit der wachsenden Angriffsfläche umzugehen ist und wie die Masse an Geräten sinnvoll verwaltet und gewartet werden kann. Der Schutz muss in die Tiefe gehen und analog zu den genutzten internen und externen Services modularisiert werden. Es gilt, in jedem der Module eine Kombination von individuellen und vernetzten Schutzmechanismen umzusetzen. Dabei ist zum einen der klassische Perimeterschutz mit Tools wie Virenscanner oder Firewalls zu gewährleisten. Andererseits muss die Früherkennung ausgeweitet werden. Um moderne Angriffe wie Advanced Persistent Threats zu erkennen, braucht es eine gesamtheitliche Überwachung der Systeme. Durch die laufende Überprüfung von Netzwerkübergängen auf Muster und Anomalien lässt sich ein Risk Score generieren. Nur durch die Korrelation solcher Daten ist eine zeitnahe Reaktion und eine Verteidigung in der gesamten Tiefe und über sämtliche Sicherheitsschalen und Module hinweg zu erreichen.

Gleichzeitig wirft die Überwachung natürlich Fragen zum Datenschutz auf: Was ist erlaubt, was nicht? Wer entscheidet, ob Sicherheit oder Privatsphäre höher zu gewichten ist? Manche Entscheidungen müssen auch auf politischem Weg gefunden und beispielsweise mit Regulatorien umgesetzt werden.

«Analog zur organisierten Kriminalität muss die Abwehr professionalisiert werden»

Thomas Zweifel

Gemeinsam sind wir stark

So wichtig es ist, als Einzelner auf Sicherheit zu achten, zur wirksamen Abwehr von Angriffen braucht es Erfahrungsaustausch und Zusammenarbeitsmodelle. Analog zur stärkeren Arbeitsteilung und Strukturierung der Angriffe aufseiten der organisierten Kriminalität muss dabei eine Professionalisierung der Abwehr Einzug halten. Neben der klassischen Schulung von Endbenutzern bedeutet dies die organisierte Kollaboration bei der Bekämpfung von Cyber Threats durch die sogenannte Threat Intelligence. Durch den koordinierten Informationsaustausch zwischen Betroffenen können Frühwarnsysteme zeitnah angepasst und feinjustiert werden. Nur so haben auch kleinere Unternehmen eine Chance, sich gegen neuartige Angriffe zu wehren und sich im ewigen Katz-und-Maus-Spiel ein Überleben zu sichern. ■

Thomas Zweifel
ist Principal IT Consultant bei AdNovum:
www.adnovum.ch