Herausforderungen des Internet of Things

IoT, das Internet der Dinge, eröffnet als logische Konsequenz einer kontinuierlich voranschreitenden Vernetzung unserer Gesellschaft eine schier unendliche Fülle an neuen Möglichkeiten und birgt ein enormes Potenzial zur Steigerung von Effizienz und Komfort. Damit einher geht aber auch eine erhöhte Angreifbarkeit und damit auch Überwachbarkeit seiner Nutzer. Ermöglicht wird dies durch die Aufweichung der Grenzen zwischen der global vernetzten digitalen Welt und den lokalen vier Wänden von Fabrikhallen, Büros und Wohnzimmern. Fertigungsanlagen können weltweit überwacht, gewartet und am Laufen gehalten werden; Die Temperatur im Büro oder zu Hause wird geregelt, noch während man sich auf dem Weg zur oder respektive von der Arbeit befindet. Die Risiken jedoch, denen wir uns aussetzen, wenn die Beleuchtung unseres Heims oder das Auto wie selbstverständlich auf Anfragen aus dem Netz reagieren können, sind keineswegs zu vernachlässigen. Ein Eindringling in unsere privaten Netzwerke etwa kann von überall herausfinden, wer in welchem Wohnviertel zu Hause ist (in welchen Wohnungen brennt Licht oder wie und was wird im Heimnetzwerk kommuniziert) und wo vermehrt Polizeifahrzeuge unterwegs sind (moderne vernetzte Fahrzeuge verfügen über GPS). Die Gefahren, die mit der Verfügbarkeit und, ob legitim oder unter Anwendung rechtswidriger Intentionen und Methoden erreichte, Bündelung dieses Wissens einhergehen, liegen auf der Hand und werden auch im Ihnen vorliegenden Themenschwerpunkt nochmals verdeutlicht.

Im Zeitalter von *IoT*, gerade in den frühen Tagen, in denen wir uns befinden, wachsen nicht einfach zwei Welten, die digitale und die physische, zusammen. Damit einher geht die Tatsache, dass deren individuelle Architekten und Baumeister sich auf neuem Terrain zurechtfinden und lernen müssen, mit neuen Risiken umzugehen. Es bedarf eines enormen Lern- und Wandlungsprozesses, um aus einem Automobil-Konzern der Spitzenklasse einen Erbauer sicherer, global vernetzter Elektrofahrzeuge hervorgehen zu lassen. Ebenso vollzieht die digitale Welt einen Kraftakt, wenn es darum geht, den Anschluss an ihre Welt in einen Hochofen, das Straßennetz, Kleidung, eine Lampenfassung oder gar jeden Joghurt-Becher zu bringen.

Es sind jedoch nicht nur die naturgegebenen Grenzen, etwa der Skalierbarkeit und Belastbarkeit der notwendigen Elektronik, deren fortwährende Erweiterung eine Herausforderung darstellt. Fast noch schwerer wiegt die grenzenlose Fülle an Möglichkeiten, die durch die Vernetzung eröffnet wird. Es bedarf einer gewissen Sensibilität für die Gefahren der neuen Welt sowie Selbstdisziplin, um mit Blick auf potenziell neu geschaffene Angriffsflächen die Möglichkeit eines kurzfristigen Marktvorteils oder persönlichen Komforts verstreichen zu lassen. Die Unternehmen und Forscher der digitalen Welt verfügen heutzutage über das Instrument der Ethik-Kommissionen, um die Möglichkeiten gegen potenzielle Gefahren abzuwägen. Nicht zuletzt stehen der Gesetzgeber und die Rechtsprechung in Anbetracht des sich mit steigender Geschwindigkeit ausbreitenden rasanten Wandels der digitalen Welt vor wachsenden Herausforderungen.

Aber nicht nur bei Herstellern und Dienstleistern oder Politikern und Richtern, auch auf Seiten der Nutzer, Anwender und Konsumenten all dessen, was wir unter dem Begriff des *Internet of Things* zusammenfassen, muss sich ein völlig neues Gefühl für potenzielle Gefahren noch einstellen, die damit einhergehen, dass man zum Beispiel ein unscheinbares neues Gerät, wie etwa einen Toaster oder eine Personenwaage, in die eigenen vier Wände bringt. Nur so kann verhindert werden, dass sich unsere Gesellschaft den Risiken allzu unbedarft aussetzt, ohne über das Bewusstsein für mögliche Konsequenzen zu verfügen.

In dem Ihnen vorliegenden Themenschwerpunkt zu Datenschutz und Sicherheit im Zeitalter des *Internet of Things* setzen sich die Autoren des vom Bundesministerium für Bildung und Forschung geförderten Kompetenzzentrums für IT-Sicherheit CISPA mit unterschiedlichen Aspekten der Thematik auseinander.

Möllers und Vogelgesang führen in die technischen Grundlagen des SmartHome ein und weisen Gefahren und Auswege auf. Darüber hinaus wird der aktuelle Stand der Rechtsprechung und die Anwendbarkeit des klassischen Kernstrafrechts diskutiert. Sven Bugiel und Stefan Nürnberger veranschaulichen die technischen, ethischen und sicherheitstechnischen Herausforderungen, die mit der Ausbreitung des Internet der Dinge einhergehen. Sebastian Gerling und Christian Rossow erläutern die Übertragung von Techniken zum Erkennen und Verfolgen von in globalen Netzen operierenden Angreifern in die Welt des IoT und stellen sogenannte Honeypots, eine Technik zum Erkennen und Analysieren laufender Angriffe auf die eigene Infrastruktur, vor. Und die Analyse von Aline Jaritz und Luigi Lo Iacono von aktuellen Smart-TV zeigt, mit welchen Datenschutz-Problemen uns das IoT konfrontieren wird. Im abschließenden Beitrag des Schwerpunktes befasst sich Andreas Zeller mit dem sogenannten Fuzzing, einer derzeit sehr erfolgreich eingesetzten Technik zum Testen und Abhärten von Betriebssystemen, Web-Browsern, Compilern und grafischen Endanwendungen.

Ich wünsche allen Leserinnen und Lesern eine aufschlussreiche und anregende Lektüre.

Michael Backes