heise Developer

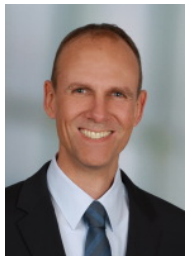
Stefan Strobel: "Das Gesamtsystem muss auf Sicherheit ausgelegt sein"

04.04.2017 08:06 Uhr – Rainald Menge-Sonnentag

In seiner Keynote auf der building IoT 2017 berichtet Sicherheitsexperte Stefan Strobel über den aktuellen Stand der Gefährdung im Internet der Dinge. Vorab teilt er mit heise Developer seine Einschätzung der Situation.

***heise Developer:* Du beschäftigst dich intensiv mit dem Thema Sicherheit und kennst zahlreiche Angriffe auf das IoT. Gib doch bitte mal ein Beispiel für eine akute Gefährdung im Internet der Dinge!**

Stefan Strobel: Ein Fall, den ich auch in meiner Keynote schildern werde, ist ein in Amerika verkauftes Smart Lock (elektronisches Türschloss, d. Red.), bei dem alles über die Cloud gesteuert wird. Das ist eine Tragödie, denn das Endgerät hat keinerlei Wissen über irgendwelche Rechte. Ein Hacker hat auf einer Konferenz einen Man-in-the-Middle-Angriff demonstriert, bei dem er die komplette Kontrolle über den Zugriff übernommen hatte.



Stefan Strobel ist Geschäftsführer der cirosec GmbH. Er verfügt über langjährige Erfahrungen in der Beratung großer Firmen mit hohem Sicherheitsbedarf und im Erstellen von Konzepten und Policies.

***heise Developer:* Unsichere IoT ist also häufig ein grundlegender Planungs- oder Designfehler. Worauf können und müssen Entwickler besonders achten, wenn sie ein neues IoT-Projekt starten?**

Strobel: Ein IoT-Gerät ist mehr als Software. Wenn der Softwareentwickler merkt, dass die Plattform keine Sicherheitsfunktionen mitbringt, muss er sofort um Hilfe rufen und den Projektverantwortlichen sagen: "Liebe Leute, das Gesamtsystem muss auf Sicherheit ausgelegt sein, sonst kann ich es nur noch falsch machen."

Aktuell sind heute viele Schwachstellen darauf zurückzuführen, dass die Hardware nicht auf IoT-Security ausgelegt ist und weder Kryptochips noch einen sicheren Schlüsselspeicher bietet. Einige Unternehmen haben versucht, darum herum zu programmieren, und beispielsweise symmetrische Kryptographie und in der Firmware versteckte Schlüssel verwendet, wo asymmetrische mit PKI-Strukturen nötig wäre. Das Ergebnis sind Systeme, die in der Öffentlichkeit stehen und früher oder später geknackt werden.

***heise Developer:* Gehen wir davon aus, dass das System stimmt. Worauf müssen Entwickler bei der IoT-Programmierung besonders achten, um Schwachstellen zu vermeiden?**

Strobel: Eigentlich sind die Unterschiede zum Programmieren von Server- oder Deskstopsystemen gar nicht so groß. Der Softwareentwickler sollte mit gutem Gewissen von sich sagen können: "Ich weiß, wie sich ein Angreifer ein solches System vornimmt und mit welchen Techniken die Hacker-Community ein Gerät angreift." Hier sind Unternehmen gefordert, ihren Entwicklern Fortbildungsmaßnahmen zu geben, damit sie verstehen, was die Gegenseite tut.

Man könnte nun argumentieren, dass es schließlich Softwareentwicklungsrichtlinien gibt. Die sind üblicherweise aber so generisch, dass ohne gutes Verständnis der Angriffstechniken eine Absicherung nahezu unmöglich ist.

***heise Developer:* Wo liegen typische Fallen für die Entwickler?**

Strobel: In der Praxis werden viele Fehler gemacht, weil die Entwickler zwar die Grundlagen kennen, aber die Prozesse nicht im Detail verstanden haben. Der Klassiker ist, dass man zwar TLS verschlüsselt, aber die Zertifikate nicht vollumfänglich in der gesamten Kette bis zum Wurzelzertifikat prüft. Im Zweifel kann hier beispielsweise Certificate Pinning helfen. Dazu müssen alle Projektverantwortlichen im Vorfeld die Techniken kennen und verstehen.

***heise Developer:* Zahlreiche Firmen setzen auf das Zusammenspiel von IoT und Cloud. Was hältst du aus sicherheitstechnischer Sicht davon?**

Strobel: Gerade in Amerika rufen alle nach der Cloud – ohne Cloud geht da gar nichts mehr. In Deutschland dürfen wir das noch etwas mehr in Frage stellen. Viele Anbieter von IoT-Consumer-Devices nutzen die Cloud, damit die Endanwender möglichst wenig mit der Technik konfrontiert werden. Soweit möglich, sollte man aber die Cloud-Anbindung meiden. Ein IoT-Gerät, das ohne die Verbindung nach außen auskommt, ist für die Sicherheit förderlich.

Auch ist durch die Sammlung der Daten und Zugriffsrechte in der Cloud der Anreiz für Angreifer größer, Daten abzugreifen oder gleich Millionen von Geräten zu übernehmen. Mein persönliches Smart Home ist eine reine Intranetlösung, die keine Verbindung – auch nicht über Portfreigaben – nach außen hat.

***heise Developer:* Ist der Bereich Industrie 4.0 besser abgesichert als Consumer-Produkte?**

Strobel: Schlicht und einfach: Nein. Die Anbieter behaupten zwar, dass alles sicher ist, aber Industrie 4.0 ist viel mehr Marketing und Politik als Realität. Häufig bekommen einfach alte Produktionsanlagen Schnittstellen, um sie zu vernetzen. Damit sind die Schwachstellen, die schon vor zehn Jahren vorhanden waren, auf einmal leichter erreichbar.

***heise Developer:* Lassen sich die IoT-Protokolle wie MQTT ausreichend absichern?**

Strobel: Die etablierten Protokolle sind nicht das Problem, sondern die Leute, die sich proprietäre Protokolle ausdenken oder ein existierendes als IoT-Protkoll missbrauchen.

***heise Developer*: Etwas weiter gedacht: Siehst du eine Chance für Blockchain im Bereich IoT?**

Strobel: Für mich klingt Blockchain zu sehr nach Hype, der für die derzeitigen Anforderungen über das Ziel hinausgeht. Das Kernproblem ist viel trivialer: Oft öffnen banale Fehler Hackern Möglichkeiten, die beispielsweise bei nicht validierten Zertifikaten Man-in-the-Middle-Angriffe fahren können. An anderen Stellen werden Updates nicht kryptographisch ordentlich abgesichert, was das Aufspielen manipulierter Firmware ermöglicht. Oder es kommen symmetrische Schlüssel statt einer Public-Key-Infrastruktur zum Einsatz. Der Schlüssel liegt dabei gerne vermeintlich sicher in der Firmware versteckt, wo er mit Reverse Engineering zu finden ist. 99 Prozent der Risiken lassen sich mit grundlegenden Security-Mechanismen absichern, ohne dass man auf neue Hypes setzen muss.

***heise Developer:* Wer die aktuellen Schlagzeilen verfolgt und deine Beispiele hört, bekommt das Gefühl, dass das Internet der Dinge eine riesige Spielwiese für Hacker bietet. Ist das IoT-Schiff sicherheitstechnisch überhaupt noch zu retten?**

Strobel: Zu spät ist es definitiv noch nicht. Es gibt viele neue Dinge, die auf den Markt kommen, bei denen sich die Entwickler gute Gedanken im Vorfeld gemacht und die gute Sicherheitskonzepte an Bord haben. Und die, die es falsch angegangen sind, können neue Produkte nachschieben und es dabei besser machen. Jetzt ist der Zeitpunkt, aus den Fehlern zu lernen, damit die Geräte in der Zukunft sicherer sind.

Das Interview führte Rainald Menge-Sonnentag, Redakteur von heise Developer. Das Online-Portal gehört zur Heise-Gruppe, genauso wie iX und der dpunkt.verlag, mit denen es die building IoT ausrichtet.
