Live-Hacking bei Cirosec

cirosec GmbH
Edisonstraße 21
74076 Heilbronn
Tel: 07131 / 59455-0
Fax: 07131 / 59455-99
info@cirosec.de
www.cirosec.de

Geldautomat als ferngesteuerter Goldesel

Im Laufe des letzten Jahrzehnts hat sich die IT-Defense der Cirosec GmbH in Heilbronn zu einer Art Familientreffen der Sicherheitsbranche entwickelt. Geschäftsführer Stefan Strobel, selbst überzeugter Techniker und IT-Experte, hält stets Ausschau nach kompetenten Referenten - durchaus nah an der Hackerszene.

Manch einem Besucher erspart das Drei-Tage-Event im Frühjahr die Reise zu den großen Sicherheitskonferenzen in den USA und Kanada. Wichtige Referenten finden nämlich meist auch den Weg zur IT-Defense. Noch im Sommer 2010 konfrontierte der Amerikaner Barnabay Jack die Besucher der Black Hat mit einem umprogrammierten Geldautomaten, der auf Knopfdruck Banknoten ausspuckte. Ganz ohne Legitimation und gültiges Konto natürlich. Auf der IT-Defense 2011 ging er noch einen Schritt weiter: Diesmal hijackte er den Automaten via Internet von Deutschland aus. Per Webcam konnten die Zuschauer verfolgen, wie ein Assistent in den USA das Geld entnahm. Umprogrammierte Hardware liegt ganz im Trend der Hackerszene. Hier gibt es weder störende Antivirenprogramme noch sensible Nutzer.

„Hardware is the New Software“, formuliert es der US-Sicherheitsexperte und Erfinder Joe Grand. Angriffziele sind alle Arten von Automaten oder normale Haushaltsgeräte, wenn sie über Mikroprozessoren verfügen. Auch diese Chips benötigen Software, die allerdings nicht auf Festplatten, sondern auf EEPROMs liegt. Auch dieser Code lässt sich verändern. Normalerweise tun dies die Hersteller, um Fehler zu beseitigen. Hacker können diese Möglichkeit aber Missbrauchen, um Schadcode einzu-schleusen und das Gerät in ihrem Sinne manipulieren.

Banknoten per Knopfdruck sind da nur eine Möglichkeit. Auch Haushaltsgeräte und Industriesteuerungen können betroffen sein. „Dieses Feld der Sicherheit wurde bislang sträflich vernachlässigt“, so Joe Grand, „für sicherheitsrelevante Anwendungen werden Hardware-Komponenten verwendet, denen man vertraut, obwohl sie oft gegenüber Angriffen verwundbar sind, die mit einfachen Mitteln durchgeführt werden und Insidern seit Jahrzehnten bekannt sind.“

Stuxnet wird das sicher ändern, doch noch liegen die Hürden niedrig. „Die Hersteller wollen das Problem meist einfach nicht wahrhaben und schieben die Sicherheitsprobleme beiseite“, meint Joe Grand. Bislang schützte die Hardware meist ihr individueller Zuschnitt und der Mangel an öffentlich bekannten Details. Die zum Hacken nötigen Informationen sind inzwischen aber über entsprechende Webseiten allgemein verfügbar, meint der Amerikaner. Sogar bei sensiblen Geräten wie Abstimmungsautomaten für lokale und nationale Wahlen waren Angriffe in der Vergangenheit schon erfolgreich.

Amerikanische, indische und holländische E-Voting-Maschinen programmierten Hacker so um, dass eine Person mehrfach abstimmen konnte. Als dankbares Angriffsziel erweisen sich auch intelligente Stromzähler. Schon so einfache Features wie die Authentifikation bei Firmware-Updates werden nicht realisiert oder nur ungenügend geschützt. „Den Ingenieuren fehlt oft die nötige Sensibilität beim Thema Sicherheit“, folgert Joe Grand. Er selbst attackierte durch eine umprogrammierte Smartcard erfolgreich die Parkautomaten von San Francisco und konnte fortan unbegrenzt, und ohne Bezahlung sein Auto abstellen.

Der Schaden bei solchen „Updates“ hält sich noch in Grenzen, da es sich um Einzelfälle und nicht um ein Massendelikt handelt. Ganz anders verhält es sich natürlich, wenn durch den Eingriff wertvolle Informationen abhandenkommen. Der Italiener IT-Berater Arrigo Triulzi stellte sein „Maux“ vor, ein Projekt, das der Frage nachgeht, wie man eine Firewall so umprogrammiert, dass ein dauerhafter, nicht zu detektierender Bypass an der Firewall vorbei entsteht. Damit will er eine permanent offenstehende „Backdoor“ für den Angreifer realisieren. Nur als Fingerübung, wie er betont. Triulzi erreichte sein Ziel, ganz ähnlich wie Joe Grand und Barnabay Jack, durch eine Kette von Firmware-Änderungen. Die Firewall begann daraufhin, die Datenpakete als Kopie umzuleiten. Da weder in der Firewall noch dahinter Veränderungen oder Schadcode auftauchen, hat der Besitzer kaum eine Chance, die Manipulation zu entdecken. Ähnliche Angriffszenarien sind auch bei ganz normalen Netzwerkkarten möglich, wie Joe Grand ergänzte.

Ob ihre intellektuellen Übungen von Nachrichtendiensten oder kommerziellen Hackern bereits angewendet werden, blieb offen. Hinweise darauf gibt es.

sicherheit.info 11.03.11