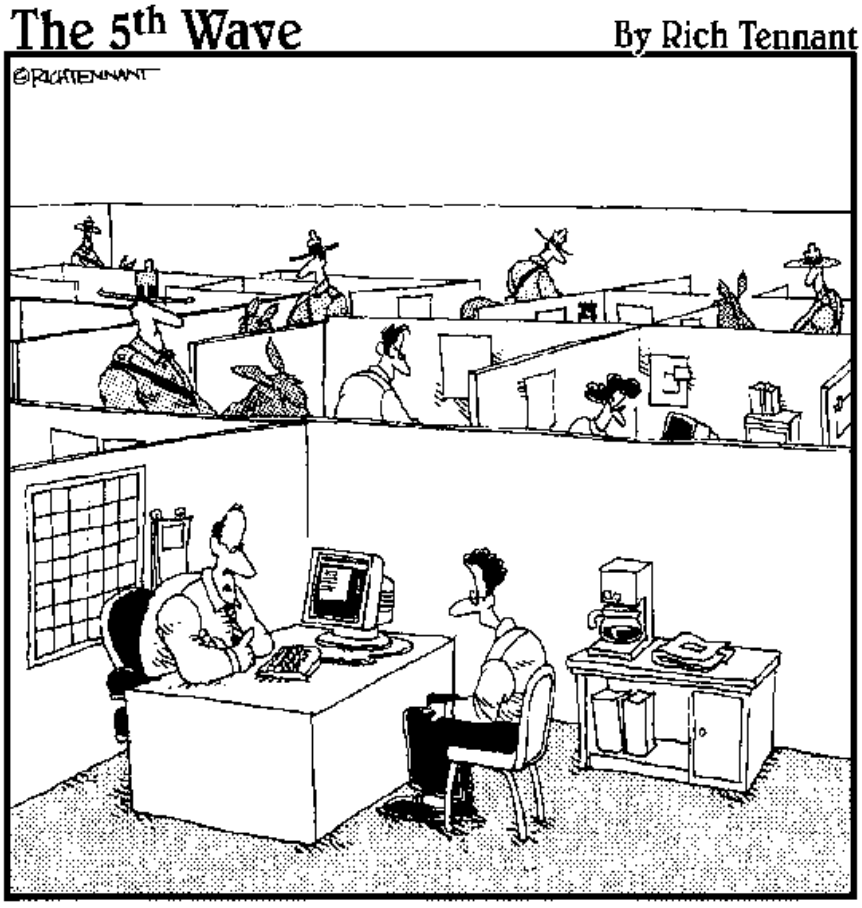
Teil I

Der Weg zu mehr Netzwerksicherheit



»In unserer Firma wird Netzwerksicherheit sehr ernst genommen.«

In diesem Teil ...

Wahrscheinlich haben Sie schon den einen oder anderen Bericht im Fernsehen verfolgt, in dem über eine bösartige neue Virusattacke berichtet wurde, die weltweit Computersysteme angreift und Riesenschäden anrichtet. Oder Sie haben einen Artikel im Wirtschaftsteil Ihrer Zeitung gelesen, der sich mit dem Thema Computerkriminalität auseinander setzt. Im Radio hörten Sie vielleicht, dass Hacker auf eine beliebte Website zugegriffen und Tausende von Kreditkartennummern gestohlen haben. Und ausgerechnet diese Site haben Sie unlängst besucht!

Das ist meist der Zeitpunkt, an dem so mancher in die Gänge kommt und von Angst erfüllt den Sicherheitsstatus seines eigenen Netzwerks unter die Lupe nimmt. Was passiert, wenn Hacker Ihr System angreifen und Sie alles verlieren? Wie bekommen Sie überhaupt heraus, ob eine Hackerattacke erfolgt ist? Und was können Sie dagegen tun?

Entspannen Sie sich erst mal und holen Sie tief Luft. Die oben erwähnten Geschichten sind zwar wahr, doch es gibt eine Reihe von Dingen, die Sie tun können, um sich zu schützen und von Ihrem Netzwerk Schaden abzuwenden. Die Kapitel in diesem Teil werden Sie auf den richtigen Weg zu mehr Netzwerksicherheit führen. Und auch wenn Sie wissen wollen, welche Sicherheitsprobleme am häufigsten auftreten, sind Sie hier genau an der richtigen Adresse.

Den Weg zu mehr Netzwerksicherheit beschreiten

1

In diesem Kapitel

- Wissen, wonach man sich in einem Netzwerk umsehen muss
- Die ersten Schritte in Angriff nehmen, um Ihr Ziel zu erreichen
- Die richtigen Werkzeuge an die entsprechenden Positionen legen
- Erkennen, wovor Sie auf der Hut sein müssen
- Die acht Gebote der Netzwerksicherheit verstehen

Der Weg zu mehr Netzwerksicherheit muss per se nicht immer mühsam und voller Hindernisse sein. Sicher – so mancher Experte, der nicht nur *Ihr* Wohlergehen im Auge hat, möchte Sie glauben lassen, dass Netzwerksicherheit kompliziert und darüber hinaus teuer ist und deshalb am besten dem fähigen Händchen des Experten überlassen werden sollte. Doch die Wahrheit ist: Jeder Benutzer, der über einen mittleren Erfahrungs-Level in Bezug auf Netzwerke und Computer verfügt, kann viele grundlegende Sicherheitsmaßnahmen selbst durchführen. Untersuchungen des FBI weisen nach, dass mehr als 80 Prozent der Attacken auf die Netzwerksicherheit hätten vermieden werden können, wenn vorab eine Reihe von bestimmten Sicherheitsmaßnahmen getroffen worden wäre. Doch oft werden diese Basismaßnahmen schlichtweg ignoriert und dies ist oftmals die Ursache für diese traurige Statistik. Dieses Buch soll Ihnen als ein Tool dazu dienen, sich und anderen beizubringen, mit welchen Maßnahmen die Sicherheit Ihres Netzwerkes erhöht werden kann.

Folgende Frage wird mir immer wieder gestellt: »Ich habe nur ein kleines Unternehmen, wirklich ganz unbedeutend. Warum sollte ein Hacker ausgerechnet in mein System eindringen wollen?« Die Antwort lautet: »Warum sollte er nicht?« Alle in einem Netzwerk zusammengefassten Computer – und das Internet ist ein Netzwerk – sind nur eine Nummer, ähnlich einer Telefonnummer. Ein Hacker kann nun anhand der Nummer nicht erkennen, ob er es mit einem großen oder nur mit einem kleinen Netzwerk zu tun hat. Für ihn sind sie so oder so nur ein weiteres Zielobjekt; er probiert einfach alles aus, was ihm interessant erscheint. Wenn nun in Ihrem Netzwerk nichts geboten wird, was sein Interesse erweckt, kann der Hacker Ihr Netzwerk auch dafür benutzen, andere zu attackieren. Sie stehen dem aber nicht hilflos gegenüber: Viele Attacken lassen sich verhindern und Sie haben vielerlei Möglichkeiten, Hackern das Leben schwerer zu machen.

In diesem Kapitel möchte ich Sie unterstützen, den Weg zu mehr Netzwerksicherheit zu beschreiten. Dabei lernen Sie im ersten Schritt, sich mit den einzelnen Komponenten Ihres Netzwerks vertraut zu machen. Denn wenn Sie nicht wissen, wie Ihr Netzwerk funktioniert, woher sollen Sie dann wissen, wenn etwas nicht stimmt?

Wichtige Sicherheitsbelange identifizieren

Obwohl Netzwerke, was Architektur, Verwendung und Komplexität betrifft, stark variieren können, sind sie sich doch in Bezug auf ihre Sicherheitsanforderungen erstaunlich ähnlich. So erfolgt beispielsweise der Zugriff auf alle Netzwerke über Passwörter und alle Netzwerke sind bis zu einem gewissen Grad anfällig für Virenattacken. Bevor Sie nun ein effektives Sicherheitssystem für Ihr Netzwerk entwerfen und implementieren, sollten Sie sich mit den entsprechenden Belangen intensiv auseinander setzen und erst dann entscheiden, ob Sie Schutz benötigen oder nicht, und wenn ja, welche Art von Schutzmaßnahmen für Ihr Netzwerk am geeignetsten ist.

Letztendlich wird Ihre tatsächliche Netzwerksicherheit von drei Faktoren beeinflusst: Schutzmethode, Sicherheitsaufwand und welche Philosophie Sie den Sicherheitsanforderungen zugrunde legen. Wenn Sie nur wenig Schutzmechanismen eingebaut haben und keinen Grund für weitere diesbezügliche Maßnahmen sehen, kann man den Sicherheitsgrad für Ihr Netzwerk als schwach oder passiv bezeichnen. Wenn Sie auf der anderen Seite in Ihr System starke Schutzmaßnahmen implementiert haben, Ihre Mitarbeiter dazu motivieren, Sicherheitsrichtlinien zu studieren und zu beachten, und auch regelmäßig überprüfen, ob die festgelegten Sicherheitsbestimmungen eingehalten werden, dann werden Sie sicherlich über ein hohes Maß an Netzwerksicherheit verfügen.

In den folgenden Abschnitten werde ich den ebenso umfangreichen wie vielfältigen Themenbereich zur Netzwerksicherheit behandeln und Sie darüber hinaus auch mit ein paar allgemeinen Informationen versorgen. In späteren Kapiteln werden diese Informationen dann ausführlicher erläutert.

Passwörter

Passwörter sind der Schlüssel zu Ihrem Netzwerk, doch leider sind sie auch am einfachsten zu »knacken«. Ein leicht zu identifizierendes Passwort kann schnell zur Folge haben, dass sich ein unbefugter Benutzer an Ihrem Computer anmeldet und auf Ihr Netzwerk zugreift. Und ich meine in diesem Zusammenhang nicht nur Hacker. So manch aufgebrachter Angestellte träumt heimlich davon, Ihnen den Tag zu verderben, indem er an Ihrem Netzwerk manipuliert. Ein schlechtes, sprich ein ungesichertes Passwort nützt genauso viel bzw. wenig wie ein gar nicht vorhandenes Passwort. Doch trotz dieser Tatsache kann man sich noch immer in vielen Firmen nicht dazu aufraffen, den entsprechenden Passwortregeln Geltung zu verschaffen, da solche Regeln eher als lästig und unbequem empfunden werden. Diese kurzsichtige Betrachtungsweise hat schon zum Untergang von etlichen Unternehmensnetzen und Regierungsnetzwerken geführt!

Es kann sehr einfach sein, Passwörter von Netzwerken zu klauen, auch wenn Sie in einem bestimmten System gar nicht eingeloggt sind. Passwörter durchlaufen Netzwerke auf einer nahezu konstanten Basis und da muss nur ein nett platziertes Lauschprogramm auftauchen (so genannte *Passwort-Sniffer*) und innerhalb weniger Stunden können hunderte oder gar tausende von Passwörtern eingesammelt werden.

Aber, werden Sie sagen, Passwörter sind doch verschlüsselt! Das mag schon sein, doch die verwendete Verschlüsselungsmethode ist gewöhnlich nicht effektiv genug. So genannte *Passwort-Cracker* – also Programme, die mit Hilfe einer Kombination von logischen Wörtern und Begriffen aus dem Wörterbuch verschlüsselte Passwortdateien entschlüsseln können – sind über das Internet frei verfügbar.

Das Verwenden von sicheren, schwer zu entschlüsselnden Passwörtern ist eine einfache, aber durchaus wirksame Methode zum Schutz gegen Eindringlinge. Siehe auch der Abschnitt *Sichere Passwörter verwenden* weiter unten in diesem Kapitel, wo Sie die entsprechenden Kriterien nachlesen können.

Viren, E-Mails und ausführbare Dateien

Mit E-Mails steht Ihnen ein wunderbares Werkzeug zur Verfügung, Ihre Arbeitsproduktivität zu erhöhen. Leider bieten E-Mails aber auch eine vortreffliche Angriffsfläche für Viren und bösartige Programme, die verheerenden Schaden anrichten und Daten zerstören können. Noch vor sechs Jahren habe ich Leute belehrt, dass sie sich durch das einfache Öffnen einer E-Mail-Nachricht keinen Virus einfangen können. Heutzutage jedoch werden Viren oder schädliche Programme in vielen Fällen über E-Mails übertragen. Dabei sind die meisten Viren, die sich in E-Mails verstecken, eher lästig als gefährlich, doch oft sind mehrere Arbeitsstunden erforderlich, um das System von den gemeinen kleinen Dingern zu befreien. Hier bieten Antiviren-Programme einen hervorragenden Schutz. (Siehe auch weiter unten im Abschnitt *Antiviren-Software einsetzen*.)

10pht crack + 15 Sekunden = 670 Sicherheitslücken

Vor einiger Zeit stellte ich mal ein Cracker-Programm mit dem Namen *l0pht crack* (l-zero-p-h-t) vor. Den darin integrierten Sniffer startete ich um 8 Uhr morgens, zu einem Zeitpunkt, an dem sich die meisten Angestellten für ihr Tageswerk anmelden. Eine Stunde später, also um 9 Uhr, hatte ich über 1.400 verschlüsselte Passwörter und Benutzer-Logins vorliegen. Ich ließ dann ein Entschlüsselungsprogramm ablaufen und es gelang mir mit dessen Hilfe, in nur 15 SEKUNDEN (!) 47 Prozent der Passwörter zu »knacken«. Wie viele Passwörter sind nötig, um ein Netzwerk betreten zu können? Eins genügt in der Regel. Doch dank des Programms l0pht crack standen mir fast 670 Passwörter zur Verfügung! Unter diesen waren u.a. das Passwort des Firmenvorstands sowie auch Passwörter von Netzwerkadministratoren.

Zwei Wochen später wiederholte ich diese Prozedur. Allerdings wurden alle Mitarbeiter der Firma dazu angehalten, sichere Passwörter anzulegen, und alle hatten auch Ihr vorheriges Passwort geändert. Das Ergebnis war, dass sich die schwieriger zu entschlüsselnden Passwörter viel standhafter zur Wehr setzen konnten, dechiffriert zu werden. Das Cracking-Programm musste fast 72 Stunden ablaufen, bevor ich ein verwendbares Passwort zur Hand hatte.

Viren sind aber nicht das einzige Problem, das in Zusammenhang mit E-Mail-Programmen auftreten kann. Wie halten Sie es beispielsweise mit Anlagen, die Ihren E-Mails beigefügt sind? Oder was ist mit ausführbaren Programmen wie Bildschirmschoner und Spiele? Viele bösartige Programme befallen ein System über derlei Umwege. Diese Programme – *Trojanische Pferde* genannt – können sowohl direkten Schaden anrichten (z.B. die Festplatte löschen), als auch indirekten Schaden (wie die Installation von Sniffern, um Logons und Passwörter einzusammeln).

Sie können mit ein paar Vorkehrungen verhindern, dass ausführbare Programme unbesehen in Ihr Netzwerk eindringen können. Dazu bietet sich beispielsweise die Konfiguration von Inhaltsfiltern und Antiviren-Software an. In Kapitel 7 finden Sie weitere Details zu diesen Themen.

Software

Alle Betriebssysteme und Software-Anwendungen haben Sicherheitslücken. Einige sind problematischer, andere weniger, doch alle beinhalten die Gefahr, dass eine nicht autorisierte Person Zugriff auf Ihr Netzwerk erhalten könnte. Diese Lücken sind zum größten Teil versehentlich bei der Software-Entwicklung entstanden, etwa durch eingeschränkte Tests von Beta-Versionen oder einem allgemeinen Mangel an Qualitätskontrolle. Programme enthalten Millionen über Millionen an Textzeilen – auch *Code* genannt – und festzulegen, welche Code-Abschnitte Sicherheitslöcher beinhalten könnten, ist äußerst schwierig und arbeitsintensiv. Die meisten Software-Firmen behaupten, dass sie die Mehrkosten, die das Durchforsten des Codes nach Sicherheitslücken nach sich ziehen würde, nicht rechtfertigen können. Der eingeweihte und erfahrene Hacker wird den Code und die Programmfunktionalität jedoch genau auf diese Fehlerstellen hin absuchen und dann Programme schreiben, die den Rechner unter Ausnutzung dieser anfälligen Stellen angreifen. Und so mancher erfahrene Hacker gibt seine Software auch über das Internet frei, so dass sie jeder benutzen kann.

Die Software-Firmen sind sich durchaus bewusst, dass Sicherheitslücken tausendfach vorhanden sind und stellen sich insofern ihrer Verantwortung, indem sie in bestimmten Zeitabständen Fehlerbehebungsroutinen freigeben. Diese kennt man auch als *Bug Fix*, *Hot Fixes*, *Patch-Programme* (zur nachträglichen Korrektur von benutzten Programmen) und manchmal treten sie auch in Form von *Updates* auf. In den meisten Fällen kann man diese Routinen einfach herunterladen und installieren, doch auf vielen Computern kann deren Installation Stunden in Anspruch nehmen. Manchmal treten Probleme mit anderer Software auf, wenn die Routinen vor ihrer Freigabe nicht genau getestet wurden. Auch mit Hilfe von Firewalls lassen sich einige Sicherheitslöcher in der Software schließen, doch um entsprechend vorbereitet zu sein, empfiehlt sich die Installation von Fixes, sobald sie verfügbar sind. Diese Informationen werden detaillierter in den Kapiteln 11, 12 und 13 behandelt.

Es stehen etliche Websites und Mail-Listen zur Verfügung, die eine Warnmeldung an Benutzer herausgeben, sobald eine Sicherheitslücke in einem bestimmten Programm gefunden wurde und eine Fehlerbeseitigung entweder in Kürze oder gegenwärtig schon verfügbar ist.

Die Herausgabe solcher Warnmeldungen war der Ausgangspunkt für eine Reihe von Auseinandersetzungen. Die Situation kann man wie ein zweischneidiges Schwert betrachten: Auf der einen Seite ist die Benachrichtigung von Benutzern über Sicherheitslöcher eine wertvolle Dienstleistung, die man Netzwerkverwaltern zukommen lassen möchte. Andererseits schielen aber nicht nur »gute Netzwerkverwalter« nach solchen Warnmeldungen, sondern es werden natürlich auch Hacker auf das Problem aufmerksam. Normalerweise wird eine Warnmeldung erst dann ausgesendet, wenn eine entsprechende Fehlerbehebungsmöglichkeit schon vorhanden ist, doch Hacker vertrauen auf die Tatsache, dass die meisten Netzwerkadministratoren nicht gleich dazu kommen, die Fehlerbehebung auf der Stelle zu installieren. Der Hacker wird das Internet nach Computern durchstöbern, die noch nicht in Ordnung gebracht wurden, und sie als Ziel für seine Attacken verwenden.

Bisweilen stellen Software-Anwendungen ein Sicherheitsproblem dar, da sie die gelegentliche Übertragung von Dateien einkalkulieren. Webserver stehen ganz oben auf meiner Liste, da sie es anderen Personen ermöglichen, sich anonym mit Ihrem Netzwerk zu verbinden. Wenn Sie Ihren Webserver nicht richtig konfiguriert haben, kann auch ein nicht autorisierter Benutzer Ihren Webserver verwenden, um sich mit den Computern in Ihrem Netzwerk zu verbinden. Einige Webserver können besser als andere Attacken durchkreuzen – ein wichtiges Thema, das ausführlich in Kapitel 14 behandelt wird.

Social Engineering (sozial motivierte Ausspähung)

Obgleich sich Hacker und andere böswillige Zeitgenossen schon viele Methoden ausgedacht haben, wie sie Ihr Netzwerk attackieren können, wird häufig eine Sicherheitslücke übersehen, die gar nicht durch äußere Bedrohung verursacht wird, sondern häufig in der Firma selbst entsteht – man könnte sie mit dem Begriff »Social Engineering« (sozial motivierte Ausspähung), in anderen Kontexten auch als Betrug bekannt, umschreiben. Denn oft führt leider das Verhalten von Firmenmitarbeitern dazu, dass Schwachstellen in der Netzwerksicherheit auftreten können. Viele Menschen sind zu vertrauensselig und daher besonders gefährdet, auf gewiefte Zeitgenossen hereinzufallen, die dieses Vertrauen ausnutzen. In einfachen Worten ausgedrückt: Betrüger haben hier ein leichtes Spiel! In der Praxis kommt es tagtäglich vor, dass Mitarbeiter einer Firma dazu verleitet werden, ungewollt Passwörter und nützliche Daten in nicht befugte Hände weiterzugeben.

Folgendes Beispiel soll verdeutlichen, wie solch ein Szenario ablaufen könnte:

»Hallo, hier ist Jenny.«

»Hallo Jenny, hier spricht Erik von der Netzwerkverwaltung. Wir haben da ein Problem damit, wie unsere Computer Passwörter gespeichert haben, und gerade heute müssen einige unserer Mitarbeiter ihr Passwort ändern. Könnten Sie mir da behilflich sein?«

»Klar, ich helfe gerne, wenn Sie mir sagen, wie?«

»Sie müssen gar nicht viel tun. Benennen Sie einfach Ihr Passwort in »Passwort99« um und lassen Sie das ein paar Tage so.«

»Kein Problem, Erik. Aber würde es Ihnen was ausmachen, mir dabei zu helfen, das Passwort zu ändern? So etwas tut man schließlich nicht jeden Tag und ich habe vergessen, wie's geht.«

»Aber klar doch, Jenny. Also, machen Sie als Erstes Folgendes ...«

So einfach geht das. Jenny hat gar nicht realisiert, woher der Anruf kam (ob aus der Firma selbst oder von außerhalb) und wahrscheinlich kennt sie noch nicht mal die Namen der Netzwerkverwalter ihrer Firma. Sie wollte einfach nur behilflich sein. Der Anruf hätte von einem Kollegen kommen können, der dazu legitimiert ist, es hätte sich aber auch um einen Hacker handeln können, der sich über einen gültigen Benutzernamen und ein gültiges Passwort Zutritt zu Ihrem Netzwerk verschaffen will.

Mit Hilfe von Firewalls oder Software-Korrekturprogrammen lässt sich die soeben geschilderte Bedrohungsvariante nicht stoppen. Sicherheitsmaßnahmen können hier nur in Form von Weiterbildung und Aufklärungsarbeit Fuß fassen. Um ein umfassendes Sicherheitsprogramm zu haben, müssen Sie also nicht nur in der Lage sein, Eindringlinge auf Netzwerkebene zu stoppen, sondern sie auch im wahrsten Sinn des Wortes »an der Tür« zurückzuweisen.

Eine Lektion in Sachen »Mitarbeiterverhalten«

Ein Freund von mir sollte einmal für eine Firma die Sicherheitslücken testen (natürlich mit Genehmigung von höchster Ebene), die, wie soeben geschildert, durch Vertrauensseligkeit von Mitarbeitern entstehen können. Er betrat also das Büro, schick gekleidet, in der einen Hand eine Aktenmappe und in der anderen ein Clipboard. Er stellte sich bei der Empfangsdame als »Prüfer« vor und fragte an, wo sich ein Raum mit bestimmten Akten befände. Sie wies ihm den Weg dorthin und bot ihm noch höflich einen Kaffee an. Sie fragte aber *nicht* nach, ob er dazu in irgendeiner Weise legitimiert sei, auch dann nicht, als er damit begann, den Aktenschrank zu durchwühlen und Akten herauszuziehen. Er schaffte es schließlich sogar, sich zu verstecken und im Büro zu bleiben, nachdem es geschlossen wurde und die Angestellten nach Hause gegangen waren.

Am nächsten Tag teilte mein Freund das Ergebnis seines Testes dem Firmenchef mit. Es bedurfte keiner großartigen Überredenskünste, sich mit dem Direktor dahingehend zu einigen, die Art und Weise, wie mit Besuchern umgegangen ist, unmittelbar zu ändern!

Ihr Netzwerk kennen lernen

Alle Sicherheitsregeln für Netzwerke lassen sich auch auf Ihr System übertragen, egal, ob Sie zwei Computer vernetzt haben oder in einem Netzwerk hunderte von Computern vernetzt sind. Um jedoch ein adäquates Sicherheitssystem für Ihr Netzwerk zu installieren, müssen Sie wissen, was bereits vorliegt, bevor Sie dann entscheiden, was noch getan werden muss. In den folgenden Abschnitten werden die einzelnen Komponenten eines Netzwerks behandelt und es

wird erläutert, wobei es sich um potenzielle Problembereiche handelt. Detailliertere Informationen, wie diese Probleme angepackt werden können, finden Sie in Kapitel 2.

Verbindungen

Über das Einrichten von Verbindungen wird die Kommunikation zwischen Computern ermöglicht. Es kann eine einzelne Verbindung in Form eines Modems vorliegen, das Sie verwenden, um einen *ISP* (Internet Service Provider) wie AOL oder Earthlink anzuwählen oder Sie können hunderte von Computern mit Netzwerkkarten haben, die eine Verbindung mit zentralen Servern herstellen. Da Verbindungen bestimmte Vertrauensverhältnisse zwischen Computern voraussetzen, ist es nicht nur wichtig zu wissen, wie Sie verbunden sind, sondern auch, womit Sie verbunden sind.

Dial up Modems

Modems sind Geräteeinheiten, die Ihren Computer über eine Telefonleitung mit dem Internet verbinden. Meist handelt es sich um sehr kleine Gehäuse, die Ihren Computer über ein normales Telefonkabel mit der Telefonleitung verbinden. Das Wort »Modem« steht für *Modulator/Demodulator*. Über ein Modem werden die von Ihrem Computer erstellten digitalen Daten in elektronische Impulse umgewandelt, die dann über die Telefonleitung übertragen werden können.

Wenn eine Verbindung zum Internet über ein Modem hergestellt wird, ist die Gefahr sehr gering, einem Hackerangriff zum Opfer zu fallen. Denn ein so verbundener Computer ist nicht die ganze Zeit online im Netz und er hat keine Set-Adresse – also eine *statische IP-Adresse*. Bei jeder Verbindungsherstellung gibt Ihnen Ihr ISP eine andere Adresse – eine *dynamische IP-Adresse*, – die unter den verfügbaren Adressen ausgewählt wird, die der ISP auf seinem Netzwerk hat. Da nun eine Nummer, die sich konstant ändert, nicht so leicht gefunden werden kann, halten sich Hacker im Allgemeinen nicht lange mit dieser Verbindungsart auf. Das heißt nicht, dass Modemverbindungen keinerlei Gefahren unterliegen: Sie können nach wie vor über E-Mail-Viren oder Trojanische Pferde angegriffen werden (siehe auch der vorherige Abschnitt *Viren, E-Mails und ausführbare Dateien*).

Für Firmen können Modems dennoch eine Gefahr darstellen. Das kann zum Beispiel der Fall sein, wenn Angestellte ein Modem von zu Hause mitbringen, an ihre Arbeitscomputer anschließen und die Modemsoftware so einstellen, dass eingehende Anrufe beantwortet werden können. Oft geschieht dies ohne Kenntnis oder Erlaubnis der Firma. Die Angestellten betrachten es als eine Annehmlichkeit, da sie sich so von ihren Heimcomputern aus bei ihren Arbeitscomputern einwählen können und auf die Daten des Arbeitscomputers Zugriff haben. Doch auch bei Firmen, die diese Praxis für Telearbeit zulassen, gilt: Wenn hier nicht alles korrekt abläuft, kann auch eine nicht autorisierte Person in die Lage versetzt werden, auf den Computer zuzugreifen.

Hacker setzen ein Gerät oder eine Software ein, das als *Demon Dialer* oder *War Dialer* bezeichnet wird. Dieser Dialer wählt in schneller Abfolge Telefonnummern innerhalb eines be-

stimmten Bereichs (beispielsweise jede Nummer zwischen 555-0000 und 555-9999). Sobald irgendeine Telefonnummer, die angewählt wird, mit dem Handshake-Signal des Modems antwortet, wird der Wahlvorgang gestoppt und der Hacker kann versuchen, sich mit dem Computer zu verbinden, der geantwortet hat. Das Modemsignal besteht aus dieser nervigen Serie von Pieptönen und summenden Geräuschen, die erklingen, sobald das Modem versucht, eine Verbindung auszuführen. Wenn ein Hacker also die Telefonnummer eines Arbeitscomputers angewählt hat und das Modem des Computers antwortet, kann er damit in die Lage versetzt werden, zu diesem Arbeitscomputer eine Verbindung herzustellen. Darüber hinaus werden Sie aber auch nicht wissen, dass ein Hacker Zugriff auf Ihren Computer erhalten und wichtige Informationen gestohlen hat.

Kabelmodems

In vielen Haushalten und auch einigen Firmen wird die Verbindung zum Internet nun über ein *Kabelmodem* hergestellt. Diese Modems nutzen die Infrastruktur der Fernsehverkabelung zur Übertragung der Daten. Kennzeichnend ist, dass TV- und Computer-Dienste geteilt sind und nicht auf demselben Kanal ablaufen. Bei dem Modem selbst handelt es sich um einen ziemlich einfachen *Router*. Einen Router kann man mit einem Wegeplanprogramm für Autoreisen vergleichen – er kennt sämtliche zur Verfügung stehenden Routen zu den Zielcomputern innerhalb Ihres Netzwerks sowie alle Wege, die daraus heraus führen. Falls es zu Engpässen oder Staus bei der Übertragung der Daten innerhalb Ihres Netzwerks kommt, leitet der Router die entsprechenden Datenpakete um. Standardmäßig erlauben Router jeglichen Datenverkehr, doch sie können so konfiguriert werden, dass sie Protokolle herausfiltern, die Sie nicht verwenden. In Kapitel 9 wird ausführlich erläutert, was Router sind und wie man sie konfigurieren kann.

Da ein Kabelmodem immer eingeschaltet und damit stets mit dem Internet verbunden ist, erhöht sich damit auch Ihr Sicherheitsrisiko. Sie besitzen wahrscheinlich eine statische IP-Adresse, was es der Außenwelt erleichtert, Ihre Computer einsehen zu können. In vielen Kabelnetzen werden auch Dienste wie Webserver und Telnet ausgeführt, so dass sich die Gefahr erhöht, dass man auf das Modem zugreifen kann. Wenn nun ein Eindringling die IP-Adresse Ihres Kabelmodems finden kann, wird er versuchen, unter Verwendung von telnet oder http darauf zuzugreifen. Wenn er zusätzlich das Passwort erraten kann – oder wenn keine Passwortangabe erforderlich ist –, kann der Eindringling die Konfiguration des Passworts so ändern, dass er zu jedem Zeitpunkt Zugriff hat. Das heißt im Klartext: Er kann auf Ihren Computer zugreifen, Daten stehlen, ändern oder löschen und darüber hinaus Hackerprogramme oder Viren installieren.

DSL

Auch über *DSL* oder Digital Subscriber Line kann eine Verbindung zum Internet hergestellt werden. DSL-Modems verwenden normale Telefonleitungen für die Schaltung. Der Datenfluss wird jedoch aufgeteilt, so dass sie gleichzeitig für ein- und ausgehende Anrufe Ihr Telefon benutzen können. Um die Verbindung aufzubauen, benötigen Sie ein DSL-Modem und einen

so genannten Splitter. Diese Technik ist etwas ausgeklügelter als beim Kabelmodem (siehe auch der vorhergehende Abschnitt), dafür haben Sie jedoch den Vorteil, die Verbindung ständig nutzen zu können, ohne andere Kommunikationsarten zu blockieren.

DSL-Router beinhalten wie Kabelmodems folgendes Gefahrenpotenzial:

- ✔ Die Verbindung ist fast immer aktiv
- ✔ Sie haben eine statische IP-Adresse
- ✔ Die Konfiguration der DSL-Verbindung kann auch über Fernzugriff erfolgen

Eine der effektivsten Sicherheitsmaßnahmen für alle Modemtypen ist die Verwendung von langen Passwörtern, die nicht so leicht erraten werden können und Zahlen sowie abwechselnd Groß- und Kleinschreibung verwenden. Personal Firewalls bieten einen guten Schutzmechanismus für kleine Systeme, wenn Sie DSL-Verbindungen verwenden. Personal Firewalls werden ausführlicher in Kapitel 8 behandelt.

Drahtlose Vernetzung

Die drahtlose Vernetzung gehört gegenwärtig zu den neuesten Verbindungsmethoden. (Ich verwende diesen Typ bei mir zu Hause. Nach dem Abendessen sitzen mein Mann und ich mit unseren Laptops auf dem Schoß im Wohnzimmer und surfen gemeinsam im Web.) Damit Sie zu Hause drahtlos arbeiten können, benötigen Sie eine Verbindung zum Internet über eine Landleitung (z.B. ein Kabelmodem oder DSL) und eine spezielle drahtlose Netzwerkkarte (Typ 802.11). Obwohl drahtlose Verbindungen außerordentlich komfortabel sind (wie sonst könnte ich so bequem von meinem Wohnzimmer aus im Web surfen?), bergen sie doch einige Gefahren.

Wenn ein drahtloser Zugang nicht korrekt konfiguriert ist, kann jeder, der eine drahtlose Karte in seinem Computer installiert hat, eine Verbindung zu dem Netzwerk herstellen! Viele Unternehmen haben vergessen oder sich dagegen entschieden, die Verschlüsselung ihrer drahtlosen Signale zu aktivieren. Das bedeutet, dass jeder Computer innerhalb der Reichweite die Übertragung empfangen und das Netzwerk »sehen« kann. Einige Übertragungen reichen ziemlich weit – über viele Stockwerke und Tausende Meter hinweg. Wenn das Unternehmen keine stringenten Zugangskontrollen für sein drahtloses Netzwerk festgelegt hat, kann eine unautorisierte Person nicht nur das Netzwerk sehen, sondern sich auch einloggen und sich mit geringen oder keinen Problemen Zugriff verschaffen.

Kürzlich fuhr ein berüchtigter Ex-Hacker in den Straßen von San Francisco herum und loggte sich bequem von seinem Wagen aus in Dutzende Unternehmensnetzwerke ein! Sich erfolgreich in ein Netzwerk einloggen zu können, ist der Traum eines jeden Hackers.

Es gibt viele Möglichkeiten, ein drahtloses Netzwerk vor unberechtigten Logins zu schützen. Zu den grundlegenden Schutzmaßnahmen zählen: solide Passwörter, gut definierte Benutzerzugriffslisten und diverse Verschlüsselungsebenen.

T1, T3 und mehr

Die ultimative Internetverbindung ist ein T1-Dienst oder partieller T1-Dienst, die direkt auf die riesigen Backbone-Leitungen des Internets aufsetzt. Diese Verbindungen ermöglichen den Transfer von riesigen Datenmengen in blitzartig schneller Geschwindigkeit. Direktverbindungen dieser Art sind sehr teuer und liegen außerhalb der Möglichkeiten von Heimbenutzern und vielen kleinen Geschäften.

T1-, T3- und OC3-Verbindungen werden überwiegend von Großunternehmen sowie von Regierung und Militär genutzt. Also alles Einrichtungen, die sehr leistungsstarke Router benötigen, die in der Lage sein müssen, tausende von Verbindungen auf einmal zu unterstützen. Das sind natürlich auch die Typen von Netzwerken, nach denen ernsthafte Hacker Ausschau halten und die auch die meisten »Schlagzeilen bringen«, wenn die Hacker erfolgreich sind. Um diese Netzwerke zu schützen, sind umfassende Sicherheitsmaßnahmen wie Firewalls, Intrusion-Detection-Systeme und Antiviren-Software erforderlich.

Fernzugriff auf das interne Netzwerk

Erlauben Sie es, dass man sich auch von außen in das interne Netzwerk einwählen kann? Wenn ja, sollten Sie die Möglichkeit der Fernverbindung auch in die Liste der Sicherheitsvorkehrungen aufnehmen. Remote-Verbindungen über Modems sind eine Angelegenheit für sich, da Sie jemandem außerhalb der physischen Grenzen Ihrer Firma die Möglichkeit geben, Ihr Netzwerk zu nutzen. Der Computer, den Sie für einen Fernzugriff nutzen lassen möchten, sollte so sicher wie Ihr internes Netzwerk sein, anderenfalls ergeben sich für Sie zusätzliche Probleme.

Nehmen wir als Beispiel einen Laptop. Viele Mitarbeiter verwenden ihre Firmenlaptops, um auch von zu Hause oder vom Hotelzimmer aus eine Verbindung mit dem Firmennetz herstellen zu können. Da Laptops oft auf diese Weise genutzt werden, lassen die Mitarbeiter auch zu – um die Verbindung schneller und einfacher herzustellen –, dass Logon-Name und Passwort gespeichert werden. Wenn der Laptop jedoch gestohlen wird und nichts den Dieb daran hindert, den Laptop zu verwenden, kann dieser sich schnell und einfach mit Ihrem Netzwerk verbinden. Und das nur, weil alle Logon-Informationen auf dem Laptop gespeichert sind und somit quasi auf dem »Präsentierteller« liegen. Und das Schlimmste ist: Sie werden noch nicht einmal merken, dass eine nicht autorisierte Person auf Ihr Netzwerk zugreift, da der Dieb ja die Anmeldung adäquat durchgeführt hat. Keine Alarmglocken werden klingeln!

Für alle Computer, die für einen Fernzugriff verwendet werden, sollte die Angabe eines BIOS-Passworts aktiviert werden. Wenn ein BIOS-Passwort verwendet wird, kann ein Computer ohne ein solches Passwort überhaupt nicht starten. Darüber hinaus sollten Sie auch in Betracht ziehen, die Daten auf Ihrem Laptop zu verschlüsseln, da die meisten Diebe nicht Zeit und Mühe investieren werden, Daten zu entschlüsseln. In den meisten Fällen werden sie das Laufwerk neu formatieren und dann den Computer verkaufen.

Wenn in Ihrer Firma ferngesteuerte Software wie PCAnywhere eingesetzt wird, sollten Sie sehr darauf achten, dass die entsprechenden Sicherheitspatches eingesetzt und strenge Passwörter verwendet werden.

Es gibt Situationen, in denen Sie es anderen erlauben müssen, sich entfernt auf Ihrem Computer einzuloggen und Befehle auszuführen. Administratoren lieben diese Möglichkeit, da sie es ihnen ermöglicht, eine Maschine entfernt zu administrieren, ohne einmal quer über das Betriebsgelände marschieren und im kalten Server-Raum sitzen zu müssen, um direkt an der betroffenen Maschine zu arbeiten. Das Programm, das meist für einen solchen entfernten Zugang verwendet wird, ist Telnet. Doch da Telnet autorisierten Personen erlaubt, auf einen Computer zuzugreifen, der irgendwo platziert ist, kann auch ein bösartiger Eindringling Ihr System betreten. Wenn das Passwort für Telnet erraten oder geknackt werden kann, kann der Eindringling in Ihrem System Konfigurationen ändern oder nicht autorisierte Programme installieren.

FTP steht für *File Transfer Protocol* und wird für das Verschieben, Kopieren oder Löschen von Dateien verwendet. Wie Telnet wird auch FTP für die Verbindungsherstellung zu einem Computer verwendet, der sich an einem anderen Ort befindet. Die in Zusammenhang mit FTP auftretenden Probleme werden in Mail-Listen von Bugtraq und SecurityFocus ausführlich behandelt. Online stehen eine Reihe von Sicherheitspatches und Konfigurationsanleitungen zur Verfügung. Die Dienste sollten außerdem durch Benutzerkonten und Berechtigungen sowie dem Einsatz von stabilen Passwörtern gesichert werden.

Workstations und Server

Computer-Workstations sind sowohl zu Hause und in kleinen Büros als auch in großen Firmennetzwerken vorzufinden. Workstations müssen mit exakt definierten Benutzerkonten und Berechtigungen geschützt werden. So sollten zum Beispiel nicht alle Mitarbeiter die Erlaubnis haben, Programme auf ihren Workstations zu installieren. Diese Verantwortlichkeit sollte am besten dem Administrator übertragen werden.

In einem Netzwerk werden oft Computer verwendet, die man als *Se*rver bezeichnet. Wie der Name schon impliziert, dienen Server den individuellen Workstations mit Dateien, die gemeinsam genutzt und untereinander ausgetauscht werden. Die Sicherheitsarchitektur der Betriebssysteme unterscheidet sich zum Teil erheblich. So war das Microsoft-Betriebssystem Windows NT, als es auf den Markt kann, als sicher angekündigt. In der Praxis war das Betriebssystem aber nur dann sicher, wenn der Computer nicht mit dem Netzwerk verbunden war. Weitere Informationen zu Betriebssystemen und deren Sicherheit finden Sie in den Kapiteln 11, 12 und 13.

Server enthalten oft Anwendungsprogramme, um bestimmte Aufgaben durchzuführen. Dazu können gehören (die Auflistung ist nicht vollständig): Webserver, Datenbankserver, FTP-Server, Mail-Server, Firewalls und Intrusion-Detection-Systeme. Alle diese Programme haben eigene Sicherheitsprobleme, die später in diesem Buch näher behandelt werden. Vorab bemerkt

kann man aber feststellen, dass sich die Gefahr erhöht, wenn Dienste auf einem Server kombiniert werden.

Den größten Fehler, den Sie machen können, ist, den Webserver und eine Datenbank auf demselben Computer zu kombinieren. Webserver gelten nicht als sicher und ein Angriff auf die Datenbank wird um einiges leichter, wenn die Dateien auf demselben Computer wie der Webserver abgelegt sind.

Den besten Schutz für Workstations und Server erreichen Sie, indem Sie Antiviren-Software installieren. Die Schäden, die der Wirtschaft durch Viren, Würmer und Trojanische Pferde entstehen, sind enorm (und verschlingen eine Menge Geld). Entgegen der weit verbreiteten Ansicht schützen Firewalls Ihre Systeme nicht gegen Viren. Sie benötigen dafür Antiviren-Software. Mehr zu diesem Thema finden Sie weiter unten in diesem Kapitel und in Kapitel 7.

Ihre Netzwerkbenutzer

Sie werden es vielleicht eigenartig finden, dass ich Netzwerkbenutzer auch unter dem Begriff »Netzwerkkomponente« aufführe, doch was nützt das beste Netzwerk, wenn sich keine Benutzer dafür finden? Auch das Wissen um Ihre Benutzer und wie sie Ihr System verwenden, kann Ihnen dabei helfen, potenzielle Schwachstellen in Ihrem System aufzudecken. In der folgenden Liste finden Sie ein paar Fragestellungen, mit denen Sie sich in Bezug auf Ihre Netzwerkbenutzer beschäftigen sollten:

- ✔ **Hat jeder Benutzer eine individuelle Logon-ID und ein sicheres Passwort?** Diese Sicherheitsmaßnahme ist äußerst wichtig, da jede Aktion im Netzwerk einem Individuum zugeordnet werden kann. Ohne individuelle Logon-IDs sind Sie nicht in der Lage zu verfolgen, wer was in Ihrem Netzwerk tut. Natürlich sollte auch jede Person ein Passwort haben, das nicht leicht zu erraten und zu knacken ist. So können Sie das Risiko vermindern, dass eine nicht autorisierte Person das Passwort errät und unter Verwendung dieses Passworts Zugriff auf das Netzwerk erhält.
- ✔ **Führen Sie ein Protokoll über alle Anmeldeversuche?** Ihr Betriebssystem beinhaltet die Fähigkeit, alle Anmeldeversuche in eine Textdatei zu schreiben, die man als *Protokoll* bezeichnet. Sie müssen Ihrem System mitteilen, ob alle erfolgreichen oder alle nicht erfolgreichen Anmeldungen protokolliert werden sollen. Sie sollten vorzugsweise alle nicht erfolgreichen Versuche bei der Anmeldung aufzeichnen lassen, da Sie dadurch herausfinden können, dass jemand versucht, ein Passwort zu erraten, und wahrscheinlich nicht autorisiert ist, Ihr System zu nutzen. Oft ist dies das erste Anzeichen für einen Hacker-Angriff auf Ihr System. Es versteht sich von selbst, dass alle diese Protokolle regelmäßig durchgesehen werden sollten!
- ✔ **Wird ein Benutzerkonto nach einer bestimmten Anzahl falsch eingegebener Passwörter gesperrt?** Wenn jemand versucht, ein Passwort zu erraten, um einen nicht autorisierten Zugriff auf Ihr System zu erhalten, wird er so oft ein Passwort angeben, bis er Erfolg hat. Hacker versuchen oft, einen brachialen, wörterbuchbasierten Angriff (Brute Force Attack)

zu starten, um das Passwort herauszufinden. Sie können nun bestimmen, dass nach einer bestimmten Anzahl falsch eingegebener Passwörter (zum Beispiel nach drei oder fünf Versuchen) das Konto gesperrt wird. Der »echte« Benutzer des Kontos muss dann nach einer solchen Sperrung den Administrator bitten, die Sperrung wieder aufzuheben. Das mag zwar manchem lästig erscheinen, doch es ist eine billige und einfache Möglichkeit, zu vermeiden, dass Hacker mit solchen Brachialangriffen Erfolg haben. Natürlich sollte auch über diese Versuche ein Protokoll geführt und überwacht werden.

- ✔ **Sind Gruppenkonten erlaubt?** Häufig verwenden Administratoren aus Bequemlichkeitsgründen Gruppenkonten. Wenn zum Beispiel eine Arbeitsschicht beendet wird, müssen sich die Benutzer nicht abmelden – und die Mitarbeiter der nächsten Schicht arbeiten einfach mit den bereits offenen Konten weiter. Diese Vorgehensweise ist absolut TABU! Um nur eine Sache zu nennen – wenn jeder unter derselben Benutzer-ID angemeldet ist, haben Sie keinen Überblick darüber, wer was auf Ihrem System tut. Sie werden erstaunt sein, wie hartnäckig sich manche Personen gegen die Abschaffung von Gruppenkonten wehren.
- ✔ **Haben Sie inaktive Konten?** Jedes Mal, wenn ein Benutzer das System für einen bestimmten Zeitraum nicht verwendet, sollten Sie das Konto dieser Person deaktivieren. Wenn sich dieser Zeitraum länger als einen Monat hinzieht oder wenn ein Benutzer das System selten nutzt, sollten Sie diese Konten löschen. Auch wenn es nicht so bequem erscheinen mag: Legen Sie besser neue Konten an, anstatt inaktive Konten zu belassen, die sich ein Hacker zu Nutze machen könnte. Wenn ein Mitarbeiter sein Arbeitsverhältnis beendet, sollten die Konten gelöscht werden, bevor die Person das Haus verlässt.

Tools und Prozeduren

Um einen Job gut zu machen, müssen Sie über die entsprechenden Hilfsmittel verfügen und wissen, wie sie diese für Ihre Arbeit einsetzen können. Auch bei der Netzwerksicherheit ist das so. Einige Hilfsmittel sind überall einsetzbar, andere sind speziell auf Netzwerktätigkeiten zugeschnitten. Die Prozeduren setzen sich aus einem planmäßigen Schritt-für-Schritt-Prozess zusammen, um Ihre Schwachstellen aufzudecken und dann die entsprechenden Sicherheitsmaßnahmen zu implementieren. Das nimmt zwar etwas Zeit in Anspruch, doch es ist nicht allzu schwierig und es lohnt sich.

Papier und Bleistift

Ja doch, Papier und Bleistift sind eines der effektivsten Hilfsmittel! Das mag altmodisch klingen, doch das Anfertigen von Listen und das Dokumentieren von Vorgängen ist der Schlüssel zur effektiven Netzwerksicherheit. Sie müssen eine Aufzeichnung darüber haben, was Sie getan haben, und vor allem, *warum* Sie es getan haben. Vorausgesetzt, das unwahrscheinliche Szenario tritt ein und Sie können für einen längeren Zeitraum nicht zur Arbeit kommen, kann diese Dokumentation anderen helfen, Ihre gute Arbeit fortzusetzen.

Sie sollten Listen von allem anfertigen, was Sie haben. Dabei sollten Sie so viele Details wie möglich einbeziehen. Ihre Liste sollte Folgendes enthalten:

- ✔ **Einen Funktions- und Organisationsplan:** Sie müssen Name und Funktion aller Mitarbeiter kennen, um für diese die entsprechenden Zugriffsrechte und Zuordnungen zu Sicherheitsebenen festzulegen.
- ✔ **Hardware-Listen:** Diese Listen sollten Ihr gesamtes Equipment enthalten, die Marken und Modelle und die Namen der Hersteller. Gehen Sie beim Anfertigen der Liste so vor, wie Sie es bei einer Aufstellung für eine Versicherung tun würden.
- ✔ **Software-Listen:** Sie müssen nicht nur wissen, welche Software-Pakete Sie in Ihrem Inventar haben, sondern Sie müssen sich auch vergewissern, dass Sie eine Programmlizenz pro Anwendung und Rechner haben. In der Liste sollten Hersteller, Programm und Software-Version sowie die Anzahl an Kopien, die Sie verwenden, enthalten sein. Wenn Sie die Software selbst entwickelt haben, handelt es sich dabei um ein wichtiges Anlagegut, das besonderen Schutz benötigt.
- ✔ **Netzwerkplan:** Zeichnen Sie einen Netzwerkplan und geben Sie das Vertrauensverhältnis der Verbindungen innerhalb und außerhalb des internen Netzwerks an. Wenn Ihr Netzwerk mit einem anderen Firmennetzwerk verbunden ist, ist dies ein Beispiel einer vertrauten Verbindung außerhalb Ihrer Domäne. Zeigen Sie alle wichtigen Computer-Ressourcen und Schutzmechanismen auf, über die Sie bereits verfügen – zum Beispiel Firewalls und Router zur Filterung.
- ✔ **Gebäudeplan:** Sie müssen auch aufzeigen, wo bzw. in welchen Räumen Sie Ihre Computer in Ihrem Büro oder Unternehmen aufgestellt haben und wo sich spezielle Bereiche wie Serverräume befinden. In diesem Plan sollten Sie auch Dinge wie Feuerleiter, Wasserlöschanlage, Türen, Treppenhaus und Fenster berücksichtigen. Damit erhalten Sie Hinweise darauf, welche physischen Sicherheitsmaßnahmen implementiert werden müssen, um Ihre Schätze zu schützen.

Diese Aufzeichnungen – ob ausgedruckt oder per Hand geschrieben – werden Ihnen wertvolle Dienste leisten, wenn Sie Ihren Sicherheitsplan aufstellen und Ihre Sicherheitsrichtlinien einrichten.

Administratorenkonten

Für viele der in diesem Buch erwähnten Implementierungen benötigen Sie ein Konto auf Administratorenebene. Sollten Sie noch nicht über ein solches Konto verfügen, sollten Sie dies jetzt einrichten oder einen Netzwerkadministrator bitten, Sie dabei zu unterstützen. Achten Sie aber darauf, dass der Administrator auch die entsprechende Vertrauensstellung hat sowie die notwendigen Fähigkeiten besitzt, die für die Änderungen an einem Netzwerk erforderlich sind.

Programm zum Durchsuchen von Ports (Port-Scanner)

Um alle Computer, Software-Anwendungen und Dienste zu erfassen, die in Ihrem Netzwerk gestartet werden, werden Sie vielleicht den Einsatz eines Programms zum Durchsuchen von Ports in Erwägung ziehen. Diese Programme überprüfen Netzwerkgeräte, identifizieren Betriebssystemversionen und welche Firewalls in Gebrauch sind. Oft wird durch Port-Scanner auch aufgedeckt, dass Dienste in Betrieb sind, die man gar nicht benötigt. Viele Programme zum Durchsuchen von Ports sind frei über das Internet verfügbar, andere müssen Sie käuflich erwerben. Auch handelt es sich oft um Unix-basierte Programme, vergewissern Sie sich also, ob sich der entsprechende Port-Scanner auch für Ihr Betriebssystem eignet.

Port-Scanner sind sehr mächtige Programme. Wenn Sie nicht vorsichtig sind, können Sie die in Ihrem Netzwerk ausgeführten Anwendungen ernsthaft beschädigen. Port-Scanner überfluten das Netzwerk mit Abfragen. Das gleichzeitige Ausführen zu vieler Abfragen kann ein funktionierendes Netzwerk in die Knie zwingen. Lesen Sie auf jeden Fall alle Anweisungen zu Ihrem Port-Scanner, bevor Sie ihn auf Ihr Netzwerk loslassen.

Netzwerkmapper

Ein Netzwerkmapper ist ein unschätzbares Tool, das das Netzwerk abfragt und Computer und deren Adressen sucht. Der Netzwerkmapper, der seinen Namen zu Recht trägt, erstellt dann anhand dieser Informationen eine physische Map Ihres Netzwerkes. Die Map zeigt alle Verbindungen als grafische Darstellung. Zusätzlich können Netzwerkmaps eine Liste aller auf Ihrem Netzwerk installierten Betriebssysteme und Anwendungen enthalten. Trotzdem eine Warnung: Diese Programme sind nicht einfach zu bedienen und einige sind sehr teuer. Eine Liste, wo Sie diese und andere Tools beziehen können, finden Sie in Kapitel 23.

Schwachstellenbewertung

Ein Tool zur Bewertung von Schwachstellen testet Anwendungen, Computer und Netzwerkgeräte, wie z.B. Router und Firewalls, auf bekannte Fehler und Mängel, die Ihr System anfällig für bösartige Attacken machen können. Anhand einer Datenbank mit Schwachstellen werden diese Mängel mit den auf Ihrem Netzwerk installierten Betriebssystemen und Anwendungen verglichen. Zu den Schwachstellen können fehlende Sicherheitspatches, das Ausführen von verwundbaren Diensten und fehlerhafte Betriebssystemkonfigurationen zählen.

Obwohl die Tools zur Bewertung von Schwachstellen nicht 100-prozentig akkurat arbeiten und falsche Angaben machen könnten, sind sie extrem nützlich und können greifbare Beweise für bekannte Schwachstellen und Mängel liefern, bevor diese ausgenutzt werden. Einige Tools zur Bewertung von Schwachstellen sind einfacher zu handhaben als andere und einige suchen ausschließlich Schwachstellen auf Windows- bzw. Unix-Plattformen. Vor dem Kauf dieser Tools müssen Sie sich vergewissern, dass sie die meisten, wenn nicht gar alle, auf Ihrem Netzwerk ausgeführten, verschiedenen Anwendungen und Betriebssysteme scannen können. Da

niemand, der die Netzwerksicherheit ernst nimmt, ohne ein solches Tool auskommen sollte, finden Sie in Kapitel 23 eine Liste dieser Tools.

Unterstützung durch das obere Management

Mit Netzwerksicherheit sollten Sie nicht in einem Vakuum beginnen. Sie brauchen wichtige Rückmeldungen von allen Benutzern und – noch wichtiger – Sie brauchen die Genehmigung und Unterstützung der Unternehmensführung. Fangen Sie mit den Mitgliedern des oberen Management an. Sagen Sie ihnen, was Sie vorhaben zu tun, warum Sie es tun müssen und wie Sie vorgehen werden. Legen Sie einen Zeitplan fest, damit Sie in regelmäßigen Abständen über Ihre Fortschritte berichten und sie Ihnen ihre Rückmeldungen geben können. Je mehr Personen Sie aus dem Kreis des oberen Managements und der normalen Benutzer einbeziehen, desto eher werden sie mit Ihnen – anstatt gegen Sie – arbeiten.

Als Erstes müssen Sie das obere Management davon überzeugen, dass Netzwerksicherheit ernst zu nehmende Arbeit ist, die getan werden muss. Wenn Sie schwierige Überzeugungsarbeit leisten müssen, können Sie sich Argumente aus dem Abschnitt *Den Feind kennen* weiter unten holen. Dieser Abschnitt beschreibt viele Attacken und Methoden, die von Hackern und Virusentwicklern praktiziert werden. Leider warten viele Unternehmen mit der Entscheidung, ihre Netzwerke zu sichern, so lange, bis sie ernsthafte Probleme erlebt haben.

Das Federal Computer Incident Response Center (FedCIRC; `www.fedcirc.gov/index.html`) und das Government Accounting Office (GAO; `www.gao.gov`) verfügen über informative Berichte mit einigen sehr interessanten Statistiken über Typ und Häufigkeit von Computerverbrechen und Infiltrationen. In der GOA-Site können Sie per Textsuche in den verfügbaren Berichten nachschlagen. Wenn Sie unter »Information Management« suchen, finden Sie Dutzende von kritischen Berichten über Erfolge und Misserfolge bei Computersicherheit von 1997 bis heute in englischer Sprache.

Bewertungsteams

Bevor Sie mit dem eigentlichen Schutz Ihres Netzwerkes beginnen, müssen Sie ein Bewertungsteam zusammenstellen. Jedes Mitglied des Teams sollte praktische Erfahrungen mit Computern und Netzwerken besitzen und den Wert eines guten Computersicherheitsprogramms verstehen. Teilen Sie die Pflichten unter den Teammitgliedern auf. Es sollten mindestens drei Teammitglieder sein:

- ✔ **Teammanager:** Legt den Anwendungsbereich und die Richtung der Sicherheitsanstrengungen fest; ist die Hauptverbindungsperson zwischen den anderen Teammitgliedern und dem oberen Management; muss Grundlagen der Risikobewertung kennen.
- ✔ **Head Geek:** Leiter der Informationstechnologie in Unternehmen, im Bewertungsteam verantwortlich für die gesamte praktische Arbeit mit Computern; muss Grundlagen der

Schwachstellenbewertung kennen; muss ein profundes Wissen über Computer und Netzwerke besitzen; muss gut mit den anderen Teammitgliedern kommunizieren können.

- ✔ **Dokumentar:** Verantwortlich für die gesamten Berichte und Dokumentationen; muss detailorientiert sein; muss praktische Kenntnisse über Computer und Netzwerke besitzen.

Das Team identifiziert gemeinsam die Einrichtungen und Anlagen, die geschützt werden müssen, und entwirft einen vorläufigen Sicherheitsplan. Der Plan beschreibt, was geschützt und wie es geschützt werden muss sowie die Sicherheitsrollen und -verantwortlichkeiten aller Firmenangehöriger.

Verzweifeln Sie nicht, wenn Sie das einzige Mitglied des Bewertungsteams sind. Für viele Unternehmen sind die Kosten für ein dreiköpfiges Team nicht akzeptabel. Eine Person kann die Arbeit bewältigen, aber Sie müssen sich die Zeit zugestehen, die zum Bewerkstelligen der Aufgaben erforderlich ist. Ordnen Sie den zu erledigenden Arbeiten Prioritäten zu. Sie müssen jetzt realisieren, dass das Einrichten von Netzwerksicherheit eine Vollzeitbeschäftigung ist. Vieles hängt von der Größe Ihres Netzwerkes und der Anzahl der Schwachstellen ab, die für Ihr System in Frage kommen. Wenn Sie nur ein paar Arbeitsplatzrechner und wenige Anwendungen haben, wird die Arbeit sehr viel leichter sein, als wenn Sie hunderte von Servern mit unterschiedlichen Anwendungen auf jedem einzelnen hätten.

Das A und O ist, langsam vorzugehen und jeden Schritt zu dokumentieren. Wenn Sie das Einrichten der Netzwerksicherheit durchpeitschen und viel von dem, was Sie gemacht haben, vergessen, kann niemand nach Ihnen Ihre Arbeit fortsetzen. Wenn irgendwann Patches und Aktualisierungen übernommen werden müssen, werden Sie außerdem mehr damit beschäftigt sein, herauszufinden, was eigentlich aktualisiert werden muss, als mit der tatsächlichen Arbeit.

Den Feind kennen

Gewiss ist es ein überstrapaziertes Klischee, aber Sie müssen Ihren Feind in der Welt der Netzwerksicherheit wirklich kennen. Wenn Sie genauso abwegig wie Ihre Feinde denken, dann könnten Sie sie auf dem Weg in Ihr Netzwerk abfangen. Viele Menschen haben Hacker, Virusentwickler und sogar ihre eigenen Angestellten unterschätzt – zum Schaden der Netzwerksicherheit. Machen Sie nicht denselben Fehler. Sie können Ihr Netzwerk schützen, indem Sie sich einfach mit dem Wissen wappnen, wer Ihr Feind ist.

Hacker

Hacker sind Computerterroristen; sie halten Sie in Atem, weil Sie nicht wissen, wann oder wo sie zuschlagen werden. Sie wissen genau, dass sie nicht aufgeben werden, deshalb müssen Sie Ihr Bestes tun, um sie von Ihrem Netzwerk fern zu halten. Hacker sind überaus organisiert. Leider teilen sie ihre Heldentaten, Tools und Erkenntnisse mit anderen Hackern, was die Bedrohung nur noch verschlimmert.

Dass Hacker ungepflegte und ungesellige Versager seien, ist ein Mythos. Hacker sind die netten Jungs vom Kurierdienst, das Mädchen an der Kasse des Kaufhauses, Ihr höflicher und ruhiger Nachbar oder sogar der kurz vor der Rente stehende Mitarbeiter in der Produktionsabteilung. Sie können Hacker nicht am Gesicht erkennen.

Ein genaues Profil eines Hackers zu erstellen, ist schwierig, weil es so viele unterschiedliche Typen gibt, die alle durch verschiedene Faktoren motiviert sind. Dennoch kann man Hacker in drei Kategorien einteilen: der Über-Hacker, der gewöhnliche Hacker und das Skript-Kiddie. Im Folgenden finden Sie Profile zu jedem Typ.

Wo Hacker sich treffen: DefCon

Die erste DefCon-Hackerkonferenz (`www.defcon.org`) fand 1992 statt. Sie hatte ungefähr 150 Teilnehmer. 2001 ist die geschätzte Teilnehmerzahl auf über 5.000 angewachsen – und für die Veranstaltung wurde noch nicht einmal geworben.

Hacker, Möchtegerns, Sicherheitsexperten und eine Myriade anderer Personen besuchen die DefCon, um an Seminaren teilzunehmen, die Sicherheitsprobleme bei Anwendungen, Netzwerkarchitekturen sowie Sicherheitsgeräten und -mechanismen detailliert behandeln. Es werden auch Hardware, Software und Bücher verkauft und einige praxisbezogene Kurse, wie z.B. über das Knacken von Sperren, angeboten. Die meisten wichtigen Informationen finden sich hinter den Kulissen und werden in Hotelzimmern und Bars unter Freunden ausgetauscht. Das sind die Orte, um Kontakte zu knüpfen und um gesehen zu werden – oder im Fall des Falles auch nicht.

Hacker sind nicht die einzigen Teilnehmer der DefCon, eine beträchtliche Anzahl Mitarbeiter vom FBI, DEA, DOJ und CIA sind auch vor Ort. Diese Konferenz ist zu so einem populären Treffpunkt für Regierungsdienststellen geworden, dass Hacker einen Wettbewerb namens »Spot The Fed« geschaffen haben. Hacker sollen die Personen outen, die sie für Spitzel oder Polizisten halten.

Über-Hacker

Ein Über-Hacker hackt für Geld oder zur persönlichen Bereicherung, nicht wegen des Ruhmes. Normalerweise leben und atmen Über-Hacker Computerprotokolle und können hoch komplizierte Programme im Schlaf schreiben.

Typische Ziele für diesen Hackertyp sind Finanzinstitutionen, militärische und Regierungs-Sites, Software-Unternehmen und Universitäten mit engen Verbindungen zu Geheimdiensten. Niemand weiß, wie viele Über-Hacker es gibt, weil so wenige erwischt werden. Viele im Sicherheitsgeschäft glauben, dass diese Hacker von feindlichen, ausländischen Regierungen angeheuert werden, um Informationen zu sammeln oder um *Information Warfare* gegen Feinde einzusetzen. Information-Warfare-Kampagnen versuchen auf vielfältige Weise, die Infrastruktur eines Landes auszuschalten: Datennetzwerke, Telekommunikation, Energie,

Transport, Bank- und Finanzwesen, Notdienste und Regierungsaktionen. Das ist eine Art von Terrorismus. Da es noch keine diesem Typ zurechenbare Attacken gegeben hat, glauben viele, dass dies das Schlachtfeld der Zukunft sein wird.

Wenn Sie in einem kleinen Unternehmen arbeiten, bedeutet das nicht, dass Sie Über-Hacker nicht fürchten müssten. Wenn Über-Hacker Ihr Netzwerk als Angriffsbasis für andere Netzwerke verwenden können, werden sie das tun. Es ist wichtig, Ihr Netzwerk gegen alle Eindringlinge zu schützen – ungeachtet der möglichen Motive dieser Eindringlinge.

Gewöhnliche Hacker

Typischerweise hegt der gewöhnliche Hacker einen Groll oder muss etwas beweisen. Dieser Hackertyp verfügt normalerweise über das Fachwissen eines Systemadministrators und weiß eine Menge über Betriebssysteme und Anwendungen. Gewöhnliche Hacker können Attackenprogramme schreiben und besitzen tiefgehende Kenntnisse über Netzwerkkommunikation. Da gewöhnliche Hacker viel über Ihr System wissen, ist es ziemlich wahrscheinlich, dass sie Ihre unternehmenseigenen Informationen stehlen werden.

Um Akzeptanz und Ansehen bei anderen Hackern zu erlangen, veröffentlichen gewöhnliche Hacker oft ihre Hackprogramme im Internet. Diese können dann von anderen verwendet werden. Gewöhnliche Hacker sind eine wirkliche Bedrohung: Sie wissen, wie man hacken muss, und werden in Ihr Netzwerk – in fast jedes Netzwerk – eindringen, wenn Sie Lücken übersehen.

Gewöhnliche Hacker suchen auch nach einfachen Angriffsmöglichkeiten – die bekannten Schwachstellen, die von Systemadministratoren noch nicht gepatched wurden. Oft greifen gewöhnliche Hacker über Websites an, um die Back-End-Server oder Datenbanken zu erreichen und dann die enthaltenen Daten zu stehlen.

Der gewöhnliche Hacker ist häufig an »Hacktivismus« beteiligt, der in Beziehung zu geopolitischen Konflikten und Problemen steht. Hacktivisten attackieren oft Netzwerke, von denen sie glauben, dass sie ihre politischen Gegner unterstützen. Website-Verunstaltungen sind in dieser Gruppe sehr populär.

Skript-Kiddies

Skript-Kiddies sind die Vandalen und Graffitikünstler des Internets. Sie haben wenige oder gar keine eigentlichen Programmierkenntnisse und können nur mit im Internet verfügbaren Tools hacken; Skript-Kiddies können keine eigenen Tools erstellen. Sie besuchen IRC-Räume (Internet Relay Chat), um ihre »Eroberungen« mit anderen zu teilen, und schreiben Nachrichten in jugendlichem Skript-Kiddie-Code, der für Buchstaben Zahlen setzt und absichtliche Schreibfehler enthält. Ein Beispiel, das Sie häufig sehen werden, ist das Wort 3l337 für eleet (Elite) – was natürlich »der Größte« bedeutet. Sie hacken nur, um zu prahlen. Sie können ihre Nachrichten oft über behackte Seiten von Websites wandern sehen.

Skript-Kiddies können und werden Ihrem Netzwerk beträchtlichen Schaden zufügen, wenn sie es finden und sich Zugang verschaffen können. Der Schaden, den sie anrichten, ist wahllos

– sie kümmern sich nicht darum, ob Sie ein großes oder kleines Netzwerk betreiben. Wenn ein automatisiertes Programm im Internet ihr Interesse weckt, werden sie es verwenden. Sie kennen das Ergebnis nicht oder kümmern sich nicht darum.

Virusentwickler

Virusentwickler sind keine Hacker. Eine Freundin von mir, Sarah Gordon, ist eine anerkannte Profilerin für Virusentwickler. In den Jahren ihres Umgangs und teilweise auch Zusammenlebens mit Virusentwicklern hat sie erstaunlicherweise entdeckt, dass die üblichen Vorurteile auf sie nicht zutreffen. Sie würden erwarten, dass sie dem Stereotyp eines Hackers entsprechen – mürrisch, ungepflegt, mit Autoritätsproblemen und unfähig, Beziehungen einzugehen. Meine Freundin hat herausgefunden, dass Virusentwickler im Alter zwischen 10 und 60 Jahren rangieren und dass viele liebevolle Beziehungen zu ihren Familien pflegen.

Das beschwört die Frage herauf: »Wenn Virusentwickler gut angepasst sind, warum schreiben sie Viren?« Ich glaube, dass sie alle ein Programm schreiben wollen, das etwas noch nie da Gewesenes ausführen kann. Virusentwickler scheinen nichts zu verlieren zu haben und ihre Aktivitäten nicht zur persönlichen Bereicherung auszuüben. Deshalb bilden sie eine große Gefahr für Netzwerke. Ich glaube, noch nie von einem Virusentwickler gehört zu haben, der einen Virus veröffentlichte, den angerichteten Schaden bemerkte und dann angeboten hat, als Entschuldigung ein Gegenprogramm zu schreiben.

Ein kleiner Bonuspunkt für Sie ist, dass Virusentwickler sich hauptsächlich – wegen der weiten Verbreitung, der Bequemlichkeit übergreifender Funktionsfähigkeiten zwischen Programmen und der zahlreichen Sicherheitsmängel – auf Microsoft-Systeme und -anwendungen konzentrieren. Wenn Sie keine Microsoft-Produkte verwenden, sind Sie daher immun gegen viele Viren. In der Netzwerkwelt ist es jedoch kaum machbar, auf Microsoft-Produkte zu verzichten, deshalb sind Antivirus-Programme ein Muss.

Angestellte - ehemalige und gegenwärtige

Menschen in einer Organisation können und werden wirkliche Sicherheitsbedrohungen für Ihr System darstellen, obwohl dieser Punkt eine sehr häufig missachtete Komponente der Netzwerksicherheit ist. Nehmen Ihre Angestellten Firmendateien mit, wenn sie aus der Firma ausscheiden? Was hält sie davon ab? Sie sollten diese Fragen ernsthaft durchdenken und dann ehrlich beantworten. Sie können die Sicherheit im physischen Umkreis Ihres Unternehmens nur gewährleisten, wenn Sie auch den Zugang zu den Informationssystemen des Unternehmens geschützt haben. In Zeiten des konjunkturellen Rückgangs kann es für Angestellte und Auftragnehmer sehr schwierig sein, der Versuchung zu widerstehen, Unternehmensdaten oder Geschäftsgeheimnisse zu stehlen oder sich sogar mit Netzwerksabotage zu befassen.

Angestellte, die sich von Ihrem Unternehmen schlecht oder ungerecht behandelt fühlen, könnten voller Groll kündigen. Diese Angestellten könnten versuchen, auf Ihr Netzwerk zuzu-

greifen, um wichtige Daten entweder zu zerstören oder zu stehlen. Falls der Zugriff auf das Netzwerk nicht gelingt, könnte er oder sie versuchen, einen Komplizen in der Firma zu gewinnen, der bei den ruchlosen Aktivitäten behilflich ist. Sie sollten deshalb sofort alle Accounts von gekündigtem Personal deaktivieren – ganz besonders, wenn das Ausscheiden nicht gütlich vor sich ging.

Im Juni 2002 stahl ein früherer Angestellter von Prudential die privaten Daten von über 60.000 Prudential-Angestellten und versuchte dann, diese Informationen im Internet zu verkaufen, um falsche Identitäten zu kreieren. Dieser ehemalige Mitarbeiter fühlte sich ungerecht behandelt, als er noch für Prudential arbeitete. Mit seinem Wissen als Datenbankadministrator des Unternehmens brach er in deren System ein und stahl die persönlichen Daten aus der Datenbank.

Im Folgenden sehen Sie eine Liste von Vorsichtsmaßnahmen, die Sie beachten sollten, wenn ein Mitarbeiter sein Beschäftigungsverhältnis in Ihrer Firma beendet:

- ✔ **Abgabe von Firmenausweis und Firmenschlüssel:** Damit kann gewährleistet werden, dass ehemalige Angestellte später nicht mehr Zutritt zum Firmengelände haben.
- ✔ **Eigentum der Firma:** In vielen Firmen wird am letzten Tag des Arbeitsverhältnisses eine Taschenkontrolle durchgeführt, um sicherzustellen, dass der Mitarbeiter keine vertraulichen Berichte, sensiblen Daten oder anderes Firmenmaterial, das nicht nach außen dringen soll, heimlich mitnimmt.
- ✔ **Netzwerkzugriff deaktivieren:** Dem Mitarbeiter sollte sofort nach Beendigung des Arbeitsverhältnisses der E-Mail- und Netzwerkzugriff verweigert werden. Wenn die Administratoren Zugriff auf Dateien des Home-Verzeichnisses des Benutzers benötigen, stehen ihnen Befehle und Tools zur Verfügung, über die sie auf die Daten zugreifen können. Stellen Sie sicher, dass ehemaligen Mitarbeitern keine Möglichkeiten zur Verfügung stehen, mit denen sie Zutritt in Ihr System erlangen können.
- ✔ **Kündigungsgespräch:** Wenn Ihre Firma Mitarbeiter kündigt, protokollieren Sie den gesamten Verlauf des Gesprächs, das bei der Übergabe der Kündigung geführt wurde. Falls der Mitarbeiter Ihrem Unternehmen droht oder gar verschleierte Drohungen ausspricht, haben Sie gerichtsverwertbare Aufzeichnungen über das Kündigungsgespräch in der Hand.

Sichern und speichern Sie E-Mail-Dateien ein paar Jahre lang, Sie wissen nie, wozu sie noch gut sein können. Es gab schon Fälle, wo alte E-Mail-Dateien Arbeitgeber vor kostspieligen Prozessen bewahrten.

Die Konkurrenz

Unterschätzen Sie nie Ihre Konkurrenz! Diese Aussage kann man gar nicht genug hervorheben! Ich möchte nun nicht unterstellen, dass Firmen bewusst Hacker rekrutieren, um in Ihre Site einzudringen, doch ich wäre nicht erstaunt, wenn einige Firmen ihren Angestellten einen derartigen Versuch erlauben würden. Leitende Angestellte einer bekannten Firma stellten mir

gegenüber mal die Behauptung auf, dass die Konkurrenz keine Chance hätte, auf ihre E-Commerce-Site zuzugreifen, um sensible Informationen zu sammeln. Ich fragte die Angestellten dann verwegen, ob sie darauf auch ihren Job verwetten würden. Die Damen und Herren wurden daraufhin etwas bleich im Gesicht und keiner wollte sich auf diese Herausforderung einlassen. Sie waren jedoch damit einverstanden, ihre Site begutachten zu lassen. Bei dieser Begutachtung fand ich Sicherheitslöcher in den Webservern und Datenbanken der E-Commerce-Site, die der Konkurrenz durchaus die Möglichkeit gegeben hätte, sensible Firmendaten in die Finger zu bekommen.

Viele Firmen machen Fehler, wenn sie ihre Websites einrichten. Dem Anschein nach harmlose Informationen können, wenn sie in die falschen Hände geraten, gefährlich werden und potenziellen Schaden anrichten. Ein Beispiel: Eine Firma listete die Namen, Adressen und privaten Telefonnummern ihrer Führungskräfte auf. Ein Mitarbeiter der Konkurrenz rief eines Abends einen der Führungskräfte zu Hause an und gab vor, im Produktionsteam seiner Firma zu sein. Er erzählte ein paar (natürlich erfundene) Details über Probleme mit dem Fertigungszeitplan und verwickelte den leitenden Angestellten in ein Gespräch darüber, wie eine Änderung des Zeitplans der Firma wirtschaftlich schaden würde. Der leitende Mitarbeiter kam gar nicht auf die Idee, dass er es mit einem Betrüger zu tun hatte, da er der Überzeugung war, dass nur Mitglieder *seiner* Firma Kenntnis von seiner privaten Telefonnummer haben könnten. Das Ergebnis war, dass die Konkurrenz nun den Fertigungszeitplan kannte und diese Information auch zu ihrem Vorteil nutzte.

Mit diesem Beispiel will ich nicht andeuten, Sie dürften überhaupt keine Namen auflisten, doch bieten Sie der Öffentlichkeit auf Ihrer Website nicht mehr Details über Ihre Firma und deren Angestellte, als unbedingt erforderlich ist.

Wie schon weiter oben in diesem Kapitel erwähnt, arbeitet die Konkurrenz auch mit den Mitteln des »Social Engineering«, um sensible Daten zu erhalten. Jemand aus der Konkurrenzfirma könnte zum Beispiel bei Ihrem Empfang anrufen und sich als ein Mitarbeiter *Ihrer* Firma ausgeben, der sich gerade auf Geschäftsreise befindet. Er kann dann die Dame oder den Herren am Empfang bitten, ihm bestimmte Informationen zu geben, beispielsweise wie er Zugriff auf bestimmte Daten erhalten kann. Je mehr er sich vorher im Internet über die Firmenstruktur und Dienstwege informieren konnte, umso leichter wird ihm das Gespräch fallen. Stellen Sie also sicher, dass Mitarbeiter nur dann interne Firmenformationen am Telefon weitergeben, wenn sie wissen, wer am anderen Ende der Leitung ist. Ungewöhnliche Fragen zu Mitarbeiterdaten oder zu dem Sicherheitsverantwortlichen sollten immer Anlass sein, die Identität Ihres Gesprächspartners in Zweifel zu ziehen.

Die Grundregeln der Netzwerksicherheit

Netzwerksicherheit kann eine einfache Angelegenheit sein, wenn konsequent die für die Sicherheit gültigen Basisregeln befolgt werden. Die Technologie allein kann nicht Hacker-Angriffe und andere Sicherheitsbrüche abwehren. Alle Netzwerkadministratoren und Sicherheitsbeauftragte stimmen darin überein, dass die Basisregeln zur Netzwerksicherheit eingehalten

werden sollten, doch kaum jemand hält sich konsequent daran. Warum nicht? Die größte Hürde ist Zeitmangel (und manchmal auch Geldmangel). Denn das Konfigurieren aller Computer im Netzwerk und das Dokumentieren der Änderungen sind zeitraubende Aufgaben. Da Ausgaben für die Sicherheit keine unmittelbaren Gewinnerwartungen mit sich bringen, sondern Investitionen scheinbar verteuern, muss die Führungsebene einer Firma oft in einem mühseligen Überzeugungsprozess dafür gewonnen werden, dass Sicherheit Geld kostet und dass sich Investitionen in die Sicherheit langfristig durchaus lohnen.

Aber auch die Benutzer tragen Schuld, weil sie möchten, dass alles einfach funktioniert. Sie möchten sich nicht die Mühe machen, sichere Passwörter anzulegen und diese dann auch alle 60 Tage zu ändern. Wenn Benutzer einen Sicherheitsmechanismus umgehen können, den sie als lästig empfinden, werden sie das auch ohne mit der Wimper zu zucken tun.

Hier sind sie, die Regeln, die »8 Gebote« der Netzwerksicherheit:

- ✔ Sichere Passwörter verwenden
- ✔ Antiviren-Software verwenden
- ✔ Standardkonfigurationen ändern
- ✔ Keine unnötigen Dienste starten
- ✔ Sicherheitsupdates installieren
- ✔ Backup des Systems
- ✔ Schutz gegen zu viel und zu wenig Strom
- ✔ Wissen, wem Sie vertrauen können

Die Regeln scheinen einfach zu sein und sie sind relativ leicht zu implementieren. Sie werden in den folgenden Abschnitten näher beleuchtet und ich möchte Sie dringend bitten, die »8 Gebote« der Netzwerksicherheit gewissenhaft zu befolgen. Denn dann gibt es auch weniger Angriffe und Probleme mit unseren Systemen.

Sichere Passwörter verwenden

Passwörter sind oft der einzige Schutz, der auf einem System eingesetzt wird. Eine Benutzer-ID ist nur ein Name und kann eine Identifizierung nicht prüfen, doch ein Passwort, das mit einer Benutzer-ID verbunden wird, kann als Identifikator agieren. Passwörter sind daher der »Schlüssel« zu Ihrem Netzwerk und Sie sollten beim Erstellen oder der Vergabe eines Passwortes äußerste Sorgfalt walten lassen. Firewalls und Intrusion-Detection-Systeme können nichts tun, wenn Ihre Passwörter versagen.

Was versteht man unter einem wirklich starken Passwort? Nun, ein solches Passwort sollte auf keinen Fall in einem Wörterbuch zu finden sein. Auch sollte es nicht leicht zu erraten sein. Längere Passwörter sind schwerer zu erraten und zu knacken als kurze Passwörter.

Die folgende Liste soll Ihnen ein paar Anregungen geben, was Sie und Ihre Benutzer beim Anlegen von Passwörtern beachten sollten:

- ✔ **Verwenden Sie eine Buchstabenkombination, die keinen Sinn ergibt.** Die besten Passwörter sind die, die auf den ersten Blick total blödsinnig zu sein scheinen. Wenn Sie zum Beispiel den Satz »Nighty, night and don't let the bed bugs bite« nehmen und dann nur den ersten Buchstaben von jedem Wort verwenden, würde Ihr Passwort »nnadltbbb« lauten. Dieses Passwort ist nicht leicht zu erraten, doch der Benutzer kann es sich leicht merken. Doch sehen Sie gleich, wie man das noch sicherer gestalten kann.
- ✔ **Variieren Sie mit Klein- und Großbuchstaben:** Dabei sollte sich ein Großbuchstabe an einer anderen Stelle als am Beginn des Passwortes befinden und es sollten auch Zahlen mit einbezogen werden. Es ist zwar vorstellbar, dass ein Hacker das Passwort mit einem brachialen, wörterbuchbasierten Angriff (*Brute Force Attack*) knacken könnte, aber dieser Prozess würde mehrere Stunden in Anspruch nehmen. Und glauben Sie mir, ein Hacker hat meist keine Lust, so viel Zeit zu vergeuden.
- ✔ **Längere Passwörter sind sicherer:** Die Länge sollte mindestens acht Zeichen umfassen.
- ✔ **Ändern Sie Ihr Passwort regelmäßig:** Auch das beste Passwort sollte regelmäßig geändert werden (zum Beispiel alle 60 Tage). Damit verhindern Sie, dass ein Passwort, das geknackt wurde, langfristig missbräuchlich eingesetzt wird. Viele Betriebssysteme ermöglichen es, dass diese Einstellung für jeden Benutzer festgelegt werden kann.
- ✔ **Legen Sie *neue* Passwörter an und verwenden Sie nicht immer wieder dieselben:** Innerhalb eines Jahres oder sogar für einen Zeitraum von 18 Monaten sollte ein einmal festgelegtes Passwort nicht noch einmal verwendet werden.
- ✔ **Verwenden Sie keine Zeichen, die auf der Tastatur direkt nebeneinander liegen:** Passwörter sollten nicht aussehen wie qwertz, 12345678 oder asdfghj. Auch wenn diese Passwörter auf den ersten Blick unsinnig erscheinen, folgen sie doch einem bestimmten Muster fortlaufender Tasten auf der Tastatur und Passwort-Cracker werden das in Sekunden herauskriegen.
- ✔ **Behandeln Sie Ihre Passwörter als streng geheime Information:** Alle Passwörter sollten geschützt und nicht gemeinsam genutzt werden! Und eine weitere schlechte Angewohnheit: Viele Benutzer schreiben ihre Passwörter auf einen Merkzettel und kleben diesen Zettel dann an ihren Computer oder legen ihn unter ihre Tastatur. Auch das ist absolut tabu!

Für einen Eindringling sind Passwörter für die Root- und Administratorenebene der Schlüssel ins Königreich. Systemadministratoren mit Root-Privilegien – also keine Zugriffsbeschränkungen und berechtigt für die Durchführung jedweder Änderung – müssen die sichersten Passwörter verwenden. Gleichzeitig sollten für diesen Personenkreis die strengsten Regeln für regelmäßiges Ändern der Passwörter und absolutes Verbot der Wiederverwendung gelten. Folgen Sie diesen Leitlinien:

- ✔ **Schreiben Sie alle Root-Passwörter nieder und bewahren Sie diese Aufzeichnungen an einem sicheren Ort (z.B. in einem Tresor) auf:** Wenn ein Administrator dann für eine

Zeit lang arbeitsunfähig ist, können Sie so ohne größeren Aufwand das Passwort des Mitarbeiters ermitteln. Es gibt zwar automatische Ermittlungsprogramme für Passwörter, doch in einem Notfall sollte man nicht unbedingt darauf angewiesen sein.

- ✔ **Ändern Sie alle Benutzerpasswörter, falls Sie den Verdacht haben, eines Ihrer Administrator-Passwörter könnte ermittelt worden sein:** In diesem Fall können Sie nicht ausschließen, dass von einer unbekannten Person mit Hilfe des bekannt gewordenen Administrator-Passworts auch alle übrigen Benutzerpasswörter ermittelt wurden.

Wenn ein Benutzer also den Verdacht hat, dass ein Passwort gestohlen oder geknackt wurde, sollte er das Passwort sofort ändern und die dafür Verantwortlichen in der Firma informieren.

Immer Antiviren-Software verwenden

Viren stellen ein ärgerliches und teures Problem dar, mit dem Sie potenziell immer rechnen müssen. Es wäre also ganz schön dumm, wenn Sie keine Antiviren-Software zum Schutz Ihrer Computer in Ihrem Netzwerk einsetzen würden. Antiviren-Software bietet zwar keinen 100%igen Schutz, doch ihr Einsatz ist immer noch besser als gar kein Schutz. Ob Sie es nun glauben oder nicht – ich habe schon Leute sagen gehört, dass sie keine Antiviren-Software verwenden, da sie noch nie mit einem Virus infiziert wurden. Sie entschuldigen schon, aber wenn man keine Antiviren-Software installiert hat, woher soll man dann wissen, dass man noch nie einen Virus hatte? Die meisten Viren sind für den Benutzer nicht evident.

Antiviren-Software besteht normalerweise aus zwei Teilen: dem eigentlichen *Scanner*, der im Englischen als *Engine* (dt. Maschine) bezeichnet wird, und den *Viren-Signaturdateien*. Damit die Antiviren-Software ihre Effektivität beibehalten kann, sollten die Engine und die Signaturdateien regelmäßig aktualisiert werden. Das Software-Programm hat in der Regel einen *Update*-Befehl, so dass Sie auf der Website des Herstellers nach Updates suchen können.

Die Engine bestimmt, welche Dateien gescannt werden sollen, welche Funktionen laufen sollen und wie reagiert werden soll, wenn ein vermeintlicher Virus gefunden wurde. Die Signaturdateien sind im Wesentlichen eine Datenbank bekannter Viren und ihre Auswirkungen. Die Engine vergleicht die Dateien auf Ihrem Computer mit den in den Signaturdateien abgespeicherten Informationen über Viren. Antiviren-Software neigt zu, lieber einmal mehr als einmal weniger zu warnen, so dass auch mal ein Fehlalarm verursacht werden kann. Dies ist jedoch nur eine kleine Unbequemlichkeit gegenüber dem großen Nutzen für Ihre Sicherheit.

Sobald neue Viren auf der Welt entdeckt werden, aktualisieren die Hersteller von Antiviren-Software ihre Datenbanken mit der gefundenen Virenstruktur. Einige Unternehmen passen jedoch auch die Dat-Dateien, die für die Engine benötigt werden, mit den neuen Viren-Informationen an. Da viele Benutzer die Aufteilung zwischen der Scan-Engine und der Datenbank nicht kennen, aktualisieren viele brav die Signaturdateien für die Datenbank, sind sich jedoch nicht bewusst, dass die Engine ebenfalls einer Aktualisierung bedarf. Es ist äußerst wichtig, zu überprüfen, ob ebenfalls Updates oder Upgrades für die Engine zur Verfügung stehen, wenn Sie nach Aktualisierungen der Signaturdateien suchen.

Damit die Antiviren-Software effektiv arbeiten kann, muss sie sowohl auf individuellen Workstations installiert werden als auch auf allen Servern und anderen Computern in Ihrem Netzwerk. Nur so können Viren an allen Einfallstellen aufgegriffen werden. Auch entfernbare Medien wie Floppydisks und CDs sollten vor ihrer Verwendung im System gescannt werden. Leider sind oft auch in legitimierten Software-CDs Viren versteckt und auch in Disketten, die von zu Hause in die Firma mitgebracht werden, können Viren stecken. Ausführlich wird Antiviren-Software in Kapitel 7 behandelt.

Wenn Sie Antiviren-Software auf Ihren Internet-Gatewayservern installieren, können alle von außen eingehenden Daten auf Viren überprüft werden.

Obwohl die meisten Viren auf Windows-Betriebssysteme abzielen, sollte man auch in Systemen, die auf Unix oder Mac basieren, Antiviren-Software einsetzen. Ein Virus kann Unix- oder Mac-Systeme durchlaufen, ohne dabei diese Systeme zu befallen. Wenn ein Virus jedoch »seine Reise« durch diese Systeme antritt und auf ein Windows-basiertes System trifft, wird er damit beginnen, seine Wirkung zu entfalten. Ich habe schon E-Mail-Viren gesehen, die auf einem Unix-basierten E-Mail-Server völlig harmlos waren. Die Workstations basierten jedoch alle auf Windows. Sobald die E-Mail also von einem Computer abgerufen wurde, auf dem Windows installiert war, begann der Computer sofort damit, alle anderen Windows-Computer, die er finden konnte, zu infizieren.

Viren: Das größte Problem, das Firmen mit Internetverbindungen betrifft

Wenn Ihre Firma mit dem Internet verbunden ist, ist Ihr System anfällig für Viren. Da gibt's leider nichts daran zu rütteln. Einer der größten Vireninfektionen, die in den letzten Jahren vorgekommen sind, war der »I Love You«-Bug. Er war auch der erste Virus, dem es gelang, U.S.-klassifizierte Netzwerke zu infiltrieren. In einer jüngst durchgeführten Bestandsaufnahme, die gemeinsam vom CSI (Computer Security Institute) und dem FBI durchgeführt wurde, berichteten 94 Prozent der Befragten, dass ihr System im Jahre 2001 von einem Virus befallen wurde. Dabei entstand ein Schaden von über 45 Millionen Dollar. Nur 40 Prozent klagten über Systemeindringlinge. Es ist also viel wahrscheinlicher, dass Ihr System von einem Virus befallen wird, als dass ein Hacker einen Angriff startet. Der Einsatz von Antiviren-Software ist also in zweierlei Hinsicht nützlich: Sie sparen damit Zeit und Geld.

Standardkonfigurationen ändern

Einer der weitverbreitetsten Fehler beim Einrichten einer Rechnerumgebung ist das Belassen der Standardkonfiguration einer Software. Standardkonfigurationen enthalten oft standardisierte Benutzerkonten und Passwörter, die nicht nur in den Handbüchern ausgedruckt, sondern auch allen Hackern der Welt bekannt sind. Dies gilt für die Software von Routern, Hubs,

Switches, Betriebssystemen, E-Mail-Systemen und andere Serveranwendungen wie Datenbanken und Webserver. Ich kenne keine einzige Software, die gegen dieses Problem immun ist.

Es sind nicht nur die bekannten Passwörter, die ein Problem darstellen. Die Standardkonfigurationen enthalten darüber hinaus Sicherheitslücken, die Sie beheben müssen. Bevor Sie auch nur mit einem Computer online gehen, sollten Sie zuvor alle Standardbenutzerkonten und -Passwörter ändern sowie die aktuellsten Sicherheitspatches anwenden. Wenn Sie sich für diese Aufgaben genügend Zeit nehmen, können Sie sich später eine Menge Kummer ersparen. Je weniger Sicherheitslücken Ihr Netzwerk aufweist, umso schwieriger wird es, in Ihr System einzubrechen. Weitere Informationen zum Ändern von Standardeinstellungen finden Sie in den Kapiteln 11, 12 und 13.

Keine unnötigen Dienste starten

Oft wird bei einer Standardkonfiguration des Betriebssystems – insbesondere der Server-Software – eine Reihe von Diensten oder kleinen Programmen aktiviert, die Sie gar nicht benötigen. Hier gilt die Faustregel: Schalten Sie alles ab, was Sie nicht wirklich benötigen, da einige der Standarddienste bekannt sind für Sicherheitslücken und so die Verwundbarkeit Ihres Netzes erhöhen. Diese Regel geht Hand in Hand mit der im Abschnitt zuvor aufgestellten Regel: Verlassen Sie sich nicht auf die Standardeinstellungen. Das Deaktivieren dieser Dienste ist einfach zu bewerkstelligen und verschafft Ihnen große Vorteile.

Einige der von mir angesprochenen Dienste werden in erster Linie zur Fernadministration eingesetzt. Dazu gehören die »r«-Befehle in Unix wie `rsh` und `rlogin`. Falls Sie Ihren Server nicht als Webserver einsetzen möchten, deaktivieren Sie die `http`- oder Webserver-Dienste. Das gilt auch für `ftp`-Dienste. Falls Sie keine Dateien mit Hilfe von `ftp`-Protokollen übertragen wollen, gibt es keinen Grund, diesen Dienst aktiviert zu halten. Eine ausführlichere Liste von gefährlichen oder nicht unbedingt notwendigen Diensten finden Sie in Kapitel 11.

Sicherheitsupdates installieren

Fast alle Software-Produkte enthalten Fehler und Sicherheitsmängel. Deshalb finden Sie auf den bekannten Sicherheitsportalen wie CERT oder BSI.de täglich aktualisierte, seitenlange Listen mit Warnungen und Hinweisen auf Sicherheitsupdates. Der Sicherheitsbeauftragte für Ihr Netzwerk sollte deshalb stets über diese aktuellen Warnungen informiert sein und sich über die Mail-Listen solcher Portale schriftliche Informationen zu bestimmten Problemen regelmäßig zukommen lassen. Viele dieser Mail-Listen bieten beim Registrieren auch die Möglichkeit der differenzierten Auswahl von Informationen an, so dass Sie dann nur die Warnungen erhalten, die für Ihre Systemauslegung relevant sind. Sorgen Sie dafür, dass möglichst schnell nach dem Bekanntwerden von Sicherheitswarnungen auf Ihren Rechnern die entsprechenden Fehlerbehebungs-Routinen und zur Verfügung gestellten Sicherheitspatches installiert werden. Denn was nützen alle Firewalls der Welt, wenn Sie die Hintertür für Hacker offen halten?

Natürlich verfolgen auch Hacker diese Warnmeldungen sorgfältig. Wenn sie auf eine interessante Meldung stoßen, beginnen sie nach Systemen im Internet zu suchen, die für die Schwachstellen (auf die sich die Warnmeldungen beziehen) anfällig sind.

Backup des Systems

Falls ein Eindringling Ihr System lahm gelegt hat, so ist es am besten, alle Online-Verbindungen zu kappen und mit Hilfe Ihrer Backup-Sicherungen das System vollständig einzurichten. Sie *haben* erst kürzlich eine Systemsicherung durchgeführt, oder? Das ist gut so. Sind Sie sicher, dass Sie mit Hilfe des vorgenommenen Backups auch das vollständige System erneuern können? (Ich lasse nicht locker, nicht wahr?) Einige Backup-Typen werden nur für Archivierungszwecke verwendet und sind nicht dazu gedacht, ein System funktionsfähig wiederherzustellen. Mancher Benutzer musste auch schon die Erfahrung machen, dass die Backup-Bänder nutzlos waren, da manche Backup-Ordner beschädigte Daten enthielten. Führen Sie gelegentliche Tests Ihrer Backups durch, um sicher zu sein, dass sie intakt sind.

Das Backup von Systemen kann man mit der Reinigung von Zähnen mit Zahnseide vergleichen: Jeder weiß, dass man das oft und gründlich tun sollte, doch nur wenige Menschen tun es oft und noch weniger tun es gründlich.

Es gibt hunderte verschiedener Vorschläge über die richtige Backup-Strategie eines Unternehmens, so dass man damit ein ganzes Buch füllen könnte. Bestimmte Methoden ziehen sich jedoch wie ein roter Faden durch viele Strategien und können auch für Ihre Firma als Faustregel formuliert werden:

- ✔ Jeweils am ersten Tag einer Arbeitswoche sollten Sie eine *komplette Datensicherung* (Backup) Ihres Systems durchführen (inklusive aller Dateien auf allen Computern).
- ✔ In den folgenden Tagen sollten Sie ein *inkrementelles Backup* durchführen. Dabei werden nur die Dateien berücksichtigt, die Sie seit dem zuletzt durchgeführten kompletten Backup geändert haben.
- ✔ Schließlich sollten Sie einmal im Monat eines der kompletten Backups zu Archivierungszwecken speichern. Wenn Sie dann einmal in die Zwangslage kommen, Ihr System wieder herstellen zu müssen, so sind Ihre Sicherungsdaten in keinem noch so ungünstigem Falle älter als eine Woche.

Backup-Medien sollten nie an demselben Ort wie Ersatzrechner aufbewahrt werden. Denn sollte ein solcher Ort Katastrophen wie zum Beispiel Feuer oder Hochwasser ausgesetzt sein, dann sind nicht auch noch die Backup-Bänder davon betroffen. Um ganz sicher zu gehen, sollten Sie die Backups außerhäusig lagern.

Backups können keine Hackerangriffe oder Intrusionen in Ihr Netzwerk verhindern. Doch sie können Ihnen helfen, bei solchen Ereignissen das System zu »retten«. Da Webserver ein beliebtes Ziel für Vandalismus bieten, halten viele Unternehmen einen zweiten zusätzlichen Webserver mit einer aktuellen Spiegelung der Daten des aktiven Webservers vor, um für einen

Ausfall gerüstet zu sein. So können Sie sofort bei einem Ausfall Ersatz mit den aktuellen Daten bereitstellen – tun Sie dies jedoch erst dann, wenn Sie auch auf dem zweiten Server die Sicherheitslücke geschlossen haben, die dem ersten Server zum Verhängnis wurde.

Schutz gegen zu viel und zu wenig Strom

Diese Schutzmaßnahme geht Hand in Hand einher mit der Durchführung regelmäßiger Backups. Wenn Sie wie ich in einer Gegend mit viel Blitz und Donner wohnen, werden Sie schnell herausfinden, dass alle elektrischen Geräte mit einem Überspannungsschutz ausgerüstet sein sollten, und darüber hinaus sollten Sie auch so genannte UDPs (Uninterruptible Power Supplies), die eine unterbrechungsfreie Stromversorgung gewährleisten, auf allen wichtigen Computern installieren.

Für bestimmte kritische Teile Ihres Systems empfiehlt sich dringend das Vorhalten einer exakten Spiegelung der betroffenen Daten, ähnlich wie im vorhergehenden Abschnitt bereits erwähnt. Diese Spiegelung der Daten setzen Sie dann ein, wenn das Teilsystem ausfällt, unabhängig, ob durch eine Naturkatastrophe oder einen Hacker verursacht. So können Sie z.B. alle Ihre Webseiten parallel auf einem zweiten Rechner speichern, um diese Maschine bei einem Ausfall des ersten Webservers einfach an die Stelle des ausgefallenen anzuschließen. Bei diesen Rechnern muss es sich nicht unbedingt um die erste Wahl handeln, wie folgendes Beispiel zeigt.

Vor kurzem stellte ein Partnerunternehmen sein Netz und all dessen Komponenten von einem etwas in die Tage gekommenen System auf ein hochaktuelles System mit brandneuen Rechnern um. Bevor das neue System gestartet wurde, wurden Netzwerk und Rechner unter Laborbedingungen ausführlich getestet und für gut befunden. Die alten Computer wurden demontiert und in das Ersatzteillager verbracht, bevor die neuen Rechner installiert wurden. Es kam, wie es in solchen Situationen oft passiert: Was vorher in einer Umgebung erfolgreich getestet wurde, muss nicht unbedingt in einer anderen Umgebung funktionieren. Das gesamte System brach unmittelbar nach dem Start zusammen und nichts ging mehr. Ärgerlich, dass die noch funktionierenden älteren Computer bereits eingemottet in dem mehrere hundert Meter entfernten Ersatzteillager untergebracht waren. Zwar kein absolutes Desaster, aber Grund zur Panik allemal!

Wissen, wem Sie vertrauen können

Natürlich wissen Sie, wer von Ihrem Büro auf Ihr Netzwerk zugreift. Sind Sie jedoch auch genau über alle sonstigen Verbindungen informiert, die Sie zur Verbesserung und Verzahnung der Zusammenarbeit z.B. Ihren Lieferanten und Geschäftspartnern oder aber Ihren Kunden eingeräumt haben? Haben Sie die Computer so eingerichtet, dass der Zugriff auf freigegebene Daten seitens Computern von andereb Firmen erlaubt ist? Sind Sie sich sicher, das die IP-Nummern der zugriffsberechtigten Rechner stimmen und zur Partnerfirma gehören? Haben Sie die Anzahl anderer Netzwerke, denen Sie vertrauen, limitiert? Wissen Sie, ob Sie

einen Fernzugriff auf Ihr System erlaubt haben, und wenn ja, wem diese Zugriffsmöglichkeit eingeräumt wurde? Es gibt Dateien in Ihrem Netzwerk, die vertraute Verbindungen auflisten. Vergewissern Sie sich, dass die Adressen dieser Netzwerke stimmen. Stellen Sie darüber hinaus sicher, dass Ihre Firewalls und Router die korrekten Adressinformationen über Ihre vertrauten Verbindungen haben. Überprüfen Sie all diese Informationen in regelmäßigen Abständen. Nur so ist gewährleistet, dass sich keine Fehler eingeschlichen haben und alle Informationen richtig und auf dem neuesten Stand sind. Wenn Sie ein Abkommen mit einem anderen Netzwerk beendet haben, stellen Sie sicher, dass alle diesbezüglichen Verbindungsinformationen gelöscht und ab jetzt alle Verbindungsversuche seitens dieses Netzwerks abgeblockt werden.

Auch der physische Zugriff muss bedacht werden. Kann jede beliebige Person einfach so in Ihre Firma hineingehen? Sind Unterlagen offen zugänglich und werden die Computer nachts abgeschaltet? Könnte es sein, dass auch Mitarbeiter wie z.B. der Hausmeister Ihre Ablagen näher als gewünscht unter die Lupe nehmen? Es ist auch wichtig, dass Sie über Sicherheitsrichtlinien und -prozeduren den Umgang mit Besuchern regeln. Manchmal macht es durchaus Sinn, Besuchern für die Zeit, in der sie in Ihrer Firma sind, eine Besucherplakette anzuheften und/oder ihnen eine Begleitperson zur Seite zu stellen. Wenn Ihre Mitarbeiter regelmäßig Ausdrucke von sensiblen Daten – wie zum Beispiel Daten aus der Buchhaltung – vornehmen, sollte sichergestellt sein, dass die Ausdrucke nicht einfach so herumliegen und neugierigen Augen zugänglich gemacht werden.

Und noch ein letzter Gedanke. Was werfen Sie in den Mülleimer bzw. Papierkorb? Sind Sie sicher, dass da nicht auch Unterlagen dabei sind, die persönliche Daten Ihrer Mitarbeiter enthalten? Sie machen sich strafbar, wenn Sie persönliche Informationen über Ihre Angestellten nicht entsprechend schützen. Und wenn Sie von Zeit zu Zeit Stichproben machen, was so in die Papierkörbe Ihrer Mitarbeiter entsorgt wird, werden Sie erstaunt sein, was Sie da alles vorfinden. Gegebenenfalls müssen Sie über eine Sicherheitsrichtlinie veranlassen, dass Unterlagen, die wichtige oder persönliche Informationen enthalten, auch entsprechend entsorgt werden – zum Beispiel über einen Papierwolf. Denn Sie möchten ja nicht, dass diese Informationen in die falschen Hände geraten.

Eine beliebte Aktivität von Hackern ist das so genannte Dumpster Diving, also das Wühlen im Müll. Da werden gezielt Papierkörbe heimlich nach Unterlagen durchsucht, die wichtig sein könnten, und die in den Unterlagen enthaltenen Informationen – wenn möglich – für einen Angriff auf Ihr Netzwerk benutzt. Deshalb noch mal der Hinweis: Werfen Sie Ihre Unterlagen nicht einfach so in den Müll, sondern entsorgen Sie sie über den Papierwolf oder Aktenvernichter.