Security-Trends von der IT-Defense 2020

Was in der IoT-Security passieren muss

18.02.2020 | Autor/ Redakteur: Oliver Schonschek / Sebastian Human

Die Security muss sich ändern, wenn das Internet der Dinge sicherer werden soll. Dabei spielt der Mensch, aber auch die künstliche Intelligenz eine zentrale Rolle, wie die IT-Defense 2020 in Bonn zeigte. Die Security im IoT muss neu gedacht werden.

Die Security befindet sich im Wandel: KI wird zunehmend wichtiger, aber der menschliche Verstand lässt sich nicht so einfach ersetzen.
(Bild: gemeinfrei / Pexels)

Bereits zum achtzehnten Mal trafen sich Sicherheitsexperten, Hacker und Fachleute aus Disziplinen von Neuro- bis Rechtswissenschaften zur Sicherheitskonferenz IT-Defense. 2020 fand diese IT-Sicherheitstagung in Bonn statt. Es ging zum Beispiel um Security Awareness, Windows-Sicherheit, rechtliche und vertragliche Updatepflichten und die Möglichkeiten von menschlicher und künstlicher Intelligenz.

Auch wenn das Internet der Dinge auf den ersten Blick kein explizites Vortragsthema war, ging es fortlaufend um IoT. Tatsächlich betreffen nämlich alle diskutierten Veränderungen im Security-Bereich auch das IoT - der notwendige Security-Wandel muss auch das Internet of Things erfassen, wenn dieses sicherer werden soll.

Was also kann man aus den auf der IT-Defense 2020 vorgestellten Security-Entwicklungen und -Prognosen für die Sicherheit im IoT ableiten? Eine ganze Menge.

Der menschliche Faktor der IoT-Sicherheit

Unternehmen müssen eine IT-Sicherheitskultur aufbauen, die schützt, erkennt und handelt, so Lance Spitzner, Leiter des Security-Awareness-Programms bei SANS. Viele Security-Awareness-Programme scheitern, weil es an Motivation und Fähigkeiten bei den Nutzern mangelt. Wer zum Beispiel die Awareness für IoT-Sicherheit steigern will, sollte nicht nur mit Security-Experten über den richtigen Weg sprechen, sondern auch mit Marketing-Fachleuten.

Damit die notwendigen Security-Maßnahmen von den Anwendern akzeptiert und angenommen werden, müssen sie noch stärker gesagt bekommen, warum IoT-Sicherheit so wichtig ist. Aber das reicht nicht. Die Nutzer müssen auch wissen, wie entsprechende Security-Maßnahmen funktionieren. Dabei muss eine andere Sicht und Sprache als bisher gewählt werden, nicht die Perspektive der Security führt zum Ziel, sondern die des einfachen Anwenders. Security muss leichter verständlich werden und einfacher umzusetzen sein.

IoT-Sicherheit muss also in Zukunft anders kommuniziert werden, auf der Anwenderebene, nicht auf der Ebene der Security-Experten. Nur wenn die Menschen für die IoT-Sicherheit gewonnen werden, kann das Internet der Dinge wirklich sicherer werden.

Ein Gespräch mit dem Sicherheitsexperten und ethischen Hacker Jayson E. Street offenbarte noch einen weiteren menschlichen Einflussfaktor auf IoT-Security: Im Internet of Things werden Cyber-Bedrohungen zu physischen Bedrohungen - Menschenleben können in Gefahr geraten, wenn IoT-Geräte erfolgreich angegriffen werden. Ein sehr wichtiger, weiterer Grund, warum der Faktor Mensch vermehrt in Security-Maßnahmen miteinbezogen werden muss, nicht nur die vernetzten Dinge selbst.

Vergleichbarkeit von Anbietern und Lösungen

Ein anderer Vortrag der IT-Defense befasste sich mit der Vergleichbarkeit der Sicherheit verschiedener Cloud-Anbieter. Hier zeigte sich, dass es nicht immer einfach ist, Security-Funktionen von Microsoft Azure und AWS zu vergleichen.

Doch im IoT gilt das sogar noch mehr, wie der Security-Experte Jayson E. Street bestätigte. Hier gibt es keine so dominanten Player wie im Cloud Computing, sondern eine Vielzahl von Anbietern, die einen Vergleich noch deutlich schwieriger machen. Auch eine Zertifizierung wird auf dem Gebiet der IoT-Sicherheit nicht so viel aussagen und helfen können wie im Cloud Computing, dazu ist das IoT zu komplex.

Digitale Assistenten als Hintertür

Die Sicherheitsforscher Amichai Shulman und Yuval Ron beleuchteten das Problem, dass Sprachassistenten immer mehr zu einem wesentlichen Bestandteil vieler Computerplattformen werden, nicht nur bei Smartphones. Dabei können sie häufig selbst bei gesperrtem Bildschirm genutzt werden. Die Bereitstellung der Sprachassistenzfunktionen bei gesperrtem Bildschirm kann jedoch die Sicherheit solcher Geräte dramatisch beeinflussen.

Es gibt Sicherheitslücken, die durch die Aktivierung der Sprachassistenten (wie Cortana, Siri, Alexa und Bixby) bei gesperrtem Bildschirm in Computern und Smartphones entstehen. Die möglichen Risiken durch den Einsatz von Sprachassistenten sollte man aber auch im IoT bedenken. Wenn die Spracheingabe Funktionen der IoT-Geräte aktivieren kann, könnte dies auch vorhandene Sicherheitsmaßnahmen umgehen.

Sicherheitslücken in Standards

Ob bei der Verschlüsselung von PDF-Dokumenten oder bei der Nutzung von LTE oder 5G: Wenn die zugrundeliegenden Spezifikationen Maßnahmen wie Verschlüsselung und Integritätsschutz nicht vorschreiben oder als Option behandeln, muss man davon ausgehen, dass die Implementierung und Nutzung solcher Standards zu Sicherheitsproblemen führt, wie zwei Vorträge darstellten.

Die Beispiele der Spezifikationen zu PDF, LTE und 5G sollten dazu anregen, auch bei IoT-Spezifikationen mehr Sicherheitsfunktionen einzufordern, bei bereits bestehenden Spezifikationen aber sollte man damit rechnen, dass Sicherheitslücken bereits in der Spezifikation existieren und nicht etwa nur durch Fehler in der Implementierung. Statt *Security by Design* gibt es sonst *Insecurity by Design*.

Risiko Vorinstallierte Apps

Dr. Ryan Johnson und Dr. Angelos Stavrou von Kryptowire wiesen am Beispiel Android auf die möglichen Gefahren durch vorinstallierte Apps hin. Wie die beiden Sicherheitsexperten zeigten, haben zahlreiche Smartphone-Modelle ab Werk gefährliche Apps installiert, die der Nutzer meist weder sehen noch entfernen kann. Selbst wenn diese vorinstallierten Apps nicht immer selbst bösartig sind, haben sie doch hohe Privilegien, die andere Apps ausnutzen könnten. Klassische Anti-Malware-Lösungen erkennen diese vorinstallierten Gefahren nicht, da sie als Werkszustand eingestuft werden.

Solche Risiken sind natürlich auch im IoT vorhanden, alleine schon dadurch, dass Android-Betriebssysteme die vorherrschenden Systeme im Internet der Dinge sind. Deshalb sind neue Security-Prüfungen notwendig, die auch vorinstallierte Apps hinterfragen.

Die Angst vor der KI

Der Informatiker und Hirnforscher Dr. Boris Nicolai Konrad zeigte auf, welche Rolle künstliche Intelligenz bereits in unserem Alltag spielt. So gibt es schon jetzt Computerprogramme, die intelligenter sind als wir Menschen, zumindest in bestimmten Bereichen, so Konrad: „Aber auch wir Menschen können intelligenter werden, wenn wir von Maschinen lernen oder die Erkenntnisse der Hirnforschung nutzen. Ob wir dazu bereit sind, wird entscheiden, ob wir auch zukünftig die Computer kontrollieren oder umgekehrt.“

Doch müssen wir vor KI Angst haben? Nein, zumal Angst immer ein schlechter Berater ist. Dr. Konrad forderte im Gespräch mehr Transparenz zu den Fähigkeiten einer KI. Ein großes Risiko sieht der Hirnforscher darin, dass KI-Technologien unwissend eingesetzt werden. Nicht die Übermacht einer KI ist das Risiko, sondern die Unwissenheit über selbst einfache, schwache KI-Systeme. Es versteht sich, dass dies auch für die KI-Nutzung im IoT gilt.

Whitelisting nicht nur bei Windows

Sami Laiho ist Experte für das Windows-Betriebssystem und für Windows-Sicherheit. Er zeigte in seinem Vortrag, wie viel einfache Maßnahmen, wie zum Beispiel White Listing, für die Sicherheit tun können. Anstatt zahllose Applikationen und Funktionen zu verbieten, macht es deutlich mehr Sinn, die wirklich genutzten Applikationen freizugeben. Das gilt für Windows-Systeme genauso wie für IoT-Geräte. Die meisten

Malware-Attacken könnten dadurch vermieden werden. Anstatt also Malware und schädliche Funktionen im Internet of Things erkennen zu wollen, sollte man stattdessen definieren, was denn genau die IoT-Geräte können sollen, welche Apps also erlaubt sein sollen.

Updatepflichten nach Recht und Gesetz

Die Sicherheit von Informationstechnologie ist eine der großen Herausforderungen der Digitalwirtschaft. Es kommen immer neue Richtlinien und Gesetze hinzu. So hat die Europäische Union mehrere Regelwerke zur Updatepflicht und zur Verbesserung der Datensicherheit verabschiedet, deren Konturen alles andere als klar sind. Hinzu kommen zahlreiche Anforderungen durch das neue Informationssicherheitsgesetz, so Prof. Dr. Thomas Hoeren von der Universität Münster.

Gerade in IT-Verträgen müssen Unternehmen deutlich genauer hinschauen, was zu den Hauptleistungen, Nebenleistungen, zur Gewährleistung, der Kündigung und zur Art des Vertrages gesagt wird. Im komplexen IoT-Feld wird dies zweifellos eine besondere Herausforderung werden, wenn mehr und mehr IoT-Services beauftragt werden.

Es zeigt sich: Wie Security bei IoT-Konferenzen einen festen Stellenwert hat, spielt der Technologiekomplex auch bei allen relevanten Security-Fragen eine Rolle. Umgekehrt sollten alle Security-Trends und -Entwicklungen auch auf das IoT bezogen und dafür geprüft werden. Security ist eine Querschnittsdiziplin in der Digitalisierung, und das Internet of Things ein Herzstück dieser Digitalisierung.