IN DIESEM KAPITEL

- Die Unterschiede zwischen den Zielen ethischer Hacker und bösartiger Angreifer
- Entstehungsgeschichte und Entwicklung von Sicherheitstests
- Gefahren für Computersysteme
- Erste Schritte beim Durchführen von Sicherheitstests

Kapitel 1
Einführung in Schwachstellen- und Penetrationstests

In diesem Buch geht es um das Testen Ihrer Computer und Netzwerke, um Sicherheitslücken aufzuspüren und aufgefundene Schwachstellen zu beheben, bevor die Schurken Gelegenheit bekommen, sie auszunutzen.

Begriffserklärungen

Jeder dürfte bereits etwas von Hackern und böswilligen Benutzern gehört haben. Viele Anwender mussten bereits selbst unter den Folgen krimineller Hackerangriffe leiden. Um wen handelt es sich bei diesen Leuten? Und was sollte man über sie wissen? Die folgenden Abschnitte sollen Ihnen einige grundlegende Fakten über diese Angreifer vermitteln.

Ich verwende in diesem Buch diese Terminologie:

- **Hacker** (oder externe Angreifer) versuchen, Computer und sensible Daten üblicherweise als Außenstehende und Unberechtigte anzugreifen, um illegale Ziele zu erreichen. Hacker greifen beinahe alle Systeme an, die sie als Angriffsziel für lohnend halten. Einige streben bevorzugt nach Ruhm und Prestige und attackieren gut geschützte Systeme. Generell gilt aber eigentlich, dass der eigene Status in Hackerkreisen steigt, wenn es überhaupt gelingt, in fremde Systeme einzudringen.
- **Böswillige Benutzer** (externe oder interne Angreifer) versuchen, als berechtigte und »vertrauenswürdige« Benutzer von außen (also Kunden oder Geschäftspartner) oder von innen heraus Computer und sensible Daten zu

attackieren. Böswillige Benutzer greifen Systeme an, weil sie illegale Ziele verfolgen oder sich rächen wollen und vielleicht Zugang zu oder spezielle Kenntnisse von Systemen besitzen, die ihnen derartige Angriffe erleichtern.

Arglistige Angreifer sind allgemein sowohl Hacker als auch böswillige Benutzer. Ich bezeichne beide der Einfachheit halber als *Hacker* und unterscheide nur dann zwischen Hackern und böswilligen Benutzern, wenn ich mich intensiver mit deren Werkzeugen, Techniken und Denkweisen beschäftigen muss.

- **Ethische Hacker** (oder »die Guten«) hacken Systeme, um Schwachstellen aufzuspüren und Schutzmaßnahmen gegen unberechtigte Zugriffe aufbauen zu können. Dazu zählen auch IT-Sicherheitsberater und entsprechendes internes Personal.

»Hacker«

Der Begriff *Hacker* hat zwei Bedeutungen:

- Traditionell basteln Hacker gerne an Software oder elektronischen Systemen herum. Hackern gefällt es, wenn sie herausfinden und lernen, wie Computersysteme funktionieren. Sie lieben es, sich sowohl mechanisch als auch elektronisch neue Möglichkeiten zu erschließen.
- In den letzten Jahren hat der Begriff *Hacker* eine neue Bedeutung erhalten. Nun versteht man hier darunter jemanden, der arglistig in Systeme eindringt, um für sich selbst Gewinne zu erzielen. Technisch gesehen handelt es sich bei diesen Kriminellen eigentlich um *Cracker* (*Criminal Hackers*). Cracker dringen mit böswilligen Absichten in Systeme ein (oder cracken sie). Zu ihren persönlichen Zielen zählen Ruhm, Profit oder auch Rache. Sie ändern, löschen und entwenden kritische Daten und machen großen Einrichtungen und selbst Regierungen und Behörden das Leben schwer.

Es gibt noch weitere Bedeutungen von »Hacken«, weil dieser Begriff mittlerweile für allerlei andere Zwecke entfremdet wurde. Bei einer geht es einfach um das Modifizieren oder Umfunktionieren elektronischer Schaltungen oder auch von Programmen. Vom Sinn her also eigentlich einfach nur so etwas wie »Basteleien«. Wie dem auch sei, lassen Sie sich dadurch nicht verwirren oder auf den Holzweg bringen.

Die guten (*White Hat*) Hacker mögen es nicht, wenn sie in dieselbe Schublade wie die heimlich operierenden Hacker (*Black Hat*) gepackt werden. (Falls es Sie interessiert: Die Einteilung in *White Hat* (weißer Hut) und *Black Hat* (schwarzer Hut) stammt aus den alten Western im Fernsehen, in denen die Guten immer weiße und die Bösen immer schwarze Hüte getragen haben.) *Gray-Hat*-Hacker (Hacker mit grauen Hüten) gehören beiden Kategorien an. Heutzutage verbinden die meisten Menschen etwas Negatives mit dem Begriff *Hacker*.

Viele der bösartigen Hacker behaupten, niemanden zu schädigen, sondern anderen zum Wohle der Gesellschaft zu helfen. Wer's glaubt, wird selig. Heimlich vorgehende Hacker sind die Verbrecher des elektronischen Zeitalters, die die verdienten Konsequenzen für ihr Handeln tragen müssen.

Passen Sie auf, dass Sie nicht versehentlich kriminelle Hacker mit Sicherheitsbeauftragten verwechseln. Diese hacken nicht nur in ehrlichen Interessen, sondern entwickeln auch jene erstaunlichen Werkzeuge, die uns bei der späteren Arbeit unterstützen, stellen sich ihrer Verantwortung und sorgen dafür, dass ihre Ergebnisse und die Quelltexte ihrer Programme veröffentlicht werden.

»Böswillige Benutzer«

Bei *böswilligen Benutzern* und damit verbrecherischen Angestellten, Vertragspartnern, internen oder sonstigen Benutzern, die ihre Privilegien missbrauchen, handelt es sich um einen Begriff, der in Sicherheitskreisen und in Überschriften zum Thema Datendiebstahl gebräuchlich ist. Hierbei geht es nicht unbedingt um Benutzer, die interne Systeme »hacken«, sondern auch um jene, die ihre Zugangsberechtigungen missbrauchen. Benutzer schnüffeln in wichtigen Datenbanksystemen, um sensible Daten zu sammeln, senden vertrauliche Informationen über Kunden per E-Mail an die Konkurrenz oder ändern oder löschen wichtige Dateien von Servern, zu denen sie eigentlich keinen Zugriff haben dürften.

Mitunter gibt es unschuldige (oder unwissende) interne Mitarbeiter, die zwar keine böswilligen Absichten haben, aber trotzdem Probleme verursachen, weil sie sensible Daten verschieben, löschen oder ändern. Selbst unschuldige Wurstfinger auf der Tastatur können in der Geschäftswelt fatale Konsequenzen haben. Denken Sie an all diese *Ransomware*-Infektionen, von denen Unternehmen weltweit erpresst und zu Zahlungen gezwungen werden sollen. Zuweilen reicht ein einziger Klick eines unachtsamen Benutzers aus, um Netzwerke ganz oder teilweise lahmzulegen.

Häufig sind böswillige Benutzer die schlimmsten Feinde von IT- und Sicherheitsexperten, weil sie genau wissen, wo sie die wertvollen Daten finden können, und über kein besonderes Computerwissen verfügen müssen, um auf sensible Daten zugreifen zu können. Diese Benutzer besitzen die benötigten Zugangsberechtigungen und ihnen wird von der Geschäftsführung oft blind vertraut.

Und wie sieht es mit Edward Snowden, dem früheren NSA-Beschäftigten (National Security Agency) aus, der seinen Arbeitgeber verraten hat? Das ist ein kompliziertes Thema, auf das ich zusammen mit der Hacker-Motivation in Kapitel 2 eingehen werde. Was Sie auch von Snowden halten mögen, er hat seinen Arbeitgeber hintergangen und seine vertragliche Schweigepflicht gebrochen. Dasselbe ließe sich auch über andere Personen sagen, die aufgrund ihrer Bekanntheit auf einen Sockel gestellt werden.

Wie aus arglistigen Angreifern ethische Hacker werden

Sie müssen sich vor dem Hacker-Schwindel schützen. Sie benötigen einen ethischen Hacker (oder müssen selbst zu einem werden). Ethische Hacker besitzen die benötigten Fähigkeiten, Einstellungen und Werkzeuge eines Hackers, sind aber zudem vertrauenswürdig. Ethische Hacker hacken, um Sicherheitsprüfungen für ihre Systeme so vorzunehmen, wie böswillige Angreifer es wohl machen würden.

Beim ethischen Hacken, das auch als Schwachstellen- und Penetrationstests bekannt ist, werden dieselben Werkzeuge, Tricks und Techniken eingesetzt, die auch von kriminellen Hackern benutzt werden. Allerdings mit einem wesentlichen Unterschied: Ethisches Hacken erfolgt im professionellen Umfeld mit Genehmigung der »Opfer«. Dabei sollen Schwachstellen aus der Perspektive der Gauner aufgespürt werden, um Systeme besser sichern zu können. Schwachstellen- und Penetrationstests gehören zum Programm der Datenverarbeitung und des Risikomanagements, das der laufenden Verbesserung der Systemsicherheit dienen soll. Durch die Sicherheitstests lässt sich auch prüfen, ob Behauptungen von Herstellern hinsichtlich der Sicherheit ihrer Produkte wahr sind.

Ethisches Hacken im Vergleich zur Auditierung

Oft werden Sicherheitstests durch Schwachstellen- und Penetrationstests mit Sicherheitsüberprüfungen (*Auditierung*) verwechselt, aber da gibt es *große* Unterschiede. Zu Sicherheitsüberprüfungen gehört ein Vergleich der Sicherheitsrichtlinien von Unternehmen mit den aktuell gültigen Standards (oder *Compliance*-Anforderungen). Sicherheitsaudits werden durchgeführt, um zu prüfen, ob es Sicherheitskontrollen gibt, wobei üblicherweise risikobasierte Ansätze verfolgt werden. Häufig umfassen Sicherheitsüberprüfungen auch das Überdenken von Geschäftsabläufen, wobei die Abläufe nicht sonderlich technisch ausgerichtet sein müssen und einfach nur auf »Prüflisten für Sicherheitsfragen« basieren.

Im Gegensatz dazu konzentrieren sich Bewertungen auf der Grundlage von ethischem Hacken auf potenziell nutzbare Schwachstellen. Dabei wird nur geprüft, ob überhaupt Sicherheitskontrollen existieren und ob sie wenigstens effektiv sind. Diese formalen Schwachstellen- und Penetrationstests können einerseits sehr technisch sein, andererseits aber auch auf weniger technischem Niveau ablaufen. Und obwohl auch dabei formal vorgegangen werden muss, sind diese Tests tendenziell weniger strukturiert als formale Sicherheitsaudits. Wenn in Ihrem Unternehmen Audits (beispielsweise für die Zertifizierungen ISO 9001 und 27001) erforderlich sind, sollten Sie darüber nachdenken, die hier vorgestellten Schwachstellen- und Penetrationstests mit in den Auditierungsprozess aufzunehmen. Auditierung, Schwachstellen- und Penetrationstests ergänzen einander wirklich gut.

Wenn Sie für Kunden ethisch hacken und Tests durchführen oder Ihre Referenzen und Leistungsnachweise einfach nur um ein zusätzliches Zertifikat erweitern wollen, sollten Sie darüber nachdenken, im Rahmen des vom EC-Council gesponserten Programms zum *Certified Ethical Hacker* (C|EH) zu werden. Weitere Informationen hierzu finden Sie unter www.eccouncil.org. Ein entsprechender Kurs in Deutsch wird zum Beispiel von der *Bremer Akademie für berufliche Weiterbildung* (www.bremerakademie.de) angeboten.

Betrachtungen zu Richtlinien

Wenn Sie Schwachstellen- und Penetrationstests zu einem wichtigen Element des IT-Risikomanagements Ihres Unternehmens machen wollen, benötigen Sie unbedingt dokumentierte Richtlinien für Ihre Sicherheitstests. Diese beschreiben, wer die Tests durchführt, welcher Art die Tests generell sind, welche Systeme (Server, Webanwendungen, Laptops

und so weiter) berücksichtigt werden und wie oft die Prüfungen vorgenommen werden sollen. Erstellen Sie Ablaufpläne und Vorgehensweisen für die in diesem Buch behandelten Sicherheitsprüfungen. Sie sollten auch über eine Dokumentation der jeweils verwendeten Testwerkzeuge nachdenken, in der diese beschrieben und in denen Termine für die Tests Ihrer Systeme vorgegeben werden. So könnte dort zum Beispiel stehen, dass externe Systeme vierteljährlich und interne Systeme halbjährlich getestet werden müssen.

Compliance und regulatorische Aspekte

Ihre eigenen internen Richtlinien schreiben vielleicht vor, wie mit Sicherheitstests in Ihrem Unternehmen umgegangen wird, aber Sie müssen auch Gesetze berücksichtigen, die speziell das Unternehmen betreffen. Viele dieser Vorschriften erfordern eine ständige Anpassung der eigenen Sicherheitsanforderungen. Dadurch, dass Ihr ethisches Hacken den jeweiligen Vorgaben folgt und an die staatlichen Anforderungen angepasst wird, lässt sich Ihr eigenes Programm gewaltig aufwerten.

Warum eigene Systeme hacken?

Um Diebe fangen zu können, müssen Sie wie Diebe denken. Diese Erkenntnis bildet auch die Grundlage für Schwachstellen- und Penetrationstests. Es ist extrem wichtig, den eigenen Feind zu kennen. Das Gesetz des Durchschnitts arbeitet der Sicherheit entgegen. Aufgrund der steigenden Anzahl der Hacker mit ständig wachsendem Wissen und der immer größer werdenden Zahl der Schwachstellen und Unbekannten werden schließlich wohl alle Computersysteme und Anwendungen irgendwie gehackt oder sind zumindest gefährdet. Es ist also ungeheuer wichtig, die eigenen Systeme vor Angreifern zu schützen – und zwar nicht nur jene Schwachstellen, die ohnehin jeder kennt. Wenn Sie die Tricks der Hacker kennen, können Sie die wirkliche Verletzlichkeit und Angreifbarkeit Ihrer Systeme ermitteln.

Hacken beutet schlechte Sicherheitsverfahren und offene Schwachstellen aus. Firewalls, Verschlüsselung und Kennwörter können für ein falsches Gefühl der Sicherheit sorgen. Die Sicherheitssysteme konzentrieren sich oft nur auf Schwachstellen der obersten Ebene wie der grundlegenden Zugangskontrolle, ohne die Arbeitsweise von Hackern zu berücksichtigen. Schwachstellen- und Penetrationstests bieten bewährte Methoden, um die eigenen Systeme gegen Angriffe zu wappnen. Wenn Sie die Schwachpunkte nicht identifizieren, ist deren Ausbeutung nur eine Frage der Zeit.

Und so, wie die Hacker ihre Kenntnisse erweitern, sollten Sie das auch tun. Sie müssen wie Hacker denken und arbeiten, um Systeme wirksam vor ihnen schützen zu können. Als ethischer Hacker müssen Sie wissen, welches Instrumentarium Hackern zur Verfügung steht, und Möglichkeiten kennen, die Angriffsbemühungen wirksam zu stoppen. Wenn Sie wissen, wonach Sie suchen müssen und wie Sie entsprechende Informationen nutzen, können Sie die Bemühungen von Hackern besser durchkreuzen.

Sie müssen Ihre Systeme nicht vor *allem* schützen. Das ist unmöglich. Dazu müssten Sie letztlich Ihre Computer abschalten und wegschließen und auch für sich selbst unzugänglich machen. Das ist hinsichtlich der Datensicherheit aber

auch nicht gerade praktisch und wenig geschäftsfördernd. Wichtig ist der Schutz Ihrer Systeme vor bekannten Schwachstellen und den üblichen Angriffen, was in vielen Organisationen zu den am meisten übersehenen Schwachstellen zählt.

Sie können nicht alle möglichen Schwachstellen Ihrer Systeme und Geschäftsvorgänge vorhersehen. Sie können sich bestimmt nicht gegen alle möglichen Angriffe wappnen, insbesondere nicht gegen noch unbekannte Schwachstellen. Je mehr Möglichkeiten Sie aber probieren und je intensiver Sie ganze Systeme und nicht einzelne Geräte testen, desto wahrscheinlicher wird es, Schwachstellen zu entdecken, die Ihre kompletten Datenverarbeitungssysteme gefährden.

Treiben Sie das ethische Hacken nicht auf die Spitze. Es ist wenig sinnvoll, Ihre Systeme mit einem Schutzwall zu umgeben, der auch unwahrscheinlichste Angriffe erfasst.

Die Gesamtzielsetzung für Sicherheitstests ist:

- ✔ Legen Sie Prioritäten für Ihre Systeme fest, um die eigenen Anstrengungen auf das Wichtige zu konzentrieren.
- ✔ Testen Sie Ihre Systeme, ohne selbst Schaden anzurichten.
- ✔ Zeigen Sie Schwachstellen auf und weisen Sie gegenüber dem Management nach, dass dadurch geschäftliche Risiken bestehen.
- ✔ Beseitigen Sie die Schwachstellen und sichern Sie Ihre Systeme besser.

Die Gefahren verstehen, denen Ihre Systeme ausgesetzt sind

Zu wissen, dass Systeme von Hackern weltweit und böswilligen Benutzern im eigenen Büro angegriffen werden können, ist eine Sache. Etwas anderes ist es, spezifische potenzielle Angriffe auf Ihr System auch zu verstehen. In diesem Abschnitt werde ich einige bekannte Angriffsmöglichkeiten vorstellen, ohne dabei Anspruch auf Vollständigkeit zu erheben.

Viele Schwachstellen sind im Bereich der Datensicherheit isoliert betrachtet nicht bedenklich. Wenn aber mehrere gleichzeitig ausgenutzt werden, können dadurch Systeme schwer gefährdet werden. So müssen Windows-Standardkonfigurationen, schwache Administratorkennwörter von SQL-Servern oder drahtlos verwaltete Netzwerkserver allein kein größeres Sicherheitsrisiko darstellen. Nutzen Hacker aber all diese Schwachstellen gleichzeitig aus, gelangen sie möglicherweise an sensible Daten und mehr.

Komplexität ist ein Feind der Sicherheit.

In den letzten Jahren hat die Anzahl der bekannten Schwachstellen und der Angriffe enorm zugenommen. Als wesentliche Ursachen dafür gelten die zunehmende Verbreitung von Virtualisierungslösungen, Cloud-Computing und soziale Netze. Diese führen zu äußerst komplexen modernen IT-Umgebungen.

Nicht-technische Angriffe

Unter *Exploits* versteht man Programme, die Sicherheitslücken in Computersystemen ausnutzen. Exploits, die Menschen – Endbenutzer und sogar Sie selbst – zu einem bestimmten Verhalten bewegen und damit manipulieren, stellen innerhalb der Computersysteme oder Netzwerkstrukturen die wohl größte Schwachstelle dar. *Soziale Manipulationen* (eigentlich *Social Engineering* missbrauchen das Vertrauen von Menschen, um mit böser Absicht – zum Beispiel über Phishing-Mails – an Daten zu gelangen. In Kapitel 6 erfahren Sie mehr über Social Engineering und darüber, wie Sie Ihre Systeme davor schützen können.

Und dann gibt es noch gängigere Angriffsformen auf IT-Systeme auf physischer Ebene. Hacker brechen in Gebäude, Computerräume oder andere Bereiche ein, um an wichtige Daten zu gelangen, indem sie Computer, Server und andere wertvolle Geräte stehlen. (Oft reicht es aus, einfach in ein unverschlossenes Büro zu gehen und einen der dort herumstehenden, ungesicherten Laptops zu stehlen.) Zu diesen Angriffen zählt auch das sogenannte *Dumpster Diving* (wörtlich: *Mülltauchen*), also das Durchwühlen von Papierkörben und Mülleimern nach geistigem Besitz, Kennwörtern, Netzwerkdiagrammen und anderen Informationen.

Angriffe auf Netzwerkinfrastrukturen

Häufig ist es für Hacker leicht, die Infrastruktur von Netzwerken anzugreifen, weil diese vielfach weltweit über das Internet erreichbar sind. Beispiele für diese Art von Angriffen sind:

- ✔ Verbindung mit einem Netzwerk über einen ungesicherten drahtlosen Zugriffspunkt (oder *Access Point*), der hinter einer Firewall hängt
- ✔ Die Schwächen von Netzwerkprotokollen wie TCI/IP oder SSL (Secure Sockets Layer) ausnutzen
- ✔ Ein Netzwerk mit zu vielen Anforderungen überlasten, was zu *Dienstblockaden* und damit der Unerreichbarkeit von Diensten für rechtmäßige Benutzer führt (*DoS – Denial of Service*)
- ✔ In einem Netzwerk einen Netzwerkanalysator installieren und alle Pakete, die durch das Netzwerk reisen, abfangen und auf vertrauliche Informationen im Klartext untersuchen

Angriffe auf Betriebssysteme

Hacker greifen am liebsten Betriebssysteme (BS) an. Das liegt schon daran, dass alle Computer ein Betriebssystem benötigen und diese für viele bekannte Exploits anfällig sind, zu denen auch Schwachstellen zählen, die teilweise selbst nach Jahren nicht beseitigt wurden.

Gelegentlich werden auch Betriebssysteme angegriffen, die zwar im Lieferzustand – wie das reichlich alte, aber immer noch existierende Novell NetWare oder OpenBSD – von Haus aus sicherer zu sein scheinen als andere, aber doch auch Schwachstellen aufweisen. Hacker greifen aber bevorzugt Windows, Linux und/oder Mac OS X an, weil diese viel weiter verbreitet sind.

Beispiele für Angriffe auf Betriebssysteme sind:

- ✔ Das Ausnutzen fehlender Aktualisierungen
- ✔ Angriffe auf Authentifizierungssysteme der Betriebssysteme
- ✔ Aushebeln der Sicherheitsfunktionen der entsprechenden Dateisysteme
- ✔ Knacken von Kennwörtern und schwache Verschlüsselungsimplementierungen

Angriffe auf Anwendungen und spezielle Funktionen

Anwendungen stehen bei Hackern hoch im Kurs. Programme wie die Software von E-Mail-Servern und Webanwendungen werden oft Opfer der Angriffe und lahmgelegt:

- ✔ Webanwendungen sind allgegenwärtig. Dank der *Schatten-IT* (*Shadow IT*), in deren Rahmen die Beschäftigten in verschiedenen Bereichen von Unternehmen eigene Technologien nutzen und verwalten, befinden sich Webanwendungen in allen Winkeln der internen Netzwerke und zunehmend auch in der Cloud. Leider sind sich viele IT-Sicherheitsprofis der vorhandenen Schatten-IT und ihrer Risiken kaum bewusst.
- ✔ Apps von Mobilgeräten sind im geschäftlichen Umfeld verstärkt Angriffen ausgesetzt. Auch in offiziellen Anwendungsquellen (wie Google Play für Android) wurden längst von Gaunern programmierte Apps entdeckt, die Ihre Umgebung vor Herausforderungen stellen können.
- ✔ Ungeschützte Dateien, die oft sensible Daten enthalten, befinden sich weit verstreut auf Freigaben von Arbeitsstationen und Servern oder auch in der Cloud auf öffentlichen Speicherangeboten, wie OneDrive oder Google Drive. Datenbanksysteme enthalten viele Schwachstellen, die böswillig genutzt werden können.

Prinzipien bei Sicherheitsbewertungen

Sicherheitsprofis müssen dieselben Angriffe auf Computersysteme, vorhandene physische Kontrollinstrumente und Menschen ausführen wie böswillige Hacker. (Ich habe diese Angriffe im vorherigen Abschnitt vorgestellt.) Das Ziel von Sicherheitsprofis besteht dabei darin, erkannte Schwachstellen aufzuzeigen. In den Teilen II bis V dieses Buches werden derartige Angriffe behandelt und Gegenmaßnahmen vorgestellt, die Sie ergreifen können.

Um dafür zu sorgen, dass geeignete Sicherheitstests professionell durchgeführt werden, müssen Sicherheitsprofis die in den nächsten Abschnitten beschriebenen grundlegenden Prinzipien beachten.

Falls Sie die Gebote ethischen Hackens nicht befolgen, kann das ziemlich negative Konsequenzen haben. Ich habe selbst erlebt, wie diese Regeln beim Durchführen von Sicherheitstests vergessen oder ignoriert wurden. Die Ergebnisse waren *nicht* positiv – glauben Sie mir.

Ethisch arbeiten

In diesem Kontext bedeutet *ethisch*, sich an professionellen Moralvorstellungen und Prinzipien zu orientieren. Ob es nun um Sicherheitstests bei eigenen Systemen oder Auftragsarbeiten geht, Sie müssen immer ehrlich bleiben und die Unternehmensziele unterstützen. Versteckte Absichten bleiben außen vor! Dazu zählt auch, Ergebnisse immer rückhaltlos darzulegen, selbst wenn Ihnen daraus Nachteile entstehen könnten. Lachen Sie nicht, bei zahlreichen Gelegenheiten konnte ich beobachten, wie Leute Sicherheitsschwachstellen ignoriert haben, weil sie für keinen Aufruhr sorgen wollten oder Auseinandersetzungen mit schwierigen Vorgesetzten oder Verkäufern vermeiden wollten.

Vertrauenswürdigkeit lautet der oberste Grundsatz. Sie stellt auch die beste Möglichkeit dar, um Mitarbeiter von Ihrem Sicherheitsprogramm auf Dauer zu überzeugen. Datenmissbrauch ist absolut verboten. So würden Übeltäter vorgehen. Sollen sie mit ihrer getroffenen Wahl doch Geldstrafen kassieren oder in den Knast wandern. Vergessen Sie nicht, dass Sie sich ethisch korrekt verhalten und dennoch nicht vertrauenswürdig sein können. Dasselbe gilt auch umgekehrt, und damit würden Sie den Spuren von Edward Snowden folgen. Derartige Schwierigkeiten sind Bestandteil der Herausforderungen Ihres Sicherheitsprogramms. Ich beneide Sie angesichts dieser komplexen Aufgabe nicht.

Die Privatsphäre respektieren

Behandeln Sie die gesammelten Daten mit allergrößtem Respekt. Alle Informationen, die Sie bei Ihren Tests erhalten, von Protokolldateien der Webanwendungen über Kennwörter im Klartext bis hin zu persönlichen Daten und allem, was es sonst noch gibt, müssen privat bleiben. Schnüffeln Sie nicht in vertraulichen Firmendaten oder dem Privatleben der Beschäftigten herum.

Sorgen Sie für Zeugen und binden Sie andere in den Prozess mit ein. Wenn Sie selbst beaufsichtigt werden, sorgt das für mehr Vertrauen und Unterstützung für Ihre Projekte zur Sicherheitsbewertung.

Bringen Sie Ihre Systeme nicht zum Absturz

Einer der größten Fehler, der beim Hacken von Systemen auftritt, besteht darin, eigene Systeme versehentlich zum Absturz zu bringen, die es eigentlich zu schützen gilt. Zu Systemabstürzen kommt es heute zwar weniger häufig als früher. Treten sie doch auf, liegt das meist an schlechter Planung oder der Auswahl ungeeigneter Zeitpunkte für die Tests.

Auch wenn es nicht sonderlich wahrscheinlich ist, können für Ihre Systeme beim Testen DoS-Bedingungen entstehen. Bei DoS (Denial of Service) kann ein Server die Anforderungen nicht mehr zügig verarbeiten. Durch zu viele, zu schnell ausgeführte Tests kann es dann zu Systemaussetzern, Datenschäden, Systemneustarts und so weiter kommen. Das gilt insbesondere beim Testen von Webseiten und (anspruchsvollen) Webanwendungen auf älteren Servern. (Ich sollte das wissen, denn das ist mir passiert.) Sie sollten jedenfalls nicht gleich loslegen und dabei annehmen, dass irgendein Host dem möglichen Ansturm der Werkzeuge für das Netz und die Schwachstellenscanner gewachsen ist.

Sie können auch versehentlich Konten dauerhaft oder vorübergehend sperren oder jemanden aus sozialen Netzen aussperren, wenn Sie jemanden dazu veranlassen, Passwörter zu ändern, ohne dass dieser die Konsequenzen derartiger Aktionen erkennt. Gehen Sie die Dinge mit Vorsicht und gesundem Menschenverstand an. Es ist aber immer besser, vorhandene Schwachstellen vor Dritten zu entdecken.

Bei vielen Programmen für die Suche nach Schwachstellen können Sie steuern, wie viele Tests auf einem System gleichzeitig ausgeführt werden. Derartige Einstellungen sind besonders dann äußerst praktisch, wenn Tests auf Produktivsystemen während der Bürozeiten durchgeführt werden müssen. Schalten Sie bei Ihren Tests lieber einen Gang herunter. Dann benötigen Tests zwar mehr Zeit, das kann Ihnen aber viel Ärger ersparen.

Die Arbeitsabläufe bei Schwachstellen- und Penetrationstests

Wie eigentlich alle IT- oder Sicherheitsprojekte muss ethisches Hacken geplant werden. Ich habe bereits darauf hingewiesen, dass versäumte Planung leicht zum Scheitern der Tests führt. Mittel- und langfristige Aspekte der Testprozesse müssen festgelegt und vereinbart werden. Damit der Erfolg Ihrer Anstrengungen auch gewährleistet ist, sollten Sie sich vor den eigentlichen Tests die Zeit nehmen, die kompletten Tests vorab zu planen. Dabei spielt es keine Rolle, ob es nur um das einfache Knacken eines Kennworts oder komplexe Tests auf Schwachstellen in Webanwendungen geht.

Wenn ein »geläuterter« Hacker die Tests mit Ihnen zusammen durchführen soll oder Sie dessen unabhängige Meinung einholen wollen, sollten Sie vorsichtig sein. Ich behandele die Vor- und Nachteile der Zusammenarbeit mit angestellten personellen Sicherheitsressourcen und was Sie dabei tun oder besser lassen sollten, in Kapitel 19.

Die Planformulierung

Für ethisches Hacken benötigen Sie unbedingt entsprechende Genehmigungen. Sorgen Sie dafür, dass Ihre Aktivitäten zumindest für Entscheidungsträger bekannt und transparent sind. Zunächst einmal muss das Projekt unterstützt werden. Für die Unterstützung können Unternehmensleitung, Vorgesetzte, Kunden oder vielleicht sogar Sie selbst (als eigener Chef) sorgen. Sie benötigen jemanden, der sich für Sie einsetzt und Ihre Pläne genehmigt. Anderenfalls kann es passieren, dass Ihre Tests ein unerwartetes Ende finden, weil jemand behauptet, Sie hätten dafür keine Genehmigung. Schlimmer noch, Sie werden vielleicht gefeuert oder strafrechtlich verfolgt!

Bei eigenen Systemen kann es sich bei Genehmigungen um einfache interne Nachrichten oder E-Mails vom Chef handeln. Bei Tests im Kundenauftrag sollten Sie sich durch unterschriebene Verträge absichern. Mit schriftlicher Bestätigung besteht zudem kaum mehr Gefahr, dass Sie Ihre Zeit und Mühe nur vergeuden. Ein solches Dokument befreit Sie auch aus dem Gefängnis, wenn sich jemand (zum Beispiel Internet-Dienstanbieter, Cloud-Anbieter

oder Lieferanten) fragen sollte, was Sie eigentlich treiben, und die Polizei alarmiert. Lachen Sie jetzt nicht, es wäre nicht das erste Mal.

Bereits ein kleiner Ausrutscher kann Ihre Systeme komplett abstürzen lassen, was sicherlich nicht gerade erwünscht ist. Sie benötigen detaillierte Pläne, was aber auch nicht bedeuten muss, dass Sie alles übermäßig komplex werden lassen. Sorgfältig ausgearbeitete Rahmenpläne enthalten diese Angaben:

- ✔ **Liste der zu testenden Systeme:** Was die Auswahl der zu testenden Systeme angeht, beginnen Sie mit den wichtigsten Systemen und Abläufen oder den Systemen, von denen Sie vermuten, dass sie besonders verletzlich sind. Sie können zum Beispiel die Sicherheit der Kennwörter eines Serverbetriebssystems oder eine über das Internet erreichbare Webanwendung testen oder soziale Manipulationen versuchen. Vielleicht versuchen Sie ja auch, mit E-Mail-Phishing Daten abzugreifen, bevor Sie auf tieferen Systemebenen mit der Schwachstellensuche beginnen.

- ✔ **Auftretende Risiken:** Halten Sie beim ethischen Hacken Notfallpläne für den Fall bereit, dass etwas schiefgeht. Was passiert, wenn Sie sich mit der Firewall oder einer Webanwendung befassen und diese lahmlegen? Dann werden Systeme vielleicht unerreichbar, was wiederum die Leistung der anderen Systeme und/oder die Produktivität von Mitarbeitern negativ beeinflussen kann. Schlimmer noch, dabei könnten Daten verschwinden oder beschädigt werden, wovon Ihr Ruf nicht gerade profitiert. Und es verärgert bestimmt die eine oder andere Person und hinterlässt keinen sonderlich guten Eindruck. All dies birgt unternehmerische Risiken.

  Gehen Sie bei sozialen Manipulationsversuchen und DoS-Angriffen vorsichtig vor. Ermitteln Sie vorher, wie sie sich auf die zu testenden Systeme auswirken.

- ✔ **Termine für die Tests und deren zeitliche Abläufe:** Terminpläne erfordern Sorgfalt und sollten gründlich überlegt werden. Führen Sie die Tests während der normalen Geschäftszeiten durch? Sollten sie spät in der Nacht, in den frühen Morgenstunden oder am Wochenende stattfinden, um keine Produktivsysteme zu beeinträchtigen? Binden Sie andere Personen ein, um dafür zu sorgen, dass Ihre Terminplanung auch die notwendige Zustimmung findet.

  Sie können auf Widerstände und DoS-Probleme stoßen. Den besten Ansatz bieten aber unbeschränkte Angriffe, bei denen an beliebigen Terminen beliebige Tests gefahren werden können. Missetäter greifen Systeme schließlich auch nicht nur zu bestimmten Zeiten an. Diese Vorgehensweise unterliegt aber einigen Ausnahmen: soziale Manipulationen, DoS-Angriffe und Geräte selbst betreffende Sicherheitstests.

- ✔ **Eigene Entdeckung:** Eine der Zielsetzungen könnte darin bestehen, bei den Tests unentdeckt zu bleiben. Sie könnten Ihre Tests beispielsweise von anderen Standorten aus durchführen. Ansonsten werden Benutzer und das IT-Team versuchen, sich vorbildlich zu verhalten oder Sie möglicherweise sogar zu stellen. Normales Verhalten sieht jedenfalls anders aus.

- ✔ **Aktive Sicherheitskontrollen:** Ein wichtiger, aber häufig übersehener Aspekt besteht darin, ob Sicherheitskontrollen wie Firewalls, IPS-Systeme (Intrusion Prevention System) und WAFs (Web Application Firewalls) aktiviert bleiben sollen, um Suchvorgänge und

Exploits blockieren zu können. Wenn diese Kontrollen aktiviert bleiben, erhält man ein Bild vom wirklichen Stand der Dinge im praktischen Einsatz. Für mich war es allerdings sehr viel wertvoller, wenn derartige Kontrollen deaktiviert wurden (oder der eigenen IP-Adresse ungehinderter Zugang eingeräumt wurde), um einen Blick hinter die Vorhänge werfen und möglichst viele Schwachstellen erkennen zu können. Viele Kunden werden ihre Sicherheitskontrollen aktiviert lassen wollen. Bei dieser Vorgehensweise stehen sie ja schließlich auch besser da, weil dann wahrscheinlich viele Sicherheitsprüfungen blockiert werden. Für mich ist dieser Ansatz mit eingeschalteten Abwehrmaßnahmen zwar auch in Ordnung, kann aber auch zu einem falschen Eindruck von der Sicherheit führen. Möglicherweise wird nicht das ganze Bild der Organisation und dessen Haltung in Sicherheitsfragen wiedergegeben.

- ✔ **Kenntnisse über die Systeme vor Beginn der Tests:** Sie müssen die zu testenden Systeme nicht umfassend kennen, sollten sie aber grundlegend verstehen. Das reicht aus, um sich selbst und die zu testenden Systeme schützen zu können. Bei eigenen Systemen oder die des eigenen Unternehmens sollte das nicht allzu schwierig sein. Bei Kundensystemen müssen Sie vielleicht ein wenig tiefer graben. Ich selbst hatte bisher jedenfalls nur ein oder zwei Kunden, bei denen ich die Systeme völlig »blind« begutachten sollte.

  IT-Manager und Sicherheitsverantwortliche mögen derartige Untersuchungen meist nicht, weil sie länger dauern, mehr kosten und weniger effektiv sind. Sorgen Sie dafür, dass anstehende Tests den Anforderungen des Unternehmens oder der Kunden gerecht werden.

- ✔ **Zu ergreifende Aktionen bei Entdeckung größerer Schwachstellen:** Hören Sie nicht gleich auf, wenn Sie die eine oder andere Sicherheitslücke gefunden haben. Fahren Sie fort, um festzustellen, was es noch zu finden gibt. Sie sollen nicht bis ans Ende aller Tage oder bis zum Zusammenbruch aller Systeme testen. Folgen Sie einfach dem eingeschlagenen Pfad, bis weitere Tests nicht mehr sinnvoll sind. Wenn Sie keine Schwachstellen finden können, haben Sie nicht intensiv genug gesucht. Die eine oder andere Schwachstelle gibt es immer. Wenn Sie große Probleme entdecken, müssen Sie das schnellstmöglich den wichtigen Personen (Entwicklern, Administratoren, IT-Managern und so weiter) mitteilen, um die Lücke zu beseitigen, bevor sie ausgenutzt werden kann.

- ✔ **Ergebnispräsentation:** Dazu gehören Berichte über die Suche nach Schwachstellen und ausführliche Berichte über die wichtigen Schwachstellen und entsprechende Gegenmaßnahmen, die es zu implementieren gilt.

Die Auswahl von Werkzeugen

Wenn Sie beim ethischen Hacken keine geeigneten Werkzeuge nutzen, werden Sie kaum befriedigende Resultate erzielen können. Womit nicht gesagt ist, dass Sie bei Einsatz passender Werkzeuge alle Schwachstellen finden. Die Erfahrung zählt.

Sie sollten Ihre persönlichen und technischen Grenzen kennen. Viele Programme zur Suche nach Schwachstellen produzieren falsche positive oder negative Ergebnisse (identifizieren Schwachstellen also nicht richtig). Andere übersehen Schwachstellen ganz. In bestimmten Situationen, zum Beispiel beim Testen von Webanwendungen, müssen Sie mehrere Suchprogramme nutzen, um alle oder wenigstens die meisten Schwachpunkte zu finden.

Viele Werkzeuge konzentrieren sich nur auf bestimmte Tests, und kein Werkzeug beherrscht alle Tests. Aus ähnlichen Gründen versuchen Sie normalerweise auch nicht, Nägel mit einem Schraubenzieher einzuschlagen oder mit einem Textverarbeitungsprogramm im Netzwerk nach offenen Ports zu suchen. Daher benötigen Sie auch einen ganzen Satz von Spezialwerkzeugen. Je umfangreicher und besser Ihre Werkzeugsammlung ausgestattet ist, desto leichter können Sie Sicherheitstests durchführen.

Achten Sie darauf, immer das richtige Werkzeug für die jeweilige Aufgabenstellung zu verwenden:

- ✔ Für das Knacken von Kennwörtern benötigen Sie Werkzeuge wie Ophcrack und Proactive Password Auditor.
- ✔ Für tiefgehende Analysen von Webanwendungen sind Prüfwerkzeuge (wie Netsparker oder Acunetix Web Vulnerability Scanner) besser geeignet als Netzwerkanalysatoren wie Wireshark oder OmniPeek.

Die Fähigkeiten vieler Sicherheits- und Hackerwerkzeuge werden oft nicht wirklich verstanden. Das hat schlechtes Licht auf ansonsten hervorragende und legale Werkzeuge geworfen. Dazu trägt gewiss auch die Komplexität vieler dieser Werkzeuge bei. Auf jeden Fall müssen Sie sich mit den Werkzeugen vor deren Verwendung vertraut machen, um sie ihrem Zweck entsprechend einzusetzen. Dazu ein paar Vorschläge:

- ✔ Lesen Sie die Readme-Dateien, Onlinehilfen und die FAQs durch (FAQ – Frequently Asked Questions, also häufig gestellte Fragen).
- ✔ Lesen Sie die Handbücher.
- ✔ Verwenden Sie die Werkzeuge in Labor- oder Testumgebungen.
- ✔ Sehen Sie sich Video-Tutorials bei YouTube an (wenn Sie deren meist schlechte Qualität aushalten).
- ✔ Erwägen Sie, offizielle Trainings der Hersteller oder Anbieter von Sicherheitswerkzeugen oder eines Drittanbieters zu besuchen.

Halten Sie in den Werkzeugen für Sicherheitstests nach diesen Merkmalen Ausschau:

- ✔ Angemessene Dokumentation
- ✔ Detaillierte Berichte über entdeckte Schwachstellen mit Angaben zu deren Ausnutzung und Beseitigung
- ✔ Allgemeine Akzeptanz der Testwerkzeuge in der Branche
- ✔ Verfügbarkeit von Updates und Reaktionstempo des Supports
- ✔ Hochwertige Berichtsfunktionen, die Geschäftsleitungen oder nicht-technischem Personal vorgelegt werden können (insbesondere für die heutige Welt mit ihren Audits und Compliance-Tests)

Diese Funktionen können Ihnen beim Durchführen von Tests und Erstellen von Abschlussberichten Unmengen Zeit und einen Haufen Anstrengungen ersparen.

Fragen Sie bei der Auswahl geeigneter Programme ruhig ein wenig herum. Fragen Sie Kollegen oder Dritte wie zum Beispiel online bei Google, LinkedIn und YouTube. Für Sicherheitstests existieren Hunderte, wenn nicht sogar Tausende Werkzeuge. Die folgende Liste gibt einen Überblick über meine Favoriten aus dem Bereich der kommerziellen, Freeware- oder Open-Source-Sicherheitswerkzeuge:

- ✔ Acunetix Web Vulnerability Scanner
- ✔ Cain & Abel
- ✔ CommView for WiFi
- ✔ Elcomsoft System Recovery
- ✔ Metasploit
- ✔ Nessus
- ✔ NetScanTools Pro
- ✔ Netsparker
- ✔ Nexpose
- ✔ OmniPeek
- ✔ SoftPerfect Network Scanner

Wenn ich mich in den Teilen II bis V mit den verschiedenen Tests beschäftige, werde ich auf diese und viele andere Werkzeuge noch näher eingehen. Im Anhang finden Sie zudem eine umfangreichere Liste geeigneter Werkzeuge, die Ihnen als Referenz dienen kann.

Planumsetzung

Gute Sicherheitstests erfordern Ausdauer. Zeit und Geduld sind wichtig. Passen Sie auch beim Ausführen der Tests auf. Kriminelle in Ihrem Netzwerk oder scheinbar nette Mitarbeiter, die Ihnen über die Schulter blicken, könnten die Vorgänge beobachten und dieses Wissen gegen Sie oder Ihr Unternehmen einsetzen.

Zu Beginn Ihrer praktischen Tests lässt sich unmöglich gewährleisten, dass sich in den Systemen keine Hacker aufhalten. Sorgen Sie dafür, dass alles möglichst ruhig und geheim abläuft. Das ist insbesondere dann wichtig, wenn Sie Testergebnisse übermitteln und speichern. Falls möglich, sollten Sie alle E-Mails und Dateien mit sensiblen Testdaten verschlüsseln. Verwenden Sie dazu PGP (Pretty Good Privacy), verschlüsselte ZIP-Dateien oder ähnliche Technologien.

Damit können Sie sich auf Erkundungsreise begeben. Sammeln Sie möglichst viele Daten über das Unternehmen und die Systeme, wie es Bösewichte tun würden. Beginnen Sie mit einem Gesamtüberblick und konzentrieren Sie sich dann zunehmend auf Details:

1. **Suchen Sie im Internet nach Namen Ihres Unternehmens, Namen der Computer- und Netzwerksysteme und deren jeweiligen IP-Adressen.**

   Als Startpunkt bietet sich dabei Google an.

2. **Engen Sie den Suchbereich dadurch zunehmend ein, dass Sie sich auf die zu testenden Systeme konzentrieren.**

   Beim Überprüfen physischer Sicherheitsstrukturen oder Webanwendungen können Sie viele Informationen über die Systeme ans Licht bringen.

3. **Engen Sie Ihr Blickfeld weiter ein und werden Sie kritischer. Führen Sie die eigentliche Suche und weitere detaillierte Tests aus, um Schwachstellen der Systeme zu erkennen.**

4. **Führen Sie die Angriffe aus und nutzen Sie dabei alle gefundenen Schwachstellen aus, wenn darin Ihre Zielsetzung besteht.**

In den Kapiteln 4 und 5 erhalten Sie weitere Informationen und Tipps zum Ablauf dieses Prozesses.

Ergebnisauswertung

Werten Sie Ihre Ergebnisse aus, um zu ermitteln, worauf Sie gestoßen sind, und gehen Sie davon aus, dass die Schwachstellen bisher noch nicht publik gemacht wurden. Hier zählt Ihr Wissen. Mit zunehmender Praxis nehmen Ihre Fähigkeiten bei der Bewertung der Ergebnisse und dem Erkennen von Zusammenhängen zwischen den entdeckten Schwachstellen zu. Am Ende kennen Sie die Systeme besser als jeder andere. Letztendlich wird es Ihnen mit zunehmender Erfahrung immer leichter fallen, Ihre Untersuchungen fortzuführen.

Übergeben Sie der Geschäftsführung oder den Kunden formale Berichte mit den Ergebnissen und Empfehlungen, die Sie weitergeben wollen. Halten Sie diese Parteien beständig auf dem Laufenden, um sie über Fortschritte zu informieren und ihnen zu zeigen, dass ihr Geld nicht vergeudet wird. In Kapitel 17 wird das Erstellen von Berichten für Sicherheitstests ausführlicher beschrieben.

Wie es weitergeht

Nach Abschluss der Tests müssen Sie (oder Ihr Kunde) noch Ihre Empfehlungen umsetzen, um die Systeme auch wirklich sicher werden zu lassen. Ansonsten wären die Arbeitszeit, das investierte Geld und Ihre Anstrengungen vergeudet gewesen. Leider muss ich das entsprechende Szenario recht häufig beobachten.

Neue Sicherheitslücken treten immer wieder auf. Informationssysteme befinden sich in stetigem Wandel und werden zunehmend komplex. Fortwährend werden auch neue Schwachstellenscanner entwickelt, mit denen sich Sicherheitslücken

aufspüren lassen, die ebenfalls besser werden. Sicherheitstests können immer nur Momentaufnahmen des aktuellen Sicherheitszustands Ihrer Systeme liefern. Jederzeit kann sich alles ändern, und zwar besonders dann, wenn Sie Software aktualisieren, Computersysteme hinzufügen oder Patches installieren. Ihre Zeitplanung sollte regelmäßige und kontinuierliche Tests (einmal im Monat, im Vierteljahr oder im Halbjahr) vorsehen. In Kapitel 19 geht es um die Verwaltung von Änderungen, zu denen es im Laufe der Zeit im Zusammenhang mit der Systemsicherheit kommt.