Datensicherheit

Wenn Sicherheitstools Sicherheitslücken haben

Viren, Trojaner, BotNets, Buffer Overflows, Exploits – um nur einige Schreckensszenarien zu nennen – sind Bedrohungen, vor denen wir uns mit Virenscannern, Anti-Spyware-Tools oder anderen Sicherheitswerkzeugen schützen. Aber auch Sicherheitstools sind Software und haben damit Fehler. Peinlich, wenn der erfolgreiche Angreifer ausgerechnet eine Lücke in einer Sicherheitssoftware ausgenutzt hat!

Die Online-Ausgabe des SPIEGEL berichtete Anfang Dezember 2005 über den Computerwurm Witty, der Anfang 2004 sein Unwesen trieb. Die Medien haben ihn damals kaum beachtet. Er stellte aber trotzdem ein wichtiges Ereignis dar. Denn Witty war der erste Wurm, der sich eine Lücke in einem Sicherheitstool zunutze machte.

Der Wurm nutze einen Fehler im so genannten „Protocol Analysis Module“ der Firma ISS. Unglücklicherweise verwenden alle Produkte von ISS das Modul, z.B. Intrusion-Detection-Systeme und Personal Firewalls.

Antivirensoftware steht weit oben auf der „Hitliste“ der Sicherheitslücken

Hersteller von Antivirensoftware, die laut Heise Newsticker vor Kurzem mit Problemen zu kämpfen hatten, waren:

- F-Prot: erkennt Viren in speziell präparierten ZIP-Archiven nicht
- Kaspersky: Pufferüberlauf bei präparierten kompilierten Hilfe-Dateien
- Symantec: erlaubt Nutzern mit eingeschränkten Rechten Zugriffe mit Systemberechtigungen
- Sophos: Pufferüberlauf

Da manche dieser Lücken nichts mit den Signaturen zu tun haben, muss gleich die komplette Scan-Engine ausgetauscht werden.

In der TOP-20-Liste vom SANS Institute steht Antivirussoftware auf Platz 2 der Sicherheitslücken bei plattformunabhängigen Anwendungen!

Ein Live-Update hätte ganze Firmennetze „killen“ können

Im Sommer 2000 lieferte Symantec für Norton Antivirus per Live-Update neue Signaturen aus. Diese waren fehlerhaft und blockierten etliche Rechner. Wurde ein so blockierter Rechner ausgeschaltet und neu gestartet, erzeugte der Virenscanner neue illegale Verzeichnisse auf der Festplatte.

Da viele Firmen die neuen Virensignaturen automatisch einspielen, können solche Fehler im Extremfall auch mal ein ganzes Firmennetz lahm legen.

OpenSSL bietet nicht nur offenen Code, sondern auch offene Flanken

OpenSSL ist eine Verschlüsselungsbibliothek. Da die Software frei verfügbar ist, ist sie entsprechend beliebt und stellt die Basis für viele Verschlüsselungsdienste dar. Sie wird z.B. vom Apache Webserver und vielen anderen Webservern für die SSL-Routinen (https-Protokoll) verwendet. Darüber hinaus ist die Bibliothek Bestandteil von Mac OS X und NETBSD.

Die letzte Sicherheitslücke dieses Produkts betraf ein Feature von OpenSSL im Umgang mit Fehlern von Client-Software. Damit konnte ein Angreifer, der sich als Man-in-the-Middle betätigte, sich also als heimlicher Dritter in eine Verbindung zwischen zwei Rechnern einklinkte, das als unsicher geltende Verschlüsselungsverfahren SSL 2.0 für die Verbindung erzwingen. Dieses Verfahren lässt sich knacken und bequem abhören.

Unabhängig von diesem Fall sollte jeder sicherheitsbewusste Betreiber eines Servers SSL 2.0 deaktivieren und nur SSL 3.0/TLS 1.0 unterstützen.

Über Secure Shell lassen sich Angriffe gegen Login-Server fahren

Die Verwendung von Secure Shell (SSH) hat sehr viel zur Sicherheit von netzbasierter Kommunikation beigetragen, da SSH die Kommunikation verschlüsselt. Neben kommerziellen Produkten ist vor allem die Implementierung OpenSSH von Bedeutung. Die Entwickler sind sehr um Sicherheit bemüht und stellen Updates kurzfristig zur Verfügung.

Diese Updates sind allerdings auch notwendig, da immer wieder Angriffe gegen Login-Server erfolgreich waren.

Vertrauen Sie auch Sicherheitssoftware nicht blind!

Egal, welche Art von Software bei Ihnen im Einsatz ist, und sei es auch Sicherheitssoftware – um zeitnahes, aber nicht ungeprüftes (!) Einspielen von Updates und Patches kommen Sie nicht herum. Die Gefahr ist groß, dass kurz nach Verfügbarkeit eines Patches und damit dem Wissen über die Lücke auch ein Angriffstool gebastelt ist.

Prof. Dr. Rainer W. Gerling

Selbst Sicherheitstools können nicht immer für die Sicherheit von Rechnern und Netzwerken garantieren.