IoT Inspector

white paper

Beschaffung sicherer IoT Geräte

Thomas Kerbl Principal Security Consultant SEC Consult
Florian Lukavsky Geschäftsführer SEC Technolgies

V092019_DE

In Analgoie zu unserem Whitepaper "Beschaffung sicherer Web-Applikationen" gibt das vorliegende Whitepaper einen generellen Überblick über die notwendigen Aktivitäten, um sicherheitskritische IoT Geräte zu beschaffen. Weitere Details können den ENISA "Baseline Security Recommendations for IoT"[1] entnommen werden.

Sicherheitskritische IoT Geräte

Auf Grund von komplexen Zusammenhängen zwischen Hardware, Sensoren und Firmware bauen IoT Geräte meist auf eine oft undurchsichtige Lieferkette auf. Um ein angemessenes Schutzniveau des IoT Geräts zu gewährleisten ist es daher unerlässlich Maßnahmen zu setzen, die von einfachen und klaren Security Vorgaben bis hin zu Security Abnahmetests reichen können.

Beim Einkauf von IoT Geräten holt sich ein Unternehmen oft eine Blackbox in die eigene Infrastruktur bzw. gibt dieser Zugriff auf vertrauliche Informationen. Insbesondere beim Zugriff auf datenschutz-relevante Informationen (GDPR) ist höchste Vorsicht geboten, um Reputationsschäden und rechtliche Folgen zu vermeiden.

Von IoT Geräten gehen unterschiedliche Bedrohungen aus:

1. Die IoT Geräte weisen Schwachstellen auf, die eine Kompromittierung des Systems, des Netzwerks oder der verarbeiteten Daten erlauben.
2. Die Sicherheitsmechanismen der IoT Geräte entsprechen nicht den Sicherheitsvorgaben des Unternehmens und sind somit nicht angemessen für den jeweiligen Schutzbedarf.
3. Die eingebundenen Backendsysteme weisen zum Beispiel Schwachstellen in der Konfiguration, der Authentifizierung oder der Autorisierung auf und exponieren dadurch Daten an Dritte.
4. Kommunikation vertraulicher Daten zu Backendsystemen Dritter erlauben diesen den Zugriff auf diese Daten.

Grund hierfür sind mangelnde Vorgaben an die Hersteller im Rahmen der Beschaffung sowie unzureichende Abnahmetests vor Übernahme der IoT Geräte. Nur eine klar nach sicherheitstechnischen Gesichtspunkten spezifiziertes IoT Gerät wird den eigenen Anforderungen des Unternehmens genügen.

1 https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot/at_download/fullReport

CHECKLISTE

Konkrete Maßnahmen für die Beschaffung

Um einen Grundschutz zu erreichen, sind mindestens folgende Aktivitäten durchzuführen:

☐ Durchführung von Schutzbedarfsbestimmung und Bedrohungsanalyse, bevor ein neues IoT Gerät beschafft wird, um die notwendigen Sicherheitsmechanismen beschreiben zu können.

☐ Definition und Verifikation von konkreten technischen Security-Anforderungen im Rahmen der Beschaffung. Diese werden in einem Security-Lastenheft beschrieben und sind vom Hersteller nachweislich umzusetzen. Orientierung bieten hierfür etablierte Vorgaben, wie z.B. die ENISA "Baseline Security Recommendations for IoT"[2]. Des Weiteren gibt es auf Sicherheit fokussierte Beschaffungsplattformen, wie z.B. „IT-Sicher kaufen"[3], von denen konkrete Beschaffungstexte entnommen werden können.

☐ Prüfung des Herstellers hinsichtlich Vertrauenswürdigkeit und Sorgfalt im Rahmen der Hardware- und Software-Entwicklung. Zur Orientierung dienen etablierten Reifegradmodellen wie OWASP SAMM[4] und BSIMM[5]. Der Hersteller muss nachweisen, dass er den geforderten Reifegrad – abhängig vom Schutzbedarf der Applikation – für alle Entwicklungsaktivitäten umsetzt.

☐ Durchführung von automatisierten Sicherheitstests beispielsweise durch Prüfung der Firmware des IoT Geräts im Rahmen einer Vorauswahl von IoT Geräten. Mit dieser kosteneffizienten Methode können Sicherheitskennzahlen bereits in den Auswahlprozess einfließen und IoT Geräte, die nicht den eigenen Sicherheitsstandards genügen, frühzeitig ausgesiebt werden.

☐ Durchführung von tiefgehenden Sicherheitstests im Rahmen der Abnahmetests der Applikation. Empfohlen werden Whitebox-Audits basierend auf den OWASP IoT Testing Guides[6].

☐ Einforderung der schriftlichen Zusicherung des Herstellers, dass alle definierten Sicherheitsanforderungen erfüllt sind. Dies stärkt die eigene Position im Falle von nachträglich identifizierten Mängeln im Sicherheitsbereich.

☐ Sichtung von Security-Dokumentation, die im Rahmen der Software-Entwicklung erstellt wurde (z.B. Dokumentation der Sicherheitsarchitektur, Datenfluss-Analysen, Ergebnisse von internen Sicherheitstests).

☐ Bekommt das IoT Gerät Zugriff auf vertrauliche Informationen oder wird diese in besonders schutzwürdigen Bereichen eingesetzt, sollte ein vollständiges Security Source Code Review der Firmware sowie eine physische Sicherheitsüberprüfung des IoT Geräts selbst mit Fokus auf versteckte Hintertüren in der Software und Hardware durchgeführt werden.

2 https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot/at_download/fullReport
3 https://www.it-sicher.kaufen/
4 https://www.owasp.org/index.php/OWASP_SAMM_Project
5 https://www.bsimm.com/
6 https://www.owasp.org/index.php/IoT_Testing_Guides

Zusammenfassung und Conclusio

Werden im Rahmen der Beschaffung von IoT Geräten die notwendigen Aktivitäten gesetzt, um angemessene Sicherheitsanforderungen zu spezifizieren und zu verifizieren, ist ein wesentlicher Grundstein für den sicheren Einsatz der IoT Geräte gelegt. Es gibt inzwischen eine Vielzahl etablierter Empfehlungen und Guidelines, die hierbei unterstützen. Die in diesem Whitepaper dargelegten Aktivitäten sollten in den Beschaffungsprozess integriert werden, um eine einheitliche Umsetzung sicherzustellen.

Die Firmware-Analyseplattform für hohe Sicherheitsansprüche

IoT Inspector wurde ursprünglich als in-house-Tool für manuelles Pentesting von IoT-Geräten entwickelt. Im Laufe der Jahre entwickelte sich daraus eine ausgereifte Firmware-Analyseplattform, die weltweit von Unternehmen, Infrastrukturanbietern, Herstellern, Beratungsunternehmen und Forschern verwendet wird.

Intelligente Maschinen, vernetzte Geräte, neue Firmware – jeder Kauf und jede Änderung im System birgt das Risiko zusätzlicher Sicherheitslücken. Die ständig wachsende Komplexität der angeschlossenen Geräte und die Forderung nach Einhaltung der Sicherheitsstandards im Internet der Dinge erfordern auch einen effizienteren Ansatz für die Risikobewertung.

IoT Inspector bietet Ihnen das notwendige Werkzeug, um Schwachstellen und Sicherheitsrisiken automatisch zu erkennen, bevor Angreifer diese ausnutzen.

IoT **Inspector**

Weitere Informationen zum IoT Inspector finden Sie auf www.iot-inspector.com
oder kontaktieren Sie uns per eMail: office@iot-inspector.com