IT-Sicherheit im Internet der Dinge

Nicht die Digitalisierung, sondern die Vernetzung von Geräten und immer mehr Gegenständen des täglichen Lebens, zunehmend mit elektronischen Komponenten ausgestattet, ist die eigentliche Herausforderung der Zukunft.

Foto: Fotoscop, Wolfram Sieber

Fahrzeuge, die sich gegenseitig über die aktuelle Verkehrslage oder wetterbedingte Gefahren informieren und daraus eigenständig die beste Fahrtstrecke bestimmen, Kühlschränke, die automatisch knapp werdende Lebensmittel nachbestellen oder eine Haus-Sensorik für Senioren, die Notlagen erkennt und Hilfe herbeiruft, sind schon längst Realität. In den kommenden Jahren wird es immer selbstverständlicher werden, dass auf Haushaltsgeräte – Stichwort „Smart Home" – Fahrzeuge oder Überwachungssysteme nicht nur aus der Ferne steuernd zugegriffen werden kann, sondern diese miteinander Daten austauschen. Jede Kommunikationsmöglichkeit eröffnet jedoch nicht nur neue Möglichkeiten, sondern schafft auch zusätzliche Angriffspunkte, die gesichert werden müssen: eine Datenübertragung kann abgehört oder verfälscht, die Konfiguration eines Geräts unberechtigt geändert oder es können Sensordaten abgehört und ein System, beispielsweise eine Videoanlage, zur Ausforschung missbraucht werden. Da die Elektronik in den vernetzten Geräten im Internet der Dinge (Internet of Things – IoT) oft nicht besonders leistungsfähig ist, ist für viele Hersteller die Versuchung groß, nur sehr einfache oder sogar gar keine Schutzmechanismen vorzusehen, denn ein wirksamer Schutz benötigt Rechenleistung, erfordert vertiefte Fachkenntnisse und verursacht Entwicklungskosten. IT-Sicherheit wird in der „IoT"-Welt immer wichtiger – die Verantwortung dafür liegt aber immer mehr bei Unternehmen aus Branchen, die wenig oder keine Erfahrung mit der Entwicklung wirksamer IT-Schutzmechanismen haben.

Daher ist zu befürchten, dass sich Fehler der IT-Hersteller aus den 90er und 2000er Jahren wiederholen werden. Dabei gibt es zahlreiche Hilfestellungen, wie sich solche Fehler vermeiden ließen. Vor allem das Open Web Application Security Projekt (OWASP) beschäftigt sich seit vielen Jahren mit dem Thema IT-Sicherheit im Internet der Dinge. Daraus sind verschiedene Handreichungen für Entwickler hervorgegangen, wie z. B. die Principles of IoT Security. Und im vergangenen Jahr hat die Cloud Security Alliance (CSA) ein sehr kenntnisreiches Papier mit dem Titel Future-proofing the Connected World veröffentlicht, in dem sie 13 Schritte zur Entwicklung sicherer IoT-Produkte vorstellt.

Dirk Fox,
Secorvo Security Consulting GmbH

www.owasp.org

9. TAG DER IT-SICHERHEIT

28.06.2017

Aktuelle Herausforderungen der IT-Sicherheit – von der neuen Datenschutz-Grundverordnung über ein effektives Risikomanagement und den Aufbau eines Information Security Management-Systems (ISMS) nach ISO 27001 bis zum „Social Hacking" sind Themen des diesjährigen 9. Tag der IT-Sicherheit, einer Kooperationsveranstaltung der IHK Karlsruhe mit dem CyberForum e.V. und der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si).

www.tag-der-it-sicherheit.de