



Institut für Telematik unter Betreuung der
Fraunhofer-Gesellschaft



 **Preprint 2002 – 10**

**Sicherheitsrisiken
und Schwachstellenanalyse
von IT-Systemen**

Michael Schmitt
Christoph Meinel

ISSN 1433-8106



Author	Dipl.-Inform. Michael Schmitt Univ.-Prof. Dr. sc. Christoph Meinel
Copyright	© 2002 Institut für Telematik e.V., Trier
Trademarks	All terms that are mentioned in this paper that are known to be trademarks or service marks have been appropriately capitalised. Use of a term in this paper should not be regarded as affecting the validity of any trademark and service mark. The product or brand names are trademarks of their respective owners.
Printing	12/2002
Document status	Version 1.0 (12.2002)
	Printed in Germany
	All rights reserved
	The documentation was accomplished through the Institut für Telematik.
	The information contained in this document represents the current view of the authors on the issues discussed as of the date of publication. Because the present methodology must respond to changing research conditions, the results of this paper should not be interpreted to be a commitment on the part of the authors. Any information presented after the date of publication are subject to change.
	The right to copy this documentation is limited by copyright law. Making unauthorised copies, adaptations or compilation works without permission of the authors or institutions mentioned above is prohibited and constitutes a punishable violation of the law.



Inhaltsverzeichnis

- 1. IT-SICHERHEITSRISIKEN 4**
- 2. SECURITY-AUDITS..... 6**
 - 2.1. PENETRATIONSTESTS..... 6
 - 2.2. ANWENDUNGSSPEZIFISCHE TESTS UND WHITE-BOX-TESTS 8
 - 2.3. RECHTLICHE ASPEKTE 9
- 3. PENETRATIONSTESTS MIT HILFE VON SECURITY-SCANNERN 10**
 - 3.1. ATTACKEN GEGEN WEB-SERVER 10
 - 3.2. DENIAL-OF-SERVICE-ATTACKEN 11
 - 3.3. CRACKEN VON PASSWÖRTERN 11
 - 3.4. BACKDOORS 12
 - 3.5. NICHT BENÖTIGTE UND VERALTETE DIENSTE..... 12
 - 3.6. ATTACKEN GEGEN FIREWALLS UND ROUTER 13
- 4. SICHERHEITSTOOLS..... 14**
- 5. REFERENZEN..... 17**

1. IT-Sicherheitsrisiken

Moderne IT-Systeme sind komplexe Gebilde, die über eine Vielzahl von Funktionen und Einstellungsmöglichkeiten verfügen. Diese Komplexität führt mittlerweile zu schwerwiegenden Sicherheitsproblemen.

Die häufigsten Schwachstellen, die den sicheren Betrieb eines Unternehmensnetzes gefährden, sind in Abbildung 1 aufgeführt. Neben Fehlern in verwendeten Software-Komponenten werden Sicherheitsprobleme auch durch fehlerhafte Konfiguration, Administration und Bedienung der IT-Systeme hervorgerufen.

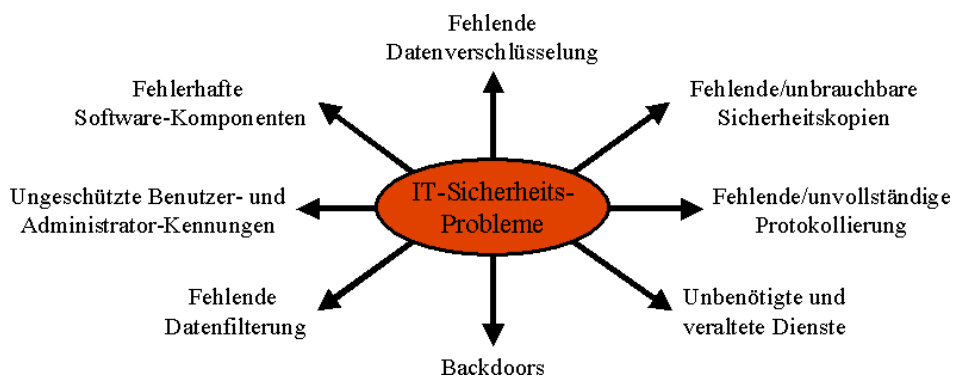


Abbildung 1: IT-Sicherheitsprobleme

Die Zahl der öffentlich bekannten Sicherheitslücken in Standard-Software-Komponenten hat in den letzten Jahren ein beängstigendes Wachstum erfahren. Allein die Firma Microsoft hat ihre Kunden von Januar bis Dezember 2002 über ihr Security-Bulletin [1] in 72 Mitteilungen über mögliche Sicherheitslücken und entsprechende Patches informieren müssen. Was früher ein einfacher Softwarefehler mit lokalen Auswirkungen war, kann heute durch den Mehrbenutzerbetrieb und die Vernetzung von Computersystemen, insbesondere durch das Internet, zu einem schwerwiegenden Sicherheitsproblem für die gesamte Infrastruktur werden.

Die ständigen Nachbesserungen der Hersteller zeigen dabei überdeutlich, wie anfällig heutige IT-Systeme trotz aller Bemühungen gegenüber gezielten Attacken sind. Auch Vorsichtsmaßnahmen von Seiten eines Unternehmens, z.B. in Form einer Firewall, können niemals einen 100%-igen Schutz gegen Hacker gewährleisten.

Hacker-Angriffe auf das unternehmenseigene Netz stellen unkalkulierbare Risiken dar: Bei einem erfolgreichen Einbruch droht einerseits der Ausfall der IT-Systeme und andererseits Verlust, Manipulation und Diebstahl sensibler Firmen- und Kundendaten. Neben den daraus resultierenden finanziellen Verlusten führt ein publik gemachter Einbruch zu einem enormen Image-Verlust. Dies trifft in besonderem Maße auf Branchen zu, bei denen die Firmen ein besonderes Vertrauensverhältnis zu ihren Kunden aufbauen müssen, wie etwa bei Banken und Versicherungen.

Dass die Gefahr von IT-Einbrüchen mehr als nur eine theoretische Größe ist, belegt das amerikanische Computer Security Institute [2]. Zusammen mit dem FBI führt es jährliche



Umfragen durch, um die Sicherheitsproblematik in Unternehmen, Verwaltungen, Finanzinstitutionen, medizinischen Einrichtungen und Universitäten der Vereinigten Staaten zu untersuchen. Die aktuelle Studie von April 2002 [3] zeigt, dass rund 90 Prozent aller Befragten (primär große Unternehmen und Verwaltungen) in den letzten 12 Monaten Ziel eines Angriffs wurden. 80 Prozent der Befragten haben infolge der Attacken finanzielle Einbußen hinnehmen müssen.

Gefahren drohen prinzipiell von verschiedenen Seiten: Professionelle Hacker können gezielte Angriffe gegen einzelne Unternehmen durchführen, um einen wirtschaftlichen Vorteil für sich oder Dritte zu erlangen. Neuerdings wird in diesem Zusammenhang auch über Aktivitäten staatlicher Einrichtungen diskutiert, die das Internet für militärische Zwecke (Stichwort *CyberWar* [4]) oder für Wirtschaftsspionage nutzen. Dagegen attackieren sogenannte Script-Kiddies mit Hilfe frei verfügbarer Hacker-Tools aus einem Spiel- und Zerstörungstrieb zumeist wahllos Rechner im Internet.

Es drohen aber auch Gefahren aus dem eigenen Netz: Momentane bzw. frühere Mitarbeiter können aus persönlichen oder finanziellen Motiven (z.B. Rache gegenüber Kollegen/Vorgesetzten oder Spielschulden) versuchen, Schäden anzurichten und nicht-autorisierte Daten auszuspähen. Eine weitere Gefahr stellen schließlich Viren, Würmer und trojanische Pferde dar. Ihr Ursprung ist oft nur schwer zu ermitteln.

2. Security-Audits

Um ihre IT-Infrastrukturen ausreichend zu schützen, sollten Unternehmen in regelmäßigen Abständen sogenannte Security-Audits durchführen. Idealerweise sollten diese Überprüfungen durch externe und unabhängige Gutachter erfolgen, die unvoreingenommen an die IT-Systeme herangehen.

Sicherheitsexperten werden häufig auch als *White Hat Hackers* (in Abgrenzung zu den *Black Hat Hackers*) oder auch als *Tiger-Team* bezeichnet. Letzterer Begriff stammt ursprünglich aus dem Militärischen und bezeichnet eine Gruppe von Profis, die im Kundenauftrag versuchen, in sicherheitskritische Anlagen (physikalisch) einzubrechen.

Zu den Aufgaben eines Tiger-Teams zählen:

- Manuelle und automatisierte Penetrationstests
- Bewertung von Firewall-Konfigurationen und Überprüfung ihrer Wirksamkeit
- Analyse des Quellcodes von sicherheitskritischen Anwendungen
- Evaluation von IT-Sicherheitsleitlinien und Notfall-Plänen
- Integration und Konfiguration von Intrusion-Detection-Systemen
- Analyse von Authentifizierungsverfahren und Webservices
- Analyse des Netzwerk-Verkehrs, z.B. hinsichtlich unverschlüsselt übertragener Passwörter

2.1. Penetrationstests

Bei den sogenannten Penetrationstests wird das zu untersuchende System als eine Art Black-Box betrachtet, über deren Interna keine anderen als die von außen zugänglichen Informationen bekannt sind (vgl. Abbildung 2). Sie grenzen sich somit von den White-Box-Tests ab, bei denen detailliertes Wissen über die eingesetzten Techniken und Softwareprodukte, den Quellcode von Programmen und Skripten, oder die Organisationsprozesse zur Verfügung steht.

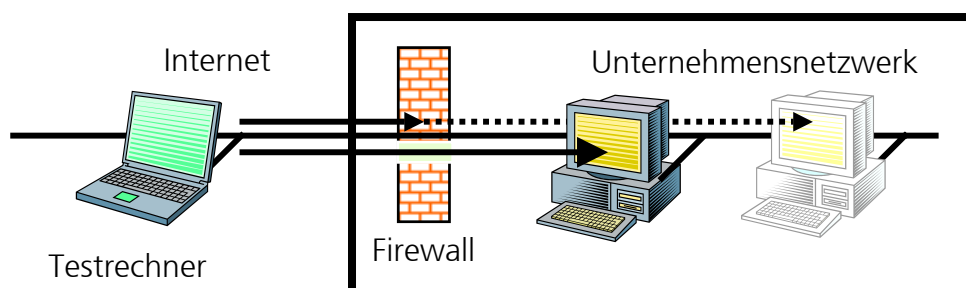


Abbildung 2: Black-Box-Test aus dem Internet

Penetrationstests können entweder vom Internet aus oder aus dem eigenen Unternehmensnetz heraus (u. U. aus einem zweitem Subnetz) initiiert werden. Dabei setzen

Sicherheitsexperten dieselben Techniken und Werkzeuge ein, die auch Hacker für ihre Einbruchsversuche benutzen. Somit lässt sich ein realistisches Bild über das vorhandene Gefahrenpotential zeichnen.

Jeder Penetrationstest beginnt analog zu einem Hacker-Angriff zunächst mit dem Sammeln von Informationen über das zu kompromittierende System. Hierzu zählen die Adressen und Namen von Rechnern ebenso wie die Versionsnummern der sichtbaren Server-Applikationen oder die Namen von Benutzern. Letztere sind hilfreich beim Erraten von Passwörtern.

Um eine Liste der verfügbaren Dienste zu erhalten, werden zunächst sogenannte *Port-Scans* durchgeführt, mit denen man die offenen TCP- bzw. UDP-Ports auf den verschiedenen Rechnern ermittelt. Verschiedene Scan-Verfahren stehen zur Verfügung, um unter Umständen auch an Informationen über Rechner zu gelangen, die durch eine Firewall vor Zugriffen von außen geschützt sind.

Für eine reibungslose Kommunikation im Internet ist per Konvention festgelegt, über welchen Port ein bestimmter Dienst angesprochen werden kann. Ein Web-Server befindet sich typischerweise auf dem Port mit der Nummer 80. Diese Regelung ist jedoch nicht bindend; durch Auswertung des beim Aufruf des Servers ausgegebenen Begrüßungstexts wird daher in einem nachfolgenden Schritt bestimmt, welcher Dienst bzw. welche Anwendung sich tatsächlich hinter einem bestimmten Port verbirgt.

Nachdem alle verfügbaren Informationen ermittelt sind, werden die spezifischen Eigenheiten und Schwächen der Anwendungen überprüft. Viele Penetrationstests können dabei mit Hilfe von Security-Scannern automatisiert durchgeführt werden (siehe nächstes Kapitel).

Ein wahrer Hacker würde nun versuchen, sich mittels speziell präparierter Anfragen an den Rechner unrechtmäßig Zugang zu verschaffen. Häufig ist seine Motivation aber auch, durch eine gezielte Denial-of-Service-Attacke (DoS-Attacke) den Rechner zu überlasten oder gar abstürzen zu lassen, so dass z.B. keine anderen Kunden mehr bedient werden können. Im Gegensatz dazu belässt es ein Sicherheitsteam nach Möglichkeit dabei, eine Schwachstelle zu identifizieren, ohne unnötigen Schäden zu verursachen.

Neben einem simulierten Angriff aus dem Internet ist es sinnvoll, die IT-Infrastruktur des Unternehmens von innen zu inspizieren. Dazu werden die Testrechner der Sicherheitsexperten in das bestehende Firmen-Netzwerk eingeklinkt. So lassen sich auch diejenigen Teile des Netzwerks analysieren, die unter normalen Umständen durch die Firewall nicht sichtbar sind. Dieser zweite Testdurchlauf hat durchaus seinen Sinn - schließlich gehen je nach Informationsquelle ca. 50 bis 80 Prozent aller Einbrüche vom eigenen Firmennetz aus. E-Mails, Gehaltstabellen und ähnlich brisante Dokumente sind daher vor allzu neugierigen Blicken zu schützen. Da prinzipiell jeder Mitarbeiter den Datenstrom jedes anderen Mitarbeiters mitlauschen kann, wird überprüft, ob kritische Informationen wie Passwörter in unverschlüsselter Form über die Leitung gehen. Zusätzlich wird eine Analyse der Benutzer-Passwörter durchgeführt.

Die Ergebnisse einer Sicherheitsanalyse werden in einem Testbericht zusammengefasst, der sowohl die entdeckten Sicherheitsprobleme als auch empfohlene Problemlösungen

enthält. Anhand eines solchen Reports sollte ein Unternehmen in der Lage sein, seine IT-Landschaft in Sachen Sicherheit zügig auf den Stand der Technik zu bringen. Eine häufige Ursache für Sicherheitslücken sind nicht eingespielte Fehlerkorrekturen (Patches) bzw. veraltete Programme. Hier hilft letztlich nur ein Update auf die neueste Version.

Ein wichtiger Aspekt beim Einsatz von Sicherheitsscannern ist deren Aktualität. Nur die neueste Generation der Testtools mit tagesaktuellen Updates garantiert eine umfassende und aussagekräftige Analyse.

Da Sicherheitsbetrachtungen immer von den aktuellen Erkenntnissen und der sich beständig verändernden IT-Infrastruktur abhängig sind, sind ebenso regelmäßige Wiederholungen der Sicherheitstests, z.B. quartalsweise, unerlässlich. Ein Unternehmen ist daher gut beraten, langfristige Vereinbarungen mit einem Sicherheitsanbieter zu treffen.

2.2. Anwendungsspezifische Tests und White-Box-Tests

Allgemeine Sicherheitsscans stellen einen ersten Schritt zur Sicherheitsbewertung dar. Für eine umfassende Analyse sind jedoch tiefergehende Maßnahmen erforderlich, die jeweils speziell auf die IT-Infrastruktur und die Sicherheitsanforderungen des Unternehmens zugeschnitten sind. Dies trifft insbesondere dann zu, wenn neben Standard-Softwareprodukten Eigenentwicklungen oder Produkte von kleineren Anbietern zum Einsatz kommen. Die Bandbreite kann dann von kundenspezifischen, d.h. manuell erstellten Testfällen, bis hin zur Analyse des Quelltextes von besonders sicherheitskritischen Programmteilen reichen.

Werden etwa Inhalte für einen geschützten Kundenkreis im Internet zur Verfügung gestellt oder ein Online-Shop betrieben, dann sollten die Verfahren zur Authentisierung der Benutzer einer detaillierten Analyse unterzogen werden. Bei einem solchen Online-System gibt der Kunde in der Regel zunächst seinen Benutzernamen samt Passwort ein und kann danach beliebig auf der Web-Site surfen. Damit der Kunde sich nicht bei jeder Web-Seite neu anmelden muss, schickt der Web-Server dem Kunden nach der Anmeldung unbemerkt einen sog. Cookie (dt.: Keks), den der Web-Browser des Kunden – ebenfalls unbemerkt – bei jeder weiteren Anfrage als "Eintrittskarte" vorzeigt. Eine wesentliche Fragestellung ist in diesem Szenario, ob die Möglichkeit besteht, ein Cookie zu fälschen oder das Cookie eines beliebigen anderen Benutzers systematisch zu ermitteln.

Auch der gesamte Aufbau der IT-Landschaft sollte auf den Prüfstand gestellt werden. So ist der Einsatz von Firewalls heute unverzichtbarer Bestandteil jeder Sicherheitsstrategie geworden. Auch eine Aufteilung des Netzes in einen Bereich mit öffentlich zugänglichen Rechnern, eine sogenannte *demilitarisierte Zone (DMZ)*, und ein internes Netz ist ein Muss. Wenn jedoch PCs über eingebaute Modems oder ISDN-Karten verfügen, über die sich Mitarbeiter von zu Hause einwählen, ist die Wirksamkeit der zentralen Firewall ausgehebelt. Eine brachiale Methode zur Erkennung solcher Seiteneingänge ist das sogenannte War-Dialing, bei dem – bevorzugt nachts – sukzessive alle Telefonnummern angewählt werden und auf ein Lebenszeichen eines Rechners am anderen Ende der Leitung gewartet wird.

2.3. Rechtliche Aspekte

Ein wichtiger Aspekt bei der Sicherheitsanalyse ist die Frage der Rechtssicherheit. Sicherheitsscans ohne vorherige Einverständniserklärung des Auftraggebers sind per se strafbar. Aber auch wenn der Auftraggeber einwilligt, ist damit noch keine Rechtssicherheit gegeben. So müssen bei Attacken über das Internet zusätzlich die Internet Service Provider (ISPs) beider Parteien informiert werden. Andernfalls droht eine Vertragsverletzung und die sofortige Sperrung des Internetzugangs. Befindet sich der zu testende Rechner zudem im Rechnerverbund eines externen Betreibers (Server Hosting) oder stellt er gar Dienste für mehrere Firmen bereit, ist das Einverständnis aller Beteiligten einzuholen. Verfügt der ISP über ein sogenanntes Intrusion Detection System (IDS) zur Erkennung von potentiellen Angriffen, kann es sonst sein, dass ein Bereitschaftsdienst aktiv wird, der dem Kunden in Rechnung gestellt wird.

3. Penetrationstests mit Hilfe von Security-Scannern

Heutige Security-Tools sind in der Lage, eine große Bandbreite von technischen Sicherheitsmängeln automatisiert aufzudecken. Dieses Kapitel gibt einen kurzen Überblick über die wichtigsten Gefahrenbereiche, die mit Hilfe von modernen Sicherheitstools und -techniken überprüft werden können und führt exemplarisch einige bekannte Fehler in konkreten Software- und Hardware-Produkten auf.

Eine Hersteller- und Tool-unabhängige Liste *aller* öffentlich bekannten IT-Sicherheitschwachstellen mit standardisierten Bezeichnungen wird im Rahmen des Projekts *Common Vulnerabilities and Exposures (CVE)* [5] unter Leitung der Firma MITRE erstellt. Das CVE-Verzeichnis ist frei zugänglich und erlaubt es, den Funktionsumfang verschiedener Security-Scanner besser miteinander zu vergleichen.

3.1. Attacken gegen Web-Server

In den vergangenen Jahren sind die WWW-Technologien mehr und mehr die treibende Kraft im Internet geworden. Die heutigen Web-Server sind zu umfangreichen Applikations-Servern mutiert, die ein breites Spektrum von Aufgaben erfüllen müssen. Aufgrund ihrer zentralen Rolle für die Internetpräsenz und der großen Zahl bekannter Sicherheitslöcher sind sie ein bevorzugtes Angriffsziel für Hacker. Nicht eingespielte Hotfixes sowie eine fehlerhafte Konfiguration können daher den sicheren Betrieb von Web-Servern gefährden.

Typische Probleme von Web-Servern sind:

- Kompromittierung des Systems durch Ausnutzung von Buffer Overflows in Server-Komponenten.
- Zugriffsrechte auf Web-Verzeichnisse und -Dateien, etwa auf Administrationsverzeichnisse (z.B. */iisadmin*), Passwortdateien oder Skript-Verzeichnisse (*/cgi-bin* und */scripts*).
- Auslesen des Quellcodes von Active Server Pages, um an hartcodierte Passwörter zu gelangen.

Buffer-Overflows sind ein allgemeines Softwareproblem, das Webserver mit vielen anderen populären Anwendungen, z.B. OpenSSH, BIND oder RPC, gemein haben. Um einen Buffer-Overflow zu provozieren, schickt ein Angreifer ein speziell präpariertes Datenpaket, bei dem die maximal zulässige Länge eines Datenfelds überschritten ist. Prüft der Server die Länge der Eingabe nicht, kann dies unter Umständen zum unzulässigen Überschreiben von Speicherbereichen auf dem Stack führen, mit der Folge, dass beliebiger Code unter der Kennung des Webserver ausgeführt wird.

Darüber hinaus haben sich viele sogenannte CGI-Skripte (Common Gateway Interface), die serverseitig ausgeführt und teilweise bereits zusammen mit dem Web-Server installiert werden, in der Vergangenheit als anfällig erwiesen:

- Ausspionieren von Benutzer-Informationen durch sogenannte *Cross Site Scripting*-Attacken, bei denen ein Hacker im Browser eines Benutzers das Cookie einer fremden Website auslesen kann.
- Ausführung beliebiger Kommandos auf dem Server (z.B. mit Hilfe von Apaches *test-cgi.bat* und IIS *.HTRI.IDA ISAPI Filter*)
- Zugriff auf das Dateisystem des Servers (z.B. durch Aufruf von Apaches *source.asp*, *viewcode.asp*, IIS WebDAV, Frontpage-Erweiterungen, PHP)

3.2. Denial-of-Service-Attacken

Denial-of-Service-(DoS)-Attacken sind Angriffe, bei denen einzelne Dienste oder ein kompletter Zielrechner außer Gefecht gesetzt werden. Oftmals reicht dabei eine erfolgreiche DoS-Attacke auf eine kritische Komponente, z.B. die Authentisierung, aus, um ein System in seiner Gesamtheit zu blockieren.

DoS-Attacken können sowohl auf der TCP/IP-Ebene als auch durch gezielte Anfragen an Applikationen erfolgen. Während DoS-Attacken auf der Netzwerkebene aufgrund verbesserter Protokollstack-Implementierungen in den Betriebssystemen mittlerweile seltener geworden sind, haben sich die unterschiedlichsten Applikationen und Produkte als anfällig erwiesen, z.B.:

- RealServer
- Exchange
- PGP Cert Server
- IBM DB2
- Firewall/1
- Netscape Enterprise Web-Server
- Lotus Domino
- Palm Hotsync Manager
- Yahoo Messenger
- Squid Proxy-Server
- Microsoft SQL Server

Bedauerlicherweise sind auch Sicherheitsanwendungen selbst, wie z.B. die BlackIce Personal Firewall, von DoS-Attacken betroffen. Dies ist insofern problematisch, als dass ein Hacker dann die vermeintlichen Schutzmechanismen aushebeln und unbemerkt seinen Angriff durchführen kann.

3.3. Cracken von Passwörtern

Die nach wie vor einfachste und effektivste Methode zum Kompromittieren von Systemen besteht im "Erraten" von Passwörtern. Insbesondere wenn Mitarbeiter Begriffe aus ihrem näheren Umfeld (Name der Freundin, des Projekts etc.) verwenden oder der Bequemlichkeit halber Passwörter mit nur wenigen Buchstaben und ohne Sonderzeichen verwenden, besteht die Gefahr, dass diese schnell geknackt werden. Sicherheitsscanner decken zu einfache bzw. zu kurze Passwörter auf, indem sie zwei verschiedene Strategien anwenden:

- Wörterbuch-Attacken, bei denen ein Repertoire von vorgegebenen Begriffen sowie Begriffskombinationen, z.B. auch mit Ziffern, überprüft wird.
- Brute-Force-Attacken, bei denen sukzessive alle möglichen Kombinationen von Buchstaben, Ziffern und Sonderzeichen ausprobiert werden.

Viele Systeme werden von den Herstellern mit Standard-Kennungen und -Passwörtern für die Administration und für Benutzer vorkonfiguriert. Werden diese Passwörter nicht nachträglich abgeändert, stehen einem Hacker Tür und Tor offen. Daher sollte man die Passwort-Vergabe u.a. bei folgenden Produkten überprüfen:

- WFTP
- AOL Web-Server
- 3COM SuperStack II Switch
- AirConnect Wireless Access Point
- Alcatel ADSL Modem
- HP Laserjet
- MySQL
- Microsoft SQL
- Microsoft Windows
- PC Anywhere

3.4. Backdoors

Bei den sogenannten Backdoors (Hintertüren) handelt es sich um Programme, die ein Hacker nach einem erfolgreichen Einbruchversuch auf dem Rechner des Opfers installiert. Sie ermöglichen ihm jederzeit ungehinderten Zugang zum System, auch wenn die ursprünglich genutzte Sicherheitslücke längst geschlossen ist. Backdoors werden zum Teil auch für verteilte Denial-of-Service-Attacken verwendet, bei denen der Rechner des Opfers selbst als Angreifer missbraucht wird. Zu den gefährlichsten Backdoors zählen:

- BackOrifice
- CDK
- Code Red
- GateCrasher
- NetBus
- Shaft
- Stacheldraht
- SubSeven
- Tribe Flood Network
- Trin00
- Trinity
- WinSATAN

Mit Hilfe von Security-Scannern kann überprüft werden, ob ein System von einer Backdoor befallen ist. Zusätzlich wird nach Anwendungen gesucht, die einen Fernzugriff erlauben und durch falsche Konfiguration als Backdoors genutzt werden können.

3.5. Nicht benötigte und veraltete Dienste

Auf Rechnersystemen stehen oftmals Dienste zur Verfügung, deren Funktionalität nicht benötigt wird oder die lediglich aus Gründen der Kompatibilität mit veralteten Rechnern installiert sind. Insbesondere im zweiten Fall haben die Dienste mitunter gravierende Sicherheitsmängel, z.B. weil sie Passwörter im Klartext übertragen oder anfällig für DoS-Attacken sind. Doch selbst wenn keine akuten Sicherheitsprobleme bekannt sind, wird präventiv von ihrem Einsatz abgeraten. Zu der Kategorie der veralteten bzw. häufig nicht benötigten Dienste zählen:

- Chargen
- Daytime
- Echo
- eDonkey
- finger
- Quote of the day
- rlogin und rsh
- Telnet
- Windows Terminal Service
- xdmcp

3.6. *Attacken gegen Firewalls und Router*

Für Firewalls gelten besonders hohe Sicherheitsanforderungen. Ist eine Firewall kompromittiert oder verhält sie sich fehlerhaft, fällt ein wichtiges Schutzschild des Unternehmensnetzwerks weg.

Bei sogenannten *Application Gateways* besteht die Gefahr, dass sicherheitskritische Daten nicht richtig gefiltert werden. Zu den bekannten Möglichkeiten, die Regeln einer Firewall zu umgehen, zählen:

- Zugriff auf Mail-Server, die eigentlich durch einen Content-Filter geschützt sind, durch spezielle SMTP-Befehle.
- Zugriff auf Telnet oder andere interaktive Dienste durch HTTP-Anfragen mit Portangaben.

Selbstverständlich können Application Gateways selbst Opfer einer Attacke werden. Daher werden z.B. für einen Web-Proxy dieselben Tests durchgeführt wie für einen normalen Web-Server.

Obwohl Router im Vergleich zu PCs einen vergleichsweise einfachen Aufbau besitzen, sind auch sie nicht gegen sicherheitskritische Fehler in ihrer Software geschützt. Für Produkte der Marke *CISCO* bietet z.B. der Sicherheitsscanner *Nessus* eine umfangreiche Testsammlung, die u.a. folgende Probleme abdeckt:

- Denial-of-Service-Attacken, die schlimmstenfalls das gesamte Netzwerk blockieren und einen Reboot erforderlich machen.
- Blockierung aller Management-Verbindungen bis zum nächsten Reboot, hervorgerufen durch eine Reihe von fehlgeschlagenen telnet-Authentisierungsversuchen.
- Ausführung beliebiger Kommandos auf einem entfernten Router.
- Ungesetzte (d.h. leere) Passwörter.
- Fehlerhafte Auswertung der Access Control Lists (ACLs) bzw. fälschlicherweise vollständige Blockierung aller Pakete.
- Vorhersagbarkeit von TCP-Sequenz-Nummern.

4. Sicherheitstools

Die Werkzeuge zur Analyse von Sicherheitsmängeln haben sich in den vergangenen Jahren deutlich verbessert. Während zunächst in der Open-Source-Gemeinde und in Hackerkreisen eine Vielzahl von kleinen Tools entwickelt wurden, um spezifische Sicherheitslücken aufzudecken, sind mittlerweile eine Reihe von sehr umfangreichen, sowohl freien als auch kommerziellen Security-Scannern verfügbar.

Ein sehr mächtiges Werkzeug ist das Open-Source-Tool *Nessus* (<http://www.nessus.org>), das die ganze Palette der in Kapitel 3 aufgeführten Sicherheitslücken abdeckt. Nessus identifiziert mit über 1.000 unterschiedlichen Einzeltests (sogenannte *Plugins*, die in einer speziellen *Nessus Attack Scripting Language* – kurz NASL – spezifiziert sind) unsichere Systemkomponenten und gibt Ratschläge zur Beseitigung der Probleme. Durch seine Client-Server-Architektur ist Nessus in der Lage, Tests von einem beliebigen Rechner im Internet aus durchzuführen, während die Sicherheitsmannschaft beim Kunden vor Ort die Auswirkungen der Tests und die Reaktion der IT-Abteilung auf den Einbruch beobachtet.

Die technischen Möglichkeiten heutiger Sicherheitstools führen durchaus zu Kontroversen. Ein häufiges Argument ist, dass damit Gelegenheitshackern in die Hände gespielt wird. Andererseits zeigt die Geschichte der Menschheit, dass sich auch durch ein Verbot oder einen einseitigen Verzicht kriminelle Machenschaften niemals verhindern lassen.

Auch Werkzeuge, die nicht unmittelbar für Sicherheitsanalysen entwickelt wurden, können für Penetrationstests eingesetzt werden. So ist es beispielsweise mit Hilfe von *cURL* bzw. der Bibliothek *libcURL* möglich, Webserver-Anfragen zu stellen, die unter Verwendung eines WWW-Browsers nicht formuliert werden können. Dies ist sinnvoll um zu testen, ob die Gültigkeit und Plausibilität von WWW-Formular-Eingaben serverseitig überprüft wird.

In der nachstehenden Tabelle sind – ohne Anspruch auf Vollständigkeit – einige Tools beschrieben, die für die Durchführung von Sicherheitstest herangezogen werden können.

Name	Hersteller	Lizenztyp	Preis	Plattform	URL	Benötigte Tools	Beschreibung
Achilles	DigiZen Security Group	„free product“ / OpenSSL License	-	Windows 98/NT/2000	http://www.digizen-security.com/projects.html	-	Proxy-Server für HTTPS-Verbindungen (Man-in-the-middle-Attacken)
AppScan	Sanctum	kommerziell	15.000\$ für einen User pro Jahr	Windows 2000 SP 2	http://www.sanctuminc.com/solutions/appscan/index.html		Security-Scanner für Web-Applikationen
cURL / libcURL	Open Source Community	wahlweise Mozilla Public License oder MIT/X derivate license	-	Windows, Linux, div. UNIX et al.	http://curl.haxx.se	-	kommandozeilenbasierter Client bzw. Bibliothek für den Austausch von Dokumenten mit URL-Syntax unter Verwendung von HTTP, HTTPS, FTP, TELNET, LDAP, etc.; Unterstützung von Proxy-Support, Benutzerauthentifizierung, HTTP POST, SSL und Cookies
Dsniff	Dug Song	freies Produkt (keine Standardlizenz)	-	Linux, div. UNIX	http://www.monkey.org/~dugsong/dsniff/	Berkeley DB, OpenSSL, libpcap, libnet, libnids	Tool-Sammlung für Netzwerkmonitoring (Passworte, eMails, Dateien, etc.) und Man-in-the-middle-Attacken
Ethereal	Gerald Combs et al.	GNU GPL	-	Windows, Linux, div. UNIX et al.	http://www.ethereal.com/	GTK+, GLib, libpcap, Perl, Zlib,(NET-SNMP)	Netzwerk-Protocol-Analysator mit grafischer Oberfläche, der Datenpakete untersucht und aufzeichnet; beinhaltet eine Filtersprache und erlaubt die Rekonstruktion von TCP-Sessions
Ettercap	A. Ornaghi & M. Valleri	GNU GPL	-	Linux, div. BSD-Systeme, Mac OS X	http://ettercap.sourceforge.net	ncurses	Netzwerk-Sniffer für switched LANs; unterstützt ARP-Poisoning und Man-in-the-middle-Attacken
ISS Database Scanner	ISS	kommerziell	4.395€ (1 DB)	Windows	http://www.iss.net		Security Scanner für relationale Datenbanken (Microsoft, Oracle, Sybase)
ISS Internet Scanner	ISS	kommerziell	1.099€ (10 Liz.); 3.075€ (30 Liz.)	Windows NT/2000	http://www.iss.net		Security Scanner
LC4 (l0phtcrack)	@stake	kommerziell	\$350 (1 Liz.); \$1750 (Consultant)	Windows 95/98/NT4/2000	http://www.atstake.com/research/lc4/index.html		Passwort-Cracker
Microsoft Baseline Security Analyzer	Microsoft	kommerziell	kostenlos	Windows NT/2000/XP	http://www.microsoft.com/technet/security/tools/Tools/mbsahome.asp	-	Graphisches Tool basierend auf HFNetChk zur Überprüfung eingespielter Sicherheitspatches für Window NT/2000/XP, IIS 4.0/5.0, SQL Server 7.0/2000, Internet Explorer >5.01 und Office 2000/2002; Remote-Einsatz möglich
Nemesis	Mark Grimes, Jeff Nathan	freies Produkt (keine Standardlizenz)	-	Linux, div. UNIX	http://jeff.wvti.com/nemesis	libpcap, libnet	Kommandozeilenbasierte Toolsuite für das Versenden von selbsterstellten TCP/UDP/ICMP/ARP-Paketen
Nessus	Renaud Deraison et al.	GNU GPL 2	-	Linux, Unix, Windows (nur Client)	http://www.nessus.org	GTK 1.2, Nmap, OpenSSL	Security Scanner mit Client-Server-Architektur, eigener Scriptsprache und fast 1000 Plugins
Netcat	hobbit, Chris Wysopal	freies Produkt (keine Lizenz)	-	Linux, Unix, Windows 95/98/NT/2000	http://www.atstake.com/research/tools	-	Kommandozeilenbasiertes Netzwerk-Debugging-Tool zum Lesen und Schreiben von Daten über eine TCP/UDP-Netzwerkverbindung



Name	Hersteller	Lizenztyp	Preis	Plattform	URL	Benötigte Tools	Beschreibung
Nmap	Fyodor et al.	GNU GPL 2	-	Linux, div. Unix, Windows (beta)	http://www.insecure.org/nmap/ (Linux) http://www.eeye.com/html/Research/Tools/nmapNT.html (Windows)	-	Portscanner mit unzähligen Optionen und graphischer Oberfläche; auch für große Netzwerke geeignet
N-Stealth HTTP Security Scanner	N-Stalker Inc.	freie Edition verfügbar; Update-Service durch Wartungsvertrag	- / ?	Win 32, Linux (Wine)	http://www.nstalker.com/stealth	-	Security-Scanner für HTTP-Server mit mehr als 19.000 Sicherheitstests
Retina	eEye Digital Security	kommerziell	\$3000 (C-Class-Netz)	Windows NT 4.0 SP6a/2000/XP	http://www.eeye.com/html/Products/Retina/overview.html		Security-Scanner mit Spezialisierung auf Windows-Plattform
Snort	Martin Roesch et al.	GNU GPL 2	-	Linux, Unix, Windows	http://www.snort.org/	libnet, libpcap	Intrusion-Detection-System; kann auch zum Mitschneiden und Auswerten von Datenpaketen eingesetzt werden
WebProxy	Frank Swiderski	kommerziell / frei für nicht-kommerzielle Zwecke	? / -	Win 32, Unix	http://www.atstake.com/research/tools	JRE v1.4	Cross-Plattform-Web-Proxy zum Mithören, Modifizieren und Loggen von HTTP- und HTTPS-Verbindungen; unterstützt u.a. dynamische Zertifikatserzeugung und Editieren von POST-Parametern und Cookies
Whisker	rfp.labs	GNU GPL 2	-		http://www.wiretrip.net/rfp/p/doc.asp/d21.htm		Whisker ist ein Sicherheitsscanner für CGI-Skripte.

5. Referenzen

- [1] Microsoft Deutschland GmbH: Microsoft Security Bulletins.
<http://www.microsoft.com/germany/ms/technetservicedesk/bulletin/index.htm>, 2002.
- [2] Computer Security Institute. <http://www.gocsi.com/>. San Francisco, California, 2002.
- [3] CSI/FBI: Computer Crime and Security Survey.
<http://www.gocsi.com/forms/fbi/pdf.html>, April 2002.
- [4] Institute for the Advanced Study of Information Warfare (IASIW).
<http://www.psycom.net/iwar.1.html>, 2002.
- [5] Common Vulnerabilities and Exposures (CVE). <http://cve.mitre.org/>, 2002.