1 Ziel dieses Buches

Dieses Buch soll Ihnen dabei helfen, Ihren Web-Server und Ihr Netzwerk besser zu schützen. Wir geben Ihnen Installationshilfen und Anregungen, wie Sie den Web-Server Ihrer Wahl schon mit den mitgelieferten „Bordmitteln“ und einfachen aber wirksamen Zusatzmodulen und Tools so sicher wie möglich installieren können. Dazu werden Möglichkeiten genannt, wie Sie lizenzfreie und kommerzielle Tools und Programme richtig einsetzen. Wir wollen mit diesem Buch die Sensibilität für das Thema IT-Sicherheit wecken, erweitern und vertiefen, damit Sie möglichst gut gewappnet sind gegen das, was draußen vor ihrer Firewall, aber auch innerhalb Ihres Netzwerkes passiert oder passieren kann.

Es soll hier keine allgemeine Verunsicherung verbreitet werden. Aber in Presse, Rundfunk, Fernsehen oder Newsforen im Internet erfahren Sie täglich von neuen Vorfällen der Internet-Kriminalität (siehe dazu das nächste Kapitel.).

Administratoren sind oftmals in einer Zwickmühle. Sie müssen ihre Systeme vor unbefugten und unberechtigten Zugriffen absichern, aber die Bedienung und den Zugriff so einfach gestalten, dass alle berechtigten Personen ohne aufwendige Schulungen arbeiten können. Dies gleichzeitig zu gewährleisten ist keine leichte Aufgabe. Die Lektüre dieses Buches und die Umsetzung unserer Ratschläge wird Sie in Ihrer wichtigen Aufgabe unterstützen.

Unser Buch ist wie folgt gegliedert:

Am Anfang werden theoretische Grundlagen gelegt: Nach allgemeinen Ausführungen in Kapitel 2 über die Notwendigkeit der Sicherheit von Web-Servern und Formen der Internetkriminalität geben wir in Kapitel 3 einen Einblick in die Struktur des Apache- und des IIS Web-Servers. In Kapitel 4 behandeln wir die Grundlagen von Protokollen, Datenverkehr und Logfiles, die zum Verständnis der nachfolgenden Kapitel notwendig sind. In Kapitel 5 werden die Zugriffsmethoden auf Daten beschrieben, die bei Web-Servern möglich sind, und in Kapitel 6 behandeln wir die im WWW verwendeten Programmiersprachen mit ihren Stärken, aber auch Schwächen.

Die nächsten Kapitel, beginnend mit Kapitel 7, beschreiben die Angreifer auf Web-Server und ihre Methoden. In Kapitel 8 zeigen wir, wie Sie die Verwundbarkeit Ihres Web-Servers in einem Penetrationstest prüfen können. In Kapitel 9 wird ge-

zeigt, wie einfach die Informationsbeschaffung von einem ungeschützten Web-Server für Kriminelle funktioniert.

Nach der detaillierten Behandlung der Architekturen und Funktionsweisen des Apache Web-Servers (Kapitel 10) und des Microsoft IIS (Kapitel 11) zeigen wir in Kapitel 12 und 13 im Sinne einer Schwachstellen-Identifikation, wie Angriffe auf diese beiden Web-Server durchgeführt werden können.

Schließlich behandeln wir in Kapitel 14, wie Sie Ihren Web-Server gegen Angriffe absichern können, und in Kapitel 15, was nach einem erfolgten Angriff zu tun ist. In Kapitel 16 ziehen wir das Fazit.

2 „Wir sind sicher – Wir haben eine Firewall“

Die Behauptung „Wir sind sicher – Wir haben eine Firewall“ hören Administratoren und Sicherheitsbeauftragte in den Unternehmen mehr als einmal in ihrem Berufsleben von ihren Vorgesetzten. Wenn sie dafür jedes Mal einen Extratag Urlaub bekommen hätten, würden viele schon im wohlverdienten und bezahlten Vorruhestand weilen.

Natürlich sichert eine Firewall ein Netzwerk in einem gewissen Sinne gegen Angriffe ab, aber bei weitem nicht ausreichend. Eine herkömmliche Firewall kann zwar z.B. Ports freigeben oder blocken, jedoch bietet sie allein keinen ausreichenden Schutz gegen das Eindringen Unbefugter in das Netzwerk des Unternehmens.

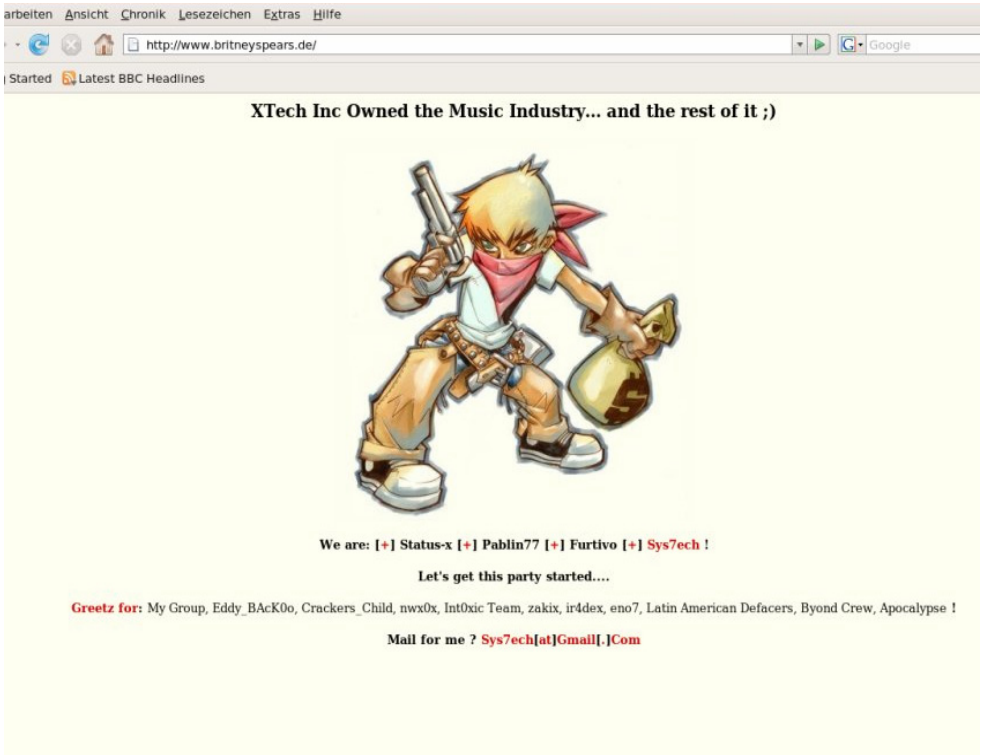

Abbildung 1: Defacing von Künstlerseiten bei Sony BMG

Meldungen[3] zeigen immer wieder, wie wichtig das Problembewusstsein für die Sicherheit der eigenen Systeme ist. Sie möchten sicher nicht, dass Sie als Verantwortlicher für die IT oder die Internet-Seiten an einem Montagmorgen von Ihrem Chef angerufen werden, der Ihnen Fragen nach der neuen Homepage stellt (siehe Abbildung 1).

Innerhalb der letzten Jahre wurden Web-Server bekannter Unternehmen und Organisationen von sogenannten Hackern heimgesucht, wie die vom Chaos Computer Club,[4] der Firma SCO und der amerikanischen Raumfahrtbehörde NASA [/1/].

In weiteren Fällen wurden durch ein Defacing die Webseiten einiger Bundesbehörden in den USA geändert.

Bedingt durch die immer schneller werdenden Internetanschlüsse und leistungsfähigere Hardware können Angriffe immer effektiver vorgenommen und koordiniert werden. Das bedeutet, dass Entwicklungen, die die Effizienz der IT der Unternehmen steigern, leider auch von Kriminellen zum Schaden der Unternehmen genutzt werden können, es sei denn, dass dies durch Sicherheitsvorkehrungen unmöglich gemacht wird. Als bestes Beispiel soll hier nur der DDoS-Angriff auf die Microsoft Update Seite 2004 angeführt werden.

Laut Handelsblatt[5] unterschätzen vor allem mittelständische Unternehmen die Gefahren, die aus der IT im Allgemeinen und dem Internet im Speziellen drohen. Deshalb sollten Sie sich und Ihren Vorgesetzten immer wieder vor Augen halten, was in einem „worst case“-Scenario passieren kann: Es könnten Kundendaten wie z.B. Kreditkartennummern in unbefugte Hände gelangen. Das Vertrauen der Kunden in Ihr Unternehmen nach einem solchen Vorfall ist erschüttert. Unternehmensleitung und Vorstand können bei einem nachgewiesenen Fehlverhalten zur Rechenschaft und somit zur persönlichen Haftung herangezogen werden. Das Resultat wäre verheerend: vom drohenden Umsatzrückgang bis zum Bankrott des Unternehmens. Diese gravierenden Folgen sollten doch jeden anspornen, in die Sicherheit der eigenen IT-Infrastruktur zu investieren.

Jedoch reicht es nicht aus, einzelne Sicherheitsmaßnahmen isoliert zu implementieren. Ein Beispiel für “Security by Obscurity”, d.h. nicht zu Ende durchgeführte Sicherheitsmaßnahmen, ist ein drastischer Fall aus Italien bei einer Filiale der Banco di Brescia. Diese Filiale hatte ihren Zugang zum Bankgebäude über ein biometrisches System geschützt. Wenn ein Kunde in die Bank wollte, musste er sich über seinen Fingerabdruck ausweisen. Doch der eingescannte Fingerabdruck wurde nicht mit einem Referenzabbild des Fingerabdrucks verglichen, sondern nur zur

[3]http://www.heise.de/newsticker/meldung/84400

[4]Vgl. http://www.ccc.de

[5]Handelsblatt. Donnerstag, 10.Mai 2007

Abschreckung gespeichert: „Wer seinen Fingerabdruck beim Betreten der Bank abgibt, wird schon nicht auf die Idee kommen, die Bank zu überfallen“, so dachte es sich die Filialleitung. So viel zur Theorie. Zwei findige Bankräuber verschafften sich Zugang zur Bank mit einem abgetrennten Finger einer unbekannten Person, überfielen die Bank und entkamen unerkannt. Die Täter wurden bis heute nicht gefasst[6].

“To rise from error to truth is rare and beautiful” (Victor Hugo, franz. Poet und Dramatiker, 1802–1885).

[6] http://www.ilmessaggero.it/index.php?data=20070127&pag=42&dorso=NAZIONALE&ediz=01_NAZIONALE&vis=G&ps=0&tt=P und http://www.heise.de/newsticker/meldung/84425

3 Allgemeines zu Web-Servern

Computer und dazugehörige Systeme (Betriebssysteme, Anwendungen etc.) gehören zum täglichen Leben, sei es im Büro oder auch im privaten Gebrauch. Alle Anwender möchten Daten empfangen und versenden. Man möchte immer „online sein“, der Zugriff auf Daten und Dienste muss permanent möglich sein. Computersysteme gibt es für die unterschiedlichsten Anwendungsbereiche, mehr oder weniger passend mit verschiedenen Merkmalen. Ein Merkmal einer Reihe heutiger Computersysteme ist der Mangel an Sicherheit. Sicherheitsaspekte wurden bei der Konstruktion vieler Computersysteme einfach nicht mit berücksichtigt (von wenigen Ausnahmen abgesehen, z.B. Hochsicherheitsanlagen im Steuerungsbereich von Atomkraftwerken, die mehrfach redundant ausgelegt sind). Für das Internet und die dort erreichbaren Server und Dienste beispielsweise trifft dies ganz sicher zu.

Die Konstrukteure und Entwickler sahen die Anwendung ihrer Geräte eher in einem Umfeld aus sich gegenseitig vertrauenden und integeren Personen und Anwendern. Daher war Sicherheit im Sinne von missbräuchlicher Verwendung kein Thema. Die ersten Server, die ihre Dienste im Internet angeboten haben, hatten ein vom Betriebssystem implementiertes Vertrauensverhältnis (in Unix-Systemen wird dazu die Unix-Datei rhosts genutzt), so dass ein Anwender auf einem Server, der auf dem eigenen System so genannte root-Rechte, also ebenfalls Administrationsrechte hatte, automatisch auf dem anderen Server diese administrativen Rechte besaß.

Viele Unix-Systeme, die noch nicht per Update auf den neuesten Stand gebracht wurden, sind somit äußerst anfällig und können problemlos von einem Angreifer – in der Presse wird immer vom Cracker oder Hacker gesprochen – übernommen werden.

Im Laufe der Zeit haben sich das Umfeld und das Einsatzgebiet von Computern geändert. Computersysteme werden heute von Millionen von Personen aus allen Gesellschaftsschichten und Kulturen für eine Unmenge von Zwecken eingesetzt. Dienste, wie das Online-Banking und Shopping, Nutzen von Auktionen bei Ebay oder der Informationsaustausch per Email und Download, werden als selbstverständlich angesehen. Fatalerweise bewegen sich in diesen Bereichen verstärkt auch Personen, die diese angebotenen Dienste missbräuchlich nutzen und in Systeme eindringen, um sich und Dritten Vorteile zu verschaffen. Diese Vorteile können

z.B. Forschungsergebnisse, Geschäfts- oder Kundendaten sein. Es kann also nicht mehr davon ausgegangen werden, dass es so etwas wie einen von allen Anwendern respektierten und eingehaltenen Ehrenkodex gibt, der die missbräuchliche Verwendung verbietet. Dieser Ehrenkodex, auch unter der Bezeichnung Hacker-Ethik zu finden, wurde in den 60er und 70er Jahren in sechs Forderungen definiert [KYAS/CAMPO00]. Doch finden sich diese ursprünglichen Ziele in der heutigen Szene nur noch selten wieder bzw. werden immer seltener beachtet.

Daher ist ein gewisser Anteil von Missbrauch eine beinahe alltägliche Erscheinung. Dass es diesen gibt, wird durch Studien, Presseberichte und auch durch „Erfahrungen aus dem Alltag" (Computerviren sind in diesem Zusammenhang das bekannteste Beispiel für eigene Erfahrungen) belegt.

Mit zunehmendem Einsatz der EDV-Technik wird eine Gesellschaft jedoch von ihr abhängig. Ein Ausfall oder eine Beeinträchtigung der Funktionsweise von EDV-Anlagen kann gravierende Auswirkungen auf die Wirtschaft und auf die Sicherheit von Personen haben. Als Beleg für diese Aussage sollen in diesem Zusammenhang die Besorgnis und die Vorkehrungen im Zusammenhang mit der Datumsumstellung auf das Jahr 2000 angeführt werden.

Der relativ glimpfliche Verlauf dieser Datumsumstellung steht damit nicht im Widerspruch. Man braucht sich nur vorzustellen, dass die Umstellung nicht so reibungslos verlaufen wäre, und sich die Folgen vor Augen führen. Was gestern die Datumsumstellung war, kann morgen etwas anderes, z.B. ein besonders „aggressiver" Virus, sein, wie der „I Love You-Virus" Mitte des Jahres 2000 oder der „Blaster-Virus" und der „Sobig-Wurm[7]" im Jahr 2003 (unter anderem DDoS-Angriff auf die *Microsoft* Update Web-Server).

Allein für das Jahr 2003 wurden nach Schätzungen 10,4 Milliarden Euro Schäden durch Spam, 8,4 Milliarden Euro Kosten durch Viren und 1 Milliarde Euro Verluste durch Hackerangriffe verursacht [/2/]. Der „MyDoom"-Virus in seinen beiden Varianten „A" und „B", der im Januar/Februar 2004 millionenfach im Internet versendet wurde, hat bis zum 2.02.2004 einen Schaden von umgerechnet US$ 21 Milliarden angerichtet [ABENDBLATT04]. Demgegenüber stehen Aussagen und Zahlen, aus denen hervorgeht, dass nur ca. 25% deutscher Unternehmen einen verantwortlichen Beauftragten für die Themen Datenschutz und Datensicherheit haben [/3/] und die meisten Unternehmen noch im Jahr 2002 mehr Geld für Kaffee ausgaben als für ihre IT-Sicherheit [/4/].

[7] Nähere Infos zu diesen Viren siehe unter http://vil.nai.com/vil/alphar.asp

Daher ist die Lösung von Sicherheitsproblemen von eminenter Bedeutung. Dafür gibt es eine Fülle (in den meisten Fällen sogar eine ausreichende Menge) an brauchbaren und verlässlichen Methoden und Verfahren, um Computersysteme hinreichend sicher zu machen. Diese Methoden müssen allerdings richtig angewandt und soweit wie möglich in die Computersysteme integriert werden (leider werden Sicherheitsprodukte heute oftmals nachträglich zu bestehenden Systemen hinzugefügt und können daher eventuell umgangen werden[8]). Und das Wichtigste: Die Sicherheitsproblematik muss verstanden werden.

Die Ziele, die es mit den Sicherheitsprodukten zu erreichen gilt, müssen eindeutig definiert sein. Was man mit einem Sicherheitsprodukt verhindern will, muss deutlich gemacht werden. Was erreicht und verhindert werden soll, steht in Zusammenhang mit der Arbeit, die mit einem EDV-System erledigt wird. In den meisten Fällen ist ein EDV-System Teil einer Organisation (z.B. Firma, Behörde etc.). Genauso, wie technische Lösungen für die Sicherheitsprobleme in das technische Produkt (Computer) integriert sein sollen, sind organisatorische Lösungen für die Sicherheitsprobleme in eine Firma oder eine Behörde einzuarbeiten.

Durch das stetig wachsende Interesse an Computern ist der Begriff „Hacker“ auch für „Nicht-Computerbesitzer“ längst kein Fremdwort mehr. Im letzten Jahrzehnt gab es kaum eine Grenze, die ein Hacker nicht überschritten hätte. In den Medien[9] werden immer wieder Schlagzeilen gemeldet, in denen Webseiten[10], Web-Server[11] und Datenbanken gehackt wurden. So wurden allein im Juli und im August 2003 die Web-Server von Microsoft [/4/] und der NASA in den USA sowie die Server des Online-Spiels *„Dark Age of Camelot“* [/7/] durch so genannte DoS-Angriffe (Denial-of-Service) angegriffen. *Microsoft* gab einen Tag später folgende Meldung bekannt [/7/]: *“Microsofts Website ist am Freitagabend deutscher Zeit Opfer einer Denial-of-Service-Attacke geworden. Wie US-Quellen berichten, wurden die Server durch extrem hohen Traffic für eine Stunde und 40 Minuten lahm gelegt. Microsoft bestätigt den Vorfall in einem Bulletin und deutet an, dass eine polizeiliche Untersuchung eingeleitet worden sei. In der Mitteilung versichert der Software-Riese, der Angriff stehe in keinerlei Zusammenhang zu einer bekannten Schwachstelle in seiner Software.“*

Die IT-Fachmesse Systems-World (München) meldete im Juli 2003 in ihrem Newsletter [/6/] für das erste Halbjahr 2003 13,7% mehr Internet-Attacken im Vergleich zum ersten Halbjahr 2002. Der Bericht beruft sich auf die Ergebnisse des Sicher-

[8] Das Prinzip des „schwächsten Gliedes in der Kette“

[9] Vgl. dazu http://www.heise.de.

[10] Z.B. im Sommer 2001 die Webseiten von Yahoo, Amazon und Quelle [/1/]

[11] Z.B. im Sommer 2000 der Application-Server von Microsoft mit dem Sourcecode zu Windows 2000

heitsspezialisten Internet Security Systems[12] (ISS). Laut ISS wurde der Port 80, also der Standardport eines Web-Servers, am häufigsten attackiert (45,54%).

Diese Arbeit wird sich mit den theoretischen Grundlagen der IT-Sicherheit, den Begriffsbestimmungen befassen und im Anschluss daran praxisnahe Beispiele für Attacken auf die Web-Server der Firma *Microsoft*, dem IIS Web-Server, und der *Open Software Foundation*, dem Apache Web-Server, erläutern und nachstellen. Es soll die Frage geklärt werden, ob und wie ein Unternehmen sich gegen Attacken wehren kann. Zu diesen Attacken gehören sowohl Zugriffe aus dem Internet als auch aus dem lokalen Netzwerk eines Unternehmens, um Angriffe eigener Mitarbeiter zu simulieren.

Was kann aus diesem Kapitel auf das eigene Netzwerk übertragen werden?

Haben Ihre Systeme eine Vertrauensstellung gegenüber anderen Systemen? Sind Ihre Systeme aktuell oder hätten diese Systeme nicht schon lange auf die nächsthöhere Betriebssystemversion mit allen aktuellen Patchständen erweitert werden müssen?

Vielleicht gibt es auch noch Systeme, die einen veralteten Virenscanner haben oder nicht in das automatische Verteilungssystem der Updates integriert worden sind? Haben Sie noch Testsysteme im Netzwerk integriert, die nach dem letzten Releasewechsel oder nach Beendigung eines Projektes noch nicht entfernt wurden und weiter fleißig vor sich hin „testen“?

Hatten Sie einen Personalwechsel in Ihrem EDV-Team? Müssen Passwörter angepasst werden? Wurden die Zugangssysteme, die eine Verbindung aus dem Internet oder eine Einwahl regeln (VPN-Verbindungen etc.), aktualisiert und mit neuen Passwörtern versehen?

[12] Vgl. dazu www.iss.net.