Kapitel 1

Wie man »Hacker« wird

Die Themen in diesem Kapitel:

- Was wir mit »Hacker« meinen
- Was Sie von diesem Buch erwarten können
- Die aktuelle Gesetzeslage verstehen
- Zusammenfassung
- FAQs

1.1 Einführung

Dieses Buch vermittelt Fähigkeiten, die für den Angriff auf Computersysteme erforderlich sind. Wenn Sie diese Aussage schockiert, können wir nur davon ausgehen, dass Sie sich noch nie mit den legitimen Gründen für Hackerangriffe auseinander gesetzt haben. Dazu zählen Sicherheitstests, Verbraucherschutz, Bürgerrechte, militärische Interessen und der politische »Hacktivismus«. Allerdings werden wir uns in diesem Buch lediglich mit den Techniken und nicht mit den Gründen befassen.

In diesem Buch wird das Wort »Hacker« ganz bewusst angewandt. Natürlich wissen wir, dass das Wort »Hacker« für unterschiedliche Menschen auch unterschiedliche Bedeutungen haben kann, und darauf gehen wir in diesem Kapitel ein. Wir werden außerdem erläutern, wie das Buch organisiert ist und welche Vorkenntnisse Sie benötigen, um die im weiteren Verlauf beschriebenen Techniken verstehen zu können. In diesem Kapitel untersuchen wir außerdem Hacking, Reverse-Engineering, Kopierschutz und die relevante Gesetzgebung aus Sicht des Durchschnittsbürgers. Es wäre ja unverantwortlich, wenn wir Ihnen dieses neue Spielzeug einfach so in die Hände drücken, ohne auf die möglichen Konsequenzen hinzuweisen.

1.2 Was wir mit »Hacker« meinen

Als ich noch klein war, bestand die Online-Welt (soweit ich sie kannte) aus Bulletin-Board-Systemen (BBSe). Viele BBSe enthielten Textdateien, die eine Variation des Themas »Wie man Hacker wird« behandelt haben. Fast alle diese Dateien waren

© by verlag moderne industrie Buch AG & Co. KG, Bonn

nutzlos: Sie enthielt Tipps wie »Versuchen Sie es mit Standardpasswörtern« oder »Drücken Sie STRG-C, um festzustellen, ob Sie aus dem Programm ausbrechen können«. Dass dieses Kapitel »Wie man Hacker wird« heißt, zeugt von meiner skurrilen Art, diese Dateien in Ehren zu halten. Für mich waren sie eine Inspiration – das heißt, sie haben mich dazu inspiriert, eine vernünftige Ansammlung von Hacking-Tipps zu schreiben.

Was meinen wir also mit »Hacker«? Damit meinen wir jemanden, der die Sicherheitsmaßnahmen von Computern oder Computernetzwerken umgeht. Das Wort »Hack« wird aber auch gebraucht, um ein schlaues oder schnelles Programm zu beschreiben. Das Problem ist, dass im wirklichen Leben (in den Nachrichten, im Gespräch, in Mailing-Listen und ähnlichem) das Wort »Hack« oder »Hacker« von vielen Menschen gebraucht wird, ohne dass sie verdeutlichen, was sie damit wirklich meinen. Man muss die Perspektive des Gesprächspartners oder Autors quasi aus dem Kontext erkennen oder indem man zwischen den Zeilen liest. Auch dieses Buch ist keine Ausnahme. Darüber hinaus benutzen wir Autoren manchmal Begriffe wie »Skript Kiddie«, um etwas zu bezeichnen, das von einer der möglichen Bedeutungen von Hacker abgeleitet wurde. Wenn Sie sich mit dem Begriff in Zusammenhang mit der beschriebenen Aktivität nicht einverstanden sind, laden Sie die Autoren ganz herzlich dazu ein, beim Lesen stattdessen ein Wort Ihrer Wahl einzusetzen und so zu tun, als hätten die Autoren dieses Wort von vornherein gewählt.

Wenn Sie einen philosophischen Diskurs zum Wort Hacker lesen möchten, besuchen Sie bitte die Syngress Solutions-Website und laden Sie sich eine elektronische Kopie von Kapitel 1 der Urfassung der Erstausgabe herunter, die den Titel »Politics« trägt. Dort habe ich mich recht ausschweifend zur Bedeutung des Wortes »Hacker« ausgelassen. In dieser Ausgabe habe ich Ihnen diese Diskussion erspart – sollte Sie sich jedoch die Mühe machen, die alte Definition zu finden, können Sie im nachhinein nicht behaupten, ich hätte Sie nicht gewarnt.

1.2.1 Motivation des Hackers

Wenn es Sie interessiert, warum sich jemand ausgerechnet mit Hackertechniken auseinander setzen möchte, verweise ich auch hier an die oben genannte Quelle für die Erstausgabe (wo Sie auch den langen Diskurs über Hacker finden). Dort finden Sie eine lange Version aller Begründungen. Wenn Ihnen allerdings eine kurze Erklärung genügt, dann lautet diese: »Angriff ist die beste Verteidigung«. Mit anderen Worten ist der einzige Weg, einen Hacker aufzuhalten, wie ein Hacker zu denken – wenn Sie Ihre eigenen Systeme nicht angreifen, müssen Sie sich letztendlich fragen, wer sie dann denn angreifen wird. Diese Sätze mögen etwas abgedroschen klingen, aber sie verkörpern die Philosophie, die nach unserem Dafürhalten den besten Schutz für unsere eigenen Systeme (oder die unseres Arbeitgebers, Kunden und so weiter) bietet.

© by verlag moderne industrie Buch AG & Co. KG, Bonn

Notizen aus dem Underground

»Wir beschäftigen keine Hacker«

Vielleicht ist es Ihnen zu Ohren gekommen, dass verschiedene Unternehmen in der Sicherheitsbranche behaupten, sie würden »keine Hacker beschäftigen«. Hier wird impliziert, dass die Unternehmen damit Kriminelle meinen – ungeachtet dessen, ob sich diese gebessert haben oder noch aktiv sind. Diese Haltung wird damit begründet, dass manche Kunden die Geschäftsbeziehung abbrechen, wenn sich das Unternehmen dazu bekennt, Personen aus diesem Umfeld zu beschäftigen. Der vorgeschobene Grund ist wohl, dass man die Sicherheit eines Kundensystems nicht in die Hände eines Kriminellen geben kann. In Wirklichkeit geht es aber um das Prinzip. Manche Menschen möchten es unbedingt vermeiden, dass ein krimineller Hacker so etwas wie eine Belohnung für seine illegalen Aktivitäten bekommt.

In manchen Fällen geht das Unternehmen jedoch von der gegensätzlichen Prämisse aus: Wenn der fragliche Kriminelle durch seine Aktivitäten berühmt (oder berüchtigt) geworden ist, wird sich die Presse sicherlich für die Einstellung interessieren. Ob dies für das Geschäft nun positiv oder negativ ist, hängt natürlich vom Business-Modell ab – bei einem Dienstleistungsunternehmen aus dem Bereich Managed Services ist mit einer eher ablehnenden Haltung zu rechnen. Wenn das Unternehmen jedoch Penetrationstests durchführt, wird die Lage vielleicht anders beurteilt.

Insgesamt ist es eine ziemlich verzwickte Lage. Aber solche Unternehmen, die »keine Hacker beschäftigen«, müssen sich natürlich eine peinliche Frage durch die Hackergemeinde gefallen lassen. Und die lautet: »Woher wollen Sie das denn wissen?«

Nach unserem Dafürhalten müssen wir in die Rolle des Angreifers schlüpfen, um festzustellen, wie unsere Schutzmechanismen auf den Hacker wirken. Bedeutet das, dass wir auch die bösen Buben aufklären, wenn wir Sie über diese Techniken informieren? Natürlich. Wir glauben an gleiches Recht für alle. Die gleichen Techniken sollten allen Beteiligten zur Verfügung stehen. Und im Übrigen: Wie wollen *Sie* die »Guten« und die »Bösen« auseinander halten?

1.3 Was Sie vom Rest dieses Buchs erwarten können

Da wir das Thema »wie« und »warum« erschöpft haben, wollen wir uns über die weiteren Inhalte dieses Buchs unterhalten. Die Einteilung der Kapitel nach Angaben für Anfänger, Mittelstufler und Fortgeschrittene beziehen sich auf das erforderliche Hintergrundwissen für jedes Kapitel.

© by verlag moderne industrie Buch AG & Co. KG, Bonn

Die nächsten drei Kapitel dieses Buchs sollen Ihnen einige theoretische Hintergrundinformationen liefern. In Kapitel 2 wird unsere Liste von Regeln untersucht, die sich mit der Funktionsweise oder der fehlenden Funktion der Sicherheit befasst. Sie werden sehen, wie sich diese Regeln auf die Hacking-Techniken in den weiteren Kapiteln dieses Buchs anwenden lassen. Kapitel 3 beschreibt die Angriffsarten, gibt Auskunft über die Schwere des potenziellen Schadens, die mit Beispielen für jeden Typ unterstrichen werden. Kapitel 4 beschreibt die unterschiedlichen Methoden, die jemand (wie Sie selbst) anwenden könnte, um Sicherheitsprobleme zu entdecken. Die ersten vier Kapitel dieses Buchs sind für Leser aller Vorkenntnisstufen geeignet. Fortgeschrittene Lesen werden diese Kapitel unter Umständen auslassen wollen, wenn sie die theoretischen Grundlagen bereits beherrschen. Wir würden Sie aber bitten, den Text jedenfalls zu überfliegen, nur für den Fall, dass Sie etwas Neues entdecken. Die Abschnitte »Lösungen Fast Track« sind bestens zu diesem Zweck geeignet.

In Kapitel 5 geht es mit den Hacker-Techniken weiter. Kapitel 5 befasst sich mit der einfachsten Hacker-Technik überhaupt, dem Diffing; dabei geht es um den Vergleich des Codes vor und nach einer bestimmten Aktivität. Diese Technik ist erstaunlich nützlich und das Kapitel besonders gut für Anfänger geeignet.

Im Kapitel 6 geht es um die Kryptografie und die verschiedenen Mittel, die es zur Gewährleistung der Vertraulichkeit von Informationen gibt. Dabei werden die amateurhaften Kryptografie-Versuche analysiert, die wir weltweit im täglichen Einsatz beobachten. Wir zeigen Ihnen, wie Sie kryptografie-ähnliche Kodierschemata erkennen können und mit dem Knacken dieser Codes beginnen können. Dieses Kapitel ist für Anfänger und Leser mit mittleren Kenntnissen geeignet (für die Leser mit geringen Vorkenntnissen dieses Themas gibt es einen einführenden Abschnitt).

Kapitel 7 befasst sich mit den Sicherheitsrisiken, die dann entstehen, wenn Programme nicht richtig mit unerwartetem User-Input umgehen. Hier werden Themen besprochen wie der Angriff auf einen Server durch ein fehlerhaftes CGI-Programm oder der SQL-Zugriff über ein Web-Formular oder der Missbrauch von Skripten, um an eine Shell zu gelangen (technisch betrachtet gehören auch Pufferüberläufe und Format-String-Sicherheitslücken in die Kategorie der unerwarteten Eingaben, aber diese Themen werden in eigenständigen Kapiteln behandelt). Dieses Kapitel ist als Anfänger- oder Mittelstufe eingestuft, weil es Diskussionen von verschiedenen Programmiersprachen umfasst und Kenntnisse des Verhaltens der Shell voraussetzt.

In Kapiteln 8 und 9 erfahren Sie, wie man Angriffe in Maschinensprache schreibt, um Pufferüberlauf- und Format-String-Sicherheitslücken auszunutzen. Diese Kapitel sind für Fortgeschrittene, aber wir haben uns bemüht, die Themen auch ohne Vorkenntnisse zugänglich zu machen. Gewisse C- und Assembler-Kenntnisse werden vorausgesetzt.

© by verlag moderne industrie Buch AG & Co. KG, Bonn

Kapitel 10 beschreibt die Überwachung von Netzwerk-Kommunikationen – Sniffing – zu Hacker-Zwecken. Einfache Anwendungen werden gezeigt, Sie erfahren, aus welchen Protokollen Passwörter am besten ausgelesen werden können, und erhalten eine Einführung in die einfache Sniffer-Programmierung. Dieses Kapitel ist als Anfänger- bis Mittelstufe eingestuft.

In Kapitel 11 wird das Hijacking von Verbindungen eingeführt. In den meisten Fällen geht es um eine Erweiterung des Sniffing-Angriffs, nur dass Sie in diesem Fall aktiv eingreifen. Dieses Kapitel beschreibt außerdem MITM-(Man-In-The-Middle-) Angriffe und ist als mittelschwer eingestuft.

In Kapitel 12 wird das Konzept des Vertrauens vorgestellt und wie man es durch Spoofing unterlaufen kann. In diesem Kapitel werden verschiedene mögliche Angriffe besprochen, und es ist als mittelschwer bis schwer einzustufen.

Kapitel 13 befasst sich mit Tunneling-Mechanismen, mit deren Hilfe Ihre Daten durch feindliche Netzwerkumgebungen geleitet werden können (und dabei sicher bleiben). SSH wird detailliert besprochen. Das Kapitel ist mittelschwer bis schwer.

In Kapitel 14 geht es um Hardware-Hacking. Auf dieser Ebene treffen sich die Bits mit den Molekülen. Dieses Kapitel befasst sich mit den Grundlagen des Hardwareangriffs, um sich einen Sicherheitsvorteil zu verschaffen (wir entreißen einem sicheren Gerät seine Geheimnisse). Das Kapitel ist für Anfänger geeignet, aber die eigentliche Implementierung der Techniken ist sicherlich schwer.

In Kapitel 15 geht es um Viren, Trojaner und Würmer – nicht nur was sie sind und wie sie funktionieren, sondern welche Design-Entscheidungen dahinter stecken, die verschiedenen Techniken, die in diesem Bereich verwendet werden, und was in Zukunft auf uns zukommt. Dieses Kapitel ist der Mittelstufe zuzuordnen.

Kapitel 16 untersucht, wie Intrusion-Detection-Systeme umgangen oder fehlgeleitet werden können, sodass sie einen Angriff nicht erkennen. Hier geht es um Angriffe, die von der Netzwerkschicht aus in die Anwendungsschichten wirksam sind, und Themen wie die Fragmentierung und polymorphe Angriffe. Dieses Kapitel ist als mittelschwer bis schwer kategorisiert (Sie müssen sich einigermaßen mit TCP/IP auskennen).

Kapitel 17 beschreibt, wie Sie einige Ihrer Aufgaben mit Hilfe von automatischen Sicherheitsüberwachungs- und Angriffstools automatisieren können (nachdem wir Ihnen zunächst beigebracht haben, wie Sie diese manuell ausführen). Das Kapitel befasst sich mit kommerziellen und Freeware-Tools. Es gibt Ihnen einen schönen Ausblick auf die nächste Generation von Tools, die nicht nur die Schwachstelle erkennen, sondern ein System erobern und es als Sprungbrett für andere Angriffe nutzen werden.

© by verlag moderne industrie Buch AG & Co. KG, Bonn

Und last, but not least verraten wir Ihnen in Kapitel 18, wie Sie ein Sicherheitsproblem nach der Entdeckung melden können. Es soll uns ja keiner vorwerfen, wir würden nicht zu verantwortungsbewussten Meldungen stehen.

1.4 Das momentane juristische Klima verstehen

Ich bin kein Rechtsanwalt. Das können Sie in etwa so übersetzen: »Ich kann Ihnen keine juristischen Ratschläge geben, und Sie sollten diese von mir auch nicht annehmen. Sollten Sie es dennoch tun, sagen Sie im Nachhinein bitte nicht, ich hätte Sie nicht gewarnt. Das soll mich allerdings nicht davon abhalten, Ihnen meine Meinung aufzudrängen.«

Dieses Buch wird Ihnen Techniken vermitteln, die Sie mit dem Gesetz in Konflikt bringen, sollten Sie diese falsch anwenden. Dass ich Ihnen das sage, ist in etwa vergleichbar mit der Aussage eines Fahrlehrers: »Ich bringe Ihnen das Autofahren bei; wenn Sie schlecht fahren, können Sie jemanden überfahren.« In beiden Fällen sind Sie ganz alleine für den Fehler verantwortlich.

Ich nutze eine sehr einfache Regel: »Bin ich dazu befugt, diese Aktivität an dieser Maschine auszuführen?« Wenn die Antwort nein ist, lassen Sie es. Es ist falsch und mit ziemlicher Sicherheit illegal. Wenn Sie es lieber komplizierter haben: es gibt viele Ausnahmen und so weiter. In den meisten Ländern (und bei Ihnen? – fragen Sie besser Ihren Rechtsanwalt) sind Portscans legal. Sie gelten zwar als eindringlich und feindlich, aber sie sind überall legal – außer dort, wo sie illegal sind.

Früher hieß die einfachste Methode, sicher zu sein, alle Hacking-Techniken im eigenen Netzwerk auszuüben (und damit meine ich Ihr Home-Netzwerk und nicht das Ihres Arbeitgebers, weil Sie auch dort viel Ärger bekommen können). Sie wollen etwas hacken, das auf einer Sun-Sparc-Hardware ausgeführt wird? Kaufen Sie sich einen alten Sparc für $ 100 bei eBay. Sie wollen ein mehrere Millionen Dollar teures Mainframe hacken? Na ja, da haben Sie wahrscheinlich Pech gehabt.

Man möchte fast annehmen, dass es absolut sicher wäre, Hacker-Angriffe auf das eigene Equipment auszuführen. Nur leider stimmt das nicht ganz, vor allem nicht, wenn Sie die Software eines anderen angreifen. Die meisten Menschen denken genau wie ich, dass ich als Käufer eines Programms das natürliche Recht besitze, auf dem eigenen Computer alles damit anzustellen, was mir gerade einfällt. Leider wird das geistige Eigentum von den Gesetzen anders gehandhabt. In den Vereinigten Staaten und durch Vereinbarungen in vielen anderen Ländern ist es illegal, Kopierschutzmechanismen zu umgehen, die dem Schutz von Copyright-Materialien dienen. In den USA wird diese Thematik durch ein Gesetz mit dem Namen *Digital Millennium Copyright Act* (DMCA) geregelt. Technisch betrachtet ist es sogar illegal, den Kopierschutz in den eigenen vier Wänden zu knacken. Sollte es Ihnen aber gelingen, ist es eher unwahrscheinlich, dass Sie damit Probleme haben werden, wenn Sie es für sich behalten. Sollten Sie aber andere Menschen darüber informieren, seien Sie besser auf der Hut.

© by verlag moderne industrie Buch AG & Co. KG, Bonn

Als Sicherheitswarnung möchte ich Ihnen ein extremes Beispiel für das nennen, was mit diesen neuen Gesetzen passieren kann. Es geht um das russische Softwareunternehmen ElcomSoft Co. Ltd., das eine Software anbietet, die Passwörter cracken, den Kopierschutz entfernen und korrumpierte Dateien wieder herstellen kann. Beachten Sie, dass es in Russland kein Gesetz gegen Reverse-Engineering gibt. Einer der ElcomSoft Programmierer, Dmitry Sklyarov, hat die DEF CON 9 in Las Vegas besucht, um eine Präsentation über Adobes eBook-Dokumentenformat zu halten. Das Format enthält einige lächerliche Sicherheitsmaßnahmen. Am nächsten Tag wurde Dmitry auf dem Weg nach Hause verhaftet, und ihm wurde »die Verbreitung eines Produkts, das der Unterminierung von Kopierschutzmaßnahmen dient« vorgeworfen. Es ging um das von seinem Unternehmen vertriebene Produkt, welches das eBook-Format in normale Adobe Acrobat .PDF-Dateien konvertiert. Es ist (oder vielleicht war) für den Käufer eines eBooks legal, diese Konvertierung durchzuführen: Sie dürfen (oder durften früher) Datensicherungen anlegen.

Der langen Rede kurzer Sinn: Dmitry wurde am 18. Juli 2001 verhaftet und durfte endlich am 31. Dezember 2001 nach Hause fahren. Adobe hatte die Klage auf Grund von Protesten außerhalb ihrer Büroräume fallen gelassen, aber die US-Regierung hat sich geweigert, den Fall abzuschließen. Wie es im Augenblick aussieht, ist Dmitry immer noch nicht vom Haken.

Alles in allem waren die Techniken, die er angewandt hat, um die »Sicherheit« des Produkts zu untersuchen, relativ einfach. In Kapitel 6 berichten wir über Entschlüsselungstechniken dieser Art.

Seien Sie also sehr vorsichtig im Umgang mit den Informationen, die Sie an dieser Stelle erfahren.

1.5 Zusammenfassung

Dieses Buch soll und wird Ihnen ganz erbarmungslos Details zur Entdeckung und zum Missbrauch von Sicherheitslücken vermitteln; dabei verwenden Sie Techniken wie Sniffing, Session-Hijacking, Spoofing, Sie brechen kryptografische Schemata, unterlaufen IDS und greifen sogar Hardware an. In diesem Buch geht es nicht um das Sicherheits-Design, um Richtlinien, Architekturen, das Risikomanagement oder die Planung. Sollten Sie das geglaubt haben, sind Sie Opfer eines Spoofing-Angriffs geworden.

Alle Lücken, die entdeckt werden, sollten veröffentlicht werden. Die öffentliche Berichterstattung über Bugs ist für jedermann von Vorteil – dazu gehören auch Sie, da Sie dadurch außerdem etwas Anerkennung ernten werden.

Sie sollten lernen, wie man Hacker-Angriffe ausführt, weil Sie wissen müssen, wie Sie Ihr Netzwerk oder das Ihres Arbeitgebers schützen werden. Aber Hacker-Angriffe machen auch Spaß. Wenn Sie mit irgendetwas nicht einverstanden sind,

© by verlag moderne industrie Buch AG & Co. KG, Bonn

was ich in diesem Kapitel geschrieben habe, oder mit irgendetwas, was wir in diesem Buch schreiben, toll! Der Hacker sollte in erster Linie unabhängig denken können. Es gibt keinen Grund dafür, dass Sie irgendetwas von dem glauben sollten, was wir Ihnen berichten, ohne es selbst untersucht zu haben. Wenn Sie mich korrigieren möchten, surfen Sie auf die Solutions-Website für das Buch (`www.syngress.com/solutions`), suchen Sie meine E-Mail-Adresse und schicken Sie mir eine E-Mail. Vielleicht werde ich sogar Ihre Kritik auf der Website veröffentlichen.

1.6 FAQ

Frage: Sollte ich für mich den Titel »Hacker« verwenden?

Antwort: Hier gibt es zwei Betrachtungsweisen: Die eine lautet, Sch... auf das, was die anderen denken. Wenn Sie Hacker sein wollen, nennen Sie sich Hacker. Und zweitens, wenn Sie sich Hacker betiteln, werden die Menschen wegen der Zweideutigkeit des Begriffs und der gegensätzlichen Definitionen des Wortes Hacker unterschiedlich auf Sie reagieren. Einige Menschen werden denken, Sie haben ihnen mitgeteilt, dass Sie Krimineller sind. Manche Menschen, die sich für Hacker halten, werden Sie beleidigen, wenn Sie der Meinung sind, dass es Ihnen an den entsprechenden Fähigkeiten mangelt. Manche werden gar nicht wissen, was sie denken sollen, aber Sie anschließend fragen, ob Sie irgendetwas für Sie knacken können. Mein Ratschlag lautet, bauen Sie zunächst Ihre Fähigkeiten aus und üben Sie fleißig. Im Idealfall warten Sie, bis Ihnen dieser Titel von jemandem anderen verliehen wird.

Frage: Ist es legal Viren, Trojaner und Würmer zu schreiben?

Antwort: Technisch gesehen (in den meisten Ländern) ja. Jedenfalls im Augenblick. Diese Aussage verdient es, näher erläutert zu werden. Es gibt einige Viren-Programmierer, die öffentlich arbeiten und ihre Arbeit veröffentlichen. Bisher hat man sie nicht belangt. Sollte allerdings eine dieser Arbeiten in die freie Wildbahn gelangen und von den Medien aufgegriffen werden, würde ich nicht mehr damit rechnen, dass es für die Programmierer ruhig bleibt. Wenn Sie unbedingt Viren schreiben müssen, stellen Sie sicher, dass sie nicht veröffentlicht werden. Als Vorsichtsmaßnahme könnten Sie auch die Vermehrungsfähigkeit Ihrer Viren künstlich einschränken. Derzeit ist es unklar, was Ihnen geschehen kann, wenn Ihre Arbeit »ausgebaut« und veröffentlicht wird. Achten Sie außerdem darauf, ob die Veröffentlichung solcher Arbeiten eventuell gegen die Geschäftsbedingungen des Providers verstößt – vor allem dann, wenn Sie Student sind. Es ist vielleicht nicht illegal, aber es kann sehr wohl dazu führen, dass Ihr Konto vom ISP gesperrt oder Ihnen gekündigt wird oder dass Sie vom Studium ausgeschlossen werden.

© by verlag moderne industrie Buch AG & Co. KG, Bonn

Frage: Gibt es irgendwelche Probleme, wenn man Systeme im eigenen Verantwortungsbereich hackt?

Antwort: Im Allgemeinen nicht, *wenn* Sie dazu autorisiert sind. Achten Sie auf das Wort *wenn*. Wenn Sie Zweifel haben, lassen Sie sich eine schriftliche Erlaubnis durch den Eigentümer der Systeme – beispielsweise das Bildungsinstitut oder Ihren Arbeitgeber – ausstellen. Viele Menschen, die für die Sicherheit ihrer Systeme verantwortlich sind, hacken sie immer wieder. Es gibt aber gelegentliche Probleme – siehe das Beispiel, das Sie unter `www.lightlink.com/spacenka/fors` lesen können.

© by verlag moderne industrie Buch AG & Co. KG, Bonn

© by verlag moderne industrie Buch AG & Co. KG, Bonn