Böse und billig: Hacking-Gadgets

Gefahr durch angriffslustige Hardware

Frei verkäufliche Hacking-Gadgets beherrschen fiese Tricks, um Rechner, Smartphones & Co. zu attackieren. Die Geräte nutzen die Schwächen von WLAN, Bluetooth, USB und NFC aus, um Systeme zu hacken oder zu stören. Einige Gadgets lassen sich auch zur Spionage missbrauchen. c't hat 15 Spezialgeräte im Labor von der Leine gelassen und die von ihnen ausgehende Gefahr bewertet.

Von Ronald Eikenberg und David Wischnjak

Spezialisierte Online-Shops verkaufen Gadgets, an denen auch James Bond seine helle Freude hätte: Die Geräte nehmen die Sicherheit moderner IT aufs Korn, indem sie Angriffe fahren, auf die viele nicht vorbereitet sind. Deshalb erfreuen sich die Hacking-Gadgets bei Pentestern, die hauptberuflich auf der Suche nach Schwachstellen in Unternehmensnetzen sind, großer Beliebtheit. Einige der Geräte wurden für Analyse-, Forschungs- und Entwicklungszwecke entworfen; etwa von Sicherheitsexperten, um Funkprotokolle ohne teure Laborausrüstung zu analysieren. In den falschen Händen lassen sich viele der Produkte aber auch als gefährliche Cyber-Waffen missbrauchen. Zu den Käufern zählen neben Pentestern auch Hacker – sowohl die guten als auch die bösen.

Bevor es jedoch ans Eingemachte geht, ist ein Warnhinweis angebracht: Mit vielen der auf den folgenden Seiten gezeigten Geräten kann man echten Schaden anrichten und gegen geltende Gesetze verstoßen. Wenn Sie mit dem Gedanken spielen, sich etwas davon anzuschaffen, sollten Sie es tunlichst nicht gegen das Eigentum anderer Personen einsetzen – und wenn doch, dann nur mit einer schriftlichen Einwilligung. Weitere Informationen zur rechtlichen Situation finden Sie ab Seite 78.

Die Angriffstechniken der Geräte könnten unterschiedlicher kaum sein. Unter unserer bunten Auswahl befindet sich etwa der **USB Rubber Ducky** (siehe S. 64), der äußerlich nicht von einem gewöhnlichen USB-Stick zu unterscheiden ist. Ein Pentester lässt das Gadget an einem öffentlichen Ort liegen und wartet einfach, bis es ein neugieriger Finder mit einem Rechner verbindet. Ehe sich der Finder versieht, ist sein Rechner kompromittiert. Der Stick meldet sich nicht als Speicher, sondern als USB-Tastatur am System an und übernimmt die Kontrolle. Der **USB Killer** (siehe S. 67) ist ebenfalls vermeintlich ein normaler USB-Stick. Steckt man ihn in einen USB-Port, stößt er –220 Volt aus, was zum sofortigen Hardware-Tod des Rechners führt.

Einige der Hacking-Gadgets beherrschen komplexe Netzwerk-Angriffe auf Knopfdruck. Ein Penetration-Tester etwa kann damit Schlupflöcher im Netz seines Auftraggebers aufspüren und demonstrieren, wie leicht sie sich ausnutzen lassen. So sieht die **LAN Turtle** (siehe S. 66) wie eine herkömmliche USB-Netzwerkkarte aus, in ihr steckt jedoch ein Mini-PC auf Linux-Basis, der mit etlichen Pentesting-Tools bestückt ist. Der Pentester muss sie lediglich in einem unbeobachteten Moment zwischen PC und Netzwerkkabel stecken, um eine permanente Backdoor zu installieren. Die Wahrscheinlichkeit, dass die Hintertür lange unentdeckt bleibt, ist groß: Wann haben Sie zuletzt die Rückseite Ihres Arbeitsrechners gesehen? Analog dazu gibt es den **WiFi Pineapple** (S. 70). Damit sind allerlei Angriffe auf WLANs und deren Clients möglich.

Unter den vorgestellten Geräten befindet sich auch ein winziger **USB-Keylogger** (S. 65), der einfach zwischen Tastatur und Rechner gesteckt wird. Fortan zeichnet er alle Tastatureingaben auf und verschickt von Zeit zu Zeit ein Protokoll über WLAN. Wer das ohne Wissen des Nutzers macht, handelt selbstverständlich gesetzeswidrig. Gänzlich ungefährlich und durchaus unterhaltsam ist das auf Seite 67 vorgestellte **TV-B-Gone-Kit:** Es probiert via Infrarot über hundert TV-Ausschaltcodes durch, bis sämtliche Mattscheiben in der näheren Umgebung schwarz werden. Wer das Gadget mal live erlebt hat, weiß, warum auf Messen und Veranstaltungen häufig die Infrarot-Empfänger der Präsentations-Displays abgeklebt werden.

Es handelt sich bei den meisten Geräten jedoch keineswegs um Spielzeuge und es werden immer wieder Fälle bekannt, in denen die Spezialhardware für echte Angriffe missbraucht wird. So wurde Anfang 2015 in der Redaktion der Tageszeitung taz ein USB-Keylogger entdeckt, der offenbar mindestens ein Jahr dazu genutzt wurde, um Redaktionsmitglieder auszuspähen. Als Verdächtiger gilt ein ehemaliger Mitarbeiter. Einer unserer Leser sandte uns gar das USB-Netzteil einer E-Zigarette zu, in das sorgfältig ein digitaler Audiorecorder eingebaut wurde. Wir konnten den Inhalt des Flash-Speichers bergen und machten die Aufnahmen unserem Leser zugänglich. Wie und warum das manipulierte Netzteil zum Betroffenen gelangte, war nicht nachvollziehbar.

Alle Herstellerseiten und Bezugsquellen finden Sie unter dem c't-Link. Auf Seite 74 haben wir die interessantesten Angriffstechniken für Sie zusammengestellt. Denn nur wer die zum Teil unkonventionellen Tricks der Hacking-Gadgets versteht, kann sich effektiv davor schützen. *(rei@ct.de)* c't

Hersteller und Shops: ***ct.de/yk39***

Da hört der Spaß auf: Ein Leser entdeckte in einem USB-Netzteil einen funktionsfähigen digitalen Audiorecorder.