Gunter Bitz

Datenschutzwüste IoT

Bei jeder neuen Technologie scheinen die Macher wenig aus den Fehlern ihrer Vorgänger zu lernen. Auch bei der Markteinführung des „Internet of Things" (IoT) wiederholt sich die Geschichte. Die spontane Akzeptanz von ‚nützlichen' Funktionen drängt Risiken ihrer Anwendung in den Hintergrund.

Auch aus diesem Grund sind 15 Jahre nach Bill Gates legendärer E-Mail[1], die Themen Datenschutz und IT-Sicherheit in vielen Bereichen des IoT noch Fremdworte.

Diese E-Mail, in der Bill Gates die Sicherheit von Software über alle übrigen wirtschaftlichen Belange stellte, markierte den Auftakt einer neuen IT Sicherheitsära, die weit über das Unternehmen Microsoft hinauswirkte. In der Softwareentwicklung hat sich weitgehend das Konzept etabliert, IT Sicherheit- und Datenschutzmaßnahmen von Anfang an einzuplanen. Diese Schutzmaßnahmen können nicht am Ende der Softwareentwicklung noch schnell nachgereicht werden.

Trotzdem entwickeln viele IoT Anbieter IoT-Geräte und Anwendungslösungen, ohne diese Prämissen zu befolgen. In vielen – aber nicht allen – Fällen sind es Start-up Unternehmen, die gar nicht über entsprechende Expertise verfügen. Daher entfällt oft auch das Nachreichen der IT Sicherheit zusammen mit dem Datenschutz, der bekanntermaßen ohne Datensicherheit nicht möglich ist.

Häufig auftretende Fehlerklassen sind:

1. Unsichere „default" Konfiguration wie z.B. das Passwort des Admin Zugangs.
2. Unsichere Kommunikation: Fehlende Verschlüsselung, fehlende Endpunkt Authentisierung, Anfälligkeit für „man-in-the-middle" und „replay" Angriffe.
3. Unsichere Update Prozesse, keine digitale Signatur der auszuführenden Dateien.
4. Fehlende Prozesse zur Softwareaktualisierung, keine automatisch einspielbaren Updates.
5. Unsichere Software, die Ausführen von Schad-code erlaubt (z.B. durch „buffer overflow").

Für Punkt 2 gibt es in der Tat eine beliebte Ausrede: Es wird angeführt, dass die typischen IoT Geräte nicht die Rechenkapazität haben, um eine sichere Verschlüsslung und Authentisierung (z.B. mit TLS 1.2) zu implementieren. Dies ist sicherlich richtig für kostengünstige 8-Bit Micro Controller, die häufig in IoT Geräten anzutreffen sind.

Solche Einschränkungen sind jedoch bereits bei dem Entwurf der Systemarchitektur bekannt und geeignete Maßnahmen zur Abhilfe sind überfällig – z.B. Verwendung eines leistungsfähigeren Relais, das die externe Kommunikation der limitierten Micro Kontroller übernimmt.

Darüber hinaus gibt es hinreichend viele Konzepte zur Lösung der aufgeführten Probleme. Eine Literaturliste zum Thema IT-Sicherheit, sichere Software-Entwicklung und Datenschutz würde den Rahmen dieser DuD Ausgabe sprengen.

So stellt man sich berechtigt die Frage, warum das IoT wenig Gebrauch von diesen etablierten Konzepten macht. Ein Mangel an Wissen kann der Grund nicht sein.

Sind es also wirtschaftliche Interessen? Indizien dafür sind:

1. In vielen Fällen bleibt ein Angriff unbemerkt, da die Funktionalität der Geräte nicht beeinträchtigt wird.
2. Zur Implementierung einer IoT Landschaft gibt es noch keine konkreten Datenschutzvorgaben durch die Aufsichtsbehörden. Daher treten Kunden mit solchen Anforderungen in der Mehrheit nicht an die Hersteller heran.
3. Nur ein kleiner Teil der IoT Geräte ist tatsächlich Datenschutz relevant[2].
4. Auf Grund fehlender Kundenanforderungen und einer quasi nicht durchsetzbaren Haftung[3] gegenüber Herstellern ist es weitgehend wirtschaftlich unrentabel, in Sicherheitsanforderungen zu investieren.

Interessanterweise haben diverse namhafte deutsche Industrie Anbieter auf die Anfrage des Herausgebers, einen Beitrag in dieser Ausgabe der DuD zu publizieren, erst gar nicht reagiert. Ein Grund ist möglicherweise, dass auch in diesen Unternehmen die Diskussion um vorzeigbare Sicherheitskonzepte für ihre IoT Produkte in vollem Gange ist.

Ein möglicher Ausweg ist zweigleisig:

Unternehmerische Anwender, die über das notwendige Fachwissen verfügen, sollten ihre Datenschutz- und Sicherheitsanforderungen klar an die Hersteller ihrer (industriellen) IoT Lösungen kommunizieren.

Die Gruppe der privaten Konsumenten, die mangels Fachwissen mit der Erstellung eines IT Sicherheitskonzepts überfordert wäre, kann besser durch Regulierung geschützt werden. Für die Konsumenten hat die EU bereits die vielfältigsten Themen reguliert: Von Roaming Kosten für Mobilfunk bis hin zum Stromverbrauch eines Staubsaugers. Warum also nicht auch die Sicherheit und den Datenschutz von IoT Geräten!

Auch der weltweit anerkannte Sicherheitsexperte Bruce Schneier plädiert nun ebenfalls für Regulierung[4].

1 Bill Gates „Trustworthy Computing", 2001. https://www.wired.com/2002/01/bill-gates-trustworthy-computing/

2 Paradoxerweise sind dann aber die Informationen umso sensibler: Körperdaten (Schrittzähler, Waagen), IP Kameras im Kinderzimmer.

3 Siehe Martin Klein-Hennig und Felix Schmidt in dieser Ausgabe.

4 Bruce Schneier, https://www.rsaconference.com/videos/regulating-the-internet-of-things RSA Conference San Francisco, February 14, 2017.