Sonderdruck aus dem DIGITAL ENGINEERING Magazin 2/2017.
Das Magazin erhalten Sie als Printausgabe unter www.digital-engineering-magazin.de/.

ZUR IT-SICHERHEIT BEI PRODUKTEN IM INTERNET DER DINGE

Wo bleibt das **S** im **IoT**?

IT-Sicherheit hat im Bereich IoT eine neue Dimension erreicht. Weltweit sind immer mehr schlecht oder gar nicht abgesicherte internetfähige Geräte erreichbar – ein offenes Tor für Angreifer. Entwickler von IoT-Produkten sollten sich daher mit existierenden Maßnahmen auseinandersetzen, mit denen sich potenzielle Risiken mindern lassen. VON DR. ERLIJN VAN GENUCHTEN


Bild: Panchenko Vladimir@shutterstock.com

Was Produktentwickler gegen das bei IoT-Geräten häufig als fehlend bemängelte „S" für Security tun können.

Oktober 2016, USA: der Domain-Name-System-Dienstleister Dyn wird Opfer eines ein großflächig angelegten Distributed-Denial-of-Service-Angriffs (DDoS). Dabei werden die angegriffenen Webserver so oft angesprochen, dass sie wegen Überlastung nicht mehr antworten können. Zudem ist das eine Form bei der Angreifer ihre eigene Identität schützen, in dem sie Datenpakete nicht direkt an das Opfer, sondern über fremde Adressen sendet. Die Folge: vor allem an der US-Ostküste sind Teile des Internets zeitweise nicht erreichbar.

In diesem Fall hat der Angreifer schlecht abgesicherte Geräte des sogenannten „Internet of Things (IoT)" ausgenutzt, um den Angriff durchzuführen. Dieser Vorfall führte vor Augen, dass IoT-Geräte nicht nur Arbeitsabläufe und den Alltag erleichtern können, sondern auch von digitalen Angreifern missbraucht werden können. Entsprechend wichtig ist es, IoT-Geräte in Zukunft besser abzusichern. Aber wo lauern die Gefahren bezüglich der Sicherheit von IoT-Geräten? Und was können Hersteller tun, um diese besser abzusichern?

Kleine Computer – große Gefahr

Eine immer größere Anzahl von Gerätegattungen, die wir vor einigen Jahren noch nicht im Bereich IT angesiedelte hätten, sind mittlerweile zu kleinen Computern geworden und mit dem Internet verbunden. Diese Technologien bieten den Nutzern viele neue Möglichkeiten und Vorteile. Damit gehen jedoch auch neue digitale Angriffsszenarien einher. Mögliche Gefahren entstehen auf verschiedenen Ebenen (Suo & Wan, 2012).

Die Gefahren auf der ersten Ebene – auf der „Wahrnehmungs- oder Hardwareebene" – beziehen sich auf die Interaktion des IoT-Geräts mit seiner Umgebung. Diese Interaktion geschieht meist über Sensoren. Laut Son et al. (2015) ist es möglich, bestimmte Signalarten so zu manipulieren, dass sie den Sensor stören und zu Fehlfunktionen führen. Außerdem beziehen sich Gefahren dieser Ebene auf einen potenziellen Zugriff auf die Hardware des IoT-Geräts, wobei sensible Daten, etwa Passwörter, entwendet werden könnten.

Die Gefahren auf der zweiten Ebene – auf der Netzwerkebene – beziehen sich auf den Informationsaustausch zwischen den Komponenten. Es besteht die Gefahr, dass ein Angreifer die Software zu ungewollten Aktionen bringt. Sofern softwareseitig keine Überprüfung stattfindet, ob es sich bei eingehenden Anfragen um legitimen Datenverkehr handelt, steht das IoT-Gerät dann unter der Kontrolle des Angreifers.

Die Gefahren auf der dritten Ebene – auf der „Back-End-Ebene" – beziehen sich auf die Back-End- oder Cloud-Lösung, auf der verschiedene Dienste bereitgestellt und Daten gespeichert werden, die für das Funktionieren eines IoT-Produkts notwendig sind. Diese können Schwachstellen aufweisen oder auf veralteter Software basieren. Sind Sicherheitslücken vorhanden, besteht die Gefahr einer möglichen Rechteausweitung des Angreifers. Als Folge ließe sich ein entsprechendes IoT-Gerät für bösartige Aktionen missbrauchen.

Die Gefahren auf der vierten Ebene schließlich – auf der Applikationsebene – beziehen sich auf Schwachstellen in der Bedienungsoberfläche, etwa in einer Webapplikation oder einer mobilen App. So ließe sich etwa bei einer für SQL-Injection-Angriffe verwundbaren Applikation die Passwortprüfung umgehen und die Datenbank auslesen, sodass unautorisierter Zugriff auf die Applikation möglich ist.

Die Verantwortung der Entwickler

Um diesen Gefahren vorbeugen zu können, besteht Handlungsbedarf. Hersteller

und Produktentwickler von IoT-Devices haben derzeit häufig noch nicht im Blick, wie wichtig – neben der eigentlichen Funktionalität – auch die Absicherung ihrer Produkte ist. In der Folge finden sich bei vielen Produkten entweder gar keine oder nur begrenzte Sicherheitsmechanismen. Beides ist unzureichend, da ein Angreifer nur eine einzige Lücke benötigt, um ein verwundbares System zu kompromittieren (Sowa, Duscha & Schreiber, 2015, S. 151ff.). Es ist deshalb unentbehrlich, ein allgemeines „digitales Gefahrenbewusstsein" zu entwickeln. Ist diese Voraussetzung erfüllt, können im nächsten Schritt konkrete Maßnahmen umgesetzt werden.

Sicherheit konzipieren

IT-Sicherheit sollte schon bei der Planung und Entwicklung von IoT-Geräten berücksichtigt werden. Passende Architekturen und geeignete sicherheitsbezogene Entwürfe können so bereits frühzeitig in die Entwicklung einfließen. So lassen sich auch eventuelle Folgekosten minimieren.

Ebenso lassen sich Angriffsflächen reduzieren, indem bereits frühzeitig im Entwicklungsprozess entschieden wird, welche Funktionen, die hard- und softwareseitig zur Verfügung gestellt werden sollen, tatsächlich auch für den Betrieb des Geräts nötig sind. Viele Hersteller gehen bislang so vor, dass bestimmte Funktionen, die etwa erst in einer Folgeversion zur Verfügung stehen sollen oder die Teil einer genutzten Standardsoftware sind, für den Nutzer nur auszublenden. In solchen Fällen ist ein Angreifer möglicherweise dazu in der Lage, dieses „Unsichtbare" sichtbar zu machen und sich neue Einstiegspunkte zu erarbeiten. Besser wäre es, nicht benötigte oder für Nutzer nicht zugängliche Funktionen gar nicht erst zu implementieren. Denn was nicht vorhanden ist, lässt sich auch nicht ausnutzen und angreifen.

Die Funktionen jedoch, die in jedem Fall für den Betrieb des IoT-Geräts benötigt werden, sollten bereits in der Konzeptionsphase in Hinblick auf ihre Sicherheit der Kommunikation zwischen den beteiligten Schnittstellen analysiert werden. Heute kann nicht mehr ohne weiteres davon ausgegangen werden, dass Signale oder Anfragen, die das System erreichen auch wirklich vom Sensor, vom Back-End oder vom Nutzer stammen. Denn es ist möglich, Anfragen und Signale zu manipulieren. Es sollten deshalb auf Ebene der Applikation Maßnahmen ergriffen werden, die dafür sorgen, dass möglicher bösartiger Input zurückgewiesen wird.

Darüber hinaus sollte auch die Sicherheit der Sensoren beachtet werden. Allgemein wirksame Schutzmaßnahmen gibt es hier bisher noch nicht. Diese müssten deshalb – je nach Sensorart und Angriffsmethode – spezifisch angepasst werden (Sokolov & Daniel 2017). Ein möglicher Sensor-unspezifischer Ansatz wäre der Einsatz von „künstlicher Intelligenz", die unglaubwürdige Sensordaten aufspürt (Son et al., 2015).

Vor der Markteinführung

Auch wenn die oben dargestellten Maßnahmen umgesetzt werden, ist es wichtig, das Produkt vor der Markteinführung einem Sicherheitstest durch einen unabhängigen Dienstleister zu unterziehen (vgl. Orcutt, 2016). Ziel eines Penetrationstests ist, möglicherweise vorhandene Sicherheitslücken aufzudecken und Wege zur Behebung aufzuzeigen. In den vergangenen Jahren wurde von führenden IT-Sicherheitsorganisationen spezifiziert, wie Penetrationstests und deren Dokumentation zu gestalten sind.

Was IoT-Geräte angeht, beziehen sich diese Spezifikationen auf die Analyse der Webapplikation und/oder der mobilen App inklusive Datenverkehr und Webservice, des Back-Ends und der Hardware.

Nach der Markteinführung

Ist es nicht möglich, einen IoT-Penetrationstest vor der Markteinführung durchzuführen, sollte dieser nach Markteinführung nachgeholt werden. Denn auch bei einem IoT-Produkt, das sich bereits auf dem Markt befindet, sollte die Sicherheit nicht aus den Augen verloren werden. Trotz einer durchdachten Konzeption und der Behebung der durch Penetrationstests während der Entwicklung identifizierten Schwachstellen, gibt es letztlich keine hundertprozentige Garantie, dass das Endprodukt frei von Sicherheitsproblemen ist.

Neue Sicherheitslücken werden regelmäßig aufgedeckt und veröffentlicht. Will der Entwickler jedoch das Vertrauen der Nutzer gewinnen, so spielt es eine Rolle, ob und wenn ja wie viele Lücken nach Markteinführung identifiziert werden. Nach wichtiger ist, auf welche Weise der Hersteller mit der Behebung von Schwachstellen umgeht. Werden öffentlich bekannte Lücken zeitnah behoben und Sicherheitsupdates zur Verfügung gestellt, ist es deutlich weniger wahrscheinlich, dass Angreifer eine Schwachstelle auch erfolgreich ausnutzen können. JBI |

Dr. Erlijn van Genuchten ist Security-Beraterin bei Syss.

Literaturverzeichnis

Orcutt, Mike (2016). Lebensgefährliches Internet der Dinge? Technology Review, 07.12.2016, https://www.heise.de/tr/artikel/Lebensgefaehrliches-Internet-der-Dinge-3562468.html.

Sokolov, Daniel A. J. (2017). Sensoren sind Angriffsflächen im Internet of Things. heise online, 31.01.2017, https://www.heise.de/newsticker/meldung/Sensoren-sind-Angriffsflaeche-im-Internet-of-Things-3611114.html

Son, Y., Shin, H., Kim, D., Park, Y., Noh, J., Choi, K., Choi, J., & Kim, Y. (2015). Rocking drones with intentional sound noise on gyroscopic sensors. In 24th USENIX Security Symposium, pp. 881-896.

Sowa, A., Duscha, P., Schreiber, S. (2015). IT-Revision, IT-Audit und IT-Compliance. Wiesbaden, Springer.

Suo, H. & Wan, J. (2012). Security in the Internet of Things: A Review. International Conference on Computer Science and Electronics Engineering, 648-651.