IT-Sicherheit

Schutzmassnahmen für das Internet der Dinge

Durch die Konvergenz von physischer und digitaler Welt entstehen neue Innovationsschübe und damit auch neue Märkte. Gleichzeitig stellt das sogenannte «Internet der Dinge» auch eine reale Bedrohung dar, da es durch Manipulationen ausser Kontrolle geraten kann. Wie IT-Sicherheit in diesem Umfeld zu optimieren ist, zeigt folgender Beitrag.

› Dr. Björn Avak

Durch das Internet der Dinge oder Englisch «Internet of Things» (IoT) werden wir verwundbarer. War die Zuverlässigkeit von Systemen früher nur 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 Kraftwerken, Fertigungsstrassen, Gebäudeleittechnik oder Fahrzeugen. Dieser Artikel wird anhand des Stuxnet-Wurms sowie einiger weiterer Beispiele zeigen, dass IT-Angriffe auf IoT-Systeme eine reale Bedrohung darstellen. Im Anschluss werden die einzelnen Facetten der IoT-Security vorgestellt. Dann wird die konkrete Umsetzung mithilfe eines Masterplans erläutert.

Der erste grosse IoT-Angriff

Zwischen November 2009 und Januar 2010 fielen nachweislich zirka tausend Gaszentrifugen der Atomanlage Natanz im Iran aus. Es gilt als erwiesen, dass dieser Ausfall durch den Computerwurm Stuxnet verursacht wurde. Dieses Beispiel zeigt, wie geschickt 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 Netz auf Siemens Steuerungssysteme vom Typ Simatic S7-300 und dazugehörige Software (Step7 und WinCC) ab. Ist dies der Fall, tarnt sich Stuxnet durch Installation von Software tief im Betriebssystem, ein sogenanntes Rootkit.
› Stuxnet prüft nun, ob die Simatic S7 Frequenzumrichter zweier bestimmter Hersteller mit für Gaszentrifugen üblichen Umdrehungsfrequenzen steuert.
› Wenn ja, werden dem Anlagenbetreiber historische Daten 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 von IoT-Systemen schliessen:

› Auch Systeme wie die Atomanlage Natanz, welche keine direkte Verbindung

kurz & bündig

› Während bei reiner IT die Gefahr durch mangelnde Sicherheit im Verfälschen, Erbeuten sowie dem Löschen von Daten besteht, drohen bei IoT-Systemen Schäden durch Manipulation und Ausfall von Kraftwerken, Gebäudeleittechnik, Fertigungsstrassen oder Fahrzeugen.
› Viele der IoT-Systeme sind 10 bis 20 Jahre im Einsatz. Die Sicherheitslücken, die im Laufe der Zeit entstehen, werden oft nicht behoben.
› Um solcherlei Sicherheitslücken zu schliessen, gibt es keine einfache Standardlösung. Drei Bereiche im Unternehmen sind zu adressieren: das Management, der Betrieb und die Technik.

mit dem Internet haben, sind – beispielsweise über Konfigurationsrechner der Serviceunternehmen – angreifbar.

- Stuxnet nutzte die Lücke der fest programmierten Zugangsdaten in der Siemens-Software. Viele der IoT-Systeme wie Industrieautomatisierungs- oder Gebäudetechnik sind 10 bis 20 Jahre im Einsatz. Die Sicherheitslücken, welche im Laufe der Zeit entstehen, werden nicht durch ein systematisches Patching behoben.
- Die Betreiber und Hersteller von IoT-Systemen sind auf IoT-Security kaum vorbereitet.

Aktuelle IoT-Bedrohungen

Hersteller und Betreiber von IoT-Anlagen haben für üblich kein Interesse daran, dass IT-Sicherheitslücken oder gar konkrete Angriffe öffentlich werden. Nichtsdestotrotz ist mittlerweile eine ganze Reihe Beispiele bekannt.

Stromnetz
Über ein Kommunikationsmodul ist es möglich, Fotovoltaikanlagen 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. Allein durch Kenntnis der jeweiligen IP-Adresse war es Angreifern möglich, nicht nur die persönlichen Daten der Betreiber, das heisst Name, Adresse, Stromproduktionsmenge und so weiter auszulesen, sondern auch 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.

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

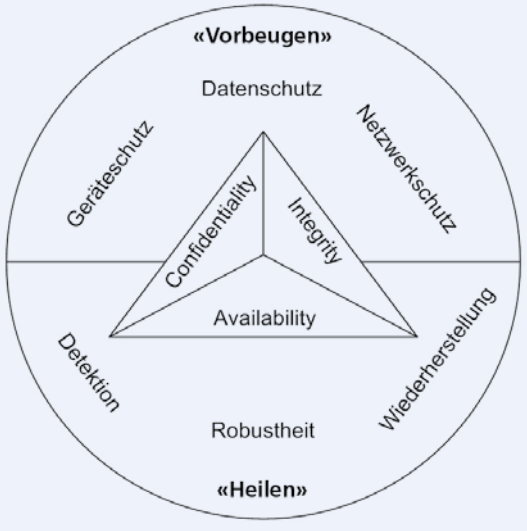
Industrieanlagen
Das Deutsche Bundesamt für Informationssicherheit veröffentlichte im Dezember 2014 den Angriff auf ein deutsches Stahlwerk. Der Angreifer erlangte zunächst über Phishing und Social Engineering Zugriff auf das Büronetzwerk. Von dort arbeitete er sich bis in das Produktionsnetzwerk für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

Die drei Beispiele zeigen einerseits die Breite des Spektrums bedrohter IoT-Systeme. Anderseits illustrieren sie auch, dass IT-Sicherheit nicht nur von den technischen Eigenschaften des Systems, sondern auch stark von menschlichem Verhalten abhängt.

Die Zielsetzungen

In der Informationstechnik wird unter dem Begriff Security üblicherweise das «CIA-Konzept» verstanden. Und das bedeutet im Kontext von IoT-Systemen das Folgende:

Abb. 1: Definition und Schutzziele von IT-Security für IoT-Systeme



Quelle: Björn Avak

- Confidentiality / Vertraulichkeit: Anlagenaufbau, -konfiguration und Laufzeitdaten sind nur autorisierten Nutzern, Geräten oder Prozessen bekannt.
- Integrity / Integrität: Veränderungen am IoT-System oder an den Laufzeitbefehlen können nur von autorisierten Nutzern, Geräten oder Prozessen vorgenommen werden. Jede Veränderung wird registriert.
- Availability / Verfügbarkeit: Wenn erforderlich, erfüllt das IoT-System stets die vorgesehene Funktion. Der autorisierte Zugriff auf das IoT-System ist jederzeit möglich.

Um diese Punkte zu gewährleisten, muss jedes der Elemente des IoT-Systems, das heisst Geräte, Netzwerk und Daten präventiv geschützt werden.

- Geräteschutz: Die Knoten sind das «Thing» des IoT-Systems. Jedes Gerät muss in sich «gehärtet» sein, das heisst nicht zwingende Zugänge und Services sind deaktiviert. Zugriffsrechte sind auf das notwendige Minimum reduziert und werden geloggt.
- Datenschutz: Die Daten sind der «digitale» Teil des IoT-Systems. Auf den Knoten gespeicherte oder über das Netzwerk versendete Daten sind vor unautorisierter Veränderung geschützt.
- Netzwerkschutz: Das Netzwerk ist die Verbindung, welche das IoT-System zusammenhält. Der Zugang zum Netzwerk wird physisch und logisch geschützt.

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

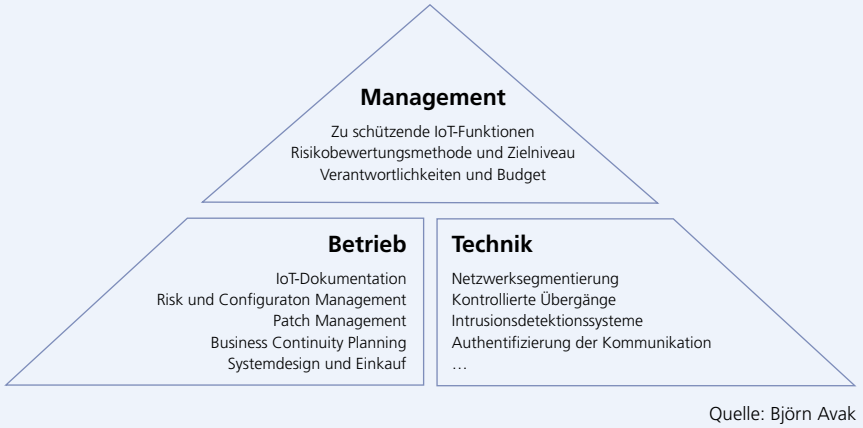
- Detektion: Veränderungen am IoT-System werden erkannt, bevor diese kritisch werden.
- Robustheit: Das IoT-System ist so gestaltet, dass selbst bei Ausfall wichtiger Geräte, des Netzwerks oder Datenverlust das System sicher bleibt.
- Wiederherstellung: Nach einem Zwischenfall kann die Funktion schnell wieder hergestellt werden.

Wird die IoT-Security-Definition mit den diskutierten Schutzzielen in den Phasen «Vorbeugen» und «Heilen» kombiniert, ergibt sich das Gesamtbild gemäss der Abbildung 1.

Masterplan zur Umsetzung

Es gibt leider keine einfache, auf alle Fälle passende Standardlösung. Es lässt sich jedoch allgemeingültig festhalten, dass IoT-Security auf drei Ebenen im Unternehmen zu adressieren ist.

Abb. 2: Elemente zur Umsetzung im Unternehmen



Quelle: Björn Avak

Management

- Zu schützende IoT-Funktionen: In einem Workshop zwischen Management und IoT-Experten werden die zu schützenden IoT-Funktionen identifiziert.
- Risikobewertungsmethode und Zielniveau: Die Festlegung einer standardisierten Bewertungsmethode durch das Management ist wichtig, um ein personenunabhängiges Risikomanagement über die Zeit zu gewährleisten. Ferner wird ein Zielniveau definiert, unter das alle Risiken abzusenken sind.
- Verantwortlichkeiten und Budget: Das Management legt die Verantwortlichen fest. Und es stattet die Verantwortlichen

mit den erforderlichen Kompetenzen und Budgets aus.

Betrieb

Die definierten Ziele werden nun auch 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» sind nur nach einem fixen Configuration-Management-Prozess erlaubt.
- Patch Management: Es ist sicherzustellen, dass Sicherheitsupdates des IoT-Herstellers vorhanden sind und zeitnah eingespielt werden.
- Business Continuity Planning: Ersatzteile für kritische Hardwarekomponenten sowie die letzte stabile Firmware werden vorgehalten. Ferner wird ein regelmässiges Backup der Konfigurationsdaten durchgeführt.
- Systemdesign und Einkauf: Nirgendwo lassen sich so einfach nachhaltige Verbesserungen erzielen als durch Integration der IoT-Security-Anforderungen in Systemdesign und Produkteinkauf.

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 die Standardanwendungen genügt eine logische Unterteilung des IoT-Netzwerks mittels VLANs, VPN-Tunnels und unidirektionale Gateways. Für kritische Anwendungen ist eine physische Trennung durch separate Netzwerke vorzuziehen.
- Kontrollierte Übergänge: Alle Übergänge zwischen Netzwerksegmenten werden durch Firewalls getrennt. Für Standardanwendungen genügt eine paketbasierte Firewall. Für Key Assets in kritischen Infrastrukturen sollte eine zustandgesteuerte (stateful) Firewall oder DMZ zum Einsatz kommen. In den nächsten Jahren werden applikationsspezifische IoT-Firewalls auf den Markt kommen, welche noch mehr Sicherheit bieten.
- Intrusionsdetektionssysteme: Solche Systeme analysieren den Netzwerkverkehr auf ein mögliches Angriffsmuster 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 Daten kann durch digitale Zertifikate oder Message Authentication Codes erfolgen.

Weitere Informationen

Als Einstieg in die IoT-Security empfehlen wir die NIST Special Publication 800–82. Diese ist speziell auf industrielle Steuerungssysteme ausgelegt und lässt sich auch auf andere IoT-Systeme applizieren. Für die spannende und informative Geschichte hinter Stuxnet empfehlen wir das Buch «Countdown to Zero Day». «

Quellenhinweise

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

S. Szlósarzyk, S. Wendzel et. al., Towards Suppressing Attacks on and Improving Relience of Building Automation Sytems – An Approach Exemplified Using BACnet, Beiträge der 7. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e. V., 2014

NIST Special Publication 800–82 Revision 2, Guide to Industrial Control System (ICS) Security

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

Porträt

Dr. Björn Avak
Vertriebsleiter

Dr. Björn Avak, zertifizierter IT-Security-Spezialist (CISSP), ist Vertriebsleiter in einem Unternehmen der Gebäudetechnikbranche. In dieser Rolle realisiert er für die Kunden Security-Lösungen für kritische IoT-Systeme. Zuvor leitete Björn Avak mehrere Jahre ein Produktmanagement-Team. In dieser Zeit entwickelte er das klassische Produkt zu einem IoT-System weiter. Neben der IoT-Security gilt sein Interesse dem generellen Wandel von Geschäftsmodellen durch die Digitalisierung.

Kontakt

bjoern@avak.ch