Sicherheitsrisiko IoT

Das Internet der Dinge ist derzeit in aller Munde. In der Spielart Industrie 4.0 steht es für die Steuerung von Produktionsanlagen über das Internet, für vernetzte Roboter und eine hoch automatisierte Logistik. Das Zuhause wird dank IoT zum Smart Home, wo sich die Heizung je nach Wetterdaten und Aufenthaltsort des Hausbesitzers ein- und ausschaltet, wo die Webcam die Haustür überwacht und die Beleuchtung auf die Anwesenheit der Bewohner reagiert. Und auch die Zahl der vernetzten Fahrzeuge wird in den nächsten Jahren rasant steigen.

Was sich für Unternehmen in effizienteren Produktions- und Transportprozessen und im Privaten in mehr Komfort niederschlägt, hat eine hässliche Kehrseite: Milliarden mit dem Internet verbundene Geräte bedeuten auch Milliarden potenzielle Sicherheitslücken. Beispiele gefällig? Im Mai ließ ein Hacker in Texas smarte Verkehrsschilder statt vor Baustellen vor Donald Trump warnen. Per Internet konnten Forscher über das Infotainment-System bei einigen Modellen von Fiat Chrysler auf den CAN-Bus zugreifen und die Klimaanlage, die Türverriegelung und sogar die Bremsen steuern. Industrieanlagen vom Hochofen bis zum Stromnetz wurden schon ebenso Opfer von Angriffen wie Smart-Home-Systeme, die eigentlich vor Einbrüchen schützen sollen.

Bei all diesen Beispielen handelt es sich allerdings um Angriffe **auf** vernetzte Geräte. Was wir hingegen in den letzten Monaten erleben, sind Angriffe **durch** das Internet of Things – und die haben eine ganz andere Qualität. Gerade erst im Oktober machte ein DDoS-Angriff auf den DNS-Provider Dyn große Dienste wie Netflix, Spotify und Twitter teilweise unerreichbar (siehe Seite 88). Die Attacke erreichte eine neue Dimension: Dyn wurde mit über einem Terabit pro Sekunde bombardiert.

Das Mirai-Botnetz, das hinter der Attacke steckte, besteht aus etwa 500 000 IoT-Geräten – überwiegend digitale Videorecorder und Webcams. Die sind geradezu lächerlich schlecht gesichert: Die Geräte lauschen auf Port 23 oder 2323 auf Telnet-Anfragen und verwenden dabei Standard-Log-in-Daten. In Zeiten, in denen Server und Desktop-PCs durch Firewalls und Antivirensoftware immer besser geschützt sind, kommt die Flut billiger IoT-Geräte den Botnetz-Betreibern wie gerufen.

Wenn nicht ein massives Umdenken bei Herstellern wie Anwendern einsetzt, wird das Internet of Things zu einem Sicherheitsalbtraum werden. Ein Zusammenbruch großer Teile des Internets durch einen gezielten Angriff rückt in den Bereich des Vorstellbaren – und wäre eine Katastrophe angesichts der Bedeutung, die das globale Netz heutzutage für alle Lebensbereiche hat.

Der Legende nach wurde das Internet mit seinen dezentralen Strukturen vom amerikanischen Verteidigungsministerium entwickelt, um auch im Fall eines Atomkriegs über ein funktionierendes Kommunikationsnetz zu verfügen. Es wäre eine arge Ironie, wenn es jetzt durch schlampig programmierte Webcams, Toaster und Kühlschränke zu Fall gebracht würde.

OLIVER DIEDRICH

© Copyright by Heise Medien
Persönliches PDF für alle Leser der iX aus 30625 Hannover