Hacking-Gadgets

c’t testet die Tools der Hacker

Im Werkzeugkasten eines Hackers findet man erstaunliche Geräte, mit denen er sich fast überall Zutritt verschaffen kann: Angriffe auf Netzwerke, Rechner, Smartphones & Co. sind damit kinderleicht. c't hat viele solcher Hacking-Gadgets in Spezialshops eingekauft und im Labor ausprobiert.

Von Ronald Eikenberg

Man muss nicht mal ins Darknet abtauchen, um im Netz auf Online-Shops zu stoßen, die eine brisante Auswahl an Hacking-Gadgets führen. Bei Hacker Warehouse, Hak5 oder Lab401 findet man fast ausschließlich Gerätschaften, die vor allem einem Zweck dienen: Angriffe auf Netze, Rechner, Smartphones & Co. so leicht zu machen, wie es nur geht. Dazu gesellen sich nicht selten perfide Spionage-Geräte, die man eher im Handgepäck eines Staatsagenten vermuten würde. Last, but not least findet man in vielen der Shops sogar Einbruchswerkzeug, mit dem man spurlos fast jedes Schloss knacken kann.

Zu den Kunden zählen illustre Namen: Offenbar kaufen das FBI, die US Army sowie der Rüstungskonzern Lockheed Martin bei einem der Shops ein, wie aus einer c't vorliegenden Kundenliste hervorgeht. Das Spezial-Equipment kann in den falschen Händen ohne Frage großen Schaden anrichten – allerdings soll es vornehmlich einem anderen Zweck dienen. Die Geräte und Werkzeuge wurden für Penetration-Tester, Security-Forscher und Sicherheitsbeauftragte entwickelt, deren Aufgabe es ist, Schwachstellen aufzuspüren und zu eliminieren. Getreu dem Motto: Hacke Dich selbst, bevor es jemand anderes tut. Und so ist es auch nicht überraschend, dass sich auf der Kundenliste auch Amazon, Apple, Google, Microsoft, Siemens und Volkswagen finden.

Gadgets im Agentenkoffer

Die meisten Geräte sind frei verkäuflich – einen Cyber-Waffenschein benötigt man für Erwerb und Besitz nicht. Wofür die Hacking-Ausrüstung eingesetzt wird, spielt für die Shops keine Rolle. Einen Vorwurf kann man den Betreibern daraus nicht machen, schließlich können sie ohnehin nicht kontrollieren, ob das Pentesting-Equipment für einen beauftragten Sicherheitscheck oder einen Cyber-Einbruch in fremde Infrastruktur genutzt wird. Dass die Spezialgeräte wohl für beides im Einsatz sind, zeigt ein spektakulärer Fall, der sich im Herbst vergangenen Jahres in den Niederlanden zugetragen hat: Das dortige Verteidigungsministerium erklärte, dass der Geheimdienst vier Männer aufgegriffen hat, die im Verdacht stehen, für den russischen Militärgeheimdienst GRU zu arbeiten.

Im Mietwagen der Männer entdeckten die niederländischen Ermittler nicht nur eine erhebliche Menge Bargeld, sondern auch eine Reihe technischer Geräte, die sich für Angriffe auf WLAN eignen. Zu dem sichergestellten Equipment zählt neben einem Notebook mit WLAN-Richtantenne auch ein **WiFi Pineapple Nano**. Dabei handelt es sich um einen leistungsfähigen portablen WLAN-Router, der die gängigen WLAN-Attacken automatisch durchführt. Die vier Russen sollen laut dem niederländischen Verteidigungsministerium Cyberangriffe auf Chemiewaffenkontrolleure vorbereitet haben. Nach Angaben des russischen Außenministers Sergej Lawrow handelte es sich jedoch um Fachleute auf einer Routinefahrt.

Hacking-Gadgets, die Zweite

c't hat sich erstmals in Ausgabe 18/2017 intensiv mit den angriffslustigen Hacking-Gadgets befasst. Damals kauften

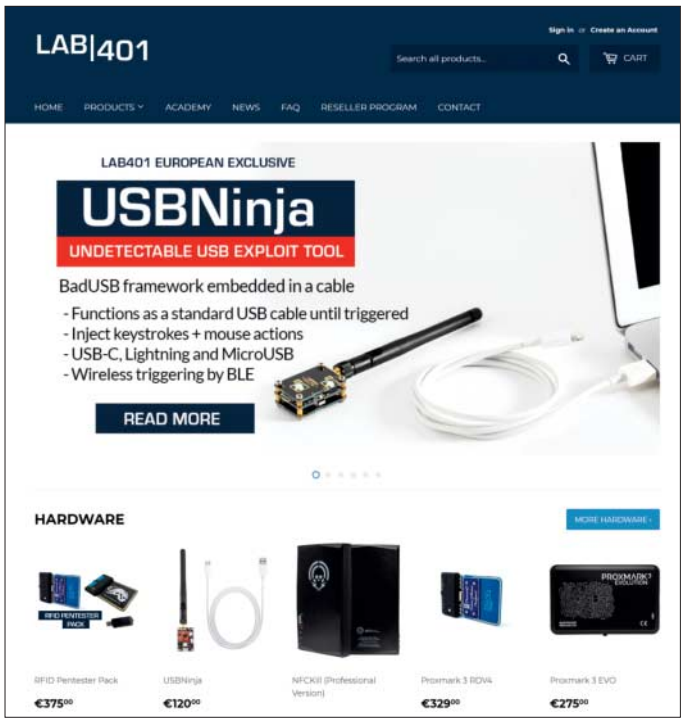
Der niederländische Geheimdienst entdeckte bei einer mutmaßlichen Hacker-Einheit der Russen verdächtiges WLAN-Equipment wie das Angriffs-Tool WiFi Pineapple.

Bild: Netherlands Ministry of Defence

Verboten oder nicht?

Bei den meisten Hacking-Gadgets handelt es sich um Werkzeuge, mit denen man sowohl konstruktiv arbeiten als auch anderen Schaden zufügen kann – vergleichbar mit einem Zimmermannshammer. Gründe für ein generelles Verbot gibt es daher nicht. Es spricht nichts dagegen, die eigenen Systeme mithilfe der Geräte auf Sicherheitslücken abzuklopfen oder sie im Rahmen einer Awareness-Schulung zu nutzen, um Mitarbeiter anschaulich über zumeist unterschätzte Gefahren aufzuklären.

Strafrechtlich relevant wird der Einsatz der Geräte ohne Frage dann, wenn sie dafür missbraucht werden, um etwa fremde Infrastruktur ohne Einwilligung des Besitzers zu manipulieren, sabotieren oder auszuspionieren. Eine ausführliche Einschätzung der rechtlichen Lage finden Sie in c't 18/2017. Wir haben den Artikel kostenlos auf ct.de/ytvk freigegeben. Grundsätzlich verboten ist etwa der Besitz von Abhörgeräten mit Funkverbindung, die als Alltagsgegenstände getarnt sind. Diese fallen unter § 90 des Telekommunikationsgesetzes („Missbrauch von Sende- oder sonstigen Telekommunikationsanlagen").



In Online-Shops wie Lab401 findet man alles, was das Hacker-Herz begehrt.

wir 15 Spezialgeräte ein – darunter auch ein WiFi Pineapple Nano von Hak 5 (siehe S. 28) – und ließen sie in unserem abgeschirmten Labor von der Leine. Es zeigte sich, dass keiner der Hersteller zu viel versprochen hatte. Die Hacking-Gadgets attackierten Funkverbindungen, schleusten Schadcode ein und zerstörten sogar eines unserer Notebooks irreparabel. Seitdem sind wir auf zahlreiche weitere Geräte gestoßen, deren Wirkung nicht weniger fatal ist.

Also sind wir erneut auf Einkaufstour gegangen und ließen die interessantesten Geräte in die Redaktion kommen. Dazu zählt ein scheinbar gewöhnliches iPhone-Ladekabel namens **USBNinja**, das den Rechner infiziert, sobald man den Funkauslöser aus sicherer Entfernung betätigt (siehe S. 17). Es attackiert alle Betriebssysteme, während die meisten Virenscanner tatenlos zusehen. Eine Armbanduhr für gerade einmal 30 Euro ist der größte Feind aller WLANs: Per Knopfdruck legt sie beliebige Funknetze effektiv lahm (siehe S. 17). Und das **Chameleon Mini** (S. 21) emuliert NFC-Zugangskarten für Hotelzimmertüren & Co., während das auf der gleichen Seite vorgestellte, vielen bekannte **Lockpicking-Set** Schlösser auf die altmodische Tour knackt – analoges Hacking sozusagen.

Weitreichende Eingriffe in den Funkverkehr bis hin zum Abhören von Mobilfunk erlaubt das **LimeSDR** von Seite 19. Wie kann ein winziges USB-Gerät für nur 10 Euro Sperrbildschirme und Festplatten-Verschlüsselungen austricksen? Auf Seite 23 erfahren Sie es. Außerdem haben wir uns dieses Mal ein besonderes Monitorkabel angesehen: Der **VideoGhost** (S. 18) erstellt in regelmäßigen Abständen Screenshots des durchgeleiteten Bildsignals. Auch hier sind Virenscanner machtlos.

Auf Seite 24 zeigen wir zwei Geräte, die Sie nicht kaufen dürfen, da sie nach deutscher Gesetzeslage verboten sind. Darunter befindet sich ein vermeintlicher Wecker, der eigentlich eine WLAN-Kamera mit Nachtsicht-Funktion ist. Genau so einen entdeckte ein britisches Pärchen im vergangenen Jahr nach eigenen Angaben auf seinem Nachttisch in einer Airbnb-Unterkunft. Schützen kann man sich vor solchen Gefahren nur, wenn man sie kennt.

Deshalb laden wir Sie ein, durch unsere umfangreiche Auswahl an Hacking-Gadgets zu stöbern. Auf den folgenden sieben Seiten stellen wir etliche neue Gerät vor und ab Seite 26 finden Sie ausgewählte Klassiker aus dem ersten Teil in Ausgabe 18/2017. Ab Seite 30 plaudert ein erfahrener Berufshacker (Pentester) im c't-Gespräch aus dem Nähkästchen und erklärt, welche Tools er besonders gerne einsetzt – und wofür. *(rei@ct.de)* c't

***Weitere Hacking-Gadgets, Schutzmaßnahmen und Rechtliches:* ct.de/ytvk**

Angriff und Verteidigung

Die Hacking-Gadgets nutzen Schwachstellen in Technik und Unachtsamkeiten im Umgang mit selbiger aus. Die gute Nachricht ist, dass man sich vor den meisten Angriffen schützen kann, indem man einige grundlegende Sicherheitstipps befolgt. Meistens setzen die Geräte einen physischen Zugriff voraus: Ein Angreifer muss also zumindest kurzzeitig vor Ort sein, um sein Spionage-Werkzeug zu installieren. Überprüfen Sie insbesondere in öffentlich zugänglichen Räumen wie Büros von Zeit zu Zeit, ob Kabel oder Geräte an Ihren Rechner angeschlossen wurden. Bei einem USB-Zwischenstecker kann es sich um einen Keylogger handeln, ein vermeintliches DVI-Verlängerungskabel kann ein Screengrabber sein. Der kleine USB-Stöpsel auf der Rückseite Ihres PC-Towers ist eventuell gar nicht der Funkempfänger der Tastatur, sondern ein Mouse Jiggler, der verhindert, dass sich Ihr Rechner in Ihrer Abwesenheit automatisch sperrt. Aktivieren Sie den Sperrbildschirm stets manuell, ehe Sie den Arbeitsplatz verlassen – unter Windows erledigen Sie dies ganz leicht mit der Tastenkombination Windows+L.

Vor allem in Unternehmen sollten Sie auch fernab des Rechners auf Geräte unbekannten Ursprungs achten, die mit dem Netzwerk verbunden sind – auch wenn diese vermeintlich harmlos aussehen. Denn auch ein Raspberry Pi lässt sich als Netzwerkwanze nutzen. Vor sogenannten BadUSB- oder auch Rubberducky-Attacken, bei denen der Angreifer eine neue USB-Tastatur anmeldet, können Sie sich unter Windows mit Tools wie dem USB Keyboard Guard von G Data schützen, unter Linux helfen udev-Regeln weiter (siehe ct.de/ytvk). Weitere Angriffswege und Schutzmöglichkeiten finden Sie in c't 18/2017. Den Artikel haben wir gratis unter ct.de/ytvk bereitgestellt.