Geleitwort

Als ich erfuhr, dass mein Freund Nitesh Dhanjani ein Buch über das Internet of Things (IoT) verfasst, war ich überaus erfreut. Schließlich ist dies ein Fachgebiet, das zumindest für mich gleichermaßen aufregende wie erschreckende Aspekte aufweist.

Wir hören heutzutage in den Nachrichten Tag für Tag von Hackern, die Sicherheitsfunktionen erfolgreich überwunden haben. Aufgrund der Häufigkeit und des Ausmaßes solcher Vorfälle sind wir mittlerweile ein wenig abgestumpft. Moderne Gesellschaften wie die unsere haben mittlerweile erkannt, dass der Nutzen, den wir durch die Akzeptanz innovativer Technologien erhalten, deren Kosten und Risiken – zumindest kurzfristig – übersteigen. Unser kollektives Versagen dabei, dieses Unsicherheitsmuster endlich wirkungsvoll in Angriff zu nehmen, sollte Beweis genug dafür sein, dass wir den Nutzen höher bewerten als die Risiken.

Ein wesentlicher Aspekt dieser Nutzen-Risiko-Analyse ist die Tatsache, dass die Risiken, die in der Vergangenheit aufgetreten sind, vor allem immaterielle Güter betreffen: Daten und Geld.

Stellen wir uns aber nun einmal vor, welche Auswirkungen es hätte, wenn die Risiken physisch erfahrbar würden: Städte liegen tagelang im Dunkeln, medizinische Geräte töten Patienten, in Kühlschränken verdirbt das Essen, Fahrer verlieren die Kontrolle über ihre Autos, Flugzeuge fallen vom Himmel usw. Ob wir in solchen Fällen weiterhin so tolerant gegenüber technischen Ausfällen bleiben würden, darf bezweifelt werden.

Ich nehme an, dass unser Konzept des Begriffs »Risiko« den Schwerpunkt vor allem auf physische Auswirkungen legt und abstrakte Risiken eher vernachlässigt. Dies ist vielleicht einer der Gründe dafür, dass Risiken im Bereich der Informationssicherheit für viele Menschen schwer zu erfassen sind. Ferner gehe ich davon aus, dass, sobald Vorfälle in diesem Bereich auch physische Konsequenzen haben, wir die Risiken des Internet of Things gewiss überdenken werden.

In der »realen« Welt gibt es zahlreiche Bauvorschriften, die Anforderungen an physische Infrastrukturen definieren, und ihre Einhaltung wird von zertifizierten Technikern oder diplomierten Ingenieuren streng überwacht. Wann endlich

werden wir uns Gedanken darüber machen, was Sicherheit in einer Welt bedeutet, in der Millionen und Abermillionen vernetzter Geräte vorhanden sind?

Ich kann nur hoffen, dass die Leser dieses Buches erkennen, dass die technologischen Investitionszyklen, die heute eine fortlaufende Innovation gewährleisten sollen, in Bezug auf IoT-Geräte überdacht werden müssen. Wenn wir die aktuellen Entwicklungs- und Qualitätssteuerungsprozesse, die vor allem auf schnelle Innovation, niedrige Kosten und kurze Produktlebenszyklen ausgelegt sind, auf das Internet of Things anwenden, werden Sicherheit und Datenschutz zweifellos noch stärker unter die Räder kommen.

Patrick Heim

Mit über 20 Jahren Erfahrung ist Patrick Heim ein Veteran der Informationssicherheit. Er hat bereits eine Vielzahl unterschiedlicher Positionen in den Bereichen Auditing, Consulting und Penetration Testing sowie als Chief Trust Officer und Chief Information Security Officer bekleidet.