IoT-Baugruppen praktisch ungeschützt

Die potenziellen Gefahren für außerhalb der IT genutzte Mikrorechnersysteme nehmen im Moment rasant zu. Aber auch schon vor dem offiziellen Bekanntwerden von Meltdown & Spectre wurde über den neuesten BSI-Lagebericht deutlich, dass inzwischen auch Mikrorechner in industriellen Steuerungsanlagen und Embedded Systeme durch Cyberattacken bedroht werden. Besonders auffällig: Immer mehr eingebettete Systeme sind bereits ohne Wissen der Nutzer in Bot-Netzwerke eingebunden und für größere Cyberattacken auf Internetservern benutzt worden.

Kurz gefasst

Die immer stärker werdende Nutzung des IoT und die fortschreitende Digitalisierung bieten leider auch zunehmend Schwachstellen für Cyberattacken. In diesem Artikel wird die Problematik erläutert und es werden Lösungsmöglichkeiten aufgezeigt.

Die Problematik

Als im November vergangenen Jahres der geschäftsführende Bundesinnenminister Thomas de Maizière und der Leiter des Bundesamtes für Sicherheit in der Informationstechnik (BSI), Arne Schönbohm in Berlin den BSI-Lagebericht zur IT-Sicherheit in Deutschland vorstellten, waren Meltdown und Spectre nur Insidern bekannt und Intel-Chef Krzanich noch im Besitz seines gesamten Aktienoptionspakets. Insofern konzentriert sich der BSI-Bericht nahezu vollständig auf die klassischen Themen aus den Vorjahren (Gefährdungslagen, Maßnahmen des BSI usw.). Dabei kommen teilweise ältere und hinreichend bekannte Vorfälle zu Sprache. Aber es wird in dem Dokument auch explizit auf die Gefahren und Schwachstellen hingewiesen, die sich durch das Internet der Dinge, die fortschreitende Digitalisierung und durch Angriffe auf industrielle Steuerungsanlagen ergeben.

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.

IoT-Bot-Netze verbreiten sich

Spektakuläre Cyberangriffe auf einzelne IoT-Lösungen wurden in den vergangenen Monaten nicht beobachtet. Obwohl die Anzahl der IoT-Funksensoren, -Funkaktoren und -Cloud-Lösungen durch Smart-Home- und Smart-Factory-Lösungen 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 genutzten 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

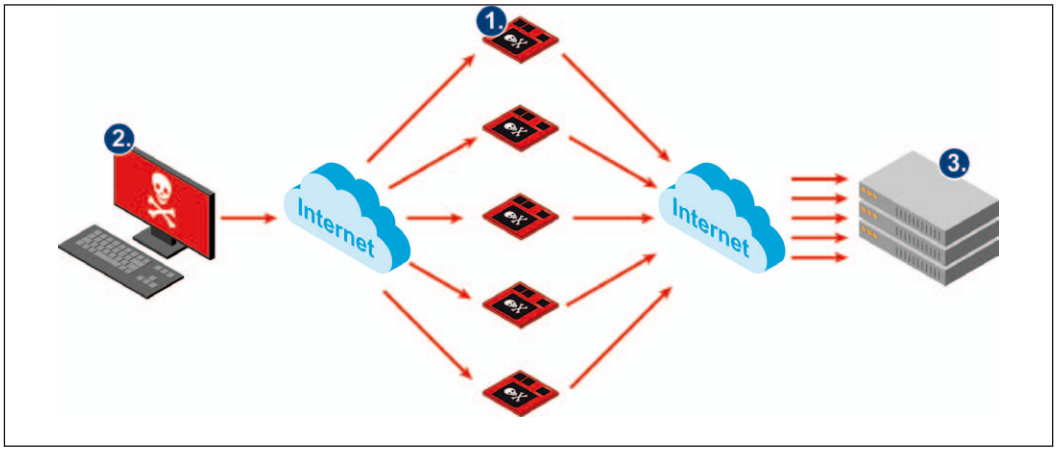

Bild 1: Die Integration eines Mikrorechnersystems in ein Botnet erfolgt in drei Schritten. 1. Einzelne eingebettete Systeme werden von den Angreifern mit einem Schadcode ausgestattet, um sie von einem zentralen Server aus fernzusteuern. 2. Aufsetzen eines Command-and-Control- (C&C-) Servers irgendwo 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

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 – 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.

Angriffe bleiben bisher unbemerkt

Es ist aus technischer Sicht eigentlich unverständlich, warum beispielsweise die Linux-basierte Firmware eines Telekom-Routers es nicht bemerkt, dass über den Internetzugang eine Veränderung 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 oder ein Logging-Server-Eintrag im Internet ausgereicht, um die Manipulation zu identifizieren und die Router-Betreiber zu benachrichtigen. Dafür muss die Firmware des Mikrorechners im Router oder ein zentraler Logging-Server lediglich automatisch 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.

Zukunftssichere IoT-Produkte

Grundsätzlich sollten alle IoT-Baugruppen und Systeme sowie die dazugehörenden Apps mit Sicherheitserweiterungen ausgestattet sein, die dem jeweiligen Stand der Technik entsprechen. Da sich dieser Zustand laufend verändert, müssen unbedingt geeignete Update-Prozesse (zum Beispiel DevOps) existieren, um beim Bekanntwerden neuer Schwachstellen – wie Meltdown und Spectre – zumindest auf der Softwareebene reagieren zu können. Insofern sollten betroffene Entwickler auch mit Blick auf zukünftige Gefahren schnellstens aktiv werden.

Gibt man bei Google „IoT Security" als Suchbegriff ein, erhält man über 10 Millionen Treffer. Da wären zunächst einmal zahlreiche Unternehmen mit bezahlter Werbung, die entsprechende Dienstleistungen anbieten und zur ersten Kontaktaufnahme ein Whitepaper zuschicken

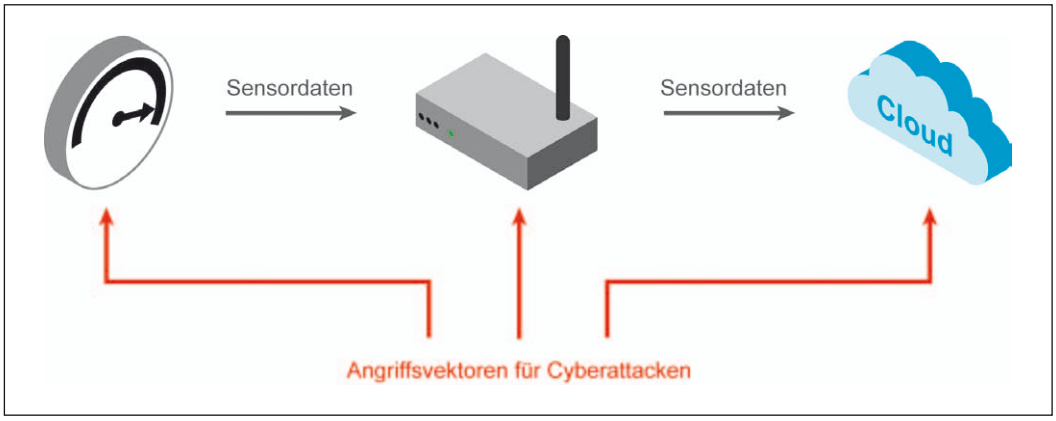

Bild 2: Besonders die unzähligen „Sensor-to-Cloud"-IoT-Anwendungen dürften in Zukunft ein attraktives Ziel für Cyberangreifer bilden. Zum einen bietet die Systemarchitektur vielfältige Möglichkeiten für verschiedene Angriffsvektoren. Zum anderen sind durch fest vereinbarte Schlüssel (Pre-Shared Keys), in die Firmware einprogrammierte Zugriffsberechtigungen zum Gateway bzw. zur Cloud und fehlende Update-Möglichkeiten nahezu keine zeitgemäßen Schutzmaßnahmen gegeben

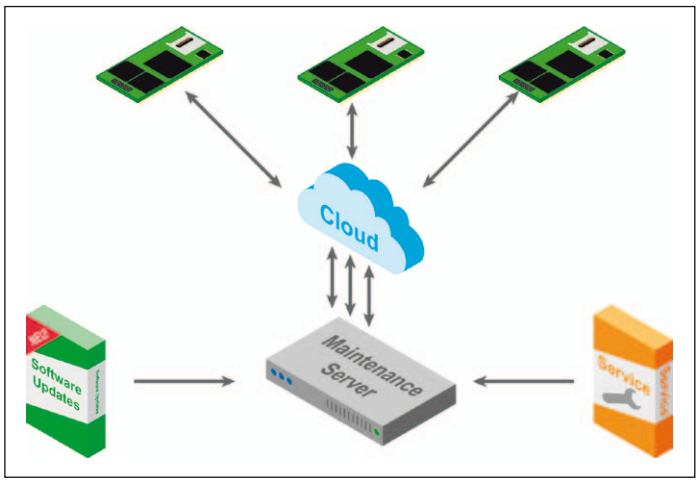

Bild 3: In professionellen Lösungen, zum Beispiel für ein industrielles Internet der Dinge in einer Produktionsumgebung, haben die eingebetteten Systeme eine Verbindung zu einem zentralen Maintenance-Server, der in einer besonders gesicherten Umgebung betrieben wird. Dort schauen sie von Zeit zu Zeit nach, ob Updates vorliegen, die installiert werden müssen. Auch eine automatische Benachrichtigung über einen Subscriber-Kanal ist möglich. Jede Veränderung an der Software wird vom betroffenen Mikrorechnersystem darüber hinaus an den Maintenance-Server gemeldet

wollen. Die von Google gefundenen Webseiten namhafter IT-Firmen bieten darüber hinaus eine kaum überschaubare Informationsvielfalt zum Thema. Sie decken vom Consumer IoT Device über Connected Car bis zur hochsensiblen Medizintechnik praktisch alle relevanten Themenbereiche ab. Fachbücher und Beiträge in Fachzeitschriften mit entsprechendem Schwerpunkt sowie verschiedene Allianzen und Blogs findet Google auch. Spezialisierte Weiterbildungsangebote sowie Vortragsveranstaltungen gibt es ebenfalls. Alles in allem kann es somit wohl nicht an einem Informationsmangel der jeweiligen Entwickler liegen, dass die im Markt verfügbaren Produkte und Lösungen – wie auch der BSI-Lagebericht feststellt – so gravierende Sicherheitsmängel aufweisen und Cyber-Angreifer bei ihren Aktivitäten nahezu freie Bahn haben.

Eine besondere Qualität hat das im Internet frei verfügbare Dokument Future-proofing the Connected World: 13 Steps to Developing Secure IoT Products der Cloud Security Alliance (CSA) und die daraus abgeleiteten Vorträge. Hier wird das IoT Security-Thema in seiner Gesamtheit betrachtet.

Dazu gehören Überlegungen bzgl. sicherer Entwicklungsmethoden mit Technologieüberprüfungen, permanenter Reviews der entwickelten Teilfunktionen im Kollegenkreis (sogenannte Peer Reviews) sowie eine systematische bzw. methodische Gefahrenmodellierung über die gesamte Lebensdauer eines Produktes bzw. Lösung. Das Ziel dabei ist, Schwachstellen zu finden und zu beheben, bevor Kunden dadurch Schäden erleiden. Neben der Integration von Security-Prinzipien in den Entwicklungsprozess spielen auch die zum Einsatz kommenden Werkzeuge eine sehr wichtige Rolle. Programmiersprachen, integrierte Entwicklungsumgebungen sowie die Integrations-, Test- und Qualitätssicherungswerkzeuge müssen ebenfalls entsprechend untersucht und an die Sicherheitsziele angepasst werden. Schwachstellen in den Werkzeugen führen zu weiteren Angriffsmöglichkeiten des Endproduktes.

Das CSA-Dokument referenziert mehrfach das Open Web Application Security Project (OWASP). Hier wurde bereits in 2014 eine Top 10 der IT-Security-Schwachstellen in IoT-Systemen veröffentlicht. Schaut man sich diese Auflistung an, stellt man fest, dass sich wohl zumindest die hinter den IoT-Botnets stehenden Angreifer hier informiert haben könnten, die Entwickler und Produktmanager der betroffenen Produkte aber offensichtlich nicht.

IoT-Sicherheit kein Thema

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 auf der Anbieterseite 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.

Darüber hinaus ist für alle IoT-Produkt- und Systementwicklungen ein professionelles System-Security-Assessment empfehlenswert. Was nutzt ansonsten die beste Verschlüsselung für die Übertragungswege, wenn z. B. der Diebstahl einer digitalen Identität noch nicht einmal bemerkt wird oder ein „geheimer" Hersteller-Servicezugang mit werksseitig eingestelltem Standardpasswort existiert. ◄

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

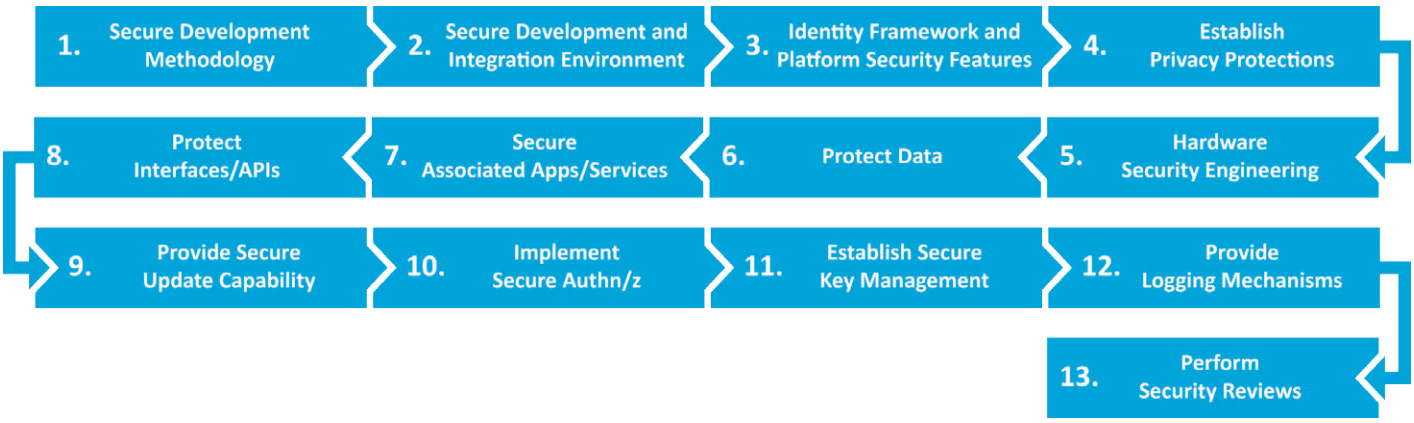

Bild 4: Ein IoT-Security-Dokument der Cloud Security Alliance (CSA) beschreibt sehr ausführlich 13 Schritte, die jeder Entwickler und Produktmanager kennen sollte, bevor eine Neuentwicklung begonnen wird. Durch die Umsetzung dieser Empfehlungen lässt sich ein dem Stand der Technik entsprechendes „Security by Design" realisieren. Aber auch bei bereits im Markt befindlichen Produkten kann man über selektive Maßnahmen die Security nachträglich optimieren