ELEKTRONIK PRAXIS Wissen. Impulse. Kontakte.

Security

Sicherheit im IoT: „Das größte Risiko ist der Mensch“

27.07.16 | Redakteur: Franz Graser

Augen auf: Das subjektive Risikoempfinden weicht beim Menschen oft von der objektiven Bewertung ab. Das gelte auch für Bedrohungen im IoT, sagt Peter Siwon von MicroConsult. Er ist auch Referent beim IoT-Kongress am 15. September in München (www.iot-kongress.de) (Bild: Clipdealer)

Durch das Internet der Dinge vervielfachen sich die Risiken von Hackerangriffen, denn jedes mit dem Netz verbundene Gerät ist ein potenzielles Einfallstor. Peter Siwon, Business Development Manager bei MicroConsult, und Michael Schnelle, Consultant bei Mixed Mode, schildern im Interview die größten Risiken und erläutern Schutzstrategien.

Wird die Gefahr durch Bedrohungen im IoT aus Ihrer Sicht unterschätzt?

Peter Siwon: Das subjektive Risikoempfinden der Menschen weicht leider oft erheblich von einer objektiven Bewertung ab. Selbst bei großem objektiven und statistisch belegbaren Risiko, etwa im Straßenverkehr, fühlen wir uns sicher, wenn wir selber oder unsere unmittelbare Umgebung noch nicht betroffen war. Das ändert sich schlagartig, wenn uns selbst oder uns bekannte Menschen betroffen (Verkehrsunfall) sind oder Katastrophen in den Medien starke Aufmerksamkeit (Terroranschläge) erregen.

So gesehen kann man davon ausgehen, dass in der Regel die subjektive Einschätzung sehr häufig in der einen oder anderen Richtung falsch liegt. Deshalb ist es wichtig, dass wir Risiken objektiv anhand nachvollziehbarer Daten bewerten, z.B. die Anzahl der Eindringversuche in ein Computernetzwerk pro Tag, die Anzahl potentiell bedrohlicher Emails oder statistischer Daten aus seriösen Quellen.

Michael Schnelle: Durch die derzeit gemachten Erfahrungen bei den unterschiedlichsten Projekten muss ich diese Frage mit Ja beantworten.

Dies ist aber auch nicht verwunderlich, denn IT-Systeme werden im Allgemeinen immer vernetzter und komplexer. Im IoT-Bereich ist das besonders ausgeprägt. Durch die gestiegene

Komplexität wird es immer schwieriger, Software sicher zu entwickeln. Jede Systemschnittstelle ist ein potentielles Einfallstor für einen Angreifer. Zusätzlich sind im IoT oft heterogene Hardwarekomponenten mit heterogener Software im Einsatz.

Jede Komponente muss separat betrachtet werden. Ein kleiner Sensor muss anders abgesichert werden, wie der verwaltende Gateway, der sich aber auch komplett von einer Client-Applikation unterscheidet.

Michael Schnelle von Mixed Mode: „Schon bei der Planung von Systemen sollten Sicherheitsaspekte berücksichtigt werden.“ (Bild: Mixed Mode)

Was ist aus Ihrer Sicht die schlimmste Bedrohung?

Peter Siwon: Wie bereits oben beschrieben ist es die Neigung des Menschen Risiken falsch zu bewerten. Hinzu kommt seine Neigung zu Bequemlichkeit (kein Passwortwechsel, ein und dasselbe Passwort für mehrere Accounts, zu simple Passworte) und seine Abneigung gegen Reglementierungen und Vorschriften.

Eine weitere Bedrohung stellt die Vermischung beruflicher und privater Kommunikation und Systemnutzung dar, etwa Smartphones, die auch privat genutzt werden, werden im Firmennetz eingesetzt. Schließlich ist es schlicht und ergreifend Unwissenheit, so etwa über Voreinstellungen der Hersteller, die geändert werden sollten, bevor ein System online geht.

Kurz: Das größte Risiko stellt der Mensch selbst dar. Ein weiteres Risiko sehe ich in der mangelnden Verfügbarkeit effektiver Prozesse und Infrastrukturen, die im Falle des Not-Falles sicherstellen, dass die Funktionen ausgefallener Systeme übernommen werden und die betroffenen Systeme schnell neu installiert werden. Die größte Bedrohung sehe ich, wenn durch diese individuellen Sicherheitslücken wichtige Infrastrukturen wie zentrale Server oder andere Anlagen über eine nicht tolerierbare Ausfallzeit oder Ausfallhäufigkeit lahmgelegt werden können.

Michael Schnelle: Die Frage nach der schlimmsten Bedrohung lässt sich nicht allgemein beantworten, da sie sehr vom Use-Case und der Einsatzumgebung eines Systems abhängt. Eine Bedrohung wird nach den Gesichtspunkten der Ausnutzbarkeit und des potentiellen Schadens betrachtet. Man spricht hier auch vom potentiellen Risiko einer Bedrohung. Wird durch das Ausnutzen einer Bedrohung ein vergleichsweise hoher Schaden verursacht, kann das Risiko trotzdem gering sein, wenn diese praktisch fast unmöglich ist auszunutzen.

Auf der anderen Seite kann das Risiko für eine Bedrohung auch hoch sein, wenn der zu erwartende Schaden niedrig ist, aber die Ausnutzbarkeit sehr einfach ist. Gegen Bedrohungen, die sehr einfach auszunutzen sind, kann man sich, in der Regel, auch einfach Schützen. Ein beliebtes Einfallstor im IoT ist – da meist unterschätzt – das Web-Interface eines Gateways,

was sich meist durch wenig Konfiguration und den Einsatz geprüfter Standardsoftware absichern lässt.

Wie kann man sich erfolgreich wehren?

Peter Siwon: Das Wichtigste ist Aufklärung, und zwar nicht einmal sondern immer wieder (aus oben genannten Gründen). Es sollte wenigstens eine kompetente Person in der Firma geben, die in der Lage ist, das Risiko objektiv zu bewerten und die notwendigen und angemessenen Sicherheitsmaßnahmen laiengerecht und möglichst leicht umsetzbar vorzubereiten.

Diese Person benötigt genügend Zeit, um sich mit dem Thema kontinuierlich zu befassen, denn Sicherheit im Internet ist ein kontinuierlicher Prozess. Schließlich sollte die Einhaltung der Sicherheitsmaßnahmen regelmäßig und möglichst automatisch erfolgen. Sollte es diese Person nicht geben, ist externe Unterstützung ratsam. Das ist jetzt nichts neues, nur, dass sich der Kreis der von solchen Bedrohungen betroffenen Systeme und Personen durch IoT explosionsartig erweitert.

Michael Schnelle: Sicherheit ist ein Prozess, der idealerweise von Beginn an Bestandteil eines Projekts ist. Sehr schwierig ist es ein fertiges Produkt oder System sicher zu machen. Schon bei der Planung sollten Sicherheitsaspekte berücksichtigt werden. Idealerweise haben auch die Entwickler ein Verständnis für Sicherheit und wissen, was beachtet werden muss um sichere System zu entwickeln. Durch Bedrohungs- und Risikoanalysen kann das optimale Verhältnis zwischen benötigter Sicherheit und den aufzuwendenden Kosten ermittelt werden.

Ein System kann auch meist nicht hundertprozentig abgesichert werden, denn solange mit der Außenwelt interagiert wird, besteht ein Restrisiko. Ziel ist es, dieses Risiko, soweit möglich zu minimieren. Die dafür nötigen Kenntnisse und Mittel vermitteln wir gerne im Zuge unserer Vorträge, Workshops und Projekte.

Peter Siwon und Michael Schnelle referieren am 15. September im Rahmen des IoT-Kongresses in München über das Thema: „IoT-Security-Check: Wie Sie Bedorhungen richtig erkennen“

Best Practices im Internet der Dinge

IoT-Kongress – die Ideenbörse für das Internet of Things

18.07.16 - Über Technik, Anwendungen, Standards und Security im Internet of Things informiert der IoT-Kongress der ELEKTRONIKPRAXIS am 14. und 15. September im Kongresszentrum München (www.iot-kongress.de). lesen

Softwaretechnik

Das Internet der Dinge braucht deutlich bessere Software

12.04.16 - Das Internet der Dinge stellt neue Anforderungen an die Sicherheit von Embedded-Software. Professor Hans-Joachim Hof von der Münchner Hochschule für angewandte Wissenschaften und Leiter der Munich IT Security Research Group (MuSe) mahnt ein Umdenken an. Zu oft werde nach dem Prinzip „verbaut und vergessen" verfahren. lesen

Softwaretechnik

Mit Secure Scrum zu mehr Softwaresicherheit im IoT

29.04.16 - In diesem Teil des Interviews mit Professor Hans-Joachim Hof von der Hochschule München geht es um Lösungsansätze, die zu besserer Embedded-Softwarequalität führen können. Konsistente Entwicklungsprozesse spielen hier eine zentrale Rolle. lesen

Michael Schnelle von Mixed Mode: „Schon bei der Planung von Systemen sollten Sicherheitsaspekte berücksichtigt werden.“ (Mixed Mode)

Augen auf: Das subjektive Risikoempfinden weicht beim Menschen oft von der objektiven Bewertung ab. Das gelte auch für Bedrohungen im IoT, sagt Peter Siwon von MicroConsult. Er ist auch Referent beim IoT-Kongress am 15. September in München (www.iot-kongress.de) (Clipdealer)