Claas Lorenz,
Researcher,
Genua GMBH

der Anforderungen an die Ausfallsicherheit oft nur unzureichend. Spätestens mit der Vernetzung der Maschinen muss also mit einem aktiven Risikomanagement begonnen werden.

Risikomanagment und IT-Sicherheit

Ein bewährtes Mittel, um Risiken zu begegnen, sind Versicherungen. Cyberversicherungen werden mittlerweile von verschiedenen Anbietern angeboten. Allerdings sind das Leistungsportfolio und die maximalen abgedeckten Schadenssummen noch recht eingeschränkt. Folglich führt an Maßnahmen zur IT-Sicherheit kein Weg vorbei. Denn ein Verzicht auf technische Maßnahmen und eine ausschließliche Nutzung von Versicherungen würde zwangsläufig zu einem allgemeinen Anstieg an Sicherheitsvorfällen und somit Schadensfällen führen. Eine Versicherungspolice ist jedoch nur günstig, wenn die Anzahl der Schadensfälle gering ist. Steigt die Zahl der Sicherheitsvorfälle, wird auch die Cyberversicherung teurer. Cyberversicherungen sind somit allenfalls eine ergänzende Maßnahme auf dem Weg zur Industrie 4.0, können die eigentliche IT-Sicherheit aber nicht ersetzen. Immaterielle Schäden durch Cyber-Attacken wie belastete Kundenbeziehungen oder ein verschlechtertes Unternehmensimage – die oft schwerwiegender sind als die materiellen Einbußen – können mit Versicherungen zudem nicht oder nur unzureichend abgedeckt werden.

Cybersicherheit im IoT

Was also sind nun die größten Herausforderungen bezüglich der Sicherheit von industriellem IoT? Zunächst einmal die langen Investitionszyklen. So ist man sich unter Sicherheitsexperten weitgehend einig, dass eine Versorgung von Geräten mit aktuellen Sicherheitsupdates den höchsten Beitrag zur Sicherheit liefert. Die gelebte Praxis in vielen Unternehmen ist jedoch eine völlig andere. So werden nämlich bei laufenden Systeme keine Updates durchgeführt, obwohl Sicherheitslücken allgemein bekannt sind. Das liegt zum einen daran, dass viele Hersteller ihre Produkte nicht mit Updates versorgen. Aber auch die Sorge vor Störungen des Produktionsprozesses durch Updates ist groß, so dass diese gar nicht oder stark zeitverzögert eingespielt werden. An dieser Stelle können wiederum Versicherungen helfen, die Auswirkungen eines Produktionsausfalls im Zuge fehlerhafter Sicherheitsupdates zu minimieren.

Die zweite zentrale Herausforderung besteht darin, wie man Security by Design im IoT realisieren kann, um eine nachträgliche, teure Absicherung zu vermeiden. Der zur Zeit vielversprechendste Ansatz sind IoT-Plattformen, welche den IoT-Anwendungen eine sichere und dennoch funktionale Basis bieten können. Datenbasierte IoT-Anwendungen bestehen typischerweise aus zwei Teilen. Zum einen werden die Maschinendaten bereits in den Produktionsanlagen vorberarbeitet und diese Zwischenergebnisse dann zur finalen Verarbeitung in die Cloud geschickt.

IoT-Gateway und Cloud-Gateway

Viele IoT-Plattformen folgen dieser Aufteilung in dem sie zwei Bestandteile zur Verfügung stellen: IoT-Gateways und das Cloud-Gateway. Die IoT-Gateways sind Geräte, die am Perimeter zwischen den Maschinen und dem Internet platziert werden. Sie stellen Basisfunktionen wie beispielsweise verschlüsselte Kommunikation oder sicheres Management zur Verfügung und bieten eine Laufzeitumgebung für IoT-Anwendungen, die eine Vorverarbeitung von Laufzeitdaten durchführen. Durch die strikte Trennung von Sicherheitssystemen und Anwendung kann ein hohes Maß an IT-Sicherheit bei größtmöglicher Flexibilität erreicht werden. Die Plattform bietet also Security by Design. Die eigentliche Datenverarbeitung führen die Anwendungen jedoch in der Cloud durch. Damit diese Daten dann vom zugehörigen IoT-Service in der Cloud verarbeitet werden können, werden sie verschlüsselt vom IoT-Gateway zu einem Cloud-Gateway geschickt.

Auch Anwendungen wie die sichere Fernwartung sind mittels IoT-Plattformen möglich. So kann ein Fernwarter sich mit einem Cloudservice verbinden, der wiederum mit einer korrespondierende Fernwartungsanwendung auf dem IoT-Gateway kommuniziert. Die Durchsetzung der Sicherheit durch Verschlüsselung, Zugriffskontrolle und Monitoring wird durch die IoT-Plattform erbracht. Zugleich ermöglicht ihre Flexibilität ein Höchstmaß an Innovationsfähigkeit bei der Umsetzung neuer Anwendungen, welche die Industrie 4.0 ausmachen.

Fazit

Das IoT bietet die herausragende Chance, das Innovationspotenzial der Cloud in die Industrie zu tragen. Um den einhergehenden Risiken der Vernetzung zu begegnen, bieten sich Lösungen mit Security by Design als solide Basis und Cyberversicherungen als ergänzende Maßnahmen an.

Insbesondere sichere IoT-Plattformen haben das Potenzial, eine größtmögliche Flexibilät auf einem hohen Sicherheitsniveau zu erbringen. Claas Lorenz

Internet der Dinge: Security Guidelines

Internet of Things (IoT) und Smart Home sind spätestens seit Amazon Alexa in der Allgemeinheit angekommen. In Deutschland beträgt die Anzahl der Smart-Home-Haushalte etwa 750.000 [1]. Viele davon besitzen mehr als nur ein Smart-Home Gerät [2]. Im Jahr 2020 wird mit mindestens einer Millionen Geräte gerechnet. Kein Wunder, helfen uns Smart-Home Geräte doch beim Energie sparen (Smarte Lampen/Steckdosen/Thermostate), sichern unser zu Hause (Smarte Türschlösser und Alarmanalagen, IP-Kameras, …) und verbessern unsere Lebensqualität im Allgemeinen. Durch Assistenzsysteme wie Amazon Alexa können nicht nur Informationen per Sprachbefehl abgerufen werden, nein es lassen sich auch Smart Home Geräte damit steuern. Durch Technologien wie IFTTT (If this then that) können Geräte Aktionen ausführen wenn ein zuvor definiertes Ereignis auf einem anderen Geräte eintritt wie das Smart Lock wird entsperrt und es ist nach 18 Uhr, dann mache das Licht im Gang an. Kurzum: Internet of Things und Smart Home kann sehr praktisch sein und bietet viele Funktionen.

Allerdings kann diese Funktionsvielfalt auch missbraucht werden. Erfolgreiche Angriffe können teuer für die Opfer sein (Thermostat wird von einem Angreifer aus der Ferne aufgedreht, während die Bewohner im Urlaub sind), sie können gefährlich sein (Smarter Sauna-Ofen überhitzt), sie können unangenehm sein (Besitzer wird durch eigene IP-Kamera ausspioniert) oder alles zusammen: Eine per Smart-Lock verschlossene Tür wird geöffnet, um einzubrechen ohne dabei Spuren zu hinterlassen. Der Einbrecher kann viel stehlen (teuer), auf Privates stoßen (unangenehm) und Zeugen angreifen (gefährlich).

Sicherheit sollte also oberste Priorität haben. Die Wirklichkeit sieht bekanntlich anders aus, da sich Funktionen und Features besser verkaufen als Sicherheit. Insbesondere wenn Technologien noch recht neu sind, wird versucht, möglichst schnell ein Produkt auf den Markt zu bringen. Dies hat zur Folge, dass IT-Sicherheitsmaßnahmen bei Release des Produkts noch nicht hinreichend implementiert sind.

Allerdings hat sich das Sicherheitsniveau schon im Vergleich zu den Vorjahren erhöht – wenn auch nicht immer ausreichend. Das liegt mit daran, dass sich Standards wie ZigBee, Apple Homekit oder Google Nest durchgesetzt haben und sich ein Trend zur Verlagerung in die Cloud erkennen lässt. Wobei letzteres zwar einen positiven Effekt für die sichere Umsetzung, jedoch negative Auswirkungen auf die Privatsphäre hat. Positiv ist die angestiegene Rechnerkapazität der Prozessoren zu sehen, die (stärkere) Verschlüsslung unterstützen. Dennoch sind noch längst nicht alle Geräte sicher. Oftmals kann der Nutzer zwar unsichere Funktionen der Geräte deaktivieren (Zugriff aus dem Internet o.ä.), doch da längst nicht mehr nur technisch versierte Nutzer IoT-Geräte beschaffen, ist dies nicht ausreichend. Ein Gerät muss von Haus aus sicher sein und sicher bleiben. Hierzu sollten folgende sechs Prinzipien umgesetzt werden:

1. Automatische und sichere Firmware Updates
2. Zufällig generierte Passwörter statt Standardpasswörtern
3. Sichere Standardeinstellungen
4. Einsatz von Verschlüsselung
5. Datensparsamkeit (Datenschutz)
6. Bewährte Algorithmen verwenden

Wilfried Kirsch,
Security Consultant
softScheck GmbH
Sankt Augustin

1 Automatische und sichere Firmware Updates

Seit 2016 befällt Mirai hunderttausende von IoT-Geräten wie IP-Kameras und fügt diese Geräte bereits existierenden Botnetzen hinzu [3]. Die ausgenutzten Sicherheitslücken sind bekannt und könnten geschlossen werden, doch für viele dieser Geräte ist gar kein Firmware-Update vorgesehen, weswegen Mirai wohl auch in den nächsten Jahren noch existieren dürfte.

IoT-Geräte sollten daher die Möglichkeit eines Firmware-Updates implementieren. Falls die Geräte Zugriff auf das Internet haben, sollte standardmäßig automatisch upgedatet werden. Doch neben automatischen Updates ist es auch wichtig, dass diese integer sind, korrekt eingespielt werden. Hat ein Angreifer die Möglichkeit die Firmware vor der Installation zu manipulieren, so wird durch das Firmware-Update ein neuer Angriffsvektor geschaffen. Für schnelle und sichere Firmware-Updates von IoT-Geräten gibt es mehrere Ansätze [4]:

- Schnorr-Updates
- PC-basiert
- Physical unclonable function (PUFs)
- Blockchain
- Schneider-IoT Update Mechanismus
- Mongoose OS

Jeder dieser Ansätze hat Vor- und Nachteile. Als Entwickler ist es daher empfehlenswert, diese Ansätze zu vergleichen, um die passende Lösung für die eigene Anwendungsumgebung zu finden.

2 Zufällig generierte Passwörter statt Standardpasswörtern

Viele IoT-Geräte besitzen Standardlogins wie admin:admin oder root:1234. Sind diese Geräte aus dem Internet aus erreichbar und ändert der Nutzer nicht das Passwort, so hat der Angreifer leichtes Spiel. Geräte mit Standard-Passwörtern sind schnell im Internet bekannt und durch Suchmaschinen wie Shodan für jedermann (!) leicht zu finden. Auch von fest enkodierten Service-Passwörtern ist abzuraten, da diese durch Reverse Engineering gefunden und dann ebenfalls ins Internet gestellt werden können. Besser wäre es so zu verfahren, wie es seit Jahren bei Routern üblich is:. Ein zufällig generiertes Passwort, welches dem Geräte durch beispielsweise einen Aufkleber beiliegt. Vergisst der Nutzer sein Passwort, so kann er durch Zurücksetzen des Gerätes den Urzustand wiederherstellen.