Hacking & Security

Das umfassende Handbuch

DAS VORWORT

Vorwort

Die Berichterstattung über Hacking-Attacken und Sicherheitslücken, die Millionen, mitunter Milliarden Geräte betreffen, ist allgegenwärtig. Sie hat die Themen »Hacking« und »IT-Security« immer stärker in den Vordergrund gerückt und auch unter »Normalanwendern« ein Bewusstsein dafür geschaffen, dass die Sicherheit der IT-Infrastruktur jeden betrifft.

Viele Computer-, Smartphone- oder ganz allgemein Internetanwender drohen angesichts der vielfältigen Risiken zu resignieren. Dass man »ordentliche« Passwörter verwenden und regelmäßig Updates einspielen sollte, ist den meisten klar – aber darüber hinaus fühlen sich Anwender den Gefahren der zunehmenden Digitalisierung weitgehend schutzlos ausgeliefert.

Tatsächlich ist es primär die Aufgabe von Administratoren, IT-Verantwortlichen und Software-Entwicklerinnen, für mehr Sicherheit zu sorgen. Immer strengere gesetzliche Rahmenbedingungen und der mit Sicherheitslücken verbundene Image-Verlust zwingen Firmen, sich mit Sicherheit intensiver auseinanderzusetzen. Es reicht nicht mehr aus, dass ein Gerät ganz einfach funktioniert, dass Software »schick« aussieht oder dass Smartphones in stylische, immer dünnere Gehäuse verpackt werden. Die Hard- und Software samt der dazugehörigen Server- und Cloud-Infrastruktur muss auch sicher sein – zumindest so sicher, wie es technisch aktuell möglich ist.

Was Hacking mit Sicherheit zu tun hat

Als »Hacking« bezeichnet man umgangssprachlich die Suche nach Wegen, die Sicherheitsmaßnahmen eines Programms oder Systems zu umgehen oder bekannte Sicherheitslücken auszunutzen. Das Ziel besteht in der Regel darin, private bzw. geheime Daten auszulesen oder zu manipulieren.

»Hacking« hat oft einen negativen Kontext, aber das stimmt so nicht: Wenn eine Firma einen sogenannten *Penetration-Test* beauftragt, um durch externe Personen die Sicherheit der eigenen IT-Infrastruktur zu überprüfen, dann bedienen sich die Penetration-Tester derselben Werkzeuge wie kriminelle Hacker. Ähnliches gilt für Sicherheitsforscher, die versuchen, neue Schwachstellen zu finden. Das erfolgt oft im Auftrag von oder in Zusammenarbeit mit großen IT-Firmen, Universitäten oder staatlichen Sicherheitsstellen. Ob ein Hacker »gut« oder »böse« ist, hängt davon ab, wie er oder sie sich nach der Entdeckung einer Schwachstelle verhält.

Wenn Sie als Administrator oder als IT-Verantwortliche für die Sicherheit eines Systems zuständig sind, müssen Sie die Werkzeuge kennen, die Hacker anwenden. Damit Sie sich bzw. Ihre Firma verteidigen können, müssen Sie wissen, wie Angreifer agieren. Insofern ist es uns in diesem Buch ein Anliegen, Ihnen einen Überblick über die wichtigsten Hacking-Tools und -Arbeitstechniken zu geben. Allerdings machen wir an dieser Stelle nicht Schluss. Vielmehr geht es uns in der Folge darum, wie Sie sich gegen Angreifer wehren können, welche Verteidigungsmaßnahmen Sie ergreifen können, wo Sie die Konfiguration Ihrer Systeme verbessern können. Oder anders formuliert:

Für dieses Buch ist Hacking der Weg, aber nicht das Ziel.
Das Ziel ist es, eine höhere Sicherheit zu erreichen.

Über dieses Buch

In diesem Werk möchten wir eine breit angelegte Einführung in die Themenfelder »Hacking« und »IT-Security« geben. Angesichts von fast 1.300 Seiten klingt es vielleicht wie ein Understatement, wenn wir von einer »Einführung« sprechen. Tatsächlich ist es aber so, dass sowohl Hacking als auch Security unermesslich große Wissensgebiete sind.

Beinahe zu jedem Thema, das wir in diesem Buch aufgreifen, könnte man gleich ein eigenes Buch schreiben. Hinzu kommen all die Spezialthemen, auf die wir in unserem Buch gar nicht eingehen. Kurzum: Erwarten Sie nicht, dass dieses Buch allumfassend ist, dass Sie mit der Lektüre dieses Buchs bereits ein Hacking- und Security-Experte sein werden.

Dessen ungeachtet muss es einen Startpunkt geben, wenn Sie sich mit Hacking und Security auseinandersetzen möchten. Diesen Startpunkt versuchen wir hier zu bieten. Konkret setzen wir uns nach einer Einführung zum Themenumfeld mit den folgenden Aspekten auseinander:

- Kali Linux (Distribution mit einer riesigen Sammlung von Hacking-Werkzeugen)
- Hacking-Tools (`nmap`, `hydra`, Metasploit, Empire, OpenVAS, SET, Burp, Wireshark usw.)
- Hacking lernen anhand von virtuellen Testsystemen (Basic Pentesting, Mr. Robot, pwn.college, OWASP Juice Shop etc.)
- Bug-Bounty-Programme
- Offline Hacking, Zugriff auf fremde Notebooks/Festplatten
- IT-Forensik
- Passwort-Hacking, sicherer Umgang mit Passwörtern
- WLAN, Bluetooth, Funk (inklusive Pwnagotchi und Flipper Zero)
- USB-Hacking und -Sicherheit, Hacking-Gadgets
- Durchführung externer Sicherheitsüberprüfungen

- Penetration-Testing
- Basisabsicherung: Windows und Linux, Active Directory und Samba
- Webanwendungen angreifen und absichern
- Intrusion-Detection-Systeme: Snort und Wazuh
- Exploit-Grundlagen: Buffer-Overflows, Fuzzing, Heap Spraying, Mikroarchitektur-Schwachstellen (Meltdown und Spectre)
- Hacking von KI-Anwendungen, Prompt Injections
- Cloud-Sicherheit: Amazon S3, Nextcloud/ownCloud, Microsoft 365
- Hacking und Security von Smartphones und anderen Mobile Devices
- Absicherung und sichere Entwicklung von IoT-Geräten

Die Breite der Themen erklärt, warum dieses Buch nicht einen Autor hat, sondern gleich zwölf. Eine kurze Vorstellung unseres Teams finden Sie am Ende des Buchs.

Neu in der 4. Auflage

Für die hier vorliegende Auflage haben wir das Buch umfassend aktualisiert und um viele neue Inhalte erweitert. Besonders erwähnen möchten wir:

- Hacking lernen (neues Kapitel mit Fokus auf den Hacking-Einstieg)
- Absicherung von Samba (Kapitel grundlegend überarbeitet und erneuert)
- Absicherung von Microsoft 365 (neues Kapitel)
- Hacking von KI-Anwendungen (neues Kapitel)
- Absicherung von Docker, Geoblocking mit Firewalls (nft)
- SIEM-Systeme (Wazuh, Microsoft Sentinel)

Die wohl größte Neuerung im Vergleich zur Auflage aus dem Jahr 2022 besteht darin, dass KI-Tools damals noch exotisch waren, heute aber allgegenwärtig sind. KI-Tools werden sowohl von Hackern (zum Angriff) als auch zur Verbesserung der Sicherheit (zur Verteidigung) genutzt. Viele Kapitel enthalten Tipps und Hinweise zur Anwendung von KI-Werkzeugen.

Zielgruppe

Wir richten uns mit diesem Buch an Systemadministratoren, Sicherheitsverantwortliche, Entwicklerinnen sowie ganz allgemein an IT-Fachkräfte, die bereits über ein gewisses Grundwissen verfügen. Um es überspitzt zu formulieren: Sie sollten zumindest wissen, was die PowerShell oder ein Terminal ist. Und Sie müssen bereit sein, betriebssystemübergreifend zu denken: Weder Hacking noch die IT-Sicherheit beschränkt sich auf Windows- oder Linux-Rechner.

Nicht im Fokus stehen dagegen reine IT-Anwender. Natürlich ist die Schulung von Computeranwendern ein unverzichtbarer Aspekt, um die IT-Sicherheit sowohl zu

Hause als auch in Unternehmen zu verbessern. Eine Zusammenstellung von mehr oder weniger trivialen Regeln und Tipps, wie Computer, Smartphones und das Internet im Allgemeinen sicher und verantwortungsvoll zu nutzen sind, erscheint uns in diesem technisch orientierten Buch aber nicht zielführend.

Los geht's!

Lassen Sie sich nicht von der Größe des Themengebiets abschrecken! Wir haben versucht, unser Buch in überschaubare Kapitel zu gliedern. Die meisten davon können Sie weitgehend unabhängig voneinander lesen und sich so Schritt für Schritt einarbeiten, Hacking-Expertise gewinnen und ein besseres Verständnis dafür entwickeln, wie Sie Ihre eigenen Systeme besser absichern können. Sie werden schnell feststellen, dass eine intensivere Auseinandersetzung mit Hacking- und Security-Techniken ungemein faszinierend ist.

Wir hoffen, mit unserem Buch dazu beizutragen, die IT-Sicherheit in Zukunft besser zu managen, als dies bisher der Fall war!

Roland Aigner, Klaus Gebeshuber, Thomas Hackner, Stefan Kania,
Peter Kloep, Michael Kofler, Frank Neugebauer, Tobias Scheible,
Aaron Siller, Matthias Wübbeling, Paul Zenker und André Zingsheim

Grußwort

IT-Sicherheit ist ein Thema, an dem niemand vorbeikommt. Insbesondere Ransomware- und Phishingangriffe sind eine enorme Bedrohung. 2024 waren 74 % der Firmen in Deutschland von Datendiebstahl betroffen, meldet der Bitkom. Und der Gesamtschaden durch Cybercrime steigt immer weiter an.

Die Devise heißt also: IT-Sicherheit muss auf der Prioritätenliste ganz nach oben – bei Unternehmen, Organisationen und im öffentlichen Dienst. Aber auch bei Privatanwendern sollte die IT-Sicherheit eine prominentere Rolle spielen.

Angriffe auf IT-Systeme sind für die Täter sehr attraktiv. Von Online-Zahlungen und Geschäftsprozessen über cloudbasierte Dienste bis hin zum Internet of Things (IoT) und Operational Technology (OT) – digitale Infrastrukturen bieten ein großes Angriffsfeld. Die Anonymität des Netzes senkt die Hemmschwelle dafür, sich an entsprechenden Angriffen zu versuchen.

Wer beim Thema IT- und Datensicherheit spart, der ist schlecht beraten. Wem es dagegen gelingt, den eigenen Mitarbeitenden beizubringen, wie »Hacker« denken und agieren, der ist einer robust abgesicherten IT-Infrastruktur schon einen großen Schritt näher. Wer die Angreifer versteht, ist der bessere Verteidiger.

Dieses Kompendium geht mit seinem Anliegen deshalb genau in die richtige Richtung: »Für dieses Buch ist Hacking der Weg, aber nicht das Ziel. Das Ziel ist es, eine höhere Sicherheit zu erreichen«, heißt es im Vorwort. Ich kann dies nur unterstützen: Als Geschäftsführer der SySS GmbH trage ich die Verantwortung für 100 IT Security Consultants, die tagtäglich nichts anderes tun, als auf Wunsch die Systeme unserer Kunden zu »hacken«.

Solche Penetrationstests spüren schnell und effizient Sicherheitslücken auf. Die IT-Verantwortlichen können diese dann beheben – bevor illegale Hacker sie ausnutzen. Gleichzeitig zeigt ein solcher Test und der dazugehörige Abschlussbericht unseren Kunden aber auch im Detail, wie wir vorgehen, um Schwachstellen aufzuspüren und auszunutzen.

Genau solches Wissen ist von unschätzbarer Bedeutung, wenn es darum geht, die eigenen Systeme immer sicherer zu machen. Das Buch »Hacking & Security« stellt dieses Know-how für die Praxis zur Verfügung. Ich kann jedem, der beruflich mit IT-Sicherheit zu tun hat, die Lektüre nur wärmstens empfehlen. Bleiben Sie den »bösen« Hackern immer den entscheidenden Schritt voraus.

Sebastian Schreiber, Geschäftsführer SySS GmbH