Das Internet der Dinge ermöglicht neue Funktionen und Effizienzgewinne. Gleichzeitig steigt jedoch die Wichtigkeit der IT-Sicherheit.
(Bild: iStock/Rawpixel)

Angriffe auf IoT-Automatisierungssysteme stellen eine reale Bedrohung dar

IT-Sicherheit in der Automatisierung

Digitalisierung, Industrie 4.0, M2M und Smart Factory. Was haben alle diese Begriffe gemeinsam? Die physische Welt der Geräte, Fabriken und Gebäude wird zunehmend um einen digitalen Gegenspieler erweitert. Es entsteht ein Internet der Dinge oder Englisch «Internet of Things» (IoT). IoT erlaubt es, die physische Welt zu überwachen, zu steuern, zu vernetzen und zu erweitern. Durch den kombinatorischen Nutzen aus physischer und digitaler Welt entsteht ein Innovationsschub, der Märkte klassischer physischer Produkte revolutioniert. Gleichzeitig machen uns IoT-Systeme jedoch verwundbarer.

DR. BJÖRN AVAK

War die Zuverlässigkeit von Systemen früher durch die Mechanik bestimmt, sind sie zunehmend anfällig für alle Schwächen von IT-Systemen. Während jedoch bei reiner IT die Gefahr lediglich im Erbeuten, Verfälschen und Löschen von Daten besteht, drohen bei IoT-Systemen Schäden durch Manipulation und Ausfall von Fertigungsstrassen, Kraftwerken oder Gebäudeleittechnik.

In diesem Artikel wird aufgezeigt, dass Angriffe auf IoT-Automatisierungssysteme eine reale Bedrohung darstellen. Anschliessend werden die einzelnen Facetten der IoT-Security vorgestellt, die heute abzudecken sind. Schliesslich wird die konkrete Umsetzung im Unternehmen mittels eines Masterplans erläutert.

Der erste grosse Angriff auf ein IoT-Automatisierungssystem. Zwischen November 2009 und Januar 2010 fielen nachweislich [1] ca. 1000 Gaszentrifugen der Atomanlage Natanz im Iran aus. Es gilt als erwiesen, dass dieser Ausfall durch den Computerwurm Stuxnet verursacht wurde [2]. Das Beispiel zeigt, wie verschachtelt derartige Angriffe ablaufen können:

- Der Anlagenbetreiber oder ein Serviceunternehmen nutzt – absichtlich oder unabsichtlich – einen infizierten USB-Stick an einem Rechner der Anlage.
- Stuxnet nutzt eine Schwäche im Windows-System, um sich vom infizierten USB-Stick auf den Zielrechner zu installieren. Anschliessend prüft Stuxnet diesen und alle anderen Computer im Netzwerk auf angeschlossene Siemens-Steuerungen vom Typ Simatic S7-300 (siehe Abbildung 1) und dazugehörige Softwarepakete Step7 und WinCC. Ist dies der Fall, tarnt sich Stuxnet durch Installation von Software tief im Kernel des Betriebssystems – ein sogenanntes Rootkit.
- Stuxnet testet nun, ob die Simatic S7-300 Frequenzumrichter zweier bestimmter Hersteller mit für Gaszentrifugen üblichen Umdrehungsfrequenzen steuert.
- Wenn ja, werden dem Scada-System historische Messdaten vorgespielt, während Stuxnet die Umdrehungsfrequenzen verändert. Dies führt zu Ausfällen der Gaszentrifugen, die für den Betreiber unerklärlich sind.

Aus dem Fall Stuxnet lassen sich mehrere Lehren in Bezug auf die Sicherheit vernetzter Automatisierungstechnik schliessen:

- Auch Systeme wie die Atomanlage Natanz, welche über keine direkte Verbindung mit dem Internet verfügen, sind – beispielsweise über Konfigurationsrechner der Serviceunternehmen – angreifbar.
- Stuxnet nutzte die Lücke der fest programmierten Zugangsdaten in der Siemens-Software. Viele der Systeme der Automatisierungstechnik sind 10 bis 20 Jahre im Einsatz. Derartige Sicherheitslücken, welche im Laufe der Zeit entstehen, werden nicht durch ein systematisches Patching behoben.
- Planer, Betreiber und Hersteller von Automatisierungssystemen sind auf IoT-Security kaum vorbereitet [3].

Angriffe und Schwachpunkte der jüngeren Zeit. Stuxnet reicht mittlerweile schon einige Jahre zurück. Inzwischen hat sich die Situation durch die anfangs diskutierten Trends noch weiter verschärft. Dies zeigen Angriffe und Schwachpunkte der jüngsten Zeit, welche mittlerweile nicht ausschliesslich Automatisierungssysteme der Industrie, sondern auch andere technische Domänen betreffen.

Beispielfall Industrieautomatisierung. Das Deutsche Bundesamt für Informationssicherheit veröffentlichte im Dezember 2014 Informationen über den Angriff auf ein deutsches Stahlwerk [4]. Der Angreifer erlangte zunächst über Phishing und Social Engineering Zugriff auf das Büronetzwerk. Von dort arbeitete er sich bis in das Produktionsnetzwerk für die Steuerung des Stahlwerks vor. Als Folge der Manipulation konnte ein Hochofen nicht mehr geregelt werden, sodass eine Notabschaltung durchgeführt werden musste. Dies führte zu massiven Schäden an der Anlage.

Beispielfall Gebäudeautomation. Der Basler St. Jakob-Park ist mit 38 500 Plätzen und angeschlossenem Einkaufszentrum das grösste Stadion der Schweiz. Der Zutritt wird mittels eines elektronischen Zutrittskontrollsystems geregelt. Das im «Joggeli» eingesetzte System war im Jahr 2013 für mehrere Monate über einen Internetbrowser frei bedienbar [5]. Dies hätte es Einbrechern im entsprechenden Zeitraum beispielsweise ermöglicht, ohne Gewalteinwirkung nachts in das Einkaufszentrum einzubrechen.

>>

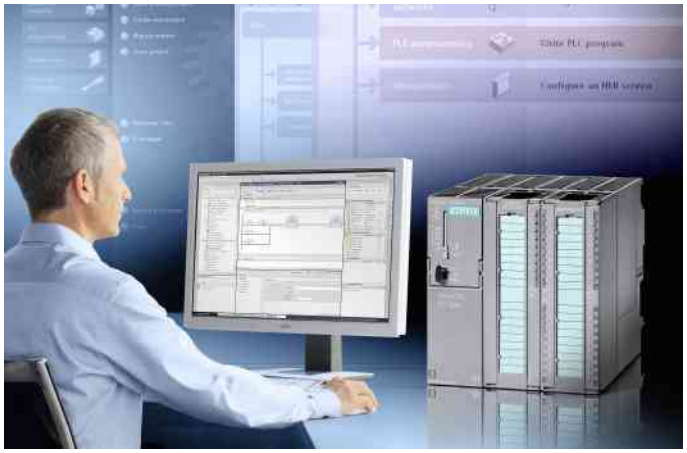
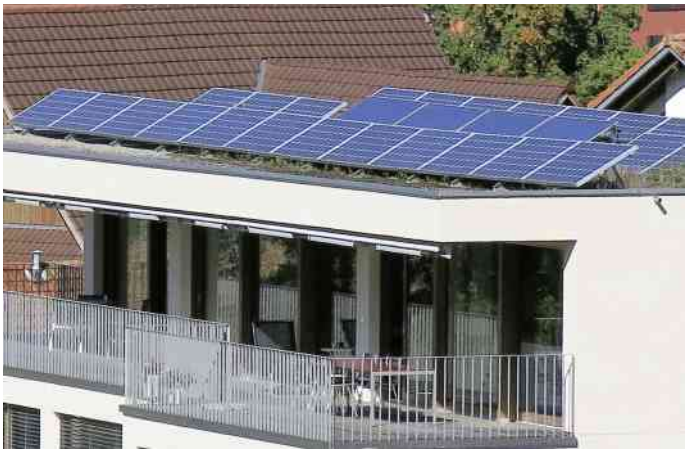


Abbildung 1: Siemens Simatic S7-300 wurde Opfer des ersten grossen Angriffs auf ein IoT-Automatisierungssystem. (Bild: Siemens)



Ob Automations- oder Photovoltaikanlage: Über IoT-Suchmaschinen wie Shodan.io können Hacker gezielt ungeschützte IoT-Systeme suchen. (Bild: Björn Avak)

Beispielfall Stromnetz. Über ein Kommunikationsmodul ist es möglich, Photovoltaikanlagen an das Internet anzubinden, um diese zu visualisieren und zu steuern. Im Herbst 2014 wurde bekannt, dass über 200 Webportale in der Schweiz ungenügend geschützt sind[6]. Allein durch Kenntnis der jeweiligen IP-Adresse war es Angreifern möglich, die persönlichen Daten der Betreiber, d. h. Name, Adresse,

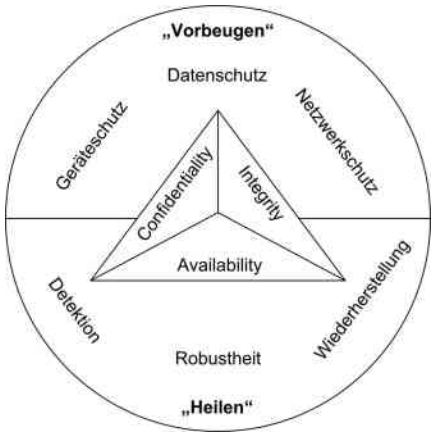


Abbildung 3: Definition und Schutzziele der IoT-Security. (Grafik: Björn Avak)

Stromproduktionsmenge usw. auszulesen sowie die Anlage an- und abzuschalten. Die Melde- und Analysestelle zur Informationssicherung des Bundes (Melani) bestätigte zu diesem Fall, dass bei systematischem Einsatz einer derartigen Sicherheitslücke – man denke an zukünftige Smart Grids – eine Destabilisierung des Stromnetzes möglich wäre. Diese drei Beispiele zeigen einerseits die Breite des Spektrums bedrohter Systeme. Anderseits illustrieren sie auch, dass IT-Sicherheit nicht ausschliesslich von technischen Eigenschaften des Systems, sondern auch von menschlichem Verhalten abhängt. Betreiber sollten insbesondere nicht davon ausgehen, dass die grosse Menge mit dem Internet verbundener Systeme Schutz bietet. Über IoT-Suchmaschinen wie Shodan.io können Hacker ungeschützte IoT-Systeme gezielt suchen und angreifen.

Zielsetzungen der IoT-Security für Automatisierungssysteme. In der IT wird unter Security üblicherweise das «CIA-Konzept» verstanden. In der Domäne der Automatisierung bedeutet dies:

- Confidentiality/Vertraulichkeit: Systemaufbau, -konfiguration und Laufzeitdaten sind ausschliesslich autorisierten Nutzern, Geräten oder Prozessen bekannt.
- Integrity/Integrität: Veränderungen am System oder Laufzeitbefehle können ausschliesslich von autorisierten Nutzern, Geräten oder Prozessen vorgenommen werden. Jede Veränderung wird Audit-sicher geloggt.
- Availability/Verfügbarkeit: Wenn erforderlich, erfüllt das System stets die vorgesehene Funktion. Der autorisierte Zugriff auf das System ist jederzeit möglich.

Um diese Punkte zu gewährleisten, muss jede der Elementklassen des Systems, d. h. Geräte, Netzwerk und Daten präventiv geschützt werden:

- Geräteschutz: Die Geräte sind das «Thing» des IoT-Systems. In der Automatisierungstechnik sind dies üblicherweise Sensoren, Aktoren, I/Os, SPS, HMIs und Leitsysteme. Jedes Gerät muss in sich «gehärtet» sein, d. h. nicht zwingende Zugänge und Services sind deaktiviert. Zugriffsrechte sind auf das notwendige Minimum reduziert und werden fälschungssicher geloggt.
- Datenschutz: Die Daten sind der «digitale» Teil des IoT-Systems. Auf den Geräten gespeicherte oder über das Netzwerk versandte Konfigurations- und Laufzeitdaten sind vor unautorisierter Veränderung und Einsicht geschützt.
- Netzwerkschutz: Das Netzwerk umfasst alle Verbindungen, welche das IoT-System zusammenhalten. Der Zugang zum Netzwerk wird physisch sowie logisch geschützt und ist hochverfügbar.

Daneben sind auch Massnahmen zu ergreifen, um das System nach einem Angriff schnellstmöglich zu «heilen»:

- Detektion: Veränderungen am IoT-System werden erkannt bevor diese kritisch werden.
- Robustheit: Das IoT-System ist so gestaltet, dass es selbst bei Ausfall wichtiger Geräte, des Netzwerks oder Datenverlust inhärent sicher bleibt.
- Wiederherstellung: Nach einem Zwischenfall kann die Funktion schnell wiederhergestellt werden. Wird die IoT-Security-Definition mit den diskutierten Schutzzielen in den Phasen «Vorbeugen» und «Heilen» kombiniert, ergibt sich das Gesamtbild gemäss Abbildung 3.

Masterplan zur Umsetzung der IoT-Security. Es gibt leider keine einfache, auf alle Fälle passende Standardlösung. Es lässt sich jedoch allgemeingültig

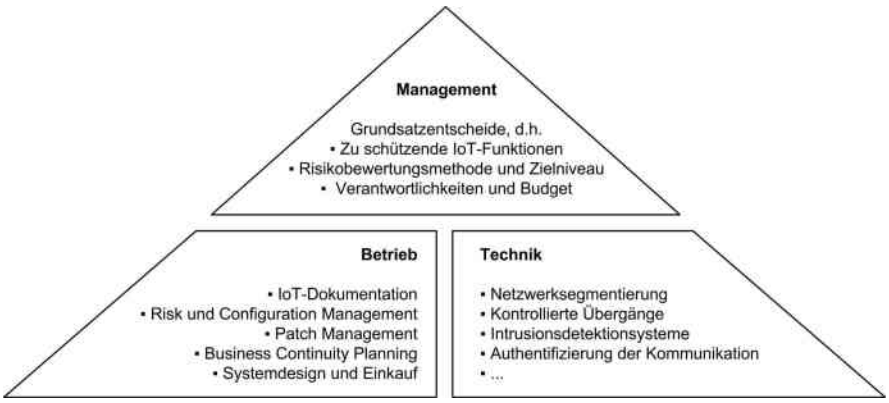


Abbildung 4: Elemente zur Umsetzung im Unternehmen. (Grafik: Björn Avak)

festhalten, dass IoT-Security auf drei Ebenen im Unternehmen zu adressieren ist.

1. Im Management

Das Management ist für das Treffen der Grundsatzentscheide verantwortlich:

- Zu schützende IoT-Funktionen: In einem Workshop zwischen Management und den jeweiligen Domänenexperten werden die zu schützenden IoT-Funktionen identifiziert.
- Risikobewertungsmethode und Zielniveau: Die Festlegung einer standardisierten Risikobewertungsmethode durch das Management ist wichtig, um ein personenunabhängiges Risikomanagement über die Zeit zu gewährleisten. Ferner wird ein Zielniveau für das akzeptierte Restrisiko definiert.
- Verantwortlichkeiten und Budget: Das Management legt die Verantwortlichen fest und stattet diese mit den erforderlichen Kompetenzen und Budgets aus. Das notwendige Budget steigt dabei exponentiell mit dem Absenken des akzeptierten Restrisikos.

2. Im Betrieb

Die Ziele werden nun betrieblich umgesetzt:

- IoT-Dokumentation: Es wird ein detailliertes Inventar der «Key Assets» in den Kategorien Geräte, Daten und Netzwerk erstellt.
- Risk und Configuration Management: Für jedes «Key Asset» wird eine Risikobewertung nach der festgelegten Methode vorgenommen. Massnahmen zur Risikoreduktion unter das Zielniveau werden umgesetzt. Änderungen an den «Key Assets» werden erst nach Abschluss eines formellen Configuration Management Prozesses durchgeführt.
- Patch Management: Es ist sicherzustellen, dass Lieferanten regelmässig Sicherheitsupdates zur Verfügung stellen und diese zeitnah eingespielt werden.
- Business Continuity Planning: Ersatzteile für kritische Hardwarekomponenten sowie die letzte stabile Firmware werden system- und ortsgetrennt vorgehalten. Ferner wird ein regelmässiges Backup der Konfigurationsdaten durchgeführt.
- Systemdesign und Einkauf: Nirgendwo lassen sich so einfach nachhaltige Verbesserungen erzielen, wie durch Integration der IoT-Security-Anforderungen in Systemdesign und Produkteinkauf.

3. In der Technik

Die konkreten technischen Sicherungsmechanismen hängen vom jeweiligen IoT-System, den Entscheidungen des Managements und der betrieblichen Umsetzung ab. Einige typische technische Sicherungsmassnahmen sind folgende:

- Netzwerksegmentierung: Für Standardanwendungen genügt eine logische Unterteilung des IoT-Netzwerks mittels VLANs, VPN-Tunnels und unidirektionalen Gateways. Für kritische Anwendungen ist eine physische Trennung durch separate Netzwerke vorzuziehen – ein sogenanntes «Air Gap».
- Kontrollierte Übergänge: Die Übergänge zwischen Netzwerksegmenten werden durch Firewalls getrennt. Für Standardanwendungen genügt eine paketbasierte Firewall. Für Key Assets in kritischen Infrastrukturen sollte eine zustandsgesteuerte (stateful) Firewall oder DMZ zum Einsatz kommen.
- Intrusionsdetektionssysteme: Diese Systeme analysieren den Netzwerkverkehr auf Muster eines Angriffs und schlagen Alarm.
- Authentifizierung der Kommunikation: Die Kommunikation des IoT-Systems mit Nutzern und anderen Geräten muss in jeder Betriebsphase authentifiziert sein. Für die Authentifizierung von Personen kommen Passwörter, Badge-Karten oder biometrische Merkmale zur Anwendung. Die Authentifizierung von Geräten und Prozessen kann durch Challenge-Response-Verfahren, digitale Zertifikate oder Hash-Funktionen erfolgen. Automatisierungssysteme steuern oft kritische Prozesse, bei denen der Bediener sich keinesfalls durch falsche Passworteingabe «aussperren» sollte. Oft ist hier die «Authentifizierung» mittels Zugangsbeschränkung zum Kontrollraum sinnvoller.

Weitere Informationen. Als Einstieg in die IoT-Security empfiehlt der Autor die NIST Special Publication 800-82[7]. Diese ist speziell auf die IoT-Security der Automatisierungstechnik ausgelegt. Für die spannende und informative Geschichte hinter Stuxnet wird das Buch «Countdown to Zero Day»[8] empfohlen. Für spezifische Fragen zum Thema IoT-Security steht der Autor zur Verfügung. *(mf)*

Referenzen

[1] www.isisnuclearіran.org/assets/pdf/ISIS_Analysis_IAEA_Report_16Nov2009.pdf

[2] www.nytimes.com/2010/09/27/technology/27virus.html

[3] www.forbes.com/sites/andygreenberg/2011/05/23/siemens-accused-of-whitewashing-critical-security-bugs/

[4] Die Lage der IT-Sicherheit in Deutschland 2014, Bundesamt für Sicherheit in der Informationstechnik, S. 31

[5] Sonntags Zeitung, 30. November 2013, S. 13

[6] Sonntags Zeitung, 14. September 2014, S.12

[7] NIST Special Publication 800-82 Revision 2, Guide to Industrial Control System (ICS) Security

[8] K. Zetter, Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon, Crown Publishing, 2014

DER AUTOR

Dr. Björn Avak, 078 751 03 45
bjoern@avak.ch, www.avak.ch