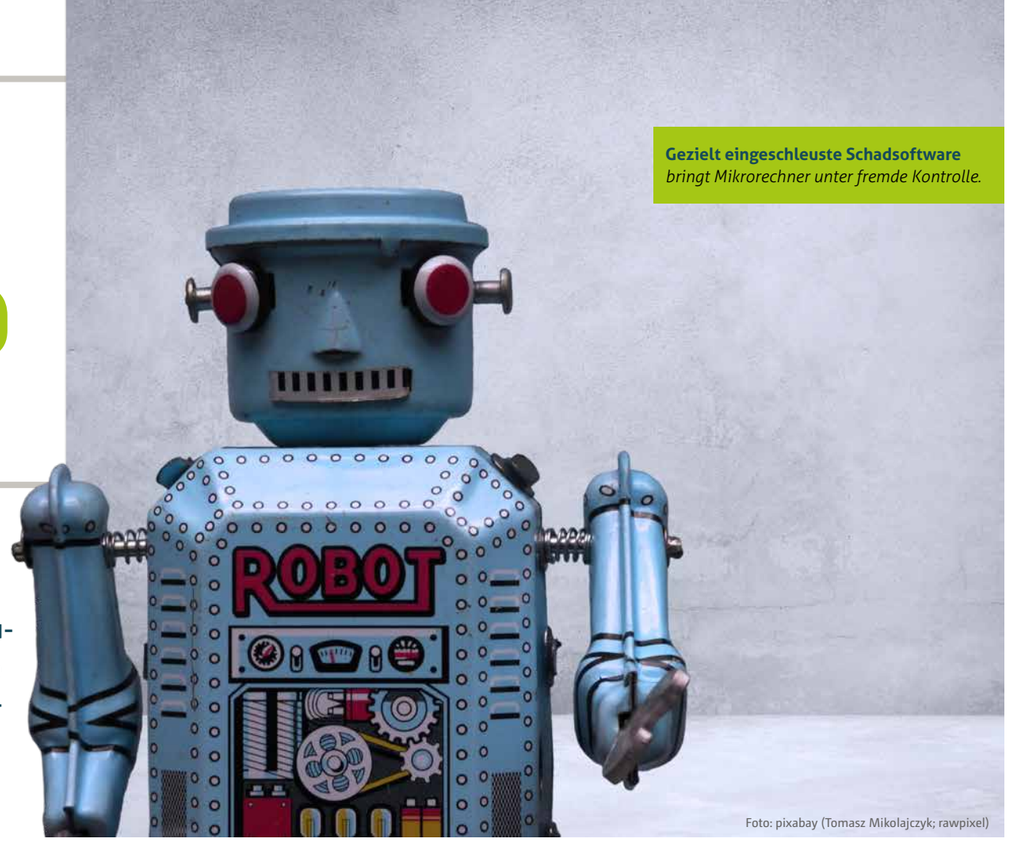
Fern-gesteuert?



Gezielt eingeschleuste Schadsoftware *bringt Mikrorechner unter fremde Kontrolle.*

Foto: pixabay (Tomasz Mikolajczyk; rawpixel)

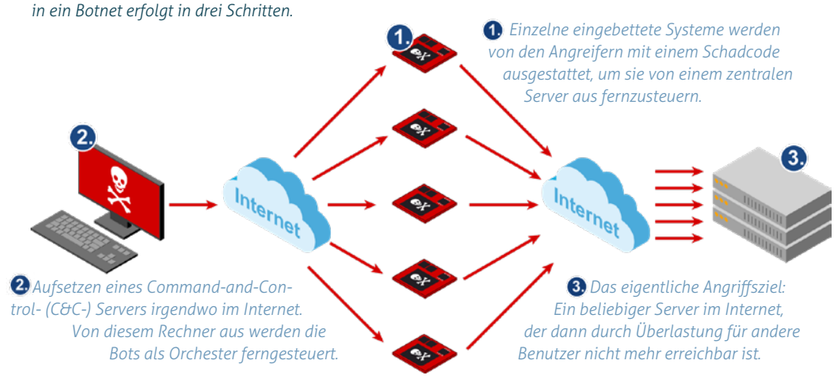
Dem neuesten BSI-Lagebericht zufolge sind inzwischen auch Mikrorechner in Steuerungs- und Energieanlagen durch Cyberattacken bedroht. Besonders auffällig: Immer mehr Rechnerbaugruppen sind bereits ohne Wissen der Nutzer in Bot-Netzwerke eingebunden und für größere Cyberattacken auf Internetserver benutzt worden. IT-Experte Klaus-Dieter Walter erläutert Hintergründe und mögliche Schutzmaßnahmen.

Spektakuläre Cyberangriffe auf einzelne IoT-Lösungen, Automatisierungs- oder Energieanlagen wurden in den vergangenen Monaten zumindest im deutschsprachigen Raum nicht beobachtet. Obwohl im Zuge von Smart Home- und Smart Energy eine wachsende Anzahl von IoT-Funksensoren, -Funkaktoren und -Cloud-Lösungen und sogar neue IoT-Funkstandards zum Einsatz kommen, sind dem aktuellen BSI-Bericht zufolge innerhalb des Betrachtungszeitraums keine gezielten DDoS-Angriffe oder andere Ransomware-Attacken auf diese Komponenten und Anwendungen identifizierbar. Im Bereich der Internet-Router gab es allerdings einen gravierenden Zwischenfall: Im Herbst 2016 wurden zigtausend Telekom-Router über eine nicht mehr zeitgemäß abgesicherte, aber nach wie vor sehr weit verbreitete Serviceschnittstelle erfolgreich manipuliert. Diese Router wurden und werden von Telekom-Kunden auch für Smart Home-IoT-Lösungen sowie Automatisierungs- und Energieanlagenanwendungen genutzt. Im Nachhinein stellte sich heraus, dass es sich mehr um ein „Versehen", aber nicht um einen gezielten Angriff auf die Anlagen von Telekom-Kunden gehandelt haben soll. Es gab wohl noch nicht einmal ein primäres Angriffsziel. Es ist aber vermutlich nur eine Frage der Zeit, bis Cyberkriminelle entsprechende „Geschäftsmodelle" gefunden haben, um auch im IoT-Segment oder zum Beispiel bei virtuellen Kraftwerken aktiv zu werden.

Abbildung 1: Aufbau eines Botnets

Foto: SSV Software Systems GmbH

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.*

Immer mehr IoT-Bot-Netze

Aktuell schon sehr viel weiter fortgeschritten ist hingegen die missbräuchliche Nutzung von IoT-Komponenten im Zusammenhang mit sogenannten Botnet-Angriffen. Ein Botnet ist eine Gruppe automatisierter Schadprogramme, die über „gekaperte" Rechner und Netzwerkressourcen verbreitet werden. 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 Prozent 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. (Abb.1)

Unzählige vernetzte Mikrorechnersysteme besitzen nach wie vor werksseitig eingestellte Standardpasswörter, die man teilweise sogar in den per Internet zugänglichen Bedienungsanleitungen findet. Hinzu kommen aus Sicht der IT-Security völlig veraltete Fernwartungsschnittstellen, wie beispielsweise das bei Hackern sehr beliebte Fernwartungsprotokoll TR-069 des Broadband World Forums. Möglichkeiten zur Software-Aktualisierung, um Sicherheitslücken zu beseitigen, werden entweder erst gar nicht angeboten oder sie sind selbst unsicher. Ein weiteres Problem: Die meisten Nutzer eingebetteter Rechnersysteme bemerken es noch nicht einmal, wenn beispielsweise eine IoT-Baugruppe, ein Fernwartungs-Router oder die mit dem Internet verbundene Fernwirk-Steuerung von Cyberkriminellen als ferngesteuerte Angriffswaffe benutzt wird.

Bei einer für 2020 prognostizierten Anzahl von über 20 Milliarden direkt oder indirekt mit dem Internet verbundenen IoT-Komponenten sollte man das IoT-Botnet-Wachstum sehr ernst nehmen. Die meisten dieser IoT-Baugruppen und die dafür genutzten Mikrorechnersysteme werden so gut wie keine zeitgemäßen Schutzmechanismen oder Update-Möglichkeiten besitzen, um professionellere Kriminelle davon abzuhalten, sie zum Angriff auf andere Infrastrukturkomponenten oder Services zu missbrauchen. Hinzu kommen noch unzählige Smartphones und die darauf laufenden

Abbildung 2: VHPready 4.0

Die klassischen Angriffsvektoren, um beispielsweise das Anlagen-Gateway eines virtuellen Kraftwerks in ein Botnet einzubinden, werden durch die VHPready 4.0-Security-Spezifikationen unterbunden.

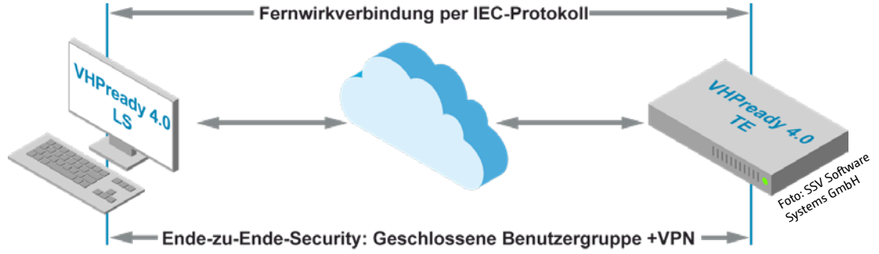


Foto: SSV Software Systems GmbH

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 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, sichere Updates ermöglichen

Es existieren für den Zuständigkeitsbereich des BSI zwar keine detaillierten Informationen, wie es etwa um die Kommunikationssicherheit in virtuellen Kraftwerken bestellt ist. Der fachliche Hintergrund und die Vielzahl der Beteiligten lässt aber zumindest Befürchtungen aufkommen, dass es mit den inzwischen hochentwickelten Ressourcen und Kompetenzen auf der Angreiferseite kein technisches Problem sein dürfte, in diesem Segment erfolgreiche Attacken durchzuführen. (Abb.2)

VHPready 4.0, der einzige Kommunikationsstandard für virtuelle Kraftwerke, hinter dem über den VHPready e. V. eine breite Unterstützerbasis steht, ist zwar durch verschiedene Security-Pflichtelemente gegen viele bekannte Angriffsmuster recht gut geschützt. Direkte Attacken aus dem Internet sind wegen OpenVPN und der geschlossenen Benutzergruppe somit eigentlich nicht möglich, indirekt über die Meltdown-Hardware-Schwachstelle eines Leitwarten-Servers aber nicht auszuschließen.

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 in dezentralen Systemen lediglich erkennen, dass eine „unbekannte“ Software installiert oder gestartet wurde. Für ein modernes VHPready-Gateway ist die dafür erforderliche Root-of-Trust-Verletzungserkennung mit überschaubarem Aufwand realisierbar und zumindest auch von einem Anbieter schon als Bestandteil einer hochsicheren Update-Lösung verfügbar.

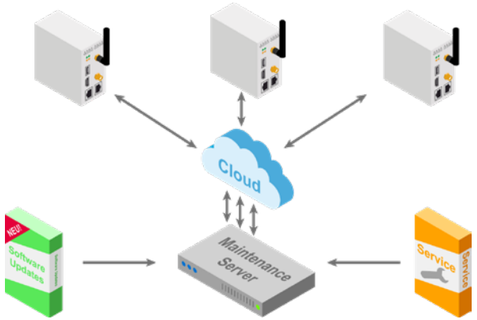


Foto: SSV Software Systems GmbH

Abbildung 3: Sichere Lösungen

In professionellen Lösungen besitzen die Rechnerbaugruppen keinen extern erreichbaren TR-069-Serviceport, sondern lediglich eine Pull-Verbindung zu einem zentralen Maintenance-Server. Dort schauen sie von Zeit zu Zeit nach, ob Updates vorliegen, die installiert werden müssen. Jede Update-Komponente ist des Weiteren mit einer digitalen Signatur versehen, die zu einem Root-of-Trust gehört. Stimmt die Signatur nicht, wird die Komponente nicht auf dem Zielsystem installiert.

Entwicklung und Engineering

Grundsätzlich sollten alle IoT-Baugruppen und Systeme mit einem Patch-fähigen Betriebssystem sowie die dazugehörenden Anwendungen 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. (Abb3.)

Für Mikrorechner ohne Betriebssystem muss eine statische Codeanalyse in der Entwicklung oder sogar nachträglich im Engineering erfolgen, um die Anwendungssicherheit 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 beispielsweise der Diebstahl einer digitalen Identität noch nicht einmal bemerkt wird oder ein „geheimer“ TR-069-Servicezugang mit werksseitig eingestelltem Standardpasswort existiert.

Klaus-Dieter Walter *ist als CEO für die SSV Software Systems GmbH in Hannover tätig. Er ist Autor von vier Fachbüchern zu den Themenbereichen Embedded Linux, Embedded Internet und ARM-basierte Mikrocontroller, Mitbegründer und langjähriges Vortsandsmitglied des M2M Alliance e.V. in Aachen. Zudem ist Walter als Vorstandsmitglied des Industrieforums VHPready tätig, um einen Standard für die Kommunikation in Virtuellen Kraftwerken zu schaffen und engagiert sich seit 2012 aktiv in der M2M Initiative Deutschland des Nationalen IT-Gipfels der Bundesregierung.*

Foto: SSV Software Systems GmbH

Kontakt: SSV Software Systems GmbH, Klaus-Dieter Walter, 30419 Hannover, Tel. +49 (0) 511-40000-0, kdw@ssv-embedded.de

IT UND PROZESSE