IT-Security im Zeitalter des Internets der Dinge

Gadgets und Geräte sind zunehmend vernetzt und kommunizieren übers Internet. Wir vertrauen ihnen, da sie im Alltag hilfreich sind. Was aber bedeutet das für die IT-Sicherheit?

DER AUTOR

Thomas Zweifel
Senior IT Consultant, Adnovum

Ohne die vielen smarten Dinge, die übers Internet vernetzt sind (Internet of Things, IoT), geht in unserem modernen Alltag fast nichts mehr. Ob sie als Jogging-Uhr sensible Daten über unsere Position und Gesundheit verarbeiten, als Kühlschrank über unsere Ernährung Bescheid wissen oder als Smartphone den schnellen, zuverlässigen Zugang zu Onlinebanking oder Mobile Payment sicherstellen, wir vertrauen ihnen, weil sie uns das Leben erleichtern. Doch geht leider oft die Sicherheit der IoT-Geräte vergessen, ein grosser Teil wird etwa bei Sicherheitspatches vernachlässigt, was zu Sicherheitslücken führt. Mit HTML5 und Javascript hat sich zudem die Applikationslogik von den Servern auf die Endgeräte verlagert, wodurch die Daten zusätzlich exponiert sind.

Für Anbieter von Webdiensten ist dies eine ernsthafte Herausforderung, denn die Möglichkeiten zur Einflussnahme sind begrenzt. Die Geräte stehen unter der Kontrolle der Hersteller und der Benutzer. Den Kunden eines Diensteanbieters ist in der Regel der Schutz ihres eigenen Geräts und allenfalls ihrer Daten wichtig, jedoch eher selten die Sicherheit der genutzten Services.

Ein Dienstanbieter sollte sich über die potenziellen Schadensszenarien im Klaren sein. Bietet er zum Beispiel kostenpflichtige Daten wie Videos oder Börsendaten an, so resultiert ein Missbrauch in entgangenem Gewinn, was allenfalls noch verkraftbar ist. Werden jedoch Kundendaten wie Bewegungsprofile entwendet, kann der Schaden um Dimensionen grösser sein, einerseits durch Drittschäden und Haftung, andererseits durch Reputationsverlust.

Protect …

Welche Möglichkeiten hat ein Dienstanbieter, seine Daten zu schützen? In einem ersten Schritt muss er seine Kunden und deren Geräte identifizieren. Die Methode dazu darf je nach Schadenspotenzial einfacher oder komplexer sein. So sollte bei heiklen Zugriffen, etwa auf Gesundheits- oder Bankdaten, konsequent eine Mehr-Faktor-Authentisierung verlangt werden. Dabei ist zwischen Usability und Security abzuwägen. Bei einer einfachen Kontostandabfrage kann allenfalls ein Passwort oder ein Fingerabdruck reichen. Die Lösung muss so sicher wie nötig und so benutzerfreundlich wie möglich sein.

Leider geht oft die Sicherheit der IoT-Geräte vergessen. Bild: Fotolia

… Detect …

Eine wichtige Ergänzung zum Gatekeeping ist die Detektion. Im Zeitalter von BYOD und IoT laufen die Angriffsszenarien vermehrt über die Geräte der Benutzer. Somit empfiehlt es sich, das Nutzungs- und Zugriffsverhalten auszuwerten, um auffällige Abweichungen zu erkennen. Doch welche Aspekte des Verhaltens sollen einbezogen werden? Können Basisinformationen zum verwendeten Gerät, Browser und Standort verwendet werden? Soll man die genutzten Serviceaufrufe mit früheren Nutzungsprofilen vergleichen? Werden Limiten überschritten, etwa durch eine massive Häufung von Abfragen oder eine besonders grosse Transaktion? Und soll jeder Service diese Analysen selbst machen oder ist ein zentralisiertes Risk-Monitoring über Systemgrenzen hinweg schlagkräftiger und präziser?

… React

Ist ein potenzieller Angriff erkannt, gilt es, darauf zu reagieren. Je nach angebotenen Services sind verschiedene Möglichkeiten denkbar, angefangen bei der gezielten Verzögerung bei der Auslieferung von Daten, dem sogenannten Throttling, über zusätzliche Sicherheitsfragen bei leicht ungewöhnlichen Situationen bis hin zur Sperrung oder Filterung.

Allen Szenarien gemeinsam ist die Aussage, dass Zugriffsschutz allein nicht mehr genügt. Ein Sicherheitskonzept muss heute auch Anomaly Detection umfassen und für die verschiedenen Situationen angemessene Reaktionen vorsehen. Denn die Frage lautet nicht, ob es einen Angriff geben wird, sondern wann er erfolgt, wie man ihn erkennt und wie man darauf reagiert.