Sicherheit im IoT

Andreas Chatziantoniou
Foxglove-IT BV
Utrecht, Niederlande

Schlüsselworte

IoT, Security

Einleitung

Seit einiger Zeit redet jeder über das Internet of Things (IoT). Smartphones und Wearable Technology, intelligente Kühlschränke und Minicomputer wie Raspberry Pi's sind schon beinahe Allgemeingut.

Wie sieht es dann mit der Sicherheit aus? Welche Bedrohungen gibt es? Was muss ich als Entwickler, Architekt und Betreiber solcher Infrastrukturen wissen?

Weiterhin wird betrachtet welche Oracle Produkte diese Zielsetzung unterstützen, wie das Identity Management umgesetzt werden kann und bis zu welcher Stelle in der Architektur die Verantwortung der verschiedenen Akteure reicht.

Daher ist die folgende Liste zu beachten:

- Security ist ein fundamentaler Bestandteil der Daseinsberechtigung von IoT.
- Es gibt zurzeit keinen Konsens wie Sicherheit in IoT Geräten implementiert werden muss
- Wir dürfen nicht den fehler machen um an zu nehmen, dass die langjährigen Erfahrungen im Securitybereich ohne weiteres in IoT übernommen wird
- Es wird keine einfache und allgemeingülltige Lösung geben um alle Risiken zu entschärfen

Technik

Wie sorge ich für die Absicherung meiner Software im IoT Umfeld? Welche Möglichkeiten bietet der Java Stack? Worauf muss ich achten wenn ich die Grenze meiner eigenen IT Umgebung verlasse?

Firewwalls und SSL sind nur ein Aspekt der hierbei eine Rolle spielt. Nur will eine Organisation auch dafür sorgen, dass die IoT Anwendung nicht modifiziert wird um zu garantieren das keine falschen Daten oder Hintertüren entstehen.

Sicherheit im IoT muss als Fundament deutlich machen, dass Anwendungen Mehrwert bieten.

Was kann das Device

Obwohl ein Gerät wie ein Raspberry Pi erstaunliche Kapazitäten hat, muss befürchtet werden, dass viele IoT Geräte zu klein sein werden um neben den angebotenen (und gewünschten) Funktionen auch noch Sicherheitsvorkehrungen ausführen zu können. Dies wird insbesondere im Bereich der "Wearables" der Fall sein. Geräte ohne Display und auf Batterieversorgung werden gebaut um genau ein oder zwei Funktionen an zu bieten. Sicherheit wird hier mit Sicherheit nicht dabei sein.

Kann ich in meiner Anwendung diesen Daten vertrauen? Während das Hundehalsband mit IoT Funktionalität scheinbar keine große Sicherheitslücke darstellt wird dies etwas anderes wenn mein SmartMeter andere Verbrauchsdaten an die Stromgesellschaft durchgibt.

Vorbereitung

Genau wie bei normalen Anwendungen müssen die folgenden Punkte angesprochen werden:

- Security ist von Anfang an dabei
- Lifecycle Unterstützung und Updatemöglichkeiten
- Zugangskontrolle und Authentizierung von Geräten
- Vorbereitung für den Ernstfall

Security and Trust Services API (SATSA)

Innerhalb des Java ME Stacks wird Security and Trust Services API (SATSA) eingesetzt. Was bedeutet dies für den Entwickler?

An Hand eines Beispiels wird gezeigt wie ich diese Sicherheitsfeatures einbauen kann.

Entwicklung

Das OWASP Internet of Things Project beschreibt eine Liste von Sicherheitsrichtlinien. Diese Liste wird im Vortrag behandelt und die Auswirkungen auf Entwickler und Tests wird aufgezeigt.

Insbesondere das "Erzwingen" von verschiedenen sicherheitsrelevanten Aspekten in der Phase der Entwicklung wird ein Mehrwert im Produkt bzw. System liefern.

Enterprise IT

IoT ist zurzeit noch sehr stark in der "Bastelphase". Hierdurch liegt der Nachdruck auf der Erkundung der Möglichkeiten, der Suche nach Use-Cases und dem IoT Äquivalent des nächsten "Angry Birds".

Wichtig für eine echte Benutzug des IoT wird die Einbindung in meine Enterprise IT sein. Wie sorge ich für eine starke Ausbreitung meiner Business Assets? Denn immerhin werden statt einigen hundert Rechnern eventuell tausende van extra Geräten Zugang zu meinen IT Systemen bekommen. Wie wird sich dies auf Netzwerke und Monitoring der Umgebung auswirken?

Architektur

Bisher waren Internet Architekturen relativ einfach - Browser (interaktiv) oder Web Services (machine2machine) kamen zu meinen Front- und Back-End Systemen. Wie gehe ich hier mit IoT um? Stellen diese System andere Anforderungen an meine Architektur? Welche Schritte sind notwendig um eine IoT Referenzarchitektur auf meine eigenen Umstände an zu passen.

Hierbei ist zu beachten welcher Kategorie ein Gerät angehört und wie sich die Sicherheitsfrage in diesem Bereich stellt.

Bei "Identifizierbaren Dingen" haben wir es mit passiven und nicht-intelligenten Sachen zu tun. Der Sicherheitsimpact ist klein, da wir kaum mit Malware und Sabotage rechnen können. Die Daten können jedoch sensitiv sein (Wo ist mein Packet?).

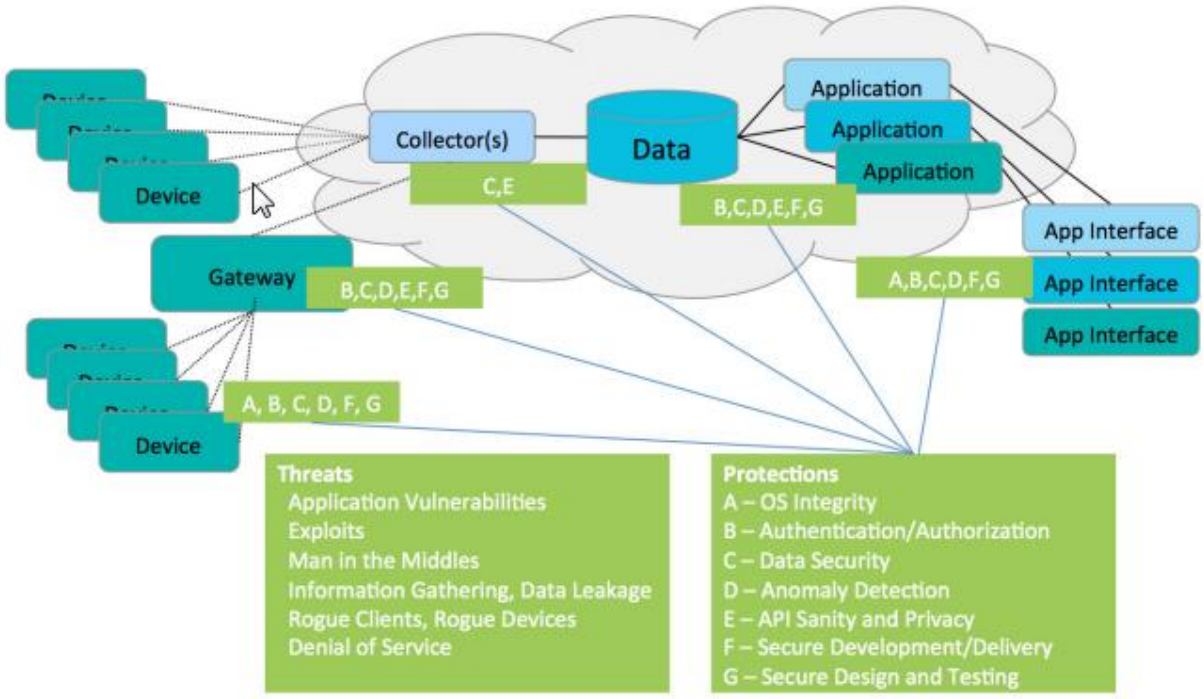
Sensoren mit Kommunikationsfunktion (Messen von Umgebungsparametern wie z.B. Luftdruck, temperatur, etc.) bieten schon andere Möglichkeiten für Hacker. Hier wird Malware schon zum Thema da diese Geräte wahrscheinlich sehr einfach konstruiert sein werden.

Bei kontrollierbaren oder autonomen Geräten (Roboter, Autos) muss der Sicherheitsanspruch sehr hoch sein.

Für meine IT Architektur bedeutet dies, dass ich mir Gedanken machen muss über Zonen in denen die Sicherheit sehr hoch ist, bis hin zu Zonen mit niedriger Sicherheit. Dies erfordert ein Umdenken, da wir bisher immer von sicheren Umgebungen innerhalb meiner Netzwerke ausgingen.

Dies kann evt. durch den Einsatz von Gateways gelöst werden. Hierbei werden IoT Geräte nicht mehr direkt auf das firmeninterne Netzwerk angeschlossen sondern wird ein Gateway zwischengeschaltet. Was muss ein solches Gateway dann können? Hier wird vom Einsatzfall abhängig eine Einschätzung erfolgen. Aber das Filtern von unsinnigen Daten und ggf. der Reset von IoT Geräten sollte dazu gehören.

Die folgende Zeichnung zeigt dies auf:



Kennzeichnen für die IT Architektur bei IoT wird es sein sich darauf zu besinnen um in der internen IT mehr Aufmerksamkeit für die Kontrolle auf zu wenden als bisher.

Continious Delivery

Die IoT Welt wird noch dynamischer sein als wir es bei herkömmlichen Systemen gewöhnt waren. Dies legt den Nachdruck auf die Behandlung von Continious Delivery.

Hier werden vor allen die folgenden Punkte wichtig sein:

- Vorbereitet sein auf die Entdeckung von Securityissues nach der Auslieferung
- Software muss in der Lage sein um Updates von device-side Code auszuführen
- Dies muss im CD Prozess unterstützt werden
- Wann kann ich Updates ausführen (bei Konsumentenartikeln oder Industrysensoren)?

Betrieb

Ein besonders wichtiger Punkt ist die Frage der Kontrolle - wie werden extern vorhandene Geräte betrieben? Wer kümmert sich darum wenn Updates stattfinden müssen? Was bedeutet es verschiedene Versionen der IoT Geräte zu haben? Kann ich dann noch alle Dienste anbieten? Will ich Lebenszyklen (und auch Desupport für Geräte und der darauf laufenden Software) anbieten, und wenn ja - wie viele?

Auditing

Noch mehr als in normalen Systemen muss ich mich um den Bereich des Auditing kümmern. Hier kommen an der Back-End Seite viele vorhandene Techniken zum Einsatz, wie z.B. Analyse von Logfiles und der Einsatz von starken Securitypolicies.

Kontaktadresse:

Andreas Chatziantoniou

Foxglove-IT BV

Texel 18, 3524 AP Utrecht

Niederlande

Telefon: +31623259167

E-Mail andreas@foxglove-it.nl

Internet: www.foxglove-it.nl