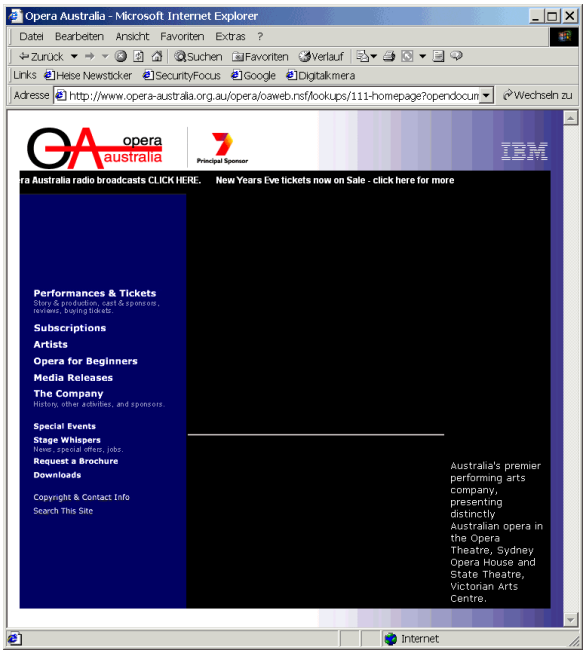
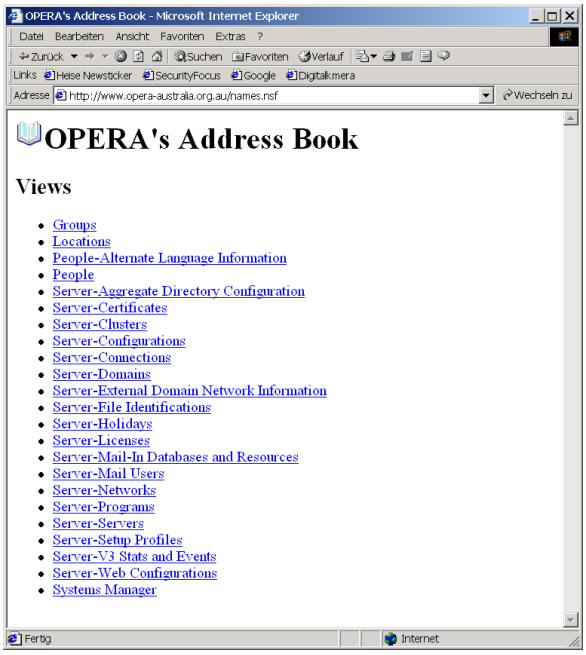
Hackereinbrüche in Domino-Server

Attacken auf Domino-Server sind oft vom Erfolg gekrönt: Domino-Server sind leicht zu knacken. Dies beruht entweder auf unsicheren Default-Konfigurationen von Lotus Domino oder auf gefährlichen Bugs in der Software. Als Beispiel sollen hier zunächst ungeschützte Domino-Datenbanken genannt werden: So kann oft man oft auf die Datenbanken names.nsf, log.nsf, catalog.nsf oder domlog.nsf zugreifen. Dieser Angriff kann komfortabel mit einem Web-Browser wie dem Internet Explorer oder dem Netscape Navigator durchgeführt werden.

Möchte man beispielsweise auf das Mitarbeiter-Adressbuch der bekannten Oper in Sydney zugreifen, braucht man lediglich folgende URL aufzurufen:
http://www.opera-australia.org.au/names.nsf



Web-Präsenz



names.nsf

Obwohl das Problem – eine unsichere Default-Einstellung - schon seit sehr langer Zeit[1] bekannt ist, findet man eine Vielzahl von Systemen mit diesem Sicherheits-Loch.

Ein anderes Problem ist die .nsf-Schwäche, die es einem Angreifer erlaubt, beliebige Dateien von einem Domino-Server herunterzuladen (diese Schwäche existiert bis zur Version 5.0.6). Mit folgender URL kann man beliebige Dateien von einem Dominoserver herunterladen:

`http://www.xy.de/.nsf/../../../../winnt/repair/sam`[2]

Unter Ausnutzung dieser Schwäche hat die Tübinger Security-Beratung SySS im Kundenauftrag eine Vielzahl von Passwortdateien heruntergeladen, die daraufhin mittels

[1] Siehe http://www.atstake.com/research/advisories/1998/domino3.txt.
[2] Diese Sicherheitsschwäche lässt sich nicht mit dem Internet Explorer, wohl aber mit Netscape oder Opera ausnutzen.

L0phtcrack[3] geknackt wurden. Die betreffenden Systeme können dann mit dem Administrator-Passwort betreten werden.

Domino Webserver bis einschließlich Version 5.0.8 lassen sich mittels gewöhnlicher Web-Anfragen zum Absturz bringen. Die URL muss lediglich den String "/./" enthalten (Bsp.: http://server/./webadmin.nsf).

Domino SMTP-Server lassen sich mit einer unzustellbaren Mail mit der Absender-Adresse xyz@[127.0.0.1] in einen Zustand versetzen, der sämtliche CPU-Ressourcen konsumiert. Diese Attacke ist auch dann wirksam, wenn der Domino-SMTP-Server nicht direkt aus dem Internet erreichbar ist.

Die vier oben diskutierten Angriffsmuster stehen repräsentativ für eine Vielzahl von Sicherheitsschwächen. Im Zeitraum vom 1.1.2001 bis zum 16.12.2001 wurden im Archiv von Security Focus[4] ganze 16 Sicherheitsschwächen von Domino dokumentiert:

2001-12-08: Lotus Domino bad URL database Denial of Service Vulnerability
2001-11-30: Lotus Domino SunRPC Denial of Service Vulnerability
2001-10-30: Lotus Domino View ACL Bypass Vulnerability
2001-10-30: Lotus Domino File Disclosure Vulnerability
2001-09-20: Lotus Domino Internal IP address Disclosure Vulnerability
2001-08-20: Lotus Domino Mail Loop Denial of Service Vulnerability
2001-07-16: Lotus Domino R5 LDAP Service Buffer Overflow Vulnerabilities
2001-07-16: Lotus Domino R5 LDAP Service Format String Vulnerabilities
2001-07-02: Lotus Domino Server Cross Site Scripting Vulnerability
2001-04-11: Lotus Domino Web Server HTTP Header DoS Vulnerability
2001-04-11: Lotus Domino R5 Server GET Request DoS Vulnerability
2001-04-11: Lotus Domino R5 Server MS-DOS Device DoS Vulnerability
2001-04-11: Lotus Domino R5 Server HTTP DoS Vulnerability
2001-04-11: Lotus Domino R5 Server DIIOP DoS Vulnerability
2001-01-23: Lotus Domino Mail Server 'Policy' Buffer Overflow Vulnerability
2001-01-05: Lotus Domino Server Directory Traversal Vulnerability

Der Domino-Server ist also nur knapp „besser“ als der IIS mit 18 Lüchen im selben Zeitraum. Pro Monat werden durchschnittlich 1,5 neue Sicherheitslücken bekannt. Die Gartner Group weist im Artikel „*Nimda Worm Shows You Can't Always Patch Fast Enough*” (FT-14-5524, http://www3.gartner.com/DisplayDocument?id=340962&acsFlg=accessBought) darauf hin, dass kaum ein Unternehmen in der Lage ist, zeitnah die verfügbaren Patches einzuspielen – auch beim Domino-Server werden Patches oft erst lange nach dem Bekanntwerden der Sicherheitslücke veröffentlicht.Es ist daher äußerst fraglich, ob man Domino guten Gewissens ins Internet stellen sollte. Im Rahmen einer Studie wurde geprüft, welche Webserver die unter http://www.notes-magazin.de/ gelisteten „Notes Partner“ im Einsatz haben.Es zeigt sich, dass der Großteil der „Notes Partner“ auch den Domino-Server einsetzen:

Produkt	**Anzahl der Installationen**
Domino	23
Apache	7

[3] Siehe http://www.atstake.com.
[4] Siehe http://www.securtyfocus.com.

IIS	5
Netscape	1

Betrachten wir nun etwas genauer die Versionsstände der Installationen:

Server	**Anzahl der Installationen**
Lotus-Domino/5.0.8	8
Lotus-Domino/5.07	5
Microsoft-IIS/4.0	3
Lotus-Domino/5.0.6	3
Netscape-Enterprise/4.1	2
Microsoft-IIS/5.0	2
Lotus-Domino/5.0.3	2
Rapidsite/Apa-1.3.14 (Unix) FrontPage/4.0.4.3 mod_ssl/2.7.1 OpenSSL/0.9.6	1
Netscape-FastTrack/2.0c	1
Lotus-Domino/Release-4.6.5	1
Lotus-Domino/5.0.7	1
Lotus-Domino/5.0.5	1
Lotus-Domino/5.0.4	1
Lotus-Domino/5.0.2	1
Apache/1.3.20 (Win32)	1
Apache/1.3.19 Ben-SSL/1.44 (Unix) PHP/4.0.5	1
Apache/1.3.14 (Unix) Resin/1.1.5	1
Apache/1.3.12 (Unix) (SuSE/Linux) mod_perl/1.24 PHP/4.0.3pl1	1
Apache/1.3.12 (Unix) (SuSE/Linux) mod_jk	1
Apache/1.3.12 (Unix) PHP/3.0.16	1

Ein Grossteil der Server sind demnach nicht auf dem neuesten Stand. Ein kurzer Test bestätigt, dass 8 der 23 Domino-Server das Logfile domlog.nsf völlig ungeschützt im Internet zum Download „bereitstellen“. Eine weitere Untersuchung der Server würde mit Sicherheit viele weitere Schwachstellen identifizieren.

Diese kleine Stichprobe beweist, dass die Systeme der sogenannten Notes-Spezialisten ungepflegt und falsch konfiguriert sind. Es stellt sich die Frage, ob Domino ein Produkt ist, das für den Einsatz im Internet geeignet ist – auf den Servern www.lotus.de und www.notes-magazin.de laufen jedenfalls Apache Webserver.

Dieser Artikel ist im Notes Magazin (1/2001, S.48ff) erschienen.

(Von Sebastian Schreiber. Schreiber ist Geschäftsführer und Consultant bei SySS. Sein Unternehmen hat sich auf die Durchführung von Penetrationstests spezialisiert.)