[SMR00] *Markus Schumacher, Marie-Luise Moschgath, and Utz Roedig:* **Angewandte Informationssicherheit: Ein Hacker-Praktikum an Universitäten;** Informatik Spektrum, 23(6), June 2000.

Angewandte Informationssicherheit Ein Hacker-Praktikum an Universitäten

M. Schumacher[1], M.-L. Moschgath[2], U. Roedig[3]

[1] Information technology Transfer Office - TU Darmstadt
[2] Institut für Informationssysteme - ETH Zürich
[3] Industrial Process- and System Communications - TU Darmstadt
schumacher@ito.tu-darmstadt.de,
moschgat@inf.ethz.ch
roedig@kom.tu-darmstadt.de

Zusammenfassung Immer mehr Geschäftsprozesse werden in der Industrie über IT Systeme abgewickelt. Neben der generellen Verfügbarkeit und Funktionstüchtigkeit dieser Systeme, wird ihre Absicherung gegen Angreifer immer wichtiger. Dem dadurch entstehenden Bedarf an qualifiziertem Sicherheitspersonal sollten sich auch die Universitäten mit ihrem Ausbildungsangebot anpassen. Zwar werden zunehmend Lehrveranstaltungen zum Thema „IT-Sicherheit" angeboten, diese betrachten jedoch typischerweise nur einen Ausschnitt aus dem Gebiet der IT-Sicherheit und sind oft eher theoretisch ausgerichtet, wie z.B. Kryptographie oder sichere Betriebssysteme. Im folgenden wird das Konzept einer erfolgreich durchgeführten, praxisorientierten Lehrveranstaltung beschrieben, die den Teilnehmern das Zusammenwirken aller Sicherheitsmechanismen anschaulich verdeutlicht.

1 Einleitung

Um ein IT-System vor einem Angreifer schützen zu können, reicht die Kenntnis der theoretischen Grundlagen der einzelnen IT-Sicherheitskomponenten (Firewalls, Kryptographie, Paßworte, etc.) allein nicht aus. Es ist vielmehr notwendig, daß das Zusammenspiel der einzelnen Sicherheitskomponenten untereinander erkannt und verstanden wird. Die Sicherheit einer Komponente hängt meist direkt von der Verwendung bzw. Sicherheit einer oder mehreren anderen ab. So nützt beispielsweise eine gesicherte (verschlüsselte) Kommunikationsverbindung zwischen zwei Rechnern nur dann etwas, wenn die Endsysteme selbst gegen Mißbrauch oder Manipulation geschützt sind. Diese Abhängigkeiten sind komplex, vielschichtig und abstrakt kaum erfaßbar. Nach unserer Auffassung lassen sich diese Zusammenhänge einfacher verstehen und erfassen, wenn sie selbst innerhalb eines IT-Systems beobachtet und ausprobiert werden können.

Neben den generellen Abhängigkeiten, die die Gesamtsicherheit eines IT-Systems beeinflussen, ist es ebenfalls nötig, die Verfahrensweise und das Verhalten eines Angreifers zu kennen. Um ein IT-System „verteidigen" zu können, muß der Verteidiger in der Lage sein, das IT-System aus der Sicht des Angreifers zu sehen und zu verstehen. Ziel des „Hacker-Praktikums" an Technischen Universität Darmstadt war es deshalb:

- den Teilnehmern den Begriff „IT Sicherheit" praxisnah und möglichst vielschichtig zu erläutern und
- die Teilnehmer sowohl in die Rolle eines Angreifers, als auch in die Rolle eines Verteidigers zu versetzt, um die jeweiligen Verhaltensmuster und Möglichkeiten zu vermitteln.

Um diese Ziele zu erreichen, wurden zunächst zwei Gruppen von Studenten gebildet, wobei jede Gruppe ein eigenes Netz mit verschiedenen Rechnersystemen erhielt. Jede Gruppe hatte nun die Aufgabe, bestimmte Dienste der anderen Gruppe (also nach „außen") zur Verfügung zu stellen (WWW, ftp, etc.). Sie wurden dadurch zum Betreiber eines IT- Systems. Die weiteren Aufgaben waren nun, die Rechner im Netzwerk der jeweils anderen Gruppe zu „knacken" und die eigenen Rechner vor unbefugten Zugriffen zu schützen.

2 Hacker, Cracker und ihre Ethik

In der heutigen Zeit wird der Begriff Hacker oftmals gleichgesetzt mit „digitale Revolverhelden" oder „Cyberpunks", die von Computer besessen sind und ihre Leidenschaft über die gesellschaftlichen Grenzen hinaus und meist mit wirtschaftlichem Schaden ausleben. Dieses Negativbild wurde jedoch erst in den 80er Jahren von den Medien geprägt.

Anfang der sechziger Jahre, als die ersten Maschinen mit Tastatur und Bildschirm für jedermann zur Verfügung standen, gab es bald einige Studenten, die so fasziniert waren von den Möglichkeiten der Rechner, daß sie nächtelang davor saßen und versuchten, Programme zu schreiben und die neue Technik bis an die Grenzen des Möglichen auszunutzen. Eine Hochburg dieser Szene entwickelte sich am Massachusetts Institute of Technology (MIT) in Boston, USA. Dort arbeiteten die ersten Leute, die als Hacker bezeichnet wurden. Darunter verstand man damals „Personen, denen es Spaß machte, die Details eines programmierbaren Systems zu erforschen und dessen Möglichkeiten zu erweitern".

Mit dem Vorläufer des Internet, dem Arpanet, eröffneten sich für die Computer-Freaks weitere faszinierende Möglichkeiten. Sie benötigten einen einfachen Home-Computer, ein Modem und einen Telefonanschluß. Da das damalige Netz zum einfachen Austausch von Daten konzipiert wurde, waren die Hürden, die genommen werden mußten, um an die Daten auf fremden Rechnern zu kommen, nicht hoch. Es bildeten sich jedoch bald ungeschriebene Gesetze heraus, die als „Hacker-Ethik" bekannt geworden sind. Es existieren die verschiedensten Versionen der Hacker-Ethik im Netz; auch ist umstritten, von wem sie ursprüngliche stammt. Eine erste Version findet man in dem Buch „Hackers" von Steven Levy. Die wichtigsten Grundsätze dieser Ethik sind:

- Der Zugang zu Computer und allem, was einem zeigen kann, wie diese Welt funktioniert, sollte unbegrenzt und vollständig sein.
- Alle Informationen sollen frei zugänglich sein.
- Daten, die gefunden werden, dürfen nicht verändert werden.

Als Hacker wurden nun Datenreisende bezeichnet, die Spaß daran hatten, die neuen, globalen Datennetze zu erforschen und miteinander zu kommunizieren, ohne jemandem Schaden zuzufügen. Der Begriff „Joy-Riding" wurde geprägt.

Neben dieser „Hacker-Szene" entwickelte sich seit Ende der 60er-Jahre die „Phreaker"-Subkultur. Das Ziel der Phreaks (Phone-Freaks) war es, anfangs ohne Computer, den Telefongesellschaften „eins auszuwischen", indem sie kostenlos um die Welt telefonierten und Telefonkonferenzen schalteten. Da das Reisen der Hacker im Datennetz kostspielig war, vereinigten sich bald beide Kulturen und es entstand eine neue Hackerart. Das primäre Ziel dieser neuen Hacker-Generation war noch immer Spaß zu haben, große Maschinen zu manipulieren und für eigene Zwecke zu nutzen, doch nun auf Kosten der Betreiber wie beispielsweise den Telefongesellschaften und anderer Benutzer.

Mit der Ausbreitung des Kommunikationsnetzes wuchsen auch die „Sicherheitsmechanismen" der Rechner. Durch das Einführen von Paßwörtern und Zugriffskontrollen waren die Hacker nun gezwungen, sich auf weniger feine Arten die Zugangscodes zu beschaffen. Das wurde ihnen aber meist nicht schwer gemacht. Einfachste Attacken wie Ausspähen am Arbeitsplatz, Durchwühlen des Mülls von Rechenzentren oder „Social Engineering" waren oft erfolgreich.

Doch nicht allen war die „Hacker-Ethik" heilig. War diese durch die Phreaker schon aufgeweicht, wurde nun aus den verschiedensten Gründen das Wissen und Können zur Beschaffung und Manipulation von Daten eingesetzt; wirtschaftlicher Schaden entstand. Zu den bekanntesten „Hacks" dieser Art zählen der KGB-Hack, der VMS-Source-Code-Klau bei DEC, der NASA-Hack und der Btx-Hack.

Das Thema „Hacken" wurde immer brisanter. Seit Anfang der 80er Jahre von der Presse und der Filmindustrie aufgegriffen, führen die verschiedensten Berichte und Filme zu einem neuen Hacker-Bild in der Öffentlichkeit. Der Hacker war nun in der öffentlichen Meinung zu einem böswilligen Eindringling mutiert. Er versucht, sensible Daten zu stehlen, zu veröffentlichen oder gar zu manipulieren.

Doch auch heute versteht der „echte" Hacker sich als Pionier, Programmier- und Netz-Magier. Hacker bauten das Internet, brachte das World Wide Web zum Laufen, machten das Unix-Betriebssystem zu dem, was es heute ist, und vieles mehr. Ein Hacker ist eine Person, die sich für die innersten Arbeitsweisen eines Betriebssystems interessiert. Hacker wissen viel über Betriebssysteme und Programmiersprachen, sie können Sicherheitslöcher in Systemen finden und die Ursachen dafür entdecken. Hacker sind ständig auf der Suche nach neuem Wissen und teilen ihre Entdeckungen mit. Sie würden niemals absichtlich Daten zerstören.

Leute, die böswillig in die Systemintegrität eines entfernten Rechners eingreifen, manipulieren und zerstören, werden von echten Hackern als „Cracker" bezeichnet. Ihre Absichten sind böswillig. Wirkliche Hacker halten Cracker für ein „faules, unverantwortliches und nicht besonders schlaues Pack".

In diesem Artikel wird es entsprechend gehalten. Wenn von „Hackern" die Rede ist, sind Profis gemeint, die ihre Rechner und die Technik beherrschen und sie sinnvoll (gegen „Cracker") einsetzen und absichern können.

3 Die Rechtslage

Das Wissen über die rechtliche Grundlage von Computerkriminalität zu vermitteln, sahen wir als wichtigen Punkt, um den Teilnehmern des Praktikums zu verdeutlichen, welche Konsequenzen ein Angriff auf ein IT-System außerhalb des Labors haben kann und wird. So wurde außerdem klar, daß es neben den technischen Maßnahmen auch juristischen Ansätze gibt, die als „Waffen" zum Schutz eines IT-System eingesetzt werden können.

Neben jugendlichen Computerfreaks stellen vor allem professionelle Industriespione, Informationsbroker und Geheimdienste eine Gefahr für die internationalen Datennetze dar. Nicht mehr Drang nach Wissen über Systeme und Spaß sind die treibende Kraft, sondern wirtschaftliche und politische Faktoren. Im heutigen Informationszeitalter gilt die populäre Formel „Wissen ist Macht" wie nie zuvor. Die richtigen Informationen führen zum wirtschaftlichen Erfolg.

Der potentielle Mißbrauch von internationalen Computernetzen kann grob in zwei Bereiche eingeteilt werden: Mißbrauch durch Handlungen und Mißbrauch durch Inhalte. Beispiele für den Mißbrauch durch Handlungen, bei denen das Internet für schädigende und rechtswidrige Aktivitäten benutzt wird, sind etwa:

- Rechtswidriges Eindringen in Informationssysteme
- Manipulation und Sabotage von Computer und Netzen
- Spionage und Weitergabe bzw. Veröffentlichung von Geheimnissen
- Rechtswidrige Erfassung, Nutzung und Weitergabe von personenbezogenen Daten
- Verstöße gegen das Urheberrecht sowie Rechte zum Schutz geistigen Eigentums

Unter Mißbrauch durch Inhalte, wobei das Internet für die Übertragung schädigender oder rechtswidriger Informationen benutzt wird, fällt beispielsweise die Verbreitung von Kinderpornographie, Volksverhetzung oder Verleumdung. Wir wollen uns auf den Mißbrauch durch Handlungen beschränken, da dieser direkt mit dem Begriff Cracker assoziiert werden kann, wobei wir natürlich keine vollständige juristische Darstellung des Problems geben können. Als kurzer Überblick über die Rechtslage soll nachfolgend aufzeigt werden, daß es sich beim Internet nicht - wie viele glauben möchten - um einen rechtsfreien Raum handelt. Auch wenn es noch keine umfassenden, internationalen Gesetze für das Internet gibt, so gelten doch in jedem Land gewisse Rechtsnormen. So wurde in Deutschland schon am 1. August 1986 das 2. Gesetz zur Wirtschaftskriminalität (WiKG) erlassen, das einen ersten Ansatz darstellte, das strafrechtliche Problem der Computerkriminalität zu erfassen.

Die wichtigsten Paragraphen, die heute bei Computerkriminalität in Deutschland Anwendung finden, sind:

- §202a StGB: Ausspähen von Daten
- §263a StGB: Computerbetrug
- §265a StGB: Erschleichen von Leistungen
- §268 StGB: Fälschung technischer Aufzeichnungen
- §269 StGB: Fälschung beweiserheblicher Daten
- §270 StGB: Täuschung im Rechtsverkehr bei Datenverarbeitung

- §303a StGB: Datenveränderung
- §303b StGB: Computersabotage

Je nach Vergehen können weitere Gesetze wie beispielsweise das Datenschutzgesetz, Urkundenfälschung, Urheberrechtsverletzung oder Unlauterer Wettbewerb Anwendung finden.

Dringt ein Cracker lediglich in ein System ein, so ist dies nach deutschem Recht straffrei. Werden dabei jedoch besonders gesicherte Daten (z.B. Systemdaten) gelesen, kopiert oder gar manipuliert, so wird die Handlung nach §202 StGB bzw. §303a und §303b StGB strafbar und kann mit einer Freiheitsstrafe von 2-5 Jahren oder einer Geldstrafe geahndet werden. Das Einschleusen von Viren in einen Computer beispielsweise kann in der Regel gemäß §303a StGB, §303b StGB und gegebenenfalls gemäß §269 StGB strafrechtlich geahndet werden; Verwendung oder gar Weiterverkauf nicht lizensierter Software ist ein Verstoß gegen §69 UrhG.

Ob das deutsche Strafrecht zur Anwendung kommt, hängt im wesentlichen von der Art des Deliktes ab. Unproblematisch ist es für diejenigen Delikte, die vom internationalen Strafrecht nicht nur nach dem Territorialitätsprinzip, sondern auch nach dem aktiven Personalitätsprinzip, dem Weltrechtsprinzip, dem Prinzip der stellvertretenden Strafpflege oder dem Schutzprinzip erfaßt werden. Bei Computerspionage, -sabotage oder -manipulation kommt im wesentlichen das Territorialitäts- (§3 StGB) und das Ubiquitätsprinzip (§9 StGB) zur Anwendung. Das Territorialitätsprinzip besagt, daß das deutsche Strafrecht für die Taten gilt, „die im Inland begangen" wurden; Das Ubiquitätsprinzip (§9 Abs. 1 StGB) gilt für Taten, die „an jedem Ort begangen, an dem der Täter gehandelt hat oder im Falle des Unterlassens hätte handeln müssen oder an dem der zum Tatbestand gehörende Erfolg eingetreten ist oder nach der Vorstellung des Täters eintreten sollte". Damit unterliegen sowohl Computerdelikte, die von einem Täter von Deutschland aus an ausländischen Rechnern begangen werden, wie auch Delikte, die vom Ausland aus an deutschen Systemen begangen werden, dem deutschen Strafrecht.

Unterliegt ein Delikt dem deutschen Strafrecht und ist die deutsche Strafverfolgungsbehörde für die Verfolgung der Tat zuständig, so kann diese nach den Regeln des Völkerrechts jedoch nur auf deutschem Staatsgebiet tätig werden. Ermittlungen im Ausland würde das Hoheitsrecht des fremden Staates verletzten. Länderübergreifende Ermittlungen sind daher nur durch Kooperation der einzelnen Ermittlungsbehörden möglich, die den einschlägigen Normen über die internationale Amts- und Rechtshilfe unterliegen.

Um der sich stark ausbreitende Computerkriminalität zu entgegnen, wurden daher verschiedene internationale Initiativen zur Verstärkung der Zusammenarbeit und Vereinheitlichung der Gesetzgebung geschaffen. So wurde beispielsweise im Januar 1997 die G8-Arbeitsgruppe „High-Tech-Kriminalität" und eine 24-Stunden-Kontaktgruppe gegründet. Die 24-Stunden-Kontaktgruppe hat das Ziel, innerhalb kürzester Zeit länderübergreifend auf einen Vorfall zu reagieren und zu ermitteln. Das Ziel der Arbeitsgruppe „High-Tech-Kriminalität" ist, die Gesetzgebung in den verschiedenen Bereichen der Computerkriminalität zu harmonisieren. Dabei kann sie keine formalen Abkommen schließen, jedoch durch ihre Studien und Berichte eine beratende Tätigkeit für den EU-Rat ausüben. Dieser arbeitet zur Zeit an einer Konvention für Cyber-Kriminalität, die

eine verbindliche Abmachung unter den EU-Mitgliedstaaten und sogenannten beobachtenden Ländern, USA, Kanada und Japan, sein wird.

4 Informationsquellen

Durch das zunehmende Interesse der Öffentlichkeit kommt immer öfter die Frage auf: „Wie werde ich ein Hacker?". Die Anworten darauf, wie sie beispielsweise in Foren wie den Newsgroups *de.comp.security* oder *de.org.ccc* gegeben werden, verweisen typischerweise darauf, daß selbst bei großem Interesse und Einsatz einige Jahre vergehen, bis man sich „Hacker" nennen kann. Allein um sein eigenes Betriebssystem zu beherrschen, ist bereits ein enormes Hintergrundwissen erforderlich.

Typischerweise dient ein freies, Unix-ähnliches Betriebssystem, wie beispielsweise Linux oder FreeBSD, als Basis für die Streifzüge im Netz. Ist dieses System richtig installiert und konfiguriert, muß noch ein IP-Zugang zum Internet geschaffen werden. Dabei werden reine Internet-Provider mit PPP-Zugang gegenüber Online-Diensten wie T-Online oder AOL bevorzugt, da letztere u.a. die eigentliche Funktionalität hinter graphischen Benutzungsoberfächen verstekken und z.T. sogar modifizierte und damit nicht kompatible Protokolle verwenden. Der fortgeschrittene Hacker weiß, wie neue Kernel für das System erstellt werden und kann so z.B. die sicherheitsrelevante Unterstützung für Firewalls und Paketfilter erreichen. Ein Muß für jeden Hacker sind umfassende Kenntnisse gängiger Programmiersprachen wie C/C++ und Perl. Um sich im Netz bewegen zu können, erweist sich ferner Erfahrung im Umgang mit den grundlegenden Netzwerkanwendungen ftp, telnet, sendmail, etc. als unverzichtbar. Das intensive Studium der entsprechenden RFCs ist dabei besonders hilfreich.

Um sich dieses Wissen und vor allem Erfahrung mit dem Umgang und den Schwachstellen von vernetzten Systemen aneignen zu könne, bieten sich eine Vielzahl von Informationsquellen an, die sich z.T. deutlich im Grad der Aktualität, der Vollständigkeit und des benötigten Vorwissens unterscheiden. Im folgenden werden einige repräsentative Informationsquellen vorgestellt, die auch im Rahmen des Praktikums intensiv zu Rate gezogen worden sind.

4.1 Computer Emergency Response Teams (CERTs)

Eines der Ziele von Organisationen wie den CERTs ist es, Informationen über bekannte Schwachstellen zu sammeln und bereitzustellen. Als Zielgruppe sind dabei im wesentlichen Systemadministratoren zu sehen. Inhaltlich werden daher eher Informationen veröffentlicht, die die Beseitigung von Sicherheitslücken betreffen. In seltenen Fällen wird bekannt gegeben, wie eine Schwachstelle ausgenutzt werden kann bzw. was genau das Problem ist, das zu der Schwachstelle geführt hat. Da ein großer Wert auf die Vollständigkeit der Informationen gelegt wird, sind diese nicht immer aktuell, da es eine gewisse Zeit dauert, bis alle Aspekte einer neuen Schwachstelle sowie deren Beseitigungsmöglichkeit bekannt geworden sind.

Vergleichbar zu den Informationen, die ein CERT anbietet, sind entsprechende Veröffentlichungen auf den WWW-Seiten der Hersteller. Dort werden oftmals die Probleme genannt und eine Problemlösung in Form eines Patches (Unix) oder Hotfixes

(Windows) angeboten. Die Informationen werden jedoch i.a. erst dann bekanntgegeben, wenn auch eine Lösung existiert.

4.2 Hackergruppen

Zahlreiche WWW-Seiten, Newsgroups, Mailinglisten und ähnliche Foren werden von Hackergruppen oder Individuen betrieben. Informationen über Schwachstellen und Skripte zur Durchführung eines Angriffs (Exploit) werden dort ausgetauscht oder einfach nur veröffentlicht. Im Gegensatz zu der CERT-Philosophie werden möglichst viele Details über eine Schwachstelle dargestellt. Mit entsprechender Erfahrung wird der Leser also vermutlich in der Lage sein, die betreffende Schwachstelle auszunutzen. Obwohl derartige Informationsquellen sehr aktuell sind, sind sie unorganisiert, zum Teil unvollständig und manchmal schlichtweg falsch.

4.3 Sicherheitsunternehmen

Beratungsfirmen oder Herstellern von Sicherheitssoftware kann man unterstellen, daß sie sicherheitsrelevante Informationen nicht ganz uneigennützig veröffentlichen. Zum einen wird so der Name der jeweiligen Firma bekannt gemacht, zum anderen wird die Kompetenz des Unternehmens in Sicherheitsfragen demonstriert. Die Information ist oftmals qualitativ schlechter, da Firmen nicht über die Ressourcen eines CERTs oder der Hackergruppen verfügt, die größtenteils auf freiwilliger Mitarbeit der Öffentlichkeit im Netz profitieren.

4.4 Bücher

Im Gegensatz zu den bisherigen Informationsquellen, die alle online zugänglich sind, haben Bücher grundlegend andere Eigenschaften. Wie im 2. Kapitel von „Maximum Security“ geschrieben wird, ist eine der Grenzen eines Buches über den Themenkomplex Sicherheit die Aktualität. Seit dem Erscheinen des Buches sind „Hunderte von Sicherheitslöchern entstanden bzw. wieder behoben worden“. Andererseits vermitteln Bücher ein solides Hintergrundwissen, ohne das es kein Hacker weit bringen wird. Gerade in unserem Praktikum haben sich Werke wie „Building Internet Firewalls“ oder „Computer Networks“ als sehr hilfreich für das Verständnis von Netzinfrastruktur, der Konfiguration und den Schwachstellen einer Firewall erwiesen.

5 Der "Kriegsschauplatz"

Ende-zu-Ende Sicherheit umfasst die Absicherung von Information von der Nachrichtenquelle bis zur Nachrichtensenke. Um dies zu bewerkstelligen, müßte also der gesamte Kommunikationspfad abgesichert werden, was in der Praxis zwar möglich, aber nicht immer realistisch ist. So nützt beispielsweise der sicherste SSL-Tunnel oder eine mit PGP verschlüsselte E-Mail nichts, wenn das Ziel- bzw. das Quellsystem zu schwach konfiguriert ist und ein potentieller Eindringling die Gelegenheit erhält, in Besitz der geheimen Schlüssel zu kommen. Ein Grund für dieses Problem ist sicherlich, daß es heute bereits Lösungen für die zahlreichen Teilprobleme gibt, die eine integrierte Lösung

(noch) nicht zulassen, weil diese entweder zu teuer für den Betreiber oder zu unkomfortabel für den Benutzer eines Systems sind. Wir haben versucht, diese ganzheitliche Sichtweise im Praktikum zu vermitteln und zumindest einige wesentliche Ansatzpunkte für die Umsetzung von Sicherheit (siehe oder) wie beispielsweise System- und Netzsicherheit, sowie organisatorische und operative Maßnahmen zu verinnerlichen. Physikalische Sicherheitsaspekte, wie beispielsweise speziell abgeschirmte Leitungen oder abschließbare Diskettenlaufwerke, sind nur am Rande berücksichtigt worden.

5.1 Die Testumgebung

Um einen kontrollierten Ablauf des Praktikums gewährleisten zu können, sind entsprechende Vorsichtsmaßnahmen getroffen worden. Den insgesamt 20 Teilnehmern standen zwei durch eine Firewall vom Universitätsnetz getrennte Teilnetze zur Verfügung, die zunächst gegeneinander nicht weiter abgesichert worden sind. Eine Verbindung zum Internet war nur über HTTP und ftp erlaubt. Durch diese restriktive Maßnahme war möglich, die Durchführung von Angriffsszenarien und Abwehrmaßnahmen auf die Praktikumsnetze zu beschränken.

Um möglichst realitätsnah zu bleiben, wurden als Betriebssysteme SUN Solaris und diverse Linux-Distributionen eingesetzt. Als professionelles Microsoft-Betriebssystem ist Windows NT 4.0 (Server und Workstation) ausgewählt worden. Die in der Geschäftswelt leider immer noch oft eingesetzten Betriebsysteme Windows 95 bzw. 98 sind nicht näher untersucht worden, da sie aus sicherheittechnischer Sicht kaum eine Herausforderung darstellen. Die Hardwareausstattung reichte von DEC AlphaStations, über SUN LX bzw. IPC bis hin zu „normalen" PCs. Obwohl nicht mehr alle Plattformen (SUN LX) sehr zeitgemäß waren, war das Arbeiten in kleinen Gruppen möglich, da darauf geachtet wurde, daß zumindest ein System pro Gruppe modernen Anforderungen bezüglich Hauptspeicher und Prozessorleistung genügte.

5.2 Sicherheit der Systeme

Ziel der ersten Praktikumsaufgabe war es, die jeweiligen Betriebsysteme von Anfang an schon bei der Installation kennenzulernen. Mit Hilfe vorgegebener Installations- und Konfigurationsrichtlinien, wie z.B. den „Windows NT Security Guidelines", wurden die jeweiligen Systeme so eingerichtet, daß sie als Basis für eine möglichst sichere Informationsverarbeitung dienen konnten. Dabei war zu beachten, daß das System während der Installation hinreichend vor Angriffen zu schützen war. Es ist nämlich ein Trugschluß zu glauben, daß man von vornherein ein sicheres System hat, da es einem Angreifer z.B. gelungen sein könnte, von Anfang an ein trojanisches Pferd zu plazieren.

Nach der Installationsphase wurden von jeder Gruppe diverse repräsentative und verschiedenartige Angriffe auf der Systemebene durchgeführt, wie beispielsweise der lokale Diebstahl und das Knacken von Paßwörtern. Diese Angriffe waren zunächst auf das interne Teilnetz der jeweiligen Gruppe beschränkt und simulierten so einen internen Angreifer. Falls möglich wurden die entsprechenden Gegenmaßnahmen getroffen und dokumentiert.

Selbst in der relativ überschaubaren Testumgebung ist den Teilnehmern des Praktikums schnell klar geworden, daß systembasierte Sicherheit ein komplexes und fehlerträchtiges Problemfeld darstellt. Bereits das Management der Sicherheit eines einzigen Systems ist sehr anspruchsvoll, so daß man annehmen kann, daß beim Management vieler heterogener Systeme Fehler gemacht und einige Sicherheitslücken einfach übersehen werden. Hinzu kommt auch, daß systembasierte Sicherheit oftmals nebenbei und daher nur oberflächlich durchgeführt wird. Ein einziges, schlecht administriertes System wird so möglicherweise das schwache Glied in der Kette sein, das alle anderen Anstrengungen zunichte machen kann. Abhilfe kann hier eigentlich nur eine Automatisierung des Installations- und Konfigurationsmanagements und eine Reduzierung der Systemvielfalt schaffen. Ersteres ist mit kommerziellen Werkzeugen möglich, aber meist sehr teuer. Geeignete freie Hilfsmittel gibt es meistens nur in der Unix-Welt (z.B. cfengine). Microsoft Windows automatisiert abzusichern dürfte nach wie vor eine anspruchsvolle Aufgabe bleiben. Eine weitere Erkenntnis ist, daß eigentlich jede sicherheitsbewußte Institution je nach Größe eine Person oder mehrere Personen für Sicherheitsfragen freistellen müßte, um wenigstens ein minimales Sicherheitsniveau zu etablieren und zu erhalten.

5.3 Netzsicherheit

Ziel der nächsten Aufgabenstellung war es, sich mit der netzwerkseitigen Sicherheit auseinanderzusetzen. Dazu wurde der bisher uneingeschränkte Datenverkehr zwischen den beiden Teilnetzen so eingeschränkt, daß wenige, notwendige Dienste von der jeweils anderen Seite zugänglich blieben. So mußte bespielsweise SSH von jedem zu jedem Rechner möglich sein, wohingegen der Zugang über HTTP und FTP nur auf einen bestimmten Rechner in jedem Teilnetz erlaubt sein sollte. Da als Firewall ein frei verfügbarer Paketfilter eingesetzt wurde, war es jeder Gruppe möglich, zumindest die syntaktische Korrektheit der Konfiguration zu überprüfen. Firewall-Regeln hängen stark vom Sicherheitskonzept (Security Policy) des Netzbetreibers ab, so daß dokumentiert werden mußte, warum welche Regeln aufgestellt worden sind und welche mögliche Gefahrenpotentiale sich daraus immer noch ergeben.

In einem weiteren Schritt sollte nun herausgefunden werden, wieviel Informationen trotz des Einsatzes eines Paketfilters von der „anderen Seite" noch immer zugänglich waren. Dazu wurden verschiedene Techniken verwendet, wie z.B. fragmentierte Pakete, Ausnutzung von Fehlkonfigurationen oder Tunnel. Damit dies überhaupt möglich war, wurde ein repräsentativer Regelsatz für die Konfiguration der Firewall aus dem vorangegangen Arbeitsschritt verwendet, der einige typische Fehler enthalten hat.

In einer abschließenden Betrachtung des Themas Netzsicherheit wurde herausgearbeitet, mit welchen Maßnahmen ein noch besserer Schutz erreicht werden kann, wie etwa durch den Einsatz von Proxies oder mehrstufigen Firewall-Architekturen. Außerdem wurde vermittelt, wann das Konzept einer Firewall keinen Schutz bieten kann, wie z.B. bei Angriffen von Innentätern oder bei unbekannten „Lecks" durch Modemverbindungen in das Internet.

5.4 Kontrolle und Überwachung

Nach der eher einführenden Natur der Aufgabenstellungen in der ersten Hälfte des Praktikums, lag der Schwerpunkt der nächsten Aufgaben auf der Vertiefung in ausgewählten Bereichen der operativen Maßnahmen. Dazu zählen Verfahren zur Entdeckung von Angriffsversuchen (Intrusion Detection) und Maßnahmen zur Verfolgung von bereits erfolgreich eingedrungenen Angreifern (Tracking). Für jedes dieser Themengebiete wurde jeweils eine größere Teilnehmergruppe gebildet. Eine dritte Gruppe widmete sich fortgeschrittenen Angriffstechniken, damit die Ergebnisse der anderen Gruppen auf Eignung und Anwendbarkeit überprüft werden konnten.

Die meisten Einbrüche in Rechnersysteme bleiben unentdeckt, da Systemmeldungen (Logs) deaktiviert sind oder nicht konsequent überwacht werden. Die meisten Betriebssysteme bieten allerdings die Möglichkeit an, Logs einzuschalten und in Dateien oder Datenbanken zu speichern. Für die lokale oder zentrale Auswertung dieser Meldungen bieten die Betriebssystemhersteller i.a. jedoch wenig Hilfsmittel an. Das Ziel dieser Aufgabe war es, auf Basis zusätzlicher Software systemübergeifend Meldungen zu sammeln und auszuwerten. Eine Auswertung in Realzeit ermöglichte so eine Alarmierung, die man durchaus als einfaches Intrusion Detection System bezeichnen kann. Das so aufgebaute System sollte den Gruppen bei der Aufdeckung unbekannter Systemzustände helfen und eine Analyse des Vorgangs ermöglichen.

Da anzunehmen ist, daß Einbrecher versuchen werden, ihre Spuren in lokalen Log-Dateien zu verwischen, müssen entsprechende Gegenmaßnahmen getroffen werden. Hierzu bietet sich beispielsweise das Schreiben auf einen gut abgesicherten zentralen Server oder ein Gerät an, das nur schreibbar ist.

Im Falle von Einbrüchen in Rechnersysteme sind Systemadministratoren schnell überfordert, wenn es darum geht, die Aktivitäten eines potentiellen Einbrechers zu überwachen, um so herauszufinden, was vorgefallen ist. Im Falle eines Einbruches, bei dem vermutet wird, daß der Angreifer noch im System aktiv ist oder Hintertüren hinterlassen hat, ist es notwendig, im laufenden Betrieb alle Vorgänge so zu überwachen, daß sämtliche Aktivitäten beobachtet und protokolliert werden. Selbst beim Einsatz von sogenannten Rootkits, die es erlauben, sich vor normalen Systemwerkzeugen zur Überwachung zu tarnen, soll es im Idealfall möglich sein, die Spuren eines Eindringlings zu verfolgen und auszuwerten. Dies ist u.a. für Beweissicherungsverfahren notwendig, aber auch zum Auffinden und Verschließen von Hintertüren. In diesem Sinne erschien es naheliegend, die Mechanismen eines Intrusion Detection Systems auf das Tracking eines Eindringlings zu erweitern. Es gibt verschiedene Mechanismen der forensischen Analyse, um anhand von Logdateien, Dateizugriffszeiten, Prozeßinformationen etc. die Aktivitäten eines unrechtmäßigen Benutzers nachzustellen. Um richtig reagieren zu können, ist es notwendig, die notwendigen Hilfsmittel greifbar zu haben und zu wissen, wie man sie einsetzt. Eine weitere Tailaufgabe bestand darin zu erörtern, ob und wo es überhaupt sinnvoll ist, eine Angreifer zu verfolgen. Möglicherweise bewahrt die Abtrennung des betroffenen Systems bzw. des gesamten Netzes einer Organisation vor größeren Schäden. Andererseits kann ein übervorsichtiges Verhalten zu häufigen Ausfallzeiten führen, die nicht immer akzeptabel sind.

6 Ausgewählte Ergebnisse

Die oben beschriebenen Aufgaben führten zu umfangreichen Ergebnissen. In diesem Abschnitt wollen wir am Beispiel der Paßwortsicherheit von Windows NT zeigen, wie diese aussehen können.

Es gibt heute bereits sehr sichere Verfahren für Identifikation und Authentifizierung in Systemen, wie etwa die Verwendung von Chipkarten oder biometrischen Verfahren. Dennoch wird oftmals aus Kosten- oder Organisationsgründen immer noch die Kombination aus Benutzernamen und Paßwort weitverbreitet eingesetzt, obwohl die Unzulänglichkeiten schon lange öffentlich bekannt sind. Aus diesem Grund wurde während des Praktikums auf Basis der Anwendung der professionellen Software *L0phtcrack* zum Knacken von Windows NT-Paßwörtern die Problematik von sicheren Paßwörtern allgemein untersucht und einige spezifische Schwächen von Windows NT herausgearbeitet.

Sowohl auf Unix- als auch auf Windows NT-Systemen werden Paßwörter gemeinsam mit dem Benutzernamen im System abgespeichert, wobei die Paßwörter mit einer bekannten Einweg-Verschlüsselungsfunktion verschlüsselt werden (Hash-Verfahren bei Windows NT, modifizierte DES-Version bei Unix). Aus dem verschlüsselten Paßwort läßt sich also auch mit Kenntnis des genauen Verschlüsselungsverfahrens das Paßwort nicht direkt wiedergewinnen. Ist das verschlüsselte Paßwort jedoch bekannt, so ist es aber dennoch möglich, das Paßwort durch systematisches Ausprobieren zu knacken. Die erste Hürde, die ein Angreifer nehmen muß, ist es, Zugang zu den entsprechenden Systemdateien zu erhalten. Bei Windows NT gibt es dazu prinzipiell mehrere Möglichkeiten, von denen die bekanntesten im folgenden vorgestellt werden.

Bei dem Microsoft-Betriebssystem sind die Hash-Werte der Paßwörter in der SAM-Datei (Security Accounts Manager) gespeichert. Das System hält diese Datei stets unter exklusivem Zugriff, so daß sie nicht direkt ausgelesen werden kann. Ein Angreifer kann diesen Schutz jedoch umgehen, indem er die SAM-Datei beispielsweise mit Hilfe einer Boot-Diskette und einem Werkzeug, das auf das NT-Dateisystem zugreifen kann, wie z.B. NTFSDOS, kopiert. Der Zugriff auf die SAM-Datei ist auch möglich, wenn auf einem Rechner mehrere Betriebssysteme installiert sind. Eine leichtere Variante ergibt sich durch fehlerhafte Schutzrechte des Verzeichnisses, in das Windows NT beim Anlegen einer Rettungsdiskette die aktuelle Version der SAM-Datei kopiert. Falls hier die Standardeinstellungen nicht geändert worden sind, kann dieses Verzeichnis von einem normalen Benutzer gelesen werden. Selbstverständlich gewinnt ein Angreifer durch Diebstahl der Notfalldiskette ebenfalls die gewünschten Paßwort-Informationen.

Die bisherigen Angriffe erfordern mehr oder weniger physikalischen Zugang zum Zielsystem. Eine andere Möglichkeit, an die Hash-Werte zu kommen, ist es, die NT-Netzkommunikation zu belauschen. Zu Autorisierungszwecken bei der Benutzeranmeldung wird ein Challenge/Response-Verfahren mit dem Domainserver durchgeführt, aus dem sich die Hash-Werte ableiten lassen. Für diesen Zweck stellt L0phtcrack einen spezialisierten Paket-Sniffer bereit, der in kürzester Zeit erstaunliche Ergebnisse liefert.

Das eigentliche Einsatzgebiet von L0phtcrack ist das Paßwort-Auditing durch den Systemadministrator, für den es noch eine weitere, viel einfachere Möglichkeit gibt, an die Hash-Werte zu kommen, nämlich durch den Aufruf privilegierter Registry-Funktionen. L0phtcrack bietet hierzu eine Funktion namens "Dump from Registry", die auch entfernt auf anderen Rechnern aufgerufen kann, sofern dort eine Abfrage der Registry über

das Netzwerks nicht deaktiviert worden ist. Falls ein Angreifer also Administrationsrechte auf einem Rechner hat, kann er möglicherweise wertvolle Paßwörter von einem schlecht konfigurierten Server stehlen.

Mit der bekannten Verschlüsselungsfunktion verschlüsselt L0phtcrack verschiedene Wörter und vergleicht diese mit den Systempaßwörtern. Fällt dieser Vergleich positiv aus, so ist das Paßwort geknackt. Im schlimmsten Fall muß der Angreifer alle möglichen Kombinationen ausprobieren, um erfolgreich zu sein. Besteht ein Paßwort aus acht Zeichen aus einem rein alphanumerischen Zeichensatz, so benötigt L0phtcrack für einen derartigen Brute-Force Angriff auf einem High-End-PC nicht einmal einen Tag. Mit zunehmender Rechenleistung oder dem Partionieren des Paßwortraums auf mehrere Systeme kann dieser Aufwand nochmals drastisch reduziert werden.

Viel schneller zum Erfolg kommt man mit einem ebenfalls unterstützten Dictionary-Angriff, dem die Annahme zugrunde liegt, daß Benutzer Paßwörter verwenden, die sich in einem Wörterbuch finden lassen. Im Internet findet man leicht thematisch sortierte Wörterbücher, die mit L0phtcrack verwendet werden können. So gibt es beispielsweise Wörterbücher, die ausschließlich aus Namen, religiösen Begriffen oder Markennamen bestehen. Vermeintlich bessere Paßwörter, die durch Anhängen zusätzlicher Zeichen, wie etwa Jahreszahlen o.ä., gebildet werden, werden durch den Hybrid-Modus enttarnt, der genau dieses Verhalten nachahmt.

Verschiedene Umstände begünstigen den bisher beschriebenen Einsatz von L0phtcrack. Zunächst verwendet Windows NT bei allen Anmeldevorgängen über das Netz zusätzlich zu seinem eigenen Authentifzierungsprotokoll aus Kompatibilitätsgründen das ältere LanManager-Protokoll. Mit Hilfe der bereits erwähnten Gewinnung der Hash- Werte durch den integrierten Paket-Sniffer ist dieses sehr leicht angreifbar. So ist es eigentlich überflüssig, sich mit dem komplexeren NT-Hash auseinanderzusetzen. Desweiteren können die Benutzerkennwörter zwar 14 Zeichen lang sein, aber die beiden Hälften aus je 7 Zeichen werden einzeln und unabhängig voneinander verschlüsselt, so daß der Aufwand zum Knacken erheblich reduziert wird. Aus dem Hash-Wert ist außerdem sofort ersichtlich, ob das Paßwort kürzer als 8 Zeichen lang ist, da die zweite Hälfte in diesem Fall stets aus einem bekannten Nullwert besteht.

Eine spürbare Verbesserung der Paßwort-Qualität ist eigentlich nur durch regelmäßige Paßwort-Audits und durch entsprechende Schulung der Benutzer und Administratoren zu erreichen. Als Beispiel dafür wollen wir zwei einfache Merkstrategien für „gute" Paßwörter vorstellen, die Teil einer umfassenden Richtlinie über den Umgang mit Paßwörtern sein können.

Bei der Akronym-Methode wählt der Benutzer einen Satz oder mehrere Sätze und verwendet dann als Paßwort die Anfangsbuchstaben der einzelnen Wörter, wobei Vokale beispielsweise durch Ziffern oder Sonderzeichen ersetzt werden können. Aus dem Satz „Mein Auto hat vier Räder und fünf Türen!" wird so das Paßwort „M@h4Ru5T!". Bei der Collage-Methode wird ein Wort aus einer natürlichen Sprache ausgewählt und in eine andere natürliche Sprache übersetzt. Danach werden beiden Wörtern drei aufeinanderfolgende Buchstaben z.B. vom Wortanfang entnommen und mit zwei Ziffern oder Sonderzeichen, die sich gut merken lassen, verbunden. Aufbauend auf dem Wort "Gewicht"könnte sich so z.B. das Paßwort „Gew79WEI" ergeben („Gewicht", „WEIGHT", Sie wiegen 79 Kilo).

7 Schlußfolgerungen

Das häufigste Gegenargument, das während der Planungsphase des „Hacker-Praktikums" angeführt worden war, lautet, daß von einer Universität „Cracker" ausgebildet werden und diese Studenten eventuell Gefallen an dieser Art der Computernutzung finden könnten. Sicherlich lernen Studenten durch diese Form der Ausbildung, wie „Hacken" bzw. „Cracken" funktioniert. Unserer Ansicht nach ist dies aber zwingend notwendig, um sich in der Praxis effektiv gegen Angreifer verteidigen zu können. Wir denken weiterhin, daß durch das Aufzeigen der rechtlichen Konsequenzen, sowie die Erkenntnis, daß ein Angriff auch nachweisbare Spuren hinterläßt, auf ein verantwortungsvolles Umgehen mit dem erworbenen Wissen hingearbeitet worden ist.

Ein weiterer problematischer Punkt ist der Zeitaufwand, den ein solches Praktikum mit sich bringt. Die Studenten hatten die Aufgabe, ihre Rechner selbst zu installieren, zu konfigurieren und dann ein Netzwerk aufzubauen. Da von Studenten nicht erwartet werden kann, daß sie mehrere verschiedene Betriebssysteme gut beherrschen, ist ein hoher Einarbeitungs- und Betreuungsaufwand nötig. Die nach dem Aufbau des Netzes nötige Recherche und vor allem die Durchführung der Angriffe hat sich ebenfalls als äußerst zeitaufwendig erwiesen. Es hat sich aber gezeigt, daß die Studenten aufgrund der interessanten Thematik bereit waren, sehr viel mehr Zeit aufzuwenden, als dies für andere Praktika notwendig ist.

Im Verlauf des Praktikums sind weit über einhundert Seiten Dokumentation entstanden, die einen guten Überblick über die aktuellen Möglichkeiten der Hacker geben. Diese Berichte beleuchten diverse Schwachstellen der unterschiedlichen Betriebssysteme, Netzkomponenten und Dienste und stellen somit ein umfassendes und aktuelles Nachschlagewerk dar. Da diese letzte Aussage sicherlich nicht lange Gültigkeit besitzt, ist es beabsichtigt, im nächsten Sommersemester wiederum ein solches Hacker-Praktikum an der Technischen Universität Darmstadt zu veranstalten und so weiter zur praxisnahen Ausbildung von IT-Sicherheitsexperten beizutragen.

Literatur

1. Anonymous. *Maximum Security.* Sams Publishing, 1998.
2. CERT. Cert Advisories. http://www.cert.org/nav/alerts.html, 2000.
3. D. B. Chapman and E. D. Zwicky. *Building Internet Firewalls.* O'Reilly & Associates, 1995.
4. Chaos Computer Club. Die Hackerethik. http://www.ccc.de/Hackerethik.html, 2000.
5. Fyodor. Fyodor's Exploit World. http://www.insecure.org/sploits.html, 2000.
6. L0pht Heavy Industries. L0phtcrack version 2.5.1. http://www.l0pht.com, 1999.
7. S. Levy. *Hackers: Heroes of the Computer Revolution.* Anchor Press/Doubleday, NY, 1994.
8. Rootshell. Rootshell Webseite. http://www.rootshell.org, 2000.
9. Trusted Systems Services. Windows NT Security Guidelines. http://www.trustedsystems.com/NSAGuide.htm, 1998.
10. C. Stoll. *Das Kuckucksei.* Fischer Verlag, 1989.
11. A. S. Tanenbaum. *Computer Networks 3rd Edition.* Prentice Hall, 1996.
12. D. R. Tzeck. Wie-werde-ich-Hacker - HOWTO. http://koeln.ccc.de/texte/hacker-werden.html, 1999.