IoT – Internet of What?

Wie immer wieder in der dynamischen IT-Welt, werden ‚Hypes‘ durch unbestimmte Begriffe ausgelöst. Ein Paradebeispiel ist gegenwärtig das Internet der Dinge (IoT). Dabei steht Internet für eine etablierte allgemein verfügbare Technologie, ‚die Dinge‘ sind dagegen zunächst unbestimmt. Ihr Spektrum reicht von einfachen Geräten (Smart Home Komponenten wie Heizkörperregler, Beleuchtung, usw.) bis zu komplexen IT-Strukturen (Smart Meter, Connected Car Systems, Industrieautomatisierung, intelligente Logistik, usw.).

Der Markt ist geprägt durch eine große Anzahl Start-up Unternehmen, die eine noch größere Zahl neuer Ideen produzieren. Allerdings kann man die Sinnhaftigkeit einiger Ideen hinterfragen, was schon zu einer Verunglimpfung des Begriffs IoT zu „Internet of Shit“ geführt hat. Viele Ideen beruhen einfach nur darauf, dass man bestehende Technologie nun vernetzt und somit fernsteuerbar macht. Die Flurbeleuchtung, die sich bei Öffnen der Haustür selbstständig einschaltet ist sicher bequem, bietet aber ansonsten keinen (finanziellen) Vorteil für den Bewohner. Man mag sogar entgegenhalten, dass dies auch ohne das Internet mit einem einfachen Bewegungssensor machbar ist.

Echte neue Anwendung sind natürlich etwas Sinnvolles. Wenn man mit dem IoT die Ankunftszeit sämtlicher Zuliefer-LKWs vorausplanen kann und dadurch bestehende Ladeflächen und Kapazitäten besser nutzen kann und Wartezeiten reduzieren kann, so ist dies sicher ein großer Gewinn, wie am Beispiel ‚Die digitale Chemieindustrie als Erfolgsrezept‘ auf dem Digital-Gipfel 2017 in Ludwigshafen gezeigt wurde.

Aus Sicht des Datenschutzes sind die sinnfreien Anwendungen sicherlich nicht das Problem. Gefährlich wird es aber, wenn die neuen Geschäftsideen ohne die notwendige gebotene Sorgfalt entwickelt werden und damit die IT Sicherheit und personenbezogene Daten auf der Strecke bleiben. Leider ist genau dies zu beobachten, obwohl die etablierte Softwareindustrie eigentlich weiß, wie es besser geht. Daher beschäftigt sich dieses Schwerpunktheft mit einem Review der Datenschutzerfordernisse für das Internet of Things.

Felix Schmidt und Martin Klein-Hennig von der Datenschutz Nord Gruppe setzen sich kritisch mit den gegenwärtig durch IoT bedingten IT Sicherheitsmängeln und ihren Auswirkungen auf Haftungskategorien auseinander. Insbesondere wird auf den etwas komplizierteren Fall des Drittschadens eingegangen, wenn also der Geschädigte nicht gleichzeitig der Käufer des fehlerhaften Geräts ist.

Heiko Koepke, Thorben Lenze, Mario Pietersz und Christian Zenger von der Firma Physec beleuchteten das wichtige Thema „Schlüsselmanagement für das IoT“. Da die vernetzten Geräte zur Erfüllung ihrer Funktion kommunizieren müssen, gilt natürlich ein besonderes Augenmerk dem Thema Verschlüsselung und Schlüsselmanagement.

Auf die industriellen Anwendungen des Internets der Dinge geht Jay Thoden van Velzen von der Firma SAP ein. In den hier diskutierten Anwendungen liegt ein großes, nicht nur finanzielles Potential. Dementsprechend groß ist die Notwendigkeit der Risikoreduzierung durch geeignete Schutzmaßnahmen.

Damit es erst gar nicht zum Schaden kommt, gehen Alexander Straßheim und Sebastian Schreiber von der Firma Syss in ihrem Artikel auf Penetrationstest von IoT Geräten ein.

Abgerundet wird der Schwerpunkt durch Aufsätze der Autoren Bettina Pospisil, Matthias Gusenbauer, Edith Huber und Otto Hellwig zu „Cyber-Sicherheitsstrategien“ sowie „Gewerblicher Rechtsschutz“ von Joachim Gruber.

Gunter Bitz