Security Auditing - Erkennung von IT-Sicherheitsrisiken

Institut für Telematik
Bahnhofstraße 30-32
D-54292 Trier

Die Zahl der bekannt gewordenen Sicherheitslöcher in IT-Systemen hat in der letzten Zeit ein beängstigendes Wachstum erfahren. Die folgende Aufstellung gibt einen Überblick über die wichtigsten Gefahrenbereiche, die mit Hilfe von modernen Sicherheitstools und -techniken überprüft werden können.

Attacken gegen Web-Server

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

- ☐ Auflistung von Web-Verzeichnissen und -Dateien, z.B. des Administrationsverzeichnisses */iisadmin*, der Passwortdatei */iisadmpwd/aexp2.htr* oder der Skript-Verzeichnisse */cgi-bin* und */scripts*
- ☐ Kompromittierung des Systems durch Ausnutzen von Buffer Overflows in Server-Komponenten (z.B. in *Active Perl perlIIS.dll*)
- ☐ Auslesen des Quellcodes von Active Server Pages, um an hartcodierte Passwörter zu gelangen (z.B. durch *%2e-Trick*, *:$DATA-Trick*, *translate f bug*)

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

- ☐ Ausspionieren von Benutzer-Informationen durch sogenannte Cross Site Scripting-Attacken (z.B. bei *Agora* und *WebSphere*)
- ☐ Ausführung beliebiger Kommandos auf dem Server (z.B. mit Hilfe von Apaches *test-cgi.bat*, *Alchemy Eye*, *Alchemy Network Monitor*, *alibaba.pl*, *auktion.cgi, IIS .HTR/.IDA ISAPI Filter*, *info2www*)
- ☐ Zugriff auf das Dateisystem des Servers (z.B. durch Aufruf von *repost.asp*, Apaches *source.asp*, *anacondaclip*, *viewcode.asp*, *IIS WebDAV*, *Frontpage*-Erweiterungen, *Oracle 9iAS*, *PHP*)

Denial-of-Service-Attacken

Denial-of-Service-Attacken sind Angriffe, bei denen einzelne Dienste oder ein kompletter Zielrechner außer Gefecht gesetzt werden. DoS-Attacken können sowohl auf der TCP/IP-Ebene als auch durch gezielte Anfragen an Applikationen erfolgen. Während DoS-Attacken auf der Netzwerkebene aufgrund verbesserter Implementierungen in den Betriebssystemen mittlerweile seltener geworden sind, haben sich viele Applikationen und Produkte als anfällig erwiesen. Hierzu zählen:

- ☐ AnalogX
- ☐ Annex
- ☐ Ascend Router
- ☐ Axent Raptor Firewall
- ☐ BFTelnet
- ☐ BlackIce Personal Firewall
- ☐ Cassandra NNTP-Server
- ☐ Chameleon SMTP-Server
- ☐ RealServer
- ☐ Cisco Router
- ☐ IBM DB2
- ☐ Lotus Domino
- ☐ Oracle WebCache-Server
- ☐ Squid Proxy-Server
- ☐ Dragon FTP-Server
- ☐ Dragon Telnet-Server
- ☐ Exchange
- ☐ Firewall/1
- ☐ Palm Hotsync Manager
- ☐ HyperARC router
- ☐ ICQ
- ☐ Microsoft Internet Information Server
- ☐ Interscan SMTP-Server
- ☐ iParty Chat-Programm
- ☐ Ken! Proxy
- ☐ MDaemon Server
- ☐ WebView
- ☐ Microsoft Media Server
- ☐ Microsoft SQL Server
- ☐ PGP Cert Server
- ☐ Netscape Enterprise Web-Server
- ☐ Novell Border Manager
- ☐ Real Video Server
- ☐ Quake3 Arena Daemon
- ☐ SalesLogic Eviewer WebApp
- ☐ Savant Web Server
- ☐ SLMail
- ☐ WebShield Server
- ☐ Wingate
- ☐ Xerver Web-Server
- ☐ Yahoo Messenger

Oftmals reicht eine erfolgreiche DoS-Attacke auf eine einzelne, kritische Komponente, z.B. die Authentisierung, aus, um das System in seiner Gesamtheit zu blockieren.

Cracken von Passwörtern

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

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

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

- ☐ MPEi/X
- ☐ SiteScope Web-Service
- ☐ WinGate
- ☐ WFTP
- ☐ Piranha
- ☐ AOL Web-Server
- ☐ LinkSys Router
- ☐ SUN JavaServer
- ☐ WhatsUp Gold Server
- ☐ 3COM SuperStack II Switch

- ☐ AirConnect Wireless Access Point
- ☐ Axis Network Camera
- ☐ CISCO Router
- ☐ Zyxel Router
- ☐ Nortel Networks Router
- ☐ Alcatel ADSL Modem
- ☐ Caiman DSL Router
- ☐ HP Laserjet
- ☐ Pocsag
- ☐ Shiva Router
- ☐ MySQL
- ☐ Microsoft SQL
- ☐ Windows SMB
- ☐ PC Anywhere

Kompromittierung durch Backdoors

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

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

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

Nutzlose und veraltete Dienste

Auf Rechnersystemen stehen oftmals Dienste zur Verfügung, deren Funktionalität in der Regel nicht benötigt wird oder die lediglich aus Gründen der Kompatibilität mit veralteten Rechnern installiert sind. Selbst wenn für einige dieser Dienste keine akuten Sicherheitprobleme bekannt sind, wird präventiv von ihrem Einsatz abgeraten. Zu der Kategorie der nutzlosen Dienste zählen:

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

Attacken gegen Firewalls

Für Firewalls gelten besonders hohe Sicherheitsanforderungen. Ist eine Firewall kompromittiert oder verhält sie sich fehlerhaft, fällt ein wichtiges Schutzschild des Unternehmensnetzwerks weg. Speziell bei sogenannten Application Gateways besteht die Gefahr, dass sicherheitskritische Daten nicht richtig gefiltert werden. Zu den bekannten Möglichkeiten, die Regeln einer Firewall zu umgehen, zählen:

- ☐ Zugriff auf Mail-Server, die eigentlich hinter einer Firewall versteckt sind, durch spezielle SMTP-Befehle
- ☐ Zugriff auf Telnet oder andere interaktive Dienste mit Hilfe von HTTP-Anfragen mit Portangaben

Daneben besteht selbstverständlich die Gefahr, dass Application Gateways selbst Opfer einer Attacke werden. Daher werden z.B. für einen Web-Proxy dieselben Angriffe getestet wie für einen normalen Web-Server.

Attacken gegen Router

Obwohl Router im Vergleich zu PCs einen vergleichsweise einfachen Aufbau besitzen, sind auch sie nicht gegen sicherheitskritische Fehler in ihrer Software geschützt. Für Produkte der Marke *CISCO* existiert z.B. eine umfangreiche Testsammlung, mit der u.a. folgende Problembereiche überprüft werden können:

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

Ausspähen von Informationen

Für einen erfolgreichen Einbruchsversuch benötigt ein Hacker zunächst Informationen über die vorhandene Netzwerk-Struktur, die verfügbaren Dienste auf den einzelnen Hosts und die angelegten Benutzerkennungen. Aus diesem Grund ist es wichtig herauszufinden, welche Daten ein Angreifer über die vorhandene IT-Infrastruktur in Erfahrung bringen kann.

Um eine Liste der verfügbaren Dienste zu ermitteln, werden zunächst sogenannte Port-Scans durchgeführt. Verschiedene Verfahren stehen zur Verfügung, um unter Umständen auch an Informationen über Rechner zu gelangen, die durch eine Firewall vor Zugriffen von außen geschützt sind. Darüber hinaus gibt es Techniken, die darauf abzielen, den Port-Scan gegenüber evtl. installierten Intrusion-Detection-Systemen zu verbergen.

Informationen über vorhandene Benutzerkennungen sind hilfreich beim Erraten von Passwörtern. Insbesondere unter Windows ist es mit Hilfe von NetBIOS und SMB sehr einfach möglich, ein Rechnerprofil zu erstellen.

- ☐ Auflistung aller Benutzer
- ☐ Gruppenrechte des "Gast"-Benutzers
- ☐ Benutzerkennungen, deren Passwort bisher nie verändert wurde
- ☐ Benutzerkennungen, deren Passwort niemals ungültig wird
- ☐ Bisher nicht verwendete Benutzerkennungen