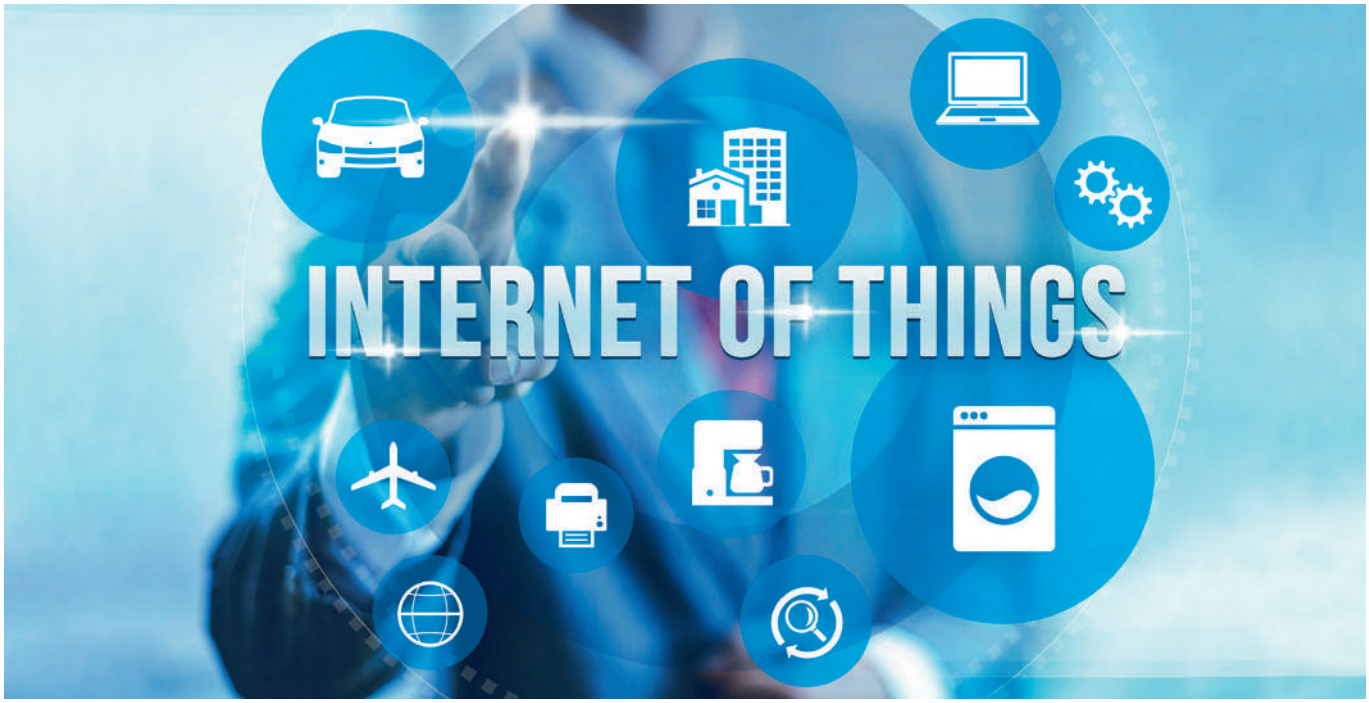
IOT PROJEKTE AUF SICHERE GELEISE FÜHREN

DURCH SYSTEMATISCHE ANALYSE UND TESTS

von Andreas Kölliker

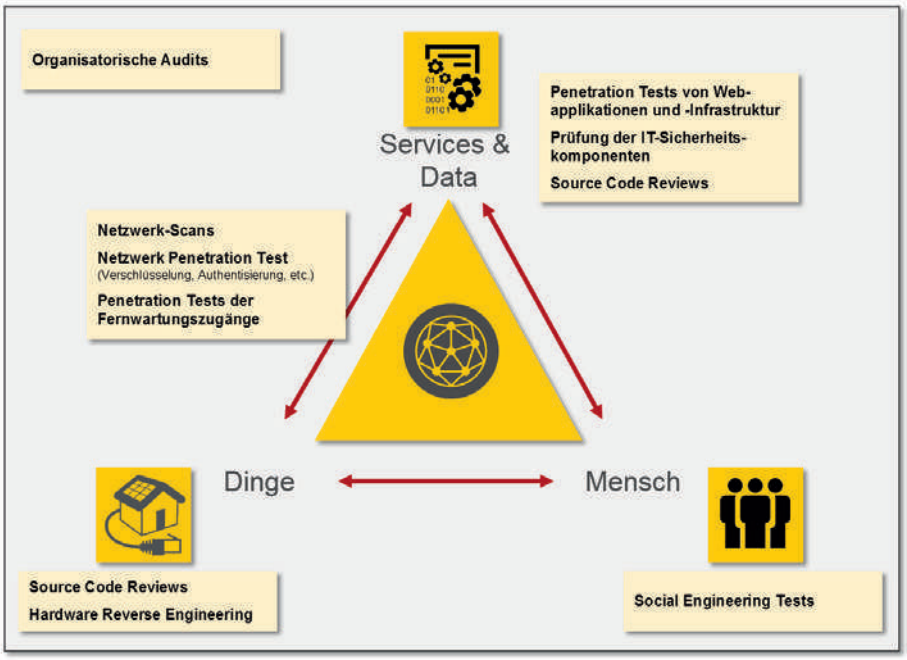
Das Internet der Dinge (IoT), der derzeit vermutlich grösste Hype in der IT-Welt, macht auch vor der Energiebranche nicht Halt. Aktuelle Cyber-Bedrohungen stellen für IoT-Projekte eine grosse Herausforderung dar. Unterschiedlich hoher Schutzbedarf trifft auf eine Vielzahl von Lösungsansätzen und Komponenten. Hier ist es ratsam, sich den unterschiedlichen Risiken und kritischen Schwachstellen bewusst zu werden und gezielt dagegen vorzugehen.



Die Energiebranche zeigt sich vorbildlich, was Safety- und Verfügbarkeitsanforderungen anbetrifft. Mit IoT entwickeln sich die Branchenlösungen jedoch in eine – in weiten Teilen – offene «OT» (Operational Technology) Welt, in der kritische Systeme nicht mehr isoliert sind. Das heisst in eine Richtung, in welcher die traditionelle IT bereits seit Jahrzenten mit klassischem Risikomanagement handelt, um Vertraulichkeit und Integrität zu gewährleisten. IoT ist zwar nichts Neues aber die heutigen Möglichkeiten mit günstigen und/oder smarten Geräten sind verlockend und eine Chance für den zukünftigen Geschäftserfolg von Energiedienstleistern. Dazu werden laufend neue Systeme mit Schnittstellen zur Aussenwelt entwickelt und auch schon erfolgreich eingesetzt. Bereits realisierte IoT-Projekte in der Schweizer Energiewirtschaft zeigen dies eindrucksvoll auf.

So steuern beispielsweise intelligente Systeme einen Park von Warmwasserboilern für die Bereitstellung von Regelenergie. Systeme automatisieren dabei ganze Meter-to-Cash-Prozesse oder komplexe Smart Grid-Komponenten übernehmen kritische Funktionen im Stromnetz. Ideen, wie der Einsatz von Drohnen zur voraussagenden Wartung von Anlagen oder der Einsatz von Low Power-Netzen für die Übertragung von Sensor-Messwerten, werden eher früher als später verbreitet zum Einsatz kommen. Dabei gilt es, nicht nur die Integrität und die Verfügbarkeit der einzelnen Systeme zu schützen, sondern auch die Daten.

Der Business Case von IoT-Systemen liegt längst nicht mehr nur in der Automatisierung von Prozessen, sondern auch in der Individualisierung und Personalisierung von Energieprodukten und den dazugehörigen Dienstleistungen. Vertrauenswürdige Dienstleister müssen den Schutz dieser personenbezogenen Daten ernst nehmen. Umso mehr, weil die Daten in der Cloud bearbeitet und über unsichere Netze zwischen Objekten, Menschen und Services übertragen werden. Der Schutzbedarf von



IoT Security-Testmethoden

IoT-Projekten verlangt also Kompetenzen aus den beiden Welten IT und OT.

RISIKEN ERKENNEN UND STRATEGIEN DEFINIEREN

Aber in welcher Entwicklungsphase und mit welchen Massnahmen soll dieser Schutzbedarf in den IoT-Systemen angegangen werden? IoT-Projekte sind zwar keine komplexe Wissenschaft mehr, weisen jedoch trotzdem einige Besonderheiten auf. Security by Design heisst das Mantra in der Security Branche. In der Realität ist dies aus Innovationssicht jedoch nicht immer möglich. Sicherlich: Bei Projekten mit einem stichhaltigen Business Case und im Kontext mit kritischen Funktionen sind alle Best Practice-Ansätze der IT-Security von Anfang an zu berücksichtigen. Beispielsweise aus ISO/IEC 27001/27002 oder IoT-spezifischen Anforderungen und Konzepten – insbesondere wenn es um die Sicherstellung der Identität, die Updatefähigkeit oder um die sichere Datenübertragung über unsichere Netze geht.

Andererseits würde diese enorme Menge von Anforderungen brillante Projektideen im Keim ersticken. Aus diesem Grund ist zu Beginn jedes Vorhabens eine entsprechende Risikoanalyse, genauer genommen eine Schutzbedarfsanalyse durchzuführen. Dabei sind die Auswirkungen von Vorfällen im Kontext des Einsatzes der IoT-Systeme und Use Cases zu hinterfragen. Folgende Fragestellungen sollten berücksichtigt werden:

- Hat ein Vorfall Auswirkungen auf kritische Services?
- Ist die Reputation des Unternehmens gefährdet?
- Entsteht ein finanzieller Schaden durch nicht erbrachte Dienstleistungen oder durch das Nichteinhalten von gesetzlichen Anforderungen?

Auf dieser Basis lässt sich erstmals eine Kritikalität abschätzen und eine erste Herangehendweise ableiten. Dies kann bedeuten, dass Security by Design tatsächlich zwingend notwendig wird oder aber auch, dass erst einzelne Sicherheitsmassnahmen implementiert werden müssen. In IoT-Vorhaben mit höherem Schutzbedarf sollte im nächsten Schritt die Eintrittswahrscheinlichkeit von Vorfällen eruiert und Prioritäten abgeleitet werden. Dies gelingt durch eine Abschätzung der potentiellen organisatorischen und technischen Verletzbarkeiten im Gesamtsystem sowie für die einzelnen Komponenten. Einen guten ersten Anhaltspunkt zur Identifikation dieser möglichen Schwachstellen liefern beispielsweise die SANS Top 20 Critical Security Controls.

TESTEN, TESTEN UND NOCHMALS TESTEN

Der nächste Schritt ist die Untersuchung und das Testen der IT-Security sowie teilweise auch die physische Resilienz der Komponenten. Aber auch die Kommunikation zwischen den Komponenten, die zentralen Datenverarbeitungssysteme und die Interaktion zwischen Anwender und Betreiber müssen berücksichtigt werden. Nicht zu vergessen ist zudem die Prüfung der Gesamtorganisation mitsamt den dazugehörigen Prozessen.

Für die Tests kommen je nach Fragestellung unterschiedliche Methoden zur Anwendung:

- Netzwerk-Scans der IoT-Infrastruktur
- Penetration Tests der verarbeitenden Netzwerke, der Applikationsinfrastruktur und der Fernwartungszugänge
- Prüfung der IT-Sicherheitskomponenten wie Firewalls, SIEM-Systeme und Authentisierungsmechanismen
- Penetration Tests von Webapplikationen wie beispielsweise Kundenportale
- Source Code Reviews der eingesetzten IoT-Komponenten und Applikationen
- Hardware Reverse Engineering der IoT-Komponenten
- Organisatorische Audits nach gewünschtem oder gefordertem Standard
- Social Engineering Tests der Betreiber von IoT-Systemen ▸

ÜBER INFOGUARD

Die InfoGuard AG ist spezialisiert auf umfassende Informationssicherheits- und innovative Netzwerklösungen. Für den effektiven Schutz von IoT- und kritischen Infrastrukturen bietet der Schweizer Cyber Security Experte InfoGuard ein modulares Dienstleistungs- und Lösungsportfolio. Dieses umfasst das Risiko Management und Threat Modeling, den Aufbau eines ISMS nach anerkannten Standards wie ISO/IEC 270xx, die Umsetzung von Governance- und Compliance-Vorgaben sowie die Definition geeigneter Netzwerk-Architektur. Gleichzeitig unterstützen wir Sie beim Aufbau eines angemessenen ICT-Sicherheitsdispositivs und Identity Management. Umfassende Security Operation Services, Source-Code Reviews, periodische Audits der Infrastruktur und Sicherheitsprozesse sowie die permanente Überwachung der Infrastruktur komplettieren das Angebot. InfoGuard hat ihren Hauptsitz in Zug und eine Niederlassung in Bern.

InfoGuard ist ISO/IEC 27001:2013 zertifiziert.

In der Praxis sind häufig Applikationen ein einfaches Ziel für Angriffe. Die Mehrheit der IoT-Anwendungen setzt auf Open Source Software, Drittkomponente sowie Eigenentwicklungen. Zudem sind sie häufig exponiert, was die Applikationen besonders verletzlich macht. Ein Applikationstest nach OWASP IoT Top 10 (siehe Kasten) kann hier ein geeignetes Mittel sein, um verwundbare Stellen ausfindig zu machen. Sicherheitstests können und sollten in jeder Phase der IoT-Lösungsentwicklung durchgeführt werden. Dabei kann es hilfreich sein, mit Testautomatisierungen zu arbeiten. So werden neue oder wiederkehrende Fehler in der Weiterentwicklung der Applikation verhindert.

FAZIT

Um IoT-Projekte zum richtigen Zeitpunkt abzusichern und somit den Schutzbedarf zu gewährleisten, empfiehlt sich die Analyse anhand realistischer Risikoszenarien. Diese helfen dem Projektteam, ein besseres Verständnis für die Sicherheitsbemühungen zu erhalten sowie Transparenz und Vertrauen zu schaffen. Zudem können diese Szenarien später auch für die Modellierung von Bedrohungen beim Testing genutzt werden. Dies schafft zusätzliche Awareness im Projekt und hilft, Schwachstellen kontinuierlich zu beseitigen. Um diese beheben zu können ist es unerlässlich, ein stabiles, verschlüsseltes und authentisiertes Update-System aufzubauen. Damit die Möglichkeit besteht Verbesserungen auf die IoT-Komponenten einzuspielen.

Abschliessend kann gesagt werden, dass kein IoT-System von Beginn an fehlerfrei sein kann. Daher ist es ratsam, als IoT-Dienstleister einen sicheren und benutzerfreundlichen Kanal für Verbraucher zu schaffen, um gefundene Sicherheitslücken zu melden.

OWASP INTERNET OF THINGS TOP TEN

OWASP definiert folgende 10 Punkte als die in Zusammenhang mit IoT relevantesten Schwachstellen:

1. Unsicheres Webinterface
2. Unzureichende Authentisierung/ Berechtigungssteuerung
3. Unsichere Netzwerkdienste
4. Fehlender Transportsicherung (Verschlüsselung)
5. Datenschutzprobleme
6. Unsichere Cloud-Schnittstellen
7. Unsichere Mobil-Schnittstellen
8. Unzureichende Scherheits-Optionen
9. Unsichere Soft-/Firmware
10. Unzureichende physische Absicherung

www.owasp.org/index.php/OWASP_Internet_of_Things_Project

KONTAKT AUTOR

Andreas Kölliker
Senior Security Consultant
InfoGuard AG
infoguard.ch