

SECBITS

Kritik an Vista-Firewall

Nach einem Bericht der Sicherheits-spezialistin Symantec kann Malware problemlos die Firewall in Windows Vista ausmanövrieren. Die Firewall blockt jegliche Software von Drittanbietern, bis die Anwender persönlich die Erlaubnis geben. Gemäss Symantec sei es nicht besonders schwierig, Malware so zu programmieren, dass die Erlaubnis umgangen respektive automatisch gegeben werden kann. Microsoft habe es verpasst, Vista mit einer guten Firewall auszustatten, behauptet Symantec.

Löcher in Antiviren-Software

Die Sicherheitsspezialistin I-Defense hat eine Lücke in Kasperskys Antivirus-Programm entdeckt, die für Denial-of-Service-Angriffe ausgenutzt werden könnte. Das Loch soll beim Dekomprimieren von Dateien des Formats UPX entstehen. Durch gezielte Manipulation solcher Archive lässt sich durch eine endlose Programmschleife ein Denial-of-Service-Angriff gegen das betroffene System ausführen. Momentan stehe noch kein Patch zur Verfügung.

labs.iddefense.com/intelligence/vulnerabilities/

Wenn Würmer bloggen

Laut der Sicherheitsspezialistin Secure Computing treibt eine neue Gattung von Würmern ihr Unwesen. Sie kann Foren- und Blogbeiträge modifizieren. Die jüngst entdeckte Malware verbreitet sich, indem sie den Datenverkehr übers Internet analysiert und Blog-Kommentare, Forenbeiträge sowie Webmails so verändert, dass ein Link eingefügt wird. Der Link führt direkt zum schädlichen Code.

Oracle-Löcher sind grösser

Eine neue Angriffstechnik soll laut David Litchfield, Sicherheitsexperte von NGS Software, das Risiko gewöhnlicher Lücken in Oracles Datenbank-Software erhöhen. Bislang ging man davon aus, dass Angreifer für Attacken gegen so genannte PL-SQL-Injection-Schwachstellen mit Sonderrechten ausgestattet sein müssen. Mit der neuen Technik sollen laut Litchfield nun auch Anwender mit minimalen Rechten die totale Kontrolle über den Datenbank-Server gewinnen können. So werden als nicht gefährlich eingestufte Lücken plötzlich zu einem Problem. In einem Dokument erklärt Litchfield seine Technik der synchronisierten Cursor-Injection. www.databasesecurity.com/dbsec/cursor-injection.pdf

SECURITY-TESTING

Selbst ist der Hacker

Um die eigene IT-Security zu testen, schlüpft man am besten in die Rolle des Hackers, wie das Computerworld-Kompaktseminar zeigte.

VON JENS STARK



BILD: CW/JUST

Martin Rutishauser von Oneconsult hackt im Namen der IT-Sicherheit.

➤ Hacken ist zwar recht einfach, es braucht aber auch eine gehörige Portion Geduld. Das konnten die Teilnehmer des Computerworld-Kompaktseminars mit ihrem eigenen Notebook erfahren. Kursleiter Martin Rutishauser von der IT-Security-Beraterin Oneconsult zeigte ihnen Schritt für Schritt, wie Attacken geplant und durchgeführt werden.

So muss sich der Angreifer erst einmal über die Zusammensetzung der IT-Umgebung schlau machen. Gleichsam bei Hackern wie bei Security-Profis beliebt ist dabei das Tool Nmap (Network Mapper). Es scannt die Anschlüsse eines Netzwerkhosts und zeigt an, welche Ports offen sind und welche Software

sich hinter diesen verbirgt. So offenbart der Scan von Rutishausers Testumgebung, dass sich hinter «Port 80» Microsofts Webserver Internet Information Server (IIS) 5.0 verbirgt.

Nun muss der Einbruchswilige eruieren, ob es für diese Version des Webserver ein Sicherheitsloch gibt, und wie dieses ausgenutzt werden kann. Hier hilft das Open-Source-Projekt

Metasploit weiter, das im Internet Exploits zu unterschiedlichen Systemen beschreibt.

Weiss man erst einmal, wie die Sicherheitslücke auszunutzen ist, lässt sich eine Attacke starten. Wie Rutishauser ausführt kann diese rein destruktiven Charakter haben, indem eine Applikation zum Absturz gebracht wird. Oder sie kann als Vorbereitung zu weiteren Angriffen dienen, indem etwa mit Administratorenrechten ein System übernommen wird. In jedem Fall muss viel mit den entsprechenden Tools hergespielt werden, um ans Ziel zu kommen – auch dies eine Erfahrung der Seminarteilnehmer.

Nicht auf Hacker-Angriff warten

Um herauszufinden, wie verwundbar die eigene IT-Umgebung ist, muss allerdings nicht gewartet werden, bis Hacker sie angegriffen haben. Wie Rutishauser ausführt, gibt es umfangreiche Methoden, um die Sicherheit eines Systems zu «messen». Er empfiehlt hierfür etwa das vom Institute of Security and Open Methodologies (Isecom) herausgegebene Open Source Security Testing Methodology Manual (OSSTMM). Damit lässt sich etwa ein Risk Assessment Value (RAV) errechnen, der auch in Audits über den Stand der Security Auskunft gibt. ■ www.isecom.org/osstmm/

COMPUTERWORLD-BLOGS

Prüfung für IP Stack und SNMP-Walking-Tool

Prüfung für den IP Stack

Der IP Stack Integrity Checker (ISIC) und seine Komponenten wurden entwickelt, um die Integrität des IP-Stacks in Version 4 und 6 zu testen. Damit können Firewalls, IDS-Systeme aber auch der IP-Stack normaler Computer getestet werden. ISIC ist in Version 0.07 als Source Code für Linux- und Unix-Systeme verfügbar und wurde unter der BSD-Lizenz veröffentlicht. Anwendungsbeispiele gibt es im Hackertools-Blog von Computerworld.

www.computerworld.ch/blogs/hackertools

Paket für SNMP-Walking

Das Simple Network Management Protocol (SNMP) wird für die Steuerung von Geräten wie Druckern, Routern, Switches oder auch Computern via Netzwerk verwendet. Bestandteil von SNMP sind Hardware-abhängige MIBs (Management Information Base), welche die OID (Object Identifiers) der Geräte zur Verfügung stellen. Das Paket Net-SNMP verfügt neben Snmpwalk auch über viele weitere nützliche Tools, um SNMP anzusprechen.

www.computerworld.ch/blogs/hackertools

Die Rubriken im Blog-Bereich werden auch als RSS-Feed angeboten.

IN EIGENER SACHE

Die Computerworld-Kompaktseminare

Computerworld führt weitere Kompaktseminare zum Thema «Security für IT-Profis» durch. Die nächsten Termine sowie die Themenübersicht finden Sie auf: www.computerworld.ch/seminare