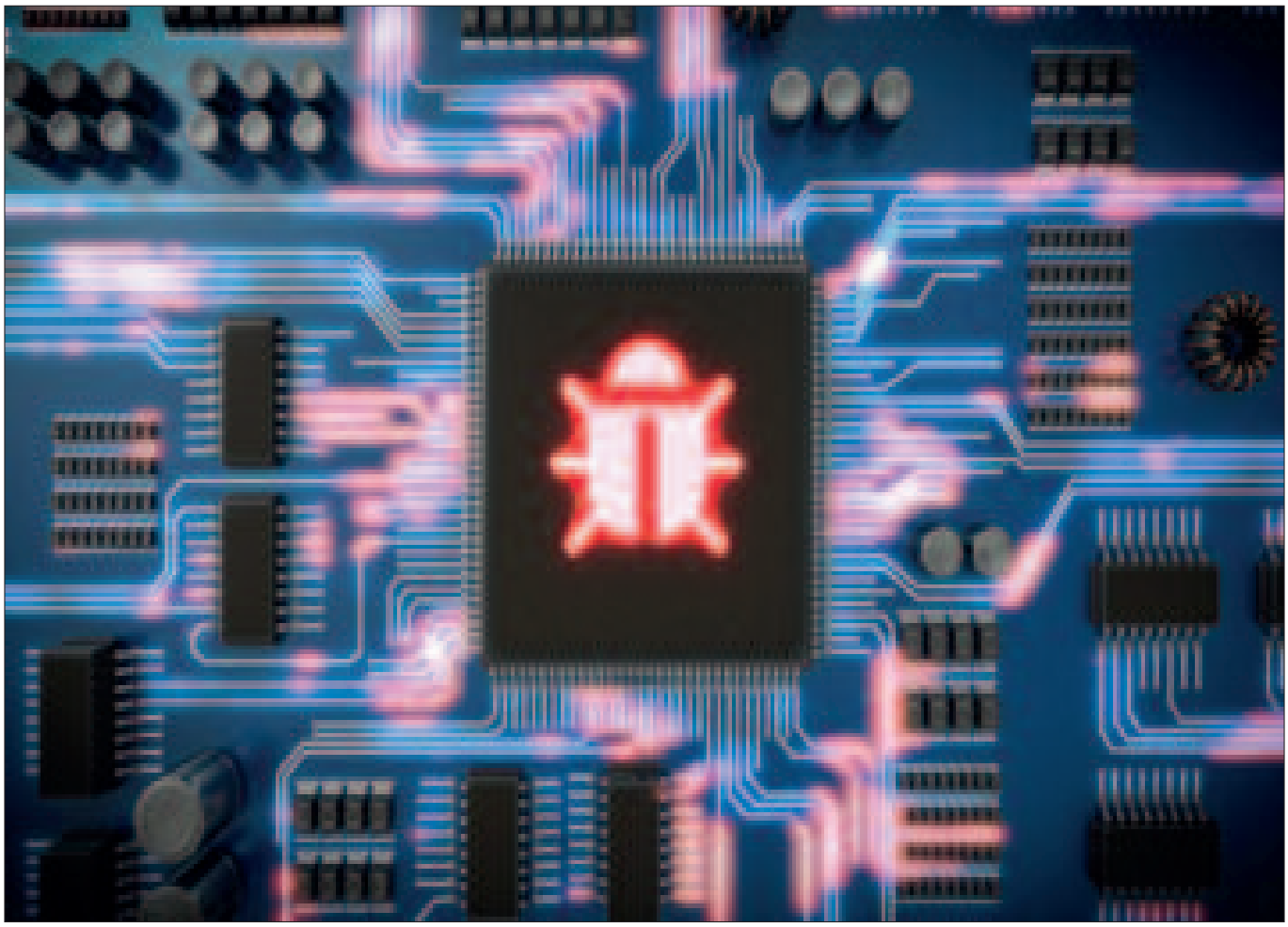


IT-Kriminalität: Hardware-Trojaner könnten bereits in Chips implementiert sein.

FOTO: VCHALUP/FOTOLIA

Verborgene Gefahren

Bei der IT-Defense 2017 in Berlin diskutierten Experten, welche Bedrohungen in der Welt der Informationstechnologie noch verborgen sein könnten.

Zur Finanzierung eines Projekts der Witwe eines früheren Präsidenten von Zambia überwies der Vorstandsvorsitzende (CEO) eines Unternehmens 336.000 Euro. Die Transaktion wurde aus Sicherheitsgründen gestoppt. Der CEO erhielt das Geld zurück – und überwies es noch einmal.

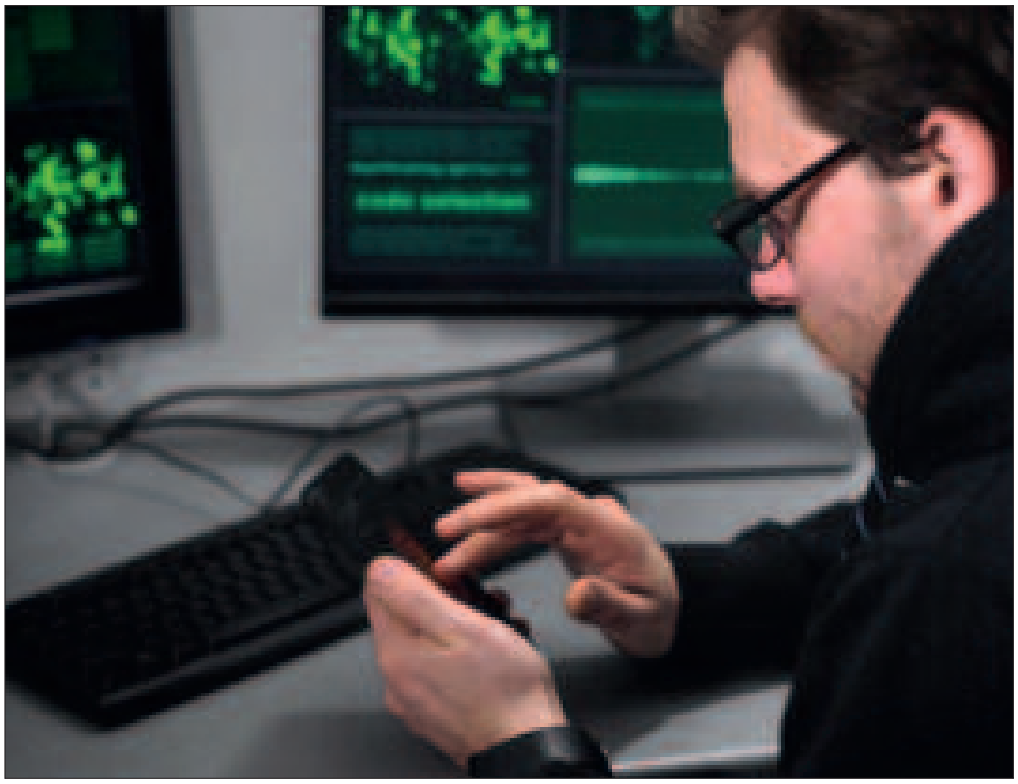
IT-Sicherheitsexperte Sami Laiho nahm dieses Fallbeispiel bei der 15. IT-Defense, die vom 15. bis 17. Februar 2017 in Berlin stattgefunden hat, zum Anlass, auf den Faktor Mensch hinzuweisen, wenn es um die IT-Sicherheit geht. Dazu gehört auch, die Sicherheitseinstellungen der Programme richtig zu nützen. Sicherheitshinweise sollten nicht einfach weggeklickt und programmgesteuerte Fragen sollten nicht gedankenlos mit „Ja“ beantwortet werden. Bei den etwa 300.000 neuen Schadprogrammen, die jeden Tag entdeckt werden, sind reaktive Schutzprogramme überfordert. Es gilt, proaktiv tätig zu werden, sich im täglichen Gebrauch auf wenige Websites zu beschränken und mit zertifizierter Software zu arbeiten.

Hardwareprobleme.

Wenn man das Rad der Zeit zurückdrehen und den Computer neu erfinden könnte, würde man vor allem auf Sicherheit mehr Bedacht nehmen, sagte Thomas Dullien, alias „Halvar Flake“. Wie bei einer Burg würde man nur wenige Zugänge schaffen und diese so eng und verwinkelt gestalten, dass sie zumindest mit dem Rammbock nicht durchbrochen werden können. Derzeit bestehe eine Vertrauenskrise: Der Nutzer eines Smartphones gibt die Kontrolle über dieses Gerät in Art einer Generalvollmacht an eine Vielzahl von Beteiligten ab, an die Hersteller des Gerätes, des Betriebssystems und der Anwendungsprogramme.

Das derzeitige Sicherheitsproblem sieht Thomas Dullien darin, dass die Softwareproduzenten nicht auch Hersteller der Hardware seien und diese nicht zur Gänze überprüfen könnten. Es gebe derzeit keinen standardisierten Weg, wie man Hardware auslesen kann. Erforderlich wäre, einen festverdrahteten, nicht uploadbaren Hardware-Teil zu schaffen, der es ermöglicht, über einen Extra-PIN erfolgte Änderungen in Kernprogrammen des Computers auszulesen und nachzuverfolgen.

Ferner müsse sichergestellt werden, dass Hardware tatsächlich von dem angegebenen Hersteller stammt. Technisch wäre es möglich, über viele Anbieter hinweg sichere Systeme zu schaffen.



Mit Malware-Baukästen aus Untergrundforen im Internet können auch technische Laien Schadprogramme verbreiten.

Die Entwicklung der Hardware würde etwa fünf bis sechs Jahre dauern.

Der Umstand, dass Hardware-Trojaner, die also bereits in Chips implementiert sind, noch nicht dokumentiert sind, bedeutet noch nicht, dass sie unmöglich wären, führte Christoph Paar aus. Da es weltweit nur wenige Chiphersteller gibt, könne niemand sicher sagen, dass keine Backdoors installiert sind.

Derartige Trojaner wären kaum zu entdecken, da die Manipulationen auf der Dotierungsebene der einzelnen Transistoren und somit im Bereich der atomaren Strukturen erfolgen würden. Würde beispielsweise der Zufallszahlengenerator, der für kryptografische Verschlüsselungen herangezogen wird, so manipuliert, dass die Menge der möglichen Zufallszahlen reduziert wird, würde sich der Zeitaufwand für die Entschlüsselung und damit der Kompromittierung durch Außenstehende drastisch reduzieren. Das Durchtesten aller möglichen Schlüssel hätte am Beispiel einer 128-bit-AES-Verschlüsselung bei einem manipulierten Zufallszahlengenerator mit immerhin noch einer Milliarde möglicher Schlüssel lediglich wenige Sekunden gedauert. Ohne Trojaner hätte das Durchtesten aller möglichen Schlüssel die Lebensdauer des Universums erreicht.

Die weltweiten Anstrengungen zum Bau eines Quantencomputers verglich Jaya Baloo mit dem „Manhattan Project“, der Entwicklung der Atombombe. Derjenige, der als Erster den Quantencomputer einsetzen kann, hat durch dessen enorme Rechenkapazität die Möglichkeit, sich verschlüsselte Informationen zugänglich zu machen, die bisher als sicher vor Kompromittierung gegolten haben. Der Angreifer sichert sich so einen enormen Informationsvorsprung. Andererseits wird bereits daran gearbeitet, quantumresistente Algorithmen zu entwickeln.

Angriffsmethoden. Nick Biasini *(www.talosintelligence.com)* berichtete über Exploit Kits, also Malware-Baukästen, die in Untergrundforen im Internet erhältlich sind und auch technisch nicht Versierten ermöglichen, Schadprogramme zu verbreiten. Die Kits werden kommerziell vertrieben, samt technischem Support und regelmäßigen Updates. Mit der zusätzlich erhältlichen „Payload“ lassen sich je nach dem gewünschten Zweck Botnets aufbauen, dDOS-Angriffe ausführen oder Erpresserprogramme (Ransomware) verbreiten.

In der Regel werden Sicherheitslücken in Browsern und Betriebssystemen ausgenützt. Der Besuch einer scheinbar seriösen Internetseite kann bereits eine Infektion nach sich ziehen. Biasini ging auf den derzeit am häufigsten verbreiteten Kit RIG-V bzw. RIG ein sowie auf Sundown, das zunehmend an Bedeutung gewinnt. Weitere Kits sind Astrum/Stegano, das sich hauptsächlich über schädliche Werbung (Malvertising) verbreitet, sowie Magnitude, dessen Zielgebiet vornehmlich der asiatische Raum ist. Dort befinden sich die meisten Internet-User. Aufgrund der vielen mobilen Geräte und ihrer weitverbreiteten Schwachstellen werden nach Auffassung von Biasini Angriffe auf Mobilgeräte stark zunehmen, mit den gleichen Angriffsmustern und -zielen, wie sie aus der PC-Welt bekannt sind.

Über Seitenkanal-Attacken berichtete Anders Fogh und verglich sie mit Angriffen auf Tresore. Man kann versuchen, einen Tresor über das Schloss zu öffnen, aber auch, indem man das Schloss abhört. Ein solcher Tresor ist auf der IT-Ebene der Zwischenspeicher (Cache), in dem häufig benötigte Daten abgelegt werden, weil er schnellere Zugriffszeiten als das dahinterliegende Speichermedium bietet. Fogh zeigte Möglichkeiten auf, auf Umwegen, eben über Seitenkanal-Attacken, Daten aus dem Cache abzuziehen.

Adam Laurie *(www.aperturelabs.com)* berichtete über seltsam anmutende Blüten, die das Internet of Things (IoT) treibt. Der smarte Teller (SmartPlate) analysiert, mit dem Smartphone verbunden, nach ernährungs- und lebensmitteltechnischen Gesichtspunkten, was an Speisen auf dem Teller liegt. Man erfährt die Tagesverfassung eines Menschen, indem über den Spiegel der Gesichtsausdruck ausgewertet wird. Ein Sitzpolster fordert einen bei zu langer Rast auf, wieder aufzustehen oder Übungen zu machen. Das Smartphone macht aufmerksam, wann es Zeit ist, wieder tief Luft zu holen oder schlafen zu gehen. Smart Bras und Smart Panties registrieren und messen Körperfunktionen und übertragen die Daten auf das Smartphone. Smart Toilets

Fotos: Kurt Hickisch (2), Kustvideo/Fotolia

Jörg Ziercke: „Nicht der Islamismus ist radikal, sondern dieser hat die Radikalität islamisiert.“

Sami Laiho: „Die Sicherheitseinstellungen der Programme sollten richtig genützt werden.“

Thomas Dullien: „Smartphone-Nutzer geben die Kontrolle über ihr Gerät an eine Vielzahl von Beteiligten ab.“

Jaya Baloo: „Wer als Erster den Quantencomputer einsetzt, hat Zugang zu verschlüsselten Informationen.“

bieten neben der Positionierung der Sitzfläche weitere einstellbare Annehmlichkeiten. Das smarte Bett verändert die Kopfposition des Schnarchers und sendet unter anderem Daten über das Verhalten im Schlaf an eine App.

Weitere technische Vorträge umfassten Möglichkeiten einer automatisierten Schwachstellensuche (Dan Guido) und versteckte Sprachkommandos (Tavish Vaidya).

Terrorismus. Über die Bedrohung durch Terrorismus referierte Dr. Jörg Ziercke, der frühere Präsident des deutschen Bundeskriminalamtes. Die Wurzeln lägen in sozialen Konflikten, die zu Radikalisierung führen. Nicht der Islamismus sei radikal, sondern dieser habe die Radikalität islamisiert.

Besonders dramatisch sei die Situation in Afrika. Durch den Klimawandel hätten Bauern ihre Existenzgrundlage verloren, was zu einer Wanderungsbewegung geführt habe. Wie seinerzeit für Deutschland, sei für Afrika ein Marshall-Plan erforderlich, wobei allerdings in Anbetracht der dort herrschenden Korruption zunächst gesicherte Institutionen zur Geldverteilung geschaffen werden müssten.

Der Terror sei nicht mit den Flüchtlingen gekommen, sondern sei schon früher präsent gewesen, sagte Ziercke, beginnend mit dem „Nine Eleven“ in New York 2001.

Waren weltweit im Jahr 2013 noch 18.211 Menschen Mordopfer des islamistischen Terrorismus, stieg deren Zahl 2014 auf 32.658. Weniger als drei Prozent der Terrortoten entfielen dabei auf die westlichen Länder. In Europa werde vielfach nicht zur Kenntnis genommen, dass die meisten Todesopfer innerhalb der Muslime selbst zu beklagen seien, betonte Ziercke. Anschläge durch Suizid-Attentäter erfolgten 2015 in Istanbul und Paris sowie 2016 in Brüssel und Nizza. Auf fanatisierte Einzeltäter sind 2016 in Deutschland die Anschläge in Essen, Hannover, Würzburg, Ansbach, Chemnitz und Berlin zurückzuführen.

In Deutschland waren 2016 550 Personen als Gefährder eingestuft und 450 als relevante Personen. 850 Ausreisen in Terrorgebiete wurden registriert, 100 verhindert. 280 in Terrorgebiete Ausgereiste kehrten zurück, 140 wurden getötet. Es gab 730 Ermittlungsverfahren mit 1.000 Beschuldigten. Pro Jahr langen etwa 500 Hinweise ein, die überprüft werden müssen. In Deutschland wurde das *Gemeinsame Terrorismusabwehrzentrum (GTAZ)* eingerichtet, in dessen Rahmen täglich in Berlin von Vertretern der Sicherheitsbehörden des Bundes und der Länder die Lage besprochen und beurteilt wird. Hier erfolgen auch Gefährdungsbewertungen und Strukturanalysen. In das Gemeinsame Extremismus- und Terrorismusabwehrzentrum (GETZ) ist auch Europol eingebunden.

In der Sicherheitsdebatte 2017 werden eine Verstärkung der Videoüberwachung, biometrische Gesichtserkennung und stärkere Nutzung der DNA-Analyse diskutiert. Weitere Themen sind praxistaugliche Haftgründe für die Abschiebehaft von gefährlichen Ausreisepflichtigen/Gefährdern sowie der Einsatz der elektronischen Fußfessel bei Gefährdern.

Thema ist auch der Cyber-Terrorismus mit Angriffen auf Anlagen der kritischen Infrastruktur (Kraftwerke, Telekommunikation, Trinkwasserversorgung). Gefährdet sind auch der Datenverbund der Banken sowie Krankenhäuser, Bahn- und Flugsicherung, Verkehrsleitsysteme und Wirtschaftsunternehmen (Industrie 4.0).

Kurt Hickisch

CIROSEC

IT-Defense

Seit 2003 veranstaltet die auf IT-Sicherheitsberatung spezialisierte Cirosec GmbH, Heilbronn, jährlich jeweils Anfang Februar in verschiedenen Städten Deutschlands die dreitägige IT-Defense. Bei diesem Kongress, dessen Teilnehmerzahl auf 200 limitiert ist, referieren Experten über technische Fragen der IT-Sicherheit und präsentieren Forschungsergebnisse. Dazu kommen Vorträge zu strategischen Lösungen und solche, die auf unterhaltsame Art auf Sicherheitsprobleme eingehen. Am ersten Konferenztag kann praktisches Erfahrungswissen in Arbeitsgruppen vertieft werden. Nach Abschluss der Veranstaltung stehen am vierten Tag ausgewählte Referenten noch zu Round Tables zur Verfügung.

Die IT-Defense 2018 wird vom 31. Jänner bis 2. Februar 2018 in München stattfinden.

www.cirosec.de;
www.it-defense.de

Fotos: Kurt Hickisch