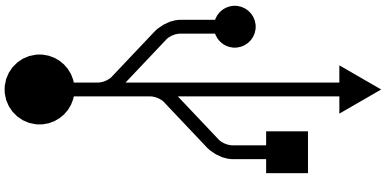
Kleine Waffenkunde

Die spannendsten Angriffstechniken der Hacking-Gadgets im Detail

Zahlreiche Hacking-Gadgets beherrschen komplexe IT-Angriffe, die sonst mit viel Aufwand und Vorwissen verbunden sind. Wir haben einige der interessantesten Attacken zusammengefasst und erklären, wie man sich vor ihnen schützen kann – sofern überhaupt möglich.

Von Ronald Eikenberg und David Wischnjak

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover



USB-HID-Angriff

Hacking-Gadgets:

USB Rubber Ducky, Bash Bunny, USB Armory, Digispark USB-Board

Beim USB-HID-Angriff gibt sich das Hacking-Gadget als Tastatur aus, um in Windeseile eine Reihe von Befehlen einzutippen. Das Gerät darf alles, was der angemeldete Nutzer darf – und das reicht zum Beispiel aus, um eine permanente Backdoor im System zu hinterlassen oder vertrauliche Dokumente und gespeicherte Passwörter abzugreifen. Dazu ruft das Hacking-Gadget etwa den Ausführen-Dialog von Windows auf, startet die Eingabeaufforderung mit Admin-Rechten, bestätigt den folgenden UAC-Dialog mit Alt+J und tippt anschließend ein Powershell-Skript ein, das den Passwort-Stealer „mimikatz“ aus dem Internet lädt und ausführt.

Im Netz findet man eine große Auswahl an Proof-of-Concept-Skripten, welche die Gefahren dieses Angriffsvektors zeigen. Einige wie das oben genannte Beispiel sind gefährlich, andere aber auch harmlos und verändern etwa nur den Desktop-Hintergrund, um den Kontrollverlust des Anwenders zu demonstrieren. Das attackierte System sieht lediglich eine neue USB-Tastatur und ziemlich viele, ziemlich schnelle Tastatureingaben. Welches Betriebssystem auf dem System läuft, ist unerheblich – das Angriffs-Skript muss lediglich darauf abstimmt sein. Über einen USB-OTG-Adapter lassen sich sogar Android-Geräte angreifen, zum Beispiel, um automatisiert alle verfügbaren PIN-Kombinationen durchzuprobieren.

Schützen kann man sich, indem man seinen Rechner in Abwesenheit sperrt und ein gesundes Misstrauen beim Umgang mit fremden USB-Sticks an den Tag legt. Verbinden Sie niemals gefundene USB-Speicher mit dem Rechner – schon gar nicht, wenn es sich um ein Windows-System handelt. Die meisten Angriffe zielen bekanntlich aufgrund der großen Verbreitung auf das Microsoft-Betriebssystem ab. Wenn es doch mal sein muss, sollten Sie ein System nutzen, das nicht im Firmennetz hängt und auf dem es ohnehin nichts zu holen gibt. Ferner besteht etwa unter Windows die Möglichkeit, die Installation neuer USB-Tastaturen zu unterbinden. Der einfache Weg ist das kostenlose Tool „USB Keyboard Guard“ von G Data (siehe ct.de/ybnn). Es hält zunächst Rücksprache mit dem Nutzer, ehe es eine neue Tastatur zulässt. Alternativ können Sie neue USB-Eingabegeräte auch mit Windows-Bordmitteln über eine Gruppenrichtlinie verbieten (siehe ct.de/ybnn).

Passwörter und Hashes übers Netzwerk klauen

Hacking-Gadgets:

Bash Bunny, LAN Tap Pro, LAN Turtle, USB Armory, WiFi Pineapple

Der Netzwerkverkehr ist für Angreifer ein lohnenswertes Ziel, schließlich gibt es hier einiges zu holen. Nach wie vor werden Zugangsdaten für Zugriffe auf Mail-Accounts, FTP-Server & Co. häufig im Klartext übertragen – auch wenn es die Nutzer inzwischen eigentlich besser wissen müssten. Zudem durchqueren die sogenannten NTLM-Hashes (NT LAN Manager) die Leitung. Diese sind gleichbedeutend mit dem Passwort des Windows-Benutzerkontos. Ein Angreifer kann sich damit im Namen seines Opfers gegenüber Diensten im lokalen Netz authentifizieren. Der einfachste Weg, um den Traffic kabelgebundener Netzwerkverbindungen passiv mitzulesen ist der **LAN Tap Pro**, den man einfach zwischen Rechner und Netzwerk hängt. Auch mit dem frei konfigurierbaren Accesspoint **WiFi Pineapple** kommt man leicht an den durchfließenden Traffic.

Ziemlich einfallsreich ist der Weg, den etwa der **Bash Bunny** einschlägt, um den Verkehr zu belauschen: Das Gerät ist weder mit einer RJ45-Buchse noch mit WLAN ausgestattet. Stattdessen zieht es den Traffic via USB ab. Und das funktioniert so: Es meldet sich als USB-Netzwerkkarte am Rechner und stattet ihn über DHCP mit einer trickreichen Netzwerkkonfiguration aus. So bringt es das System dazu, das neue Interface künftig gegenüber den bereits vorhandenen Schnittstellen zu priorisieren. Der Rechner versucht künftig, über Bash Bunny mit dem Netzwerk zu sprechen. Darüber antworten jedoch nicht die legitimen Gegenstellen, sondern das Pentesting-Tool „Responder“ (siehe ct.de/ybnn) auf alle Anfragen. Es ist auf das Abgreifen von Klartext-Zugangsdaten und Hashes spezialisiert und lauert darauf, dass der Rechner einen Authentifizierungsversuch startet. Ganz gleich, ob SMB, HTTP(S), LDAP, FTP, POP3, IMAP oder SMTP gefragt ist, der Responder antwortet und nimmt die Datenbeute bereitwillig entgegen.

Besonders gefährlich ist dieser Angriff, weil er auch dann funktioniert, wenn der Rechner gesperrt ist. Das laufende System unternimmt auch in diesem Zustand Login-Versuche, etwa um nach neuen E-Mails zu schauen. Schützen kann man sich vor einem solchen Attacke kaum. Selbst wenn die USB-Schnittstellen deaktiviert und mit Heißkleber zugeklebt wären, gäbe es da meist auch noch die Netzwerkschnittstelle. Wer zumindest Angriffe über USB-Netzwerkkarten abwehren möchte, kann etwa unter Windows über die Gruppenrichtlinien verhindern, dass sich neue USB-Netzwerkkarten am System anmelden dürfen (siehe ct.de/ybnn).

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover

NFC-Karten klonen

Hacking-Gadgets:
Proxmark3

RFID beziehungsweise NFC-Technik ist allgegenwärtig. In passiver Ausführung steckt sie in Personalausweisen, Zugangskarten, EC-Karten oder Autoschlüsseln. Das Funktionsprinzip ist meist gleich: Im Inneren befindet sich eine Spule, die an einen Mikrochip angeschlossen ist. Das Lesegerät erzeugt ein Magnetfeld, welches eine Spannung in der Spule induziert und so den Chip mit Energie versorgt. Der Chip nutzt die Spule als Antenne, um dem Lesegerät Informationen zu schicken, beispielsweise einen Identifikationscode. Die Reichweite beträgt bewusst nur wenige Zentimeter. Ersetzt man das Lesegerät aber durch das **Proxmark3**, lassen sich nicht nur die Reichweiten erhöhen, sondern auch allerhand Angriffe auf RFID-Technik fahren. Einige Smartcards und RFID-Tags bedienen sich bereits geknackter oder gar keiner Sicherheitskonzepte. Das gibt Angreifern die Gelegenheit, sie auszulesen, zu manipulieren oder zu klonen.

Insbesondere die weit verbreiteten Smartcards des Typs MIFARE Classic sind davon betroffen. Sie enthalten 1 oder 4 KByte an EEPROM-Speicher, der in Blöcke unterteilt ist und nur mit Kenntnis der jeweiligen Schlüssel gelesen und beschrieben werden kann. Durch eine Schwachstelle reicht allerdings die Kenntnis eines einzigen Schlüssels aus, um an die restlichen zu kommen („nested attack“). Ungenutzte Blöcke verwenden oft voreingestellte Schlüssel. Diese sind bereits bekannt und können schnell durchprobiert werden. So gelang es uns innerhalb von wenigen Minuten, eine Kantinenkarte auszulesen und auf eine zweite Karte zu kopieren. Falls das Guthaben lokal auf der Karte gespeichert wird, wäre es jetzt kein Problem, den Dump einer aufgeladenen Karte immer wieder neu einzuspielen und sich so Mahlzeiten zu erschleichen. Bei speziellen Smartcards aus China lässt sich auch die sonst unveränderliche Seriennummer (UID) ersetzen. Damit ist die geklonte Karte technisch nicht vom Original zu unterscheiden.

Das Problem betrifft auch viele Zugangskarten. In einem unachtsamen Moment könnte sich ein Angreifer eine Karte schnappen, klonen und unbemerkt wieder zurückbringen. Theoretisch reicht schon eine volle Bahn aus, um nah genug an eine NFC-Karte heranzukommen. Neuere Kartentypen wie beispielsweise die MIFARE DESFire EV1, die auch im neuen Personalausweis (nPA) zum Einsatz kommen, gelten dagegen aufgrund besserer Krypto-Verfahren bisher als sicher.

GSM knacken

Hacking-Gadgets:
HackRF One

Der Mobilfunkstandard GSM gilt nicht mehr als sicher. Schon seit Längerem setzen staatliche Dienste und Ganoven sogenannten IMSI-Catcher ein, die sich nicht nur zur lokalen Erfassung von Teilnehmerkennungen (IMSI) und Handy-Seriennummern (IMEI) eignen, sondern auch zum Abhören: Die Geräte können einen Man-in-the-Middle-Angriff fahren, um sich in die GSM-Verbindung einer Zielperson einzuklinken.

Dazu spannen die IMSI-Catcher eine Funkzelle auf, mit der sich das Mobiltelefon des Opfers bei ausreichend hoher Signalstärke automatisch verbindet. Die Funkzelle zwingt das Mobiltelefon, alle Daten unverschlüsselt (A5/0) zu übertragen, wodurch sich die Verbindung leicht belauschen lässt. Der IMSI-Catcher leitet die Daten an die legitime Funkzelle weiter, damit die Verbindung zustande kommen kann.

Viel gefährlicher, weil nicht nachverfolgbar, sind passive Lauschangriffe. Im Jahr 2009 errechnete der Sicherheitsforscher Karsten Nohl zwei Terabyte an Rainbow Tables, mit denen sich die bei GSM verwendete A5/1-Verschlüsselung innerhalb weniger Minuten offline knacken lässt. Die sogenannten A5/1-Tables sind online verfügbar. Laut gsmmap.org (Stand: Sommer 2017) verwenden in Deutschland immer noch über 40 Prozent der Funkzellen das A5/1- statt des sichereren A5/3-Verfahrens und sind damit potenziell angreifbar.

Damit brauchen Angreifer mit einem Software Defined Radio (SDR) wie dem **HackRF One** lediglich auf den richtigen Frequenzen zu lauschen, um anschließend mit dem Tool „Kraken“ SMS oder Sprach-Streams zu dekodieren. Und es geht noch billiger: DVB-T-Sticks mit RTL2832U-Chip lassen sich mit entsprechenden Treibern ebenfalls als SDR-Empfänger benutzen (RTL-SDR). Sie sind zwar nicht so präzise wie HackRF, kosten allerdings mit rund 20 Euro nur einen Bruchteil. Die Sticks decken immerhin das GSM-900-Band ab, nicht aber GSM-1800.

Da ab UMTS sich nicht nur das Handy gegenüber der Basisstation, sondern auch die Basisstation gegenüber dem Handy authentifizieren muss, sind Man-in-the-Middle-Angriffe dort nicht mehr ohne Weiteres möglich. Außerdem ist die verwendete Verschlüsselung stärker als bei GSM. Um sich zu schützen, sollte man daher möglichst auf GSM (2G) verzichten und stattdessen ausschließlich UMTS (3G) oder LTE (4G) verwenden. Dies ist jedoch mit Verzicht verbunden, denn die Netzabdeckung der einzelnen Netzbetreiber reicht dafür nicht immer aus. Des Weiteren bieten nicht alle Smartphones in den Einstellungen an, nur GSM abzuschalten. Daher bleibt oft nur abzuwarten, bis die restlichen 40 Prozent der Basisstationen auf das A5/3-Verfahren umgestellt wurden oder GSM gänzlich abgeschaltet wird.

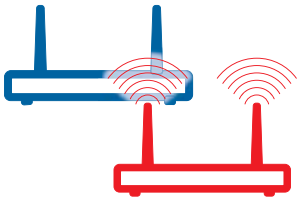
© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover

Reverse SSH Tunneling

Hacking-Gadgets:
LAN Turtle, WiFi Pineapple

Secure Shell (SSH) ist das Standardverfahren, um aus der Ferne auf ein Unix-System zuzugreifen. Damit ein System über SSH aus dem Internet erreichbar ist, muss eine Port-Weiterleitung eingerichtet sein, die dafür sorgt, dass der Router Anfragen von außen, die auf einen bestimmten Port eingehen, an ein System in seinem lokalen Netz durchreicht. Das stellt einen Angreifer, der ein Gerät wie die **LAN Turtle** im lokalen Netz platziert, vor ein Problem, wenn es ihm nicht gelingt, den Router oder die Firewall umzukonfigurieren. Sobald er den Ort des Geschehens verlässt, kann er nicht auf die Hacking-Hardware zugreifen. Allerdings gibt es einen einfachen Trick, wie er aus der Ferne trotzdem Zugriff erlangen kann: Er baut nicht darauf, dass sein Gerät aus dem Internet erreichbar ist, sondern nutzt ausgehende Verbindungen, die normalerweise gar nicht oder nur wenig eingeschränkt sind.

Die **LAN Turtle** etwa kann mit dem Tool „AutoSSH“ einen sogenannten Reverse SSH Tunnel aufbauen. Dabei stellt das Gerät eine ausgehende SSH-Verbindung zu einem Server im Internet her. Der Angreifer verbindet sich ebenfalls mit dem Server und kann über diesen fortan beliebige Befehle an das Gerät im fremden Netz schicken. Admins können dies nur schwer unterbinden, da der Angreifer seine SSH-Verbindung etwa über den erlaubten Port 80 für HTTP aufbauen kann. Um solche rückwärts gerichteten Verbindungen zu unterbinden, ist eine sogenannte Deep Packet Inspection (DPI) notwendig. Dabei achtet etwa die Firewall darauf, dass über Port 80 tatsächlich HTTP gesprochen wird – und nicht das ganz anders aufgebaute SSH. Das ist jedoch in der Praxis leichter gesagt, als getan.



Böser WLAN-Zwilling

Hacking-Gadgets:
WiFi Pineapple, WiFi Deauther

Angriffe auf WLAN sind sehr vielfältig. Das Knacken von WLAN-Netzen mit veralteter Verschlüsselung, Lücken in WPS oder berechenbaren Standardpasswörtern ist längst keine hohe Kunst mehr. Anstatt in fremde Netze einzubrechen, können Angreifer ihre Ziele auch einfach zu sich locken. Mit geeigneter Hardware wie dem **WiFi Pineapple** lassen sich besonders einfach WLAN-Hotspots einrichten und damit Man-in-the-Middle-Angriffe durchführen. Am naheliegendsten ist es, den Pineapple über USB, Ethernet oder ein anderes WLAN-Netz mit dem Internet zu verbinden und gleichzeitig ein eigenes Netz mit einem vielversprechenden Namen wie „Telekom“ oder „Vodafone Hotspot“ aufzuspannen. War der Client zu einem früheren Zeitpunkt mit einem gleichnamigen Netz verbunden, wird er die Verbindung sogar automatisch herstellen. Noch raffinierter ist die KARMA-Attacke: Dabei lauscht der Pineapple nach den sogenannten Probe-Requests der umliegenden WLAN-Clients. Damit suchen die Clients nach Netzen, mit denen sie bereits zuvor verbunden waren. Empfängt ein Accesspoint in Funkreichweite einen solchen Request, antwortet er mit einem „Hallo, hier bin ich!“, sofern er sich für den gesuchten Netzwerknamen (SSID) zuständig fühlt.

Auch der Pineapple antwortet auf Probe Request – allerdings auf alle. Fragt ein Client nach dem Netz „Heise-Besucher“, behauptet der Pineapple, dass er zuständig ist und der Client baut eine Verbindung zu dem bösen Zwillingsnetz auf. So bekommt jeder Client sein eigenes, ihm vermeintlich bekanntes WLAN-Netz vorgegaukelt. Den Traffic der Clients kann ein Angreifer anschließend beliebig mitschneiden, umleiten oder manipulieren. Phishing-Seiten lassen sich in dieser Position ebenfalls leicht einrichten und dank IP-Umleitungen mit „dnsspoof“ werden die von den WLAN-Nutzern auch garantiert besucht – egal, welche URLs eigentlich angesteuert wurden. Der Angreifer kann seine Opfer außerdem auf mit Exploits bestückte Websites locken. Da alle Clients im eigenen lokalen Netzwerk sind, kann er sie darüber hinaus mit dem Angriffs-Tool „Metasploit“ ungestört auf Schwachstellen abklopfen.

Falls sich die Clients nicht freiwillig mit dem Zwillingsnetz verbinden wollen, weil sie bereits in ein anderes WLAN-Netz eingebucht sind, kann sie der Angreifer auch mit Nachdruck dazu überreden. Der WLAN-Standard sieht sogenannte Deauthentication-Pakete vor, mit denen ein Accesspoint den mit ihm verbundenen Clients signalisiert, dass die Verbindung getrennt werden soll. Die meisten Clients trennen die Verbindung anschließend. Diese speziellen Pakete sind nicht verschlüsselt und können leicht gefälscht werden. Verschickt der Angreifer einige Deauthentication-Pakete mit der MAC-Adresse eines legitimen Accesspoints als Absender, kappen dessen Clients die Verbindung. Der **WiFi Deauther** attackiert auf diese Weise beliebige Netze sogar auf Knopfdruck und macht sie unbenutzbar. Im Anschluss suchen die Clients nach dem nächstbesten Netz und finden den bösen Zwilling des Angreifers.

WLAN-Hotspots sollte man also mit Vorsicht genießen, da sie nicht vertrauenswürdig sind. Nutzen Sie lieber eine Mobilfunkverbindung oder schützen Sie sich in einem öffentlichen WLAN zumindest durch einen verschlüsselten VPN-Tunnel.

(rei@ct.de) c't

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover