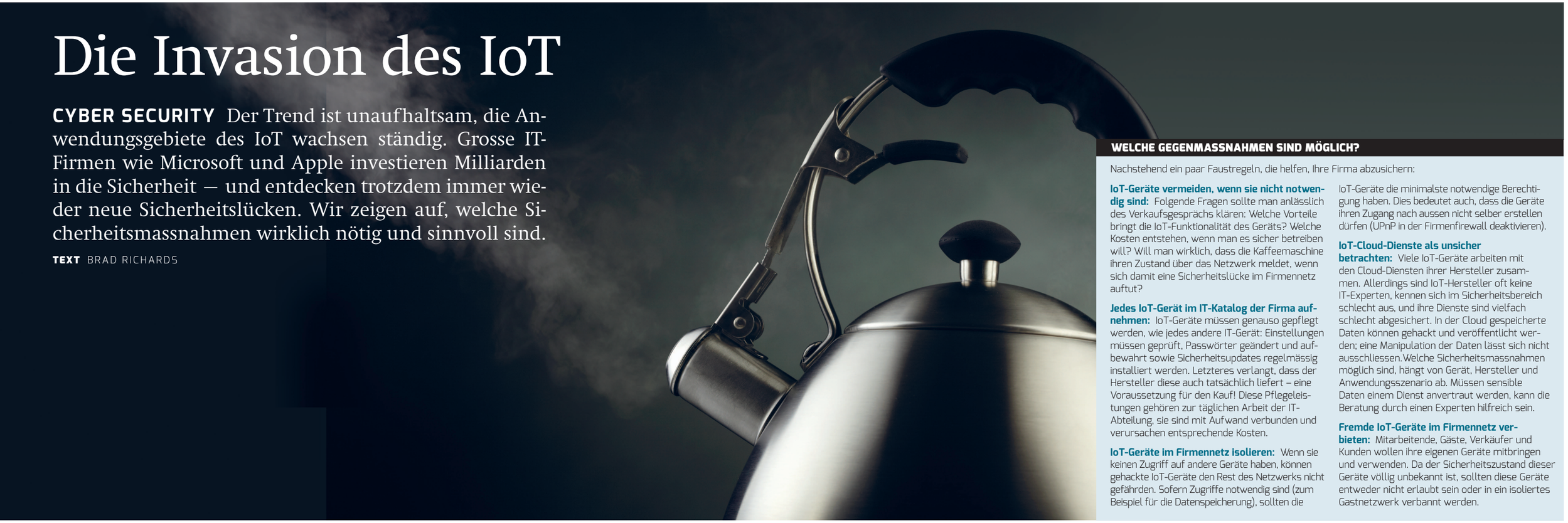
Die Invasion des IoT

CYBER SECURITY Der Trend ist unaufhaltsam, die Anwendungsgebiete des IoT wachsen ständig. Grosse IT-Firmen wie Microsoft und Apple investieren Milliarden in die Sicherheit — und entdecken trotzdem immer wieder neue Sicherheitslücken. Wir zeigen auf, welche Sicherheitsmassnahmen wirklich nötig und sinnvoll sind.

TEXT BRAD RICHARDS



Lassen Sie sich nicht von Ihrem Toaster, Ihrer Kaffeemaschine oder Ihrem Teekessel hacken! Wer seine Geräte ins Internet bringen möchte, …

WELCHE GEGENMASSNAHMEN SIND MÖGLICH?

Nachstehend ein paar Faustregeln, die helfen, Ihre Firma abzusichern:

IoT-Geräte vermeiden, wenn sie nicht notwendig sind: Folgende Fragen sollte man anlässlich des Verkaufsgesprächs klären: Welche Vorteile bringt die IoT-Funktionalität des Geräts? Welche Kosten entstehen, wenn man es sicher betreiben will? Will man wirklich, dass die Kaffeemaschine ihren Zustand über das Netzwerk meldet, wenn sich damit eine Sicherheitslücke im Firmennetz auftut?

Jedes IoT-Gerät im IT-Katalog der Firma aufnehmen: IoT-Geräte müssen genauso gepflegt werden, wie jedes andere IT-Gerät: Einstellungen müssen geprüft, Passwörter geändert und aufbewahrt sowie Sicherheitsupdates regelmässig installiert werden. Letzteres verlangt, dass der Hersteller diese auch tatsächlich liefert – eine Voraussetzung für den Kauf! Diese Pflegeleistungen gehören zur täglichen Arbeit der IT-Abteilung, sie sind mit Aufwand verbunden und verursachen entsprechende Kosten.

IoT-Geräte im Firmennetz isolieren: Wenn sie keinen Zugriff auf andere Geräte haben, können gehackte IoT-Geräte den Rest des Netzwerks nicht gefährden. Sofern Zugriffe notwendig sind (zum Beispiel für die Datenspeicherung), sollten die IoT-Geräte die minimalste notwendige Berechtigung haben. Dies bedeutet auch, dass die Geräte ihren Zugang nach aussen nicht selber erstellen dürfen (UPnP in der Firmenfirewall deaktivieren).

IoT-Cloud-Dienste als unsicher betrachten: Viele IoT-Geräte arbeiten mit den Cloud-Diensten ihrer Hersteller zusammen. Allerdings sind IoT-Hersteller oft keine IT-Experten, kennen sich im Sicherheitsbereich schlecht aus, und ihre Dienste sind vielfach schlecht abgesichert. In der Cloud gespeicherte Daten können gehackt und veröffentlicht werden; eine Manipulation der Daten lässt sich nicht ausschliessen.Welche Sicherheitsmassnahmen möglich sind, hängt von Gerät, Hersteller und Anwendungsszenario ab. Müssen sensible Daten einem Dienst anvertraut werden, kann die Beratung durch einen Experten hilfreich sein.

Fremde IoT-Geräte im Firmennetz verbieten: Mitarbeitende, Gäste, Verkäufer und Kunden wollen ihre eigenen Geräte mitbringen und verwenden. Da der Sicherheitszustand dieser Geräte völlig unbekannt ist, sollten diese Geräte entweder nicht erlaubt sein oder in ein isoliertes Gastnetzwerk verbannt werden.

… sollte auch für deren Sicherheit sorgen.

Bildquelle: Depositphotos.com, silverjohn

Das Internet of Things (IoT) revolutioniert den Alltag: Es verbindet elektronische Geräte miteinander und soll die Menschen bei ihren Tätigkeiten unmerklich, aber effizient unterstützen. So sehr dieses «neue Internet» die Marketingabteilungen begeistert, so wenig erfreut es die IT-Gemeinschaft. Denn jedes Elektrogerät mit Internetzugang bedeutet eine potentielle Sicherheitslücke, eine Hintertür ins Firmennetz, ein mögliches Werkzeug der Hacker-Community. Der Trend ist unaufhaltsam, die Anwendungsgebiete des IoT wachsen ständig: Demnächst wird es internetfähige Bürostühle geben, die mittels Messwerten von Sensoren im Stuhl exakt auf die Körpereigenschaften des Nutzers eingestellt werden können, oder winzige Computer, sogenannte Wearables, die direkt in Kleidungsstücke eingearbeitet werden, sowie persönliche medizinische Geräte wie Insulinpumpen, die per Fernbedienung gesteuert werden können. Die Vorteile von IoT sind vielversprechend: Fernsteuerung und Automation, Datensammlung und Datenbearbeitung in der Cloud, Effizienzgewinne durch Monitoring und Fernzugriff. Die Nachteile lassen sich in einem Wort zusammenfassen: Sicherheit. Grosse IT-Firmen wie Microsoft und Apple investieren Milliarden von Dollars in die Sicherheit – und trotzdem entdecken sie immer wieder Sicherheitslücken. Die alles beherrschende Frage ist: Wie viel Aufwand investieren die Hersteller von elektronischen Geräten in Sicherheit? Wird diese vernachlässigt, werden die Hacker die nächsten Jahre auf ihre Rechnung kommen: Sie können ihren Lebensunterhalt mit Ransomware und DDoS-Attacken bestreiten.

«Beginnend in 2017 wird jedes neue Haushaltsgerät von LG fortgeschrittene WLAN-Fähigkeiten haben»
LG Vizepräsident für Marketing David VanderWaal, CES 2017

Israeli researchers demonstrated an attack on Philips Hue lightbulbs, where the bulbs network directly interacted with each other, in order to spread a malware infection across an entire city.
IoT Goes Nuclear: Creating a ZigBee Chain Reaction

WARUM SIND IOT-GERÄTE PROBLEMATISCH?

Alle Firmennetzwerke stellen einen Kompromiss zwischen Nutzen und Sicherheit dar. So erhält bei der Mehrheit der KMU-Netzwerke jedes intern angeschlossene Gerät automatisch eine gültige Netzwerkadresse. Viele Geräte wollen einen Schritt weitergehen und direkt von aussen erreichbar sein. In einfach konfigurierten Netzwerken wird ein entsprechendes Loch in der Firmenfirewall automatisch geöffnet (Universal Plug-and-Play = UPnP); in sicher konfigurierten Netzen muss dies manuell bewilligt werden. In vielen Fällen ist diese Erreichbarkeit für die Funktionalität des Geräts notwendig. So ist beispielsweise der Hersteller-Support erforderlich, damit das Gerät sich an einen Cloud-Dienst anschliessen kann. In weiteren Fällen dient die Erreichbarkeit lediglich dem Sammeln von Daten durch den Hersteller.

Es leuchtet ein: Von aussen erreichbare Geräte sind angreifbar. Schlecht abgesicherte Netzprotokolle können leicht geknackt werden, und die besten Netzprotokolle sind nutzlos, wenn die Default-Passwörter nicht geändert werden. Support-Hintertüren können von jedermann benutzt werden. Schlimmer noch: Geräte, die im internen Netzwerk angemeldet sind, dienen als Sprungbrett, um andere Geräte im Firmennetz anzugreifen und den Firmenserver mit Ransomware zu infizieren. Sicherheitskameras und sprachgesteuerte Geräte mit Sensoren sind potentielle Spione: Einbrecher können prüfen, ob Mitarbeitende noch im Büro sind, Sitzungen können abgehört werden und vieles mehr. Eine Aussperrung aus dem Firmennetzwerk ist kein Allheilmittel. Weil IoT-Netzwerkzugänge meistens per Funk aufgebaut werden, verbinden sich installierte Geräte freiwillig mit jedem erreichbaren WLAN. Werden Geräte aus dem eigenen Firmennetzwerk ausgesperrt, melden sie sich einfach beim Nachbarn oder beim Laptop eines Hackers an.

Spät arbeitende Mitarbeitende wollen am Abend die nächste Fussball-EM verfolgen. Jemand bringt den eigenen (IoT)-Fernseher von zuhause mit. Kaum in der Firma installiert, meldet sich der Fernseher ans Firmennetz an, bohrt ein Loch durch die Firewall, und schon hängt die Sicherheit der Firma von derjenigen dieses Geräts ab – ein Gerät, das möglicherweise bereits infiziert ist.

RAUS AUS DEN KINDERSCHUHEN

Das Internet-of-Things bietet vielversprechende Möglichkeiten. Allerdings ist die Technologie noch unausgereift, und sehr viele unerfahrene Hersteller drängen auf den Markt. Das Thema Sicherheit ist ein nicht zu unterschätzendes Problem. In grossen Firmen sind die Netzwerke meistens gut abgesichert, in vielen KMU und Kleinstbetrieben ist dies hingegen oft nicht der Fall. Beim Umgang mit IoT-Geräten ist höchste Vorsicht geboten, um die Sicherheit der Firma nicht zu gefährden. Ein ganz wichtiger Aspekt: Jedes IoT-Gerät ist in erster Linie ein IT-Gerät, das die gleiche Betreuung wie jedes andere IT-Gerät benötigt. Darüber hinaus sollten alle Firmen die Sicherheit ihrer Netzwerke im Kontext des IoT überprüfen.

Das IoT bringt allgegenwärtige Konnektivität. Neue Informationsflüsse entstehen, die noch nie dagewesene und unerwartete Vorteile mit sich bringen werden. Wir stehen noch in den Startlöchern, müssen aber bereits jetzt dafür sorgen, dass die Kinderkrankheiten dieser neuen Welt bald auskuriert sind.

DER AUTOR

Prof. Dr. Brad Richards doktorierte an der University of Texas. Nach Projektarbeiten bei der University of Aberdeen und der EPFL wurde er als Professor in den Bereichen Künstliche Intelligenz und Software Engineering an die Fachhochschule Furtwangen berufen. Im Jahr 2001 gründete er zusammen mit seiner Frau eine eigene Softwarefirma. 2009 nahm er eine Professur an der FHNW an, wo er technische Vorlesungen hält.