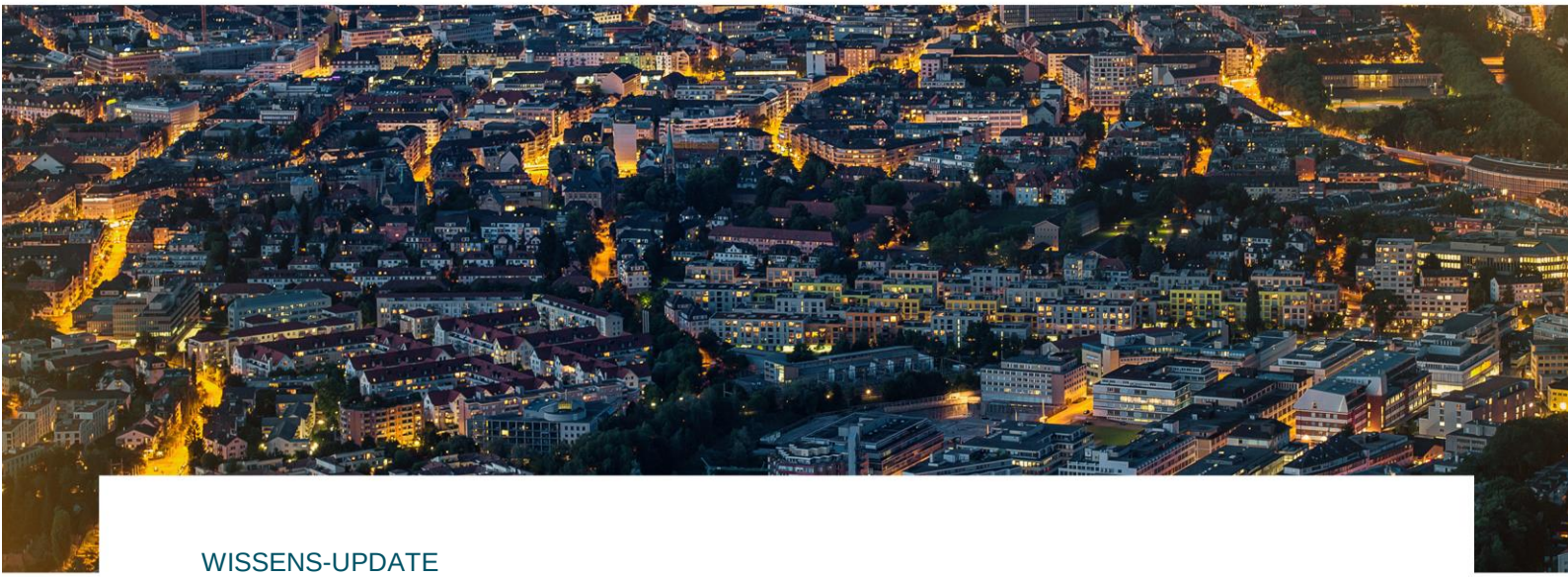
CyOne Security AG
Hinterbergstrasse 18
6312 Steinhausen

Telefon +41 41 748 85 00
info@cyone.ch
cyone.ch



WISSENS-UPDATE

IoT-Vernetzung birgt Sicherheits-risiken

Ivo Steiner | Sales Manager IoT Security | Steinhausen, 13. August 2020

Das Internet of Things (IoT) gilt vielen als Schlüssel zur Zukunft des Internets. Bis alle Internet-tauglichen Geräte autonom kommunizieren, gilt es aber noch einige Hürden zu nehmen. Zentral für die weitere Vernetzung sind der Ausbau der Leistungsfähigkeit der digitalen Infrastruktur sowie die Klärung offener Sicherheitsfragen.

Unsere physische Welt wird durch das Internet of Things (IoT) immer stärker mit der virtuellen verbunden. Die Auswirkungen dieser Vernetzung auf Businessmodelle sowie auf Beruf und Privatleben sind tiefschürfend: Der Mensch tritt in den Hintergrund, Gegenstände in den Vordergrund. In diesem Ausmass sind die mit dem IoT verbundenen Veränderungen neu, abgezeichnet hatte sich eine solche Entwicklung aber bereits vor Jahrzehnten.

Vom Bankautomaten zum IoT

An Netzwerke angeschlossene Geräte gibt es seit den 70er-Jahren. Geldautomaten oder Getränkespender lieferten damals auf elektronischem Weg Informationen über Kontoveränderungen oder Füllstatus. Mit der technischen Weiterentwicklung wurde das Einsatzfeld der Technologie laufend erweitert, wobei insbesondere der Bereich Logistik profitierte: Abläufe in Grosslagern wurden zunehmend automatisiert und Waren mit Radio-Frequency-Identification (RFID)-Transpondern ausgerüstet.

Diese RFID-Transponder oder Funketiketten haben den Onlinehandel beschleunigt und sind nicht mehr wegzudenken. Firmen wie Amazon arbeiten dank RFID konsequent auf vollautomatisierte Logistikzentren hin: Nach Bestellungseingang wird die Ware über die Funketikette lokalisiert, zur Sammelstelle transportiert und dort zum Versand von einem Sensor erfasst.

Das technologische Fundament des IoT, die drahtlose Technologie und vernetzte Sensoren, sind keine neuen Erfindungen, sondern stehen seit längerem zur Verfügung. Für den Durchbruch sorgte der rasante Fortschritt im Design von multifunktionalen Chips. In den letzten Jahren sind integrierte Wireless-Chips und smarte Sensoren deutlich kleiner und günstiger geworden. Damit hat sich ihr Einsatzgebiet massiv ausgeweitet.

Maschinen sprechen mit Maschinen

Heute wird erwartet, dass Unternehmen am meisten von IoT profitieren werden. Ein Stichwort dazu ist die Smart Factory, eine vernetzte Produktion, die kontrolliert und rationalisiert ihre Aufgaben erledigt. Die Maschinen in dieser Fertigung werden untereinander kommunizieren können und lernfähig sein. Überwacht wird die Produktion von Fachleuten am Computer. Experten der Beratungsfirma McKinsey rechnen allein im industriellen Bereich mit einem Potenzial von bis zu 3,7 Billiarden US-Dollar.

Auch im öffentlichen Sektor ist das Potenzial immens: Städte können in den Bereichen Energie, Sicherheit und Unterhalt Milliarden einsparen, wenn sie sich zu Smart Cities wandeln. Doch diese Einschätzungen sind derzeit noch Trommelwirbel der Zukunftsmusik. Denn noch fehlt es an der leistungsstarken Infrastruktur und an der vollständigen Umsetzbarkeit von «Deep learning», der künstlichen Intelligenz (AI), um das volle Potenzial des IoT zu nutzen.

5G ist der nächste grosse Schritt

In den nächsten Monaten steht die Einführung des 5G-Mobilfunkstandards an. Damit wird die Kapazität des Mobilfunknetzes erhöht und die Übertragung der Daten beschleunigt – und dies bei geringerem Energieverbrauch. Mit 5G werden Geräte ihre Informationen über das Mobilnetz versenden.

Eine der einschneidenden Veränderungen von 5G wird sein, dass durch den neuen Standard autonome Fahrzeuge für gewisse Szenarien einsetzbar sein werden, weil ihre Bordcomputer dank der schnelleren Datenübertragung problemlos über die 5G-Infrastruktur kommunizieren können. So teilen sie sich etwa Tempo und Standort mit und verhindern dadurch Kollisionen. Eine entsprechende direkte voll vermaschte Netzwerktopologie, in welcher die Bordcomputer direkt d. h. ohne Infrastruktur untereinander kommunizieren können, wird aber erst in einem nächsten Schritt umgesetzt werden können.

20 Milliarden neue Schnittstellen

Noch nicht gelöst ist die Interoperabilität zwischen den unterschiedlichen Geräten der verschiedenen Hersteller. Momentan ist die Verständigung unter den IoT-Geräten noch nicht durchgängig und einfach möglich. Es gibt aktuell rund 50 verschiedene Protokolle für die Sensordatenkommunikation und deshalb müssen jeweils mit individuellen Kommunikationsschnittstellen entsprechende Übersetzungen implementiert werden. Dies ist aufwändig und teuer.

Sicherheit als Herausforderung

Die vielleicht grösste Herausforderung aber ist die Sicherheit. Durch die fortschreitende Vernetzung nimmt die Zahl der Schnittstellen in den nächsten Jahren exponentiell zu – und jede ist angreifbar. Vor allem, wenn es sich um Geräte handelt, die mehrheitlich mit Standardpasswörtern ausgerüstet sind und über keine weiteren Absicherungen verfügen. Eine Studie des US-Softwareunternehmens Symatec kam zum Schluss, dass heute zwei Drittel aller internetfähigen Geräte unveränderbare Usernamen wie «admin» und Standard-Passwörter wie «12345» haben. Damit können sie leicht manipuliert werden.

Am Beispiel des smarten Kühlschranks zeigen sich die Risiken. Angenommen, dieser ist mit dem Internet verbunden und bestellt selbständig online Lebensmittel des täglichen Bedarfs nach, wenn sie verbraucht sind. Dringt nun jemand über das Netzwerk in das Betriebssystem des Kühlschranks ein, könnte er dessen Funktionsweise verändern: Ihn abtauen lassen oder kiloweise Lebensmittel bestellen. Es liesse sich aber auch das WLAN-Passwort des lokalen Netzwerks herausfinden und so ein Smart Home unter Kontrolle bringen. Was im Kleinen möglich ist, gilt auch für das Grosse: Einer Smart Factory, die über eine solche Schwachstelle verfügt, könnte dasselbe widerfahren. Oder der Angreifer könnte sich über diese Schwachstellen Zugriff auf das Firmennetz verschaffen und so alle verfügbaren Daten kopieren oder manipulieren.

Neue Bedrohung: Botnetze

Eine weitere Möglichkeit, das IoT zu missbrauchen, ist der Zusammenschluss von Geräten zu Botnetzen, die dann Webseiten und Server angreifen. Ziel eines solchen Angriffs ist eine Überlastung von Netzen, der Distributed Denial of Service (DDoS). Seit 2016 ist die Schadsoftware Mirai bekannt, die das Internet nach Geräten mit Sicherheitslücken scannt. Findet sie solche, versucht sie, ins System einzudringen. Gelingt dies, bombardieren die Geräte einen Server mit Traffic. Weil es sich häufig um Tausende Absender handelt, sind die Server bald überlastet. Damit lassen sich ganze Bereiche des Internets lahmlegen. So wirken die vielen mangelhaft geschützten IoT-Geräte als Multiplikatoren für kriminelle Machenschaften.

Hohe Anforderungen an IT-Architektur

Trotz all dieser Bedrohungen gilt: Das IoT ist ein Schlüssel für das Internet der Zukunft. Viele neue Geschäftsopportunitäten sind für Unternehmen dadurch denkbar und neue Anwendungen für die Gesellschaft sind zu erwarten. Es geht nach Ansicht von Experten allerdings darum, die Entwicklung auch mit Blick auf die Sicherheit zu vollziehen. Diese erreicht man, nicht zuletzt in Unternehmen, mit einer dafür vorbereiteten IT-Architektur. Sie sieht die Authentifizierung der Geräte im Netzwerk vor, den Schutz der Daten, die Segmentierung des Netzwerks und das Einrichten verschiedener passiver und aktiver Verteidigungslinien. Wichtige Bereiche eines Unternehmens können ganz vom Internet abgekoppelt sein und ein lokales «Network of Things» bilden.

CyOne Security ist der kompetente Partner für IoT-Sicherheit

Bei der Entwicklung vernetzter Produkte und Systeme bleibt die Sicherheit jedoch oft auf der Strecke, weshalb bisher erfolgreiche Sicherheitsansätze grundlegend überdacht werden müssen. Verfügbarkeit, Verhinderung von Zweckentfremdung und Wahrung der Datensicherheit sind zwingende Voraussetzungen für eine seriöse Nutzung des enormen Potenzials, das die neuen digitalen Welten für uns bereithalten.

Informations- und Datensicherheit ist bei jedem IoT-Entwicklungsprojekt ein substanzieller Bestandteil. Um die vernetzten Produkte und Systeme vor Cyber-Attacken zu schützen, bringt die CyOne Security AG tiefes Expertenwissen in Cipher und Cyber Security in die Sicherheitskonzepte und -lösungen ein, die auf der 360°-Sicherheitskompetenz von Product Security, System Security und Operational Security basieren.

Beginnen Sie heute und schützen Sie Ihr Internet der Dinge vor Cyber-Risiken.

Machen Sie den ersten Schritt: Analysieren Sie gemeinsam mit unseren Experten Ihre aktuellen und zukünftigen Sicherheitsbedürfnisse Ihrer vernetzten Produkte, damit wir mit Ihnen über zielgerichtete Sicherheitslösungen diskutieren können.

Kontaktieren Sie uns für ein kostenloses Expertengespräch.