„Security by Design“ noch nicht Standard

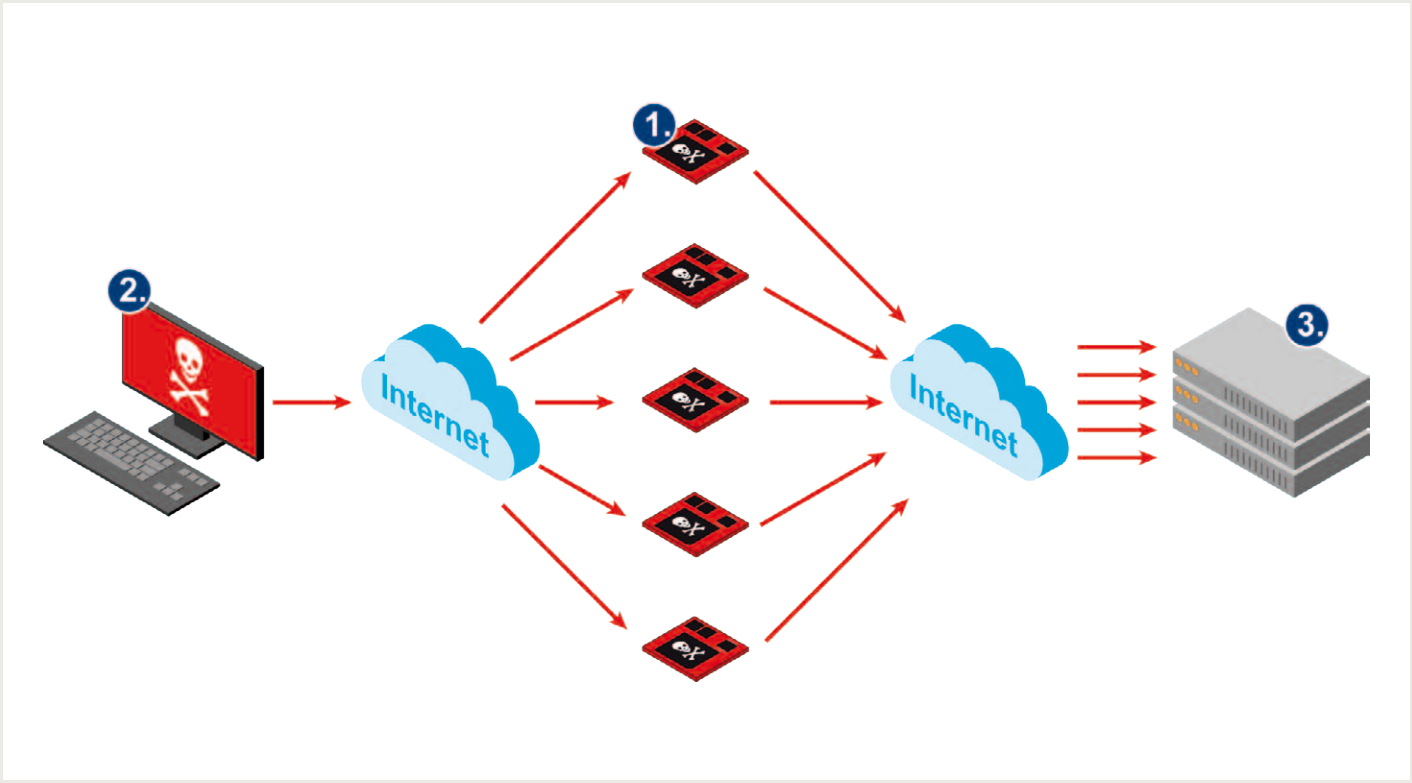

Bild 1: Die Integration eines Mikrorechnersystems in ein Botnet erfolgt in drei Schritten. 1. Einzelne eingebettete Systeme werden von den Angreifern mit einem Schadcode ausgestattet, um sie von einem zentralen Server aus fernzusteuern. 2. Aufsetzen eines Command-and-Control- (C&C-) Servers irgendwo im Internet. Von diesem Rechner aus werden die Bots als Orchester ferngesteuert. 3. Das eigentliche Angriffsziel: Ein beliebiger Server im Internet, der dann durch Überlastung für andere Benutzer nicht mehr erreichbar ist

Kurz gefasst:

Der BSI-Lagebericht zur IT-Sicherheit in Deutschland weist auf die Gefahren und Schwachstellen im Internet der Dinge hin. Diese Problematik wurde bisher unterschätzt. Wie Sicherheitslücken erkannt und geschlossen werden können, beschreibt der folgende Bericht.

Der Nachweis, dass sich mit dem Internet verbundene Rechnersysteme unterschiedlicher Leistungsklassen sehr einfach angreifen lassen, wurde inzwischen nicht nur in unzähligen Live-Hacks erbracht. So musste im August vergangenen Jahres der Medizingerätehersteller Abbott wegen einer Warnung der US-Behörde für Lebens- und Arzneimittel (FDA) weltweit rund 500.000 Herzschrittmacher zurückrufen. In Deutschland waren 13.000 Patienten davon betroffen. Grund für diese Rückrufaktion war eine Sicherheitslücke in der Systemsoftware, die es Hackern ermöglichte, per Funk die Schrittmacher zu manipulieren und so bspw. die Taktrate zu ändern oder die Batterie zu entladen. Ein Szenario was vor 10 oder 15 Jahren noch wie Science-Fiction klang, ist also inzwischen Realität.

Auf die dafür verantwortlichen Schwachstellen geht auch der aktuelle BSI-Lagebericht zur IT-Sicherheit in Deutschland ein. Besonders auffällig: Immer mehr eingebettete Systeme werden ohne Wissen der Nutzer in Bot-Netzwerke eingebunden und für größere Cyberattacken auf Internetserver genutzt.

Die Problematik

Im November haben der geschäftsführende Bundesinnenminister Thomas de Maizière

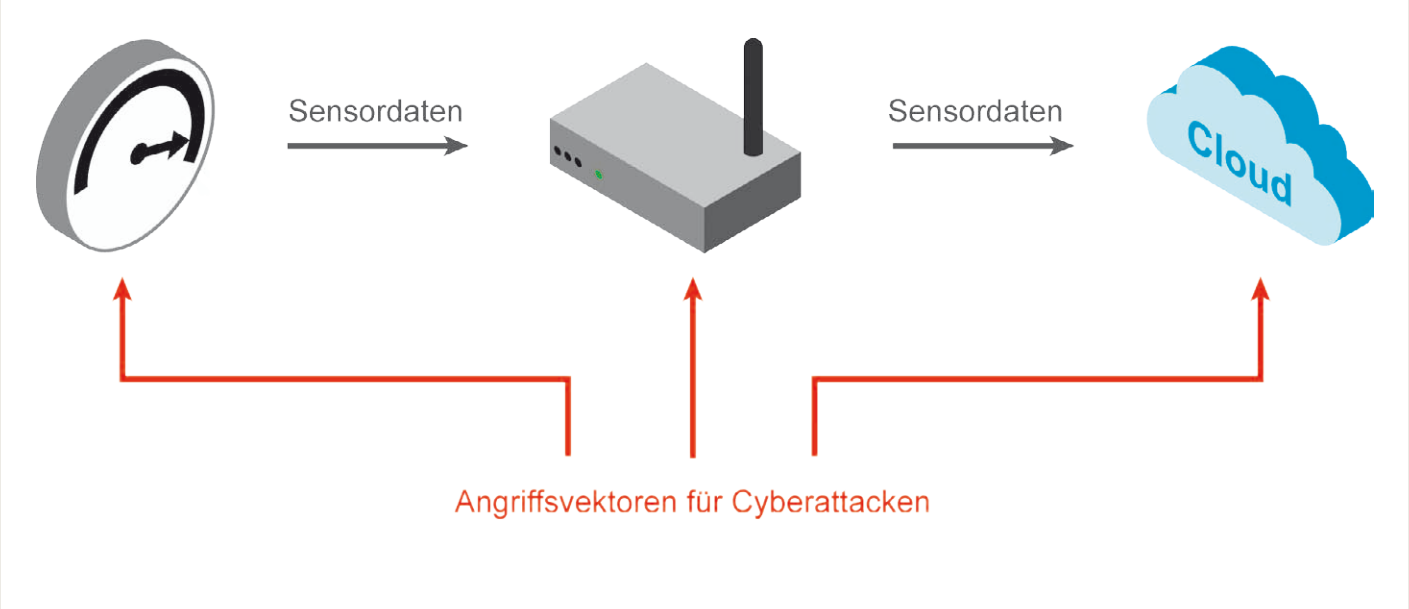

Bild 2: Besonders die unzähligen „Sensor-to-Cloud"-IoT-Anwendungen dürften in Zukunft ein attraktives Ziel für Cyberangreifer bilden

und der Leiter des Bundesamtes für Sicherheit in der Informationstechnik (BSI), Arne Schönbohm in Berlin den BSI-Lagebericht zur IT-Sicherheit in Deutschland vorgestellt. Neben den klassischen Themen aus den Vorjahren (Gefährdungslagen, Maßnahmen des BSI usw.) wurde diesmal explizit auf die Gefahren und Schwachstellen im Internet der Dinge hingewiesen. Die Situation hier ist besorgniserregend. Unzählige vernetzte Mikrorechnersysteme haben nach wie vor werksseitig eingestellte Standardpasswörter, die man teilweise sogar in den per Internet zugänglichen Bedienungsanleitungen findet. Möglichkeiten zur Software-Aktualisierung, um Sicherheitslücken zu beseitigen, werden erst gar nicht angeboten. Hinzu kommt, dass die meisten Nutzer von IoT-Baugruppen es noch nicht einmal merken, wenn z. B. ein Smart-Home-Thermostat oder die Smartphone-App eines Wearables von Cyberkriminellen als ferngesteuerte Angriffswaffe benutzt wird.

Immer mehr IoT-Bot-Netze

Größere Cyberangriffe auf einzelne IoT-Systeme wurden in den vergangenen Monaten zwar nicht beobachtet. Obwohl die Anzahl der IoT-Funksensoren, -Funkaktoren und -Cloud-Lösungen durch Smart-Home-, Smart-Factory und natürlich auch Smart-Health-Anwendungen mit bemerkenswertem Tempo zunimmt und sogar neue IoT-Funkstandards zum Einsatz kommen, sind bis zum gegenwärtigen Zeitpunkt keine gezielten DDoS-Angriffe oder andere Ransomware-Attacken auf die Komponenten und Infrastrukturen identifizierbar. Smart-Home-IoT-Lösungen waren zwar durch den Angriff auf Telekom-Router im Herbst 2016 betroffen, aber wohl nicht das primäre Angriffsziel. Es ist aber vermutlich nur eine Frage der Zeit, bis staatliche Cyberkrieger oder Cyberkriminelle entsprechende „Geschäftsmodelle" gefunden haben, um auch im IoT-Segment aktiv zu werden.

Völlig anders sieht es hingegen mit der missbräuchlichen Nutzung von IoT-Komponenten innerhalb von Botnet-Angriffen aus. Bemerkenswert ist hier vor allem die Geschwindigkeit, mit der die Anzahl der als Bot genutzter IoT-Baugruppen solcher Angriffsnetzwerke in den vergangenen Jahren angewachsen ist. 2014 hatte das damals größte beobachtete IoT-Botnet gerade einmal 75.000 befallene Verbundsysteme. Im August 2016 war mit *Mirai* schon ein fast 700 % größeres Botnet aktiv: Mehr als 500.000 infizierte Mikrorechnersysteme in digitalen Videorecordern, Überwachungskameras, Routern und anderen IoT-Devices bildeten erstmals einen fernsteuerbaren Netzwerkverbund, mit dem der Betrieb des Internets nachhaltig gestört wurde. Alle von der Mirai-Schadsoftware betroffenen Bot-Systeme hatten ein eingebettetes Linux-Betriebssystem ohne besondere Sicherheitsvorkehrungen inklusive fest kodierter Passwörter (hard-coded Passwords) als Schwachstellen, die von den Mirai-Betreibern zur Installation der Fernsteuersoftware ausgenutzt wurden.

Bei einer für 2020 prognostizierten Anzahl von über 20 Milliarden direkt oder indirekt mit dem Internet verbundenen IoT-Komponenten sollten wir das IoT-Botnet-Wachstum sehr ernst nehmen. Die meisten dieser ca. 20 Milliarden IoT-Baugruppen und die dafür genutzten Mikrorechnersysteme werden so gut wie keine zeitgemäßen Schutzmechanismen oder Update-Möglichkeiten haben, um immer professionellere Kriminelle davon abzuhalten, sie zum Angriff auf andere Infrastrukturkomponenten oder Services zu missbrauchen. Hinzu kommen noch unzählige Smartphones und die darauf laufenden Apps – zum Beispiel für Wearables wie Fitnessarmbänder – mit sehr geringem Sicherheitsniveau, für die praktisch keine Sicherheits-Updates zur Verfügung stehen. Es ist daher davon auszugehen, dass wir bis 2020 noch den ersten Botnet-Angriff durch ein ferngesteuertes Verbundnetz mit zig-Millionen einzelnen eingebetteten Rechnersystemen und Smartphones erleben werden. Die Auswirkungen einer solchen Attacke könnten durch die fortschreitende Digitalisierung sehr dramatisch ausfallen und Folgeschäden verursachen, die sich im Moment noch nicht einmal ansatzweise abschätzen lassen.

Veränderungen erkennen, Updates ermöglichen

Es ist aus technischer Sicht eigentlich unverständlich, warum beispielsweise die Linux-basierte Firmware eines Telekom-Routers es nicht bemerkt, dass über den Internetzugang eine Verände-

rung vorgenommen wurde, um eine Botnet-Integration zu ermöglichen. Es ist sogar sehr wahrscheinlich, dass auch unzählige andere Systeme nahezu identische Schwachstellen aufweisen, weil „Security by Design“ noch kein Bestandteil der Entwickler-Lastenhefte war.

Im Telekom-Angriffsszenario hätte bereits eine simple Software-Change-Meldung an einen zentralen Maintenance-Server im Internet ausgereicht, um die Manipulation zu identifizieren und die Router-Betreiber zu benachrichtigen. Dafür muss die Firmware des Mikrorechners im Router lediglich erkennen, dass eine „unbekannte“ Software installiert oder gestartet wurde. Für ein Embedded Linux wäre eine solch einfache Root-of-Trust-Erkennung mit relativ wenig zusätzlichen Codezeilen realisierbar. Des Weiteren sollten alle Systeme, die eine Netzwerkschnittstelle haben, unbedingt auch eine zeitgemäße Vor-Ort-Software-Update-Möglichkeit aufweisen. Besonders einfach ist ein Update wenn – wie bei einem Router – eine permanente Internetverbindung besteht. In diesem Fall könnten die eingebetteten Mikrorechner von Zeit zu Zeit auf dem Maintenance-Server nach Updates schauen oder sich per Subscribe-Nachricht über ein anstehendes Update benachrichtigen lassen.

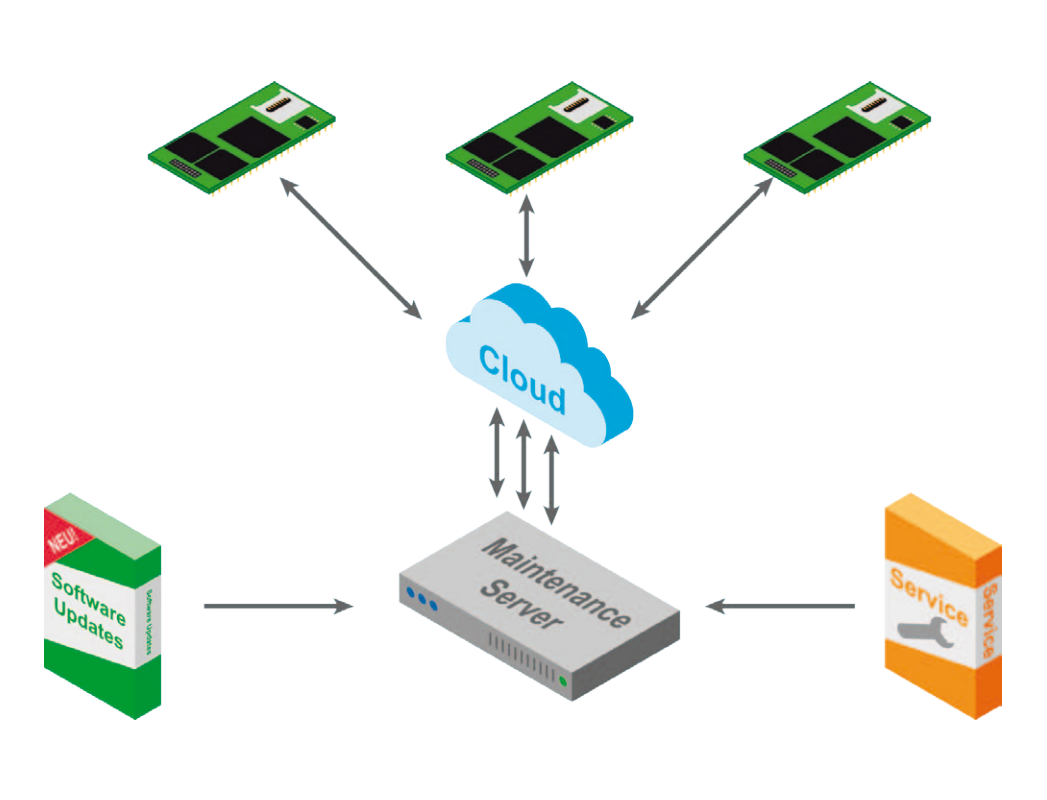

Bild 3: In professionellen Lösungen haben die eingebetteten Systeme eine Verbindung zu einem zentralen Maintenance-Server, der in einer besonders gesicherten Umgebung betrieben wird. Dort schauen sie von Zeit zu Zeit nach, ob Updates vorliegen, die installiert werden müssen

Systematisches Vorgehen erforderlich

Grundsätzlich sollten alle IoT-Baugruppen und Systeme mit einem Embedded-Betriebssystem sowie die dazugehörenden Apps mit Sicherheitserweiterungen ausgestattet sein, die dem jeweiligen Stand der Technik entsprechen. Da dieser Stand der Technik sich laufend verändert, müssen Update-Möglichkeiten vorgesehen werden. Für Mikrorechner ohne Betriebssystem sollte zumindest eine statische Codeanalyse in der Entwicklung erfolgen, um die Anwendungssicherheit zu gewährleisten. Darüber hinaus ist ein professionelles System-Security-Assessment empfehlenswert. Was nutzt ansonsten die beste Verschlüsselung für die Übertragungswege, wenn der Diebstahl einer digitalen Identität noch nicht einmal bemerkt wird oder ein „geheimer“ Hersteller-Servicezugang mit werksseitig eingestelltem Standardpasswort existiert.

Massenprodukte besonders gefährdet

Die erkannten Angriffe auf Mikrorechnersysteme in Smart-Home-Anwendungen, Telekom-Routern, Überwachungskameras und anderen IoT-Devices machen deutlich, dass grundsätzlich alle vernetzten Baugruppen mit direktem oder indirektem Internetzugang ein geeignetes Angriffsziel darstellen. Dazu gehören inzwischen auch Wearables. Hier ist es beispielsweise die App, die sich als Roboter in einem Botnet missbrauchen lässt. Da Wearables Massenprodukte sind, die in großer Stückzahl gefertigt und vermarktet werden, dürfte es für Cyberkriminelle besonders interessant sein, eine infizierte App mit gut getarnter Schadsoftware für ein sehr weit verbreitetes Wearable z. B. in den Google Play Store zu stellen. Aber auch hier schreitet die Entwicklung voran. Durch neue Weitbereichsfunktechnologien, wie beispielsweise NB-IoT und LTE-Cat M1, haben auch kleinste Wearables und Pet Tracker (siehe Samsung Connect Tag) in Zukunft einen direkten Internetzugang. Dadurch ist dann nicht nur die App ein mögliches Angriffsziel, sondern auch die Sensorkomponente selbst.

Fazit

Hinsichtlich der Security ist nahezu die gesamte IoT-Welt sehr weit von den recht ausgefeilten Schutzmaßnahmen entfernt, die sich in der Unternehmens-IT etabliert haben. Die Ursachen dafür sind vielfältig. Teilweise fehlt es an dem erforderlichen Fachwissen und systembezogenen Denken. Vielfach geht man aber wohl auch davon aus, das IT-Security ein Anwenderthema sei, zumal die rechtliche Seite sich hier bisher auch noch nicht eindeutig positioniert hat. Sinnvoll wäre auf der Herstellerseite – analog zur Entwicklung der Funktionen und Gerätesicherheit – aber auf jeden Fall der Einsatz professioneller Methoden und Werkzeuge, um die IT-Security eines IoT-Produktes zu gewährleisten.

Autor:
Klaus-Dieter Walter
CEO bei der
SSV Software Systems GmbH
www.ssv-embedded.de