Cyber-Angriffe: Sicherheitslücken im Internet der Dinge

Interview mit Rüdiger Kügler, Sicherheitsexperte der Wibu-Systems AG, über aktuelle Sicherheitslücken im Internet der Dinge und wie sich Unternehmen vor Cyber-Angriffen schützen können

Rüdiger Kügler, Sicherheitsexperte der Wibu-Systems AG

IT-DIRECTOR: Herr Kügler, welche großen Sicherheitslücken existieren aktuell im Internet der Dinge?
R. Kügler: Aktuell befinden wir uns in einer Hypephase. Alle wollen im Internet der Dinge mitspielen und versprechen sich großen Profit bzw. befürchten, den Anschluss zu verlieren, wenn sie es nicht tun. Dabei kümmern sich aber aktuell nur die wenigsten um Sicherheit. Oft steht man vor heterogenen Landschaften, in denen das schwächste Glied die Sicherheit des Gesamtsystems bestimmt. Und nicht zu vergessen die beiden Klassiker: den Implementierungsfehler und die Hintertür. Dies zeigt sich gerade aktuell im Streit zwischen Apple und den Behörden.

IT-DIRECTOR: Wie lassen sich diese Lücken möglichst schnell und nachhaltig schließen?
R. Kügler: Sicherheit muss bereits im Konzept berücksichtigt werden. Firewalls, Virenscanner und Passwörter sind zwar ein erster Ansatz, aber nicht ausreichend. Jeder Teilnehmer im Internet der Dinge steht vor zwei Herausforderungen: Er muss sich selber gegen Manipulationen schützen und er muss andere Teilnehmer sicher erkennen. Ein sicherer Schutz gegen eine Veränderung beinhaltet Secure Boot und Verschlüsselung von ausführbarem Code. Sichere Erkennung erfordert den Einsatz von Zertifikaten.

IT-DIRECTOR: DDoS-, Man-in-the-Middle- oder Ransomware-Attacken: Welche Methoden nutzen Cyber-Kriminelle bevorzugt zum Angriff auf IoT-Installationen?
R. Kügler: Dies hängt vom Ziel des Angreifers ab. Ist das Ziel das „Lahmlegen“ eines Teilnehmers, dann ist die DDoS-Attacke die Waffe der Wahl. Ein Teilnehmer wird mit so vielen Anfragen quasi bombardiert, dass er nicht mehr antworten kann. Ist das Ziel das Ausspähen von Daten oder die Manipulation, dann sind die gewählten Methoden diffiziler und hängen von den gewählten Schutzmaßnahmen ab. Speziell hochentwickelte Viren und trickreiche Mechanismen, um diese Viren zu verstecken und somit sicher zum Ziel zu gelangen, sind das Fazit von Stuxnet. In anderen Fällen ist es einfach nur Sozial Engineering und Bestechung.

IT-DIRECTOR: Stichwort „Internet der Dinge“: Werden Connected Cars oder Industrie-4.0-Anlagen gehackt, ist großer Schaden vorprogrammiert. Wie sollte eine umfassende Sicherheitsstragie für die Geräte im Internet der Dinge aussehen?
R. Kügler: Sicherheit muss während der Architekturphase bereits im Design berücksichtigt werden. Ein nachträgliches Überstülpen hat selten funktioniert. Mit Zertifikaten und Secure Boot stehen starke

Methoden zur Verfügung, um Sicherheit by Design zu schaffen. Aber diese kosten Geld und sind – speziell Zertifikate – unhandlich. Das heißt, die Umsetzung beginnt in den Köpfen des Anwenders, „Geiz darf nicht mehr geil sein“ und Anwender müssen Sicherheit bewusst leben.

IT-DIRECTOR: Welche Rolle spielen dabei Verschlüsselungsmechanismen?
R. Kügler: Verschlüsselungsmechanismen sind ein Kernpunkt der Abwehrmaßnahmen. Wobei man allgemeiner von kryptographischen Mechanismen sprechen sollte, denn neben der Verschlüsselung spielen Einwegfunktionen (Hash) für einen Fingerabdruck, elektronische Unterschriften (Signaturen) und Beglaubigungen (Zertifikate) eine wichtige Rolle. Neben den Mechanismen selber sind die Erzeugung und die Speicherung von kryptographischen Schlüsseln für den Erfolg maßgeblich. Die Verschlüsselung eines PDFs wird sicher mit AES mit einem 256-Bit-Schlüssel durchgeführt. Aber der Schlüssel wird durch ein Passwort erzeugt. Wählt der Anwender also nur ein vierstelliges Passwort, dann ist der ganze Mechanismus nichts mehr wert. Und hier sind wir wieder beim Faktor: Der Anwender muss die Sicherheit bewusst leben.

IT-DIRECTOR: Was spricht für die Nutzung von Verschlüsselung im Internet der Dinge (z.B. Schutz, Verfügbarkeit) und was dagegen (z.B. erforderliche Bandbreiten, Performance)?
R. Kügler: Der Bewegungssensor eines Telefons kann den persönlichen Autofahrstil erfassen. Abhängig davon erhalten die Nutzer bessere oder schlechtere Konditionen ihrer Autoversicherung. Der neue Arbeitgeber sieht im Internet der Dinge sofort, dass man beim vorhergehenden Arbeitgeber wegen Stresses krankgeschrieben waren. Anhand der Ortung des Handys erkennen organisierte Einbrecher, dass die eigene Wohnung gerade unbewacht ist und brechen ein. Der gläserne Mensch und seine kleinen Geheimnisse sind ein kleiner Punkt, der für Verschlüsselung und Schutz von Daten stehen. Aber das Ausnutzen von ungesicherten Daten durch Kriminelle ist der wesentliche Punkt, warum ein Internet der Dinge ohne Schutz und damit ohne Verschlüsselung wie eine Blase zerplatzen würde. Die Mehrkosten, die dem entgegenstehen, erscheinen unter diesen Gesichtspunkt wie Peanuts.