idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Press release

Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE
Silke Wiesemann

09/04/2017
http://idw-online.de/en/news680387

Research projects, Research results
Information technology
transregional, national

FKIE-Forscher zeigen akute Bedrohungslage durch Hardware-Trojaner auf

Die Botschaft ist eindeutig: Von Hardware- und hardwarenahen Trojanern geht weltweit eine große Bedrohung für bestehende IT-Systeme aus. Allerdings wird diese Gefahr von vielen IT-Verantwortlichen und Entscheidern in Unternehmen entweder nicht wahrgenommen oder zumindest unterschätzt. Dabei gibt es bereits Gegenmaßnahmen, mit denen Gerätehersteller und Nutzer eine bessere Absicherung für die Geräte erreichen können. Dies geht aus einem Bericht des Fraunhofer-Instituts für Kommunikation, Informationsverarbeitung und Ergo-nomie FKIE hervor, der einen umfassenden Überblick über die Bedrohungslage durch Hardware- und hardwarenahe Trojaner liefert.

So zeigt der Bericht eine Dimension der Bedrohung für Computer, Embedded Devices und das Internet of Things (IoT) auf, die vielfach bei IT-Sicherheitsüberlegungen unbeachtet bleibt. Denn anders als bei klassischer »Malware« für PCs, gibt es nur wenige IT-Security-Lösungen, die Wirkung gegen Hardware-Trojaner zeigen.
Manipulationen an der Hardware bzw. der eingesetzten Firmware können in ganz unterschiedlichen Lebensphasen erfolgen. In einigen Fällen werden bereits während der Entwicklung Hintertüren eingebaut oder Geräte während der Produktion oder dem Transport manipuliert. Solche präparierten Geräte können einen immensen Schaden im Unternehmen anrichten, da sie zum Ausspähen persönlicher Daten und Firmen-geheimnisse bis zur Sabotage von Produktionsprozessen eingesetzt werden können. »Zwar sind Hardware-Trojaner in vielen Fällen schwerer zu installieren und implementieren als eine vergleichbare klassische Malware, allerdings ist es auch sehr viel schwieriger, diese überhaupt zu entdecken«, erläutert Peter Weidenbach von der Abteilung »Cyber Analysis and Defense« am Fraunhofer FKIE. Er gehört zu einem Autorenteam um Dr. Elmar Padilla und Raphael Ernst, die den durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) geförderten Bericht erstellt haben.
Die immer größer werdende Verbreitung von Hardware- und hardwarenahen Trojanern erklären sich die FKIE-Forscher damit, dass diese Bedrohungslage bislang relativ vernachlässigt wurde – sowohl von den Geräteherstellern wie auch den Nutzern. Neben einer Aufstellung der potenziellen Infektionswege und Angriffsmöglichkeiten für Hardware in den unterschiedlichen Geräteklassen enthält der Bericht daher auch eine Zusammenstellung von Handlungsoptionen und Schutzmaßnahmen. »Es gibt viele Gegenmaßnahmen wie die konsequente Netztrennung, Signaturen oder eine automatisierte Firmware-Analyse. Wenn bestehende Optionen gezielt eingesetzt würden, wären wir schon einen großen Schritt in Sachen Cybersicherheit weiter«, erklärt Weidenbach.
Längst sind allerdings nicht mehr nur klassische IT-Geräte wie Festplatten, Netzwerkkarten, Router oder Drucker von der Bedrohung durch Hardware-Trojaner betroffen. Die hardwarenahen Trojaner haben Einzug bei den Geräten gehalten, die unter dem Schlagwort »Internet of Things« (IoT) zusammengefasst werden: beispielsweise Smart-TVs, aber auch Kühlschränke und Überwachungskameras. Damit ist fast jedes elektronische Gerät anfällig für eine derartige Manipulation. Dies betrifft auch Geräte, die in sensiblen Bereichen wie der Medizintechnik oder bei kritischen Infrastrukturen eingesetzt werden.
Dass »der Countdown läuft«, betont auch Thomas Tschersich, Senior Vice President Internal Security and Cyber Defense bei T-Systems, in seinem Vorwort zu dem FKIE-Bericht. Durch die zunehmend vernetzte Welt werde die Angriffsfläche für Cyberattacken zwangsläufig größer. Aus diesem Grund sei es unerlässlich, dass Schwachstellen unverzüglich nach ihrer Detektion beseitigt werden. Der FKIE-Bericht liefere hierfür einen guten Überblick und schaffe die dringend notwendige Transparenz. »Nur wenn wir verstehen, wie die Angreifer arbeiten und welcher Schwachstellen sie sich bedienen, können wir als Industrie wirksame Gegenmittel entwickeln und Boden im Kampf für

die Sicherheit aller Nutzer gut machen«, so Tschersich.
Um die Detektion dieser Schwachstellen kümmern sich Peter Weidenbach, Raphael Ernst und Dr. Elmar Padilla, die sich für die Zukunft eine Qualitätssicherung in Form einer neutralen Prüfstelle bzw. eines Prüfsiegels wünschen.
Weidenbach: »So könnte jeder, vom Hersteller bis zum Nutzer, seinen Beitrag zur Netzwerksicherheit leisten.«

URL for press release: http://www.fkie.fraunhofer.de/de/Pressemeldungen/hwt-bericht.html

Attachment Presseinformation HWT-Bericht http://idw-online.de/en/attachment58383

Von Hardware- und hardwarenahen Trojanern geht weltweit eine große Bedrohung für bestehende IT-Systeme aus.
iStock/123RF

72 Seiten stark ist der FKIE-Bericht über die Bedrohungslage durch Hardware- und hardwarenahe Trojaner.
Fraunhofer FKIE