„Mit diesen Gadgets kann jeder angreifen“

Sicherheitsforscher Tobias Scheible über Gefahren und Nutzen von Hacking-Gadgets

Hacking-Gadgets sind ein kontroverses Thema: Sie helfen Pentestern beim Aufspüren von Sicherheitslücken – können in den falschen Händen aber auch große Schäden anrichten. Der Sicherheitsforscher Tobias Scheible hat ein besonderes Faible für die angriffslustigen Geräte und stellt sie im Rahmen von Vorlesungen, Seminaren und Workshops vor. Wir haben mit ihm über Gefahren und Nutzen der Hacker-Werkzeuge gesprochen.

Von Ronald Eikenberg

c’t: Kommen die Hacking-Gadgets, die wir in c’t vorstellen, bei tatsächlichen Angriffen zum Einsatz?

Tobias Scheible: Definitiv – gerade die jüngste Vergangenheit hat gezeigt, dass Angreifer solche Geräte etwa für Ransomware-Angriffe einsetzen. So hat das FBI in den USA vor einer Bande von Cyberkriminellen gewarnt, die präparierte USB-Sticks an Unternehmen geschickt hat. In einer Angriffswelle gaben die Täter vor, es handele sich um Corona-Richtlinien, in einer weiteren ahmten sie Lieferungen von großen Elektronikhändlern nach – inklusive bedruckter Verpackung mit passendem Paketklebeband und fingiertem Lieferschein.

Beim Einstecken der Sticks melden sie sich als USB-Tastatur am Rechner (BadUSB-Angriff) und infizierten die Systeme mit einem Kryptotrojaner, der die Daten der Unternehmen verschlüsselt. Weiterhin gibt es auch immer wieder Berichte über gefundene Keylogger, unter anderem bei Zeitungen und sogar bei der Polizei. Mit einem USB-Killer, der den angeschlossenen Rechner durch Überspannung zerstört, hat eine Person zudem viele Computer lahmgelegt.

c’t: Das klingt besorgniserregend. Wie oft kommt das vor?

Scheible: Anders als bei großen Schadsoftware-Kampagnen gibt es nur sehr wenige Berichte darüber, da die Angreifer immer nur einzelne Unternehmen oder Personen attackieren. Die tatsächliche Anzahl der Angriffe kann man daher gar nicht einschätzen. Gleichzeitig fliegen viele Angriffe nicht auf, etwa wenn der Täter den Keylogger nach einer bestimmten Zeit wieder mitnimmt, bevor jemand das Gerät entdeckt. Die Dunkelziffer an erfolgreichen und nie erkannten Angriffen mit Hacking-Gadgets ist daher hoch.

c’t: Wird man mit den Hacking-Gadgets auf Knopfdruck zum Hacker oder sind weiterhin gewisse Vorkenntnisse erforderlich?

Scheible: Viele dieser Geräte sind sehr einfach und ohne spezielles Know-how zu bedienen. Einen USB-Keylogger zum Beispiel schließt man einfach an, konfigurieren oder programmieren muss man ihn zuvor nicht. Genauso einfach funktionieren USB-Killer, die Rechner zerstören: anschließen reicht. Allerdings gibt es auch komplexere Tools, die raffinierte Angriffe durchführen können. Diese muss man speziell konfigurieren, was einiges an Wissen und Erfahrung voraussetzt.

c’t: Wann sind Sie auf die Hacking-Gadgets aufmerksam geworden und welches war Ihr erstes?

Scheible: Das müsste so 2014 gewesen sein, als ich auf das Peensy-Projekt von Offensive Security gestoßen bin. Zu dieser Zeit wurde auch auf der Black-Hat-Konferenz in den USA das BadUSB-Konzept vorgestellt. Dabei ging es um die Manipulation der Firmware von normalen USB-Sticks. Mit der „Teensy Penetration Testing Payload“ (Peensy) konnte man dies auch mit einem Teensy realisieren. Der Teensy ist ein für seine Größe sehr leistungsstarkes USB-Development-Board mit guter Dokumentation. Den Angriff habe ich dann in der Lehre mit Studenten durchgeführt.

Der Sicherheitsforscher Tobias Scheible arbeitet mit Hacking-Gadgets und klärt über ihr Gefahrenpotenzial auf. Ein Verbot der Hacker-Werkzeuge hält er jedoch für den falschen Schritt, da nur die Angreifer davon profitieren würden.

c't: Ist es problematisch, dass jeder diese Geräte einfach so im Internet bestellen kann?

Scheible: Grundsätzlich ja – aber auch hier gilt das gleiche Prinzip wie in anderen Bereichen der IT-Sicherheit. Würden diese Geräte nicht so einfach zu bestellen sein, würde es sie trotzdem geben. Dann vielleicht in Form von Anleitungen zum Selbstbauen oder als Produkte auf dem Schwarzmarkt. Oftmals kommen auch Standardkomponenten zum Einsatz, die nur mit einer angepassten Software ihre spezielle Funktionsweise bekommen. Diese Standardkomponenten könnte man gar nicht verbieten.

Auf der anderen Seite ist es aber auch immer wichtig, dass Sicherheitsbeauftragte die Möglichkeit haben, ihre eigenen Systeme zu testen. Wäre der Verkauf verboten, würden Angreifer trotzdem rankommen, aber die Personen auf der Gegenseite, die ihre Systeme schützen möchten und müssen, nicht mehr. Viele Beispiele, auch in der physischen Welt, haben gezeigt, dass ein Verbot die Sicherheit nicht erhöht.

c't: Muss man im Zweifel also darauf vorbereitet sein, unfreiwillig Bekanntschaft mit den Hacking-Geräten zu machen?

Scheible: Die bisher bekannten Fälle zeigen, dass häufig Innentäter diese Hacking-Geräte einsetzen. Das heißt, dass Angreifer zum Beispiel externes Personal anheuern, zum Beispiel schlecht bezahlte Reinigungskräfte, Geräte an einen Rechner anzuschließen. Oder dass ehemaliges Personal oder frustrierte Mitarbeiter Hacking-Gadgets einsetzen, um sich zu rächen oder durch Ausspähen von Informationen versuchen, sich einen Vorteil zu verschaffen.

Und da ein Großteil dieser Gadgets so einfach zu bedienen ist, kann damit auch jeder angreifen. Daher gibt es einige Szenarien für fast jedes Unternehmen, bei dem es mit Hacking-Geräten attackiert werden kann.

c't: Sind die IT-Abteilungen von Behörden, Unternehmen & Co. auf die Gefahren vorbereitet?

Scheible: Die allgemeine Vorbereitung gegen solche Angriffe sieht eher schlecht aus. Zwar wissen Sicherheitsbeauftragte oft von diesen Gefahren, aber das Umsetzen von Schutzmaßnahmen ist natürlich immer aufwendig. Häufig wird kein umfassender Schutz der IT-Systeme umgesetzt, sondern es werden nur die wichtigsten Gefährdungen betrachtet.

Und hier schätzen Sicherheitsbeauftragte die Risiken durch Ransomware oft höher ein als durch Innentäter. Wie in vielen Bereichen der IT-Sicherheit gibt es auch hier kein Erkenntnis-, sondern ein Handlungsdefizit.

c't: Welche Angriffsvektoren werden häufig vernachlässigt?

Scheible: Die Verfügbarkeit von frei zugänglichen Schnittstellen ist in meinen Augen ein Angriffsvektor, der häufig unterschätzt wird. Dazu gehören allein schon die Schnittstellen, die außerhalb des Gebäudes geführt werden, wie vernetzte Klingelanlagen oder Beleuchtungssysteme und selbst Überwachungskameras, die neben den genutzten Anschlüssen noch weitere Schnittstellen bieten. Hierüber können sich potenzielle Angreifer einen Zugang zu den Systemen verschaffen oder allein schon mit einem Stromschlag größere Bereiche lahmlegen.

Im Inneren des Gebäudes gibt es oft in vielen Bereichen mit Publikumsverkehr Netzwerkdosen, die zum Teil Zugang zu internen Systemen bieten. Access-Points oder Drucker sind so platziert, dass Angreifer daran leicht Hacking-Gadgets anschließen können, die den gesamten Netzwerkverkehr mitschneiden. Solche kleinen Tools können dabei so platziert werden, dass sie niemandem auffallen.

c't: Wie kann man sich vor solchen Angriffen schützen?

Scheible: Da die Bandbreite der Angriffsvektoren sehr groß ist, gibt es nicht nur die eine Lösung, sondern mehrere Maßnahmen für einen effektiven Schutz. Grundsätzlich sollte man den physischen Zugriff auf die Systeme beschränken, zum Beispiel durch bauliche Maßnahmen, damit ein Angreifer nicht einfach an die Schnittstellen herankommt. Sind Systeme frei zugänglich, sollte man die nicht genutzten Schnittstellen deaktivieren oder verschließen.

Auf Softwareseite sollte man USB-Geräte verbieten oder zumindest nicht automatisch einbinden. Im Netzwerkbereich empfiehlt sich ein Zero-Trust-Ansatz, dazu gehört auch, interne Verbindungen zu verschlüsseln und Anomalien zu detektieren. Funkverbindungen sollten überwacht werden, ob es Unterbrechungen gibt oder neue Signalquellen auftauchen, um potenzielle Angriffe zu erkennen. Eine Unterbrechung des WLAN-Signals einer Überwachungskamera ist mit dem Auslösen eines Alarms gleichzusetzen.

c't: Wie wichtig ist die gezielte Aufklärung von Mitarbeitern über die Risiken von Hacking-Hardware und anderen IT-Angriffen?

Scheible: Da technische Sicherheitsmaßnahmen keinen kompletten Schutz gegen Hacking-Gadgets bieten, ist Sicherheitsbewusstsein essenziell. Dazu gehört sowohl die Wahrnehmung, dass solche Angriffe existieren, als auch der Umgang mit unbekannten Geräten. Zum Beispiel sollte das Personal geschult werden, dass es den Inhalt von gefundenen USB-Sticks nicht selbst anschaut, um den Besitzer zu finden, sondern die Fundstücke der IT-Abteilung übergibt.

Dazu gehört auch zu vermitteln, dass man Bestellungen, die man nicht selbst beauftragt hat, und Geschenke wie USB-Tassenwärmer oder -Ventilatoren nicht einfach an Rechner anschließt. Gleichzeitig eignen sich die Hacking-Gadgets aber auch optimal für Schulungen, da die Teilnehmer hier die Bedrohungen in die Hand nehmen können und die Wirkungsweise und daraus hervorgehende Gefährdungen direkt sehen.

c't: Ist es sinnvoll, selbst mit Hacking-Gadgets herumzuexperimentieren, um deren Funktionsweise zu verstehen und passende Schutzmaßnahmen treffen zu können?

Scheible: Auf jeden Fall. Einfache Tools sind günstig und leicht zu erwerben – gerade im BadUSB-Bereich. Damit kann man dann die eigenen Systeme testen und anschließend entsprechende Gegenmaßnahmen planen. Und auch gegenüber Kollegen oder Vorgesetzten, gerade wenn es um das Thema Budget geht, haben diese Hacking-Gadgets einen Nutzen. Hier wird das Thema IT-Sicherheit als physischer Gegenstand sichtbar und jeder kann nachvollziehen, dass eine einfache Handlung zu einem Sicherheitsvorfall führen kann. *(rei@ct.de)* c't