DuD
Datenschutz und Datensicherheit

Personal Firewall

Dirk Fox

Computer, die über ein Netzwerk mit dem Internet verbunden sind, können nicht nur die Kommunikationsdienste und Informationsangebote des Internet, wie z. B. E-Mail oder das WWW nutzen, sondern sind auch zahlreichen Bedrohungen wie Viren, Würmern und systematischen Angriffen ausgesetzt. Viele dieser Angriffe erfolgen heute mit automatisierten Tools, die große Netzbereiche im Internet flächendeckend nach Systemen mit Schwachstellen durchsuchen. Daher vergehen inzwischen nach der Verbindung eines Rechners mit dem Internet nur noch wenige Sekunden, bis ein erster Angriffsversuch beobachtet werden kann.

Computer sind in Unternehmensnetzen vor Angriffen dieser Art heute üblicherweise durch ein geeignet konfiguriertes und gepflegtes zentrales Firewallsystem, einen Virenscanner und einen Content-Filter, der z. B. aktive Inhalte in Webseiten sperrt, geschützt.

Dieser Schutz greift allerdings nur innerhalb eines Unternehmensnetzwerks. Mit der wachsenden Verbreitung von mobilen Systemen (Laptops) in Unternehmen und der Zunahme von DSL-Anschlüssen in Privathaushalten steigt jedoch die Zahl der Internet-Zugänge ohne ausreichenden Schutz. Die Auswirkungen sind dramatisch:

- So waren in den vergangenen Jahren in vielen Unternehmen Laptops die Verursacher erheblicher Virenschäden: Unterwegs ungeschützt mit dem Internet verbunden, wurden sie von Schadsoftware befallen und verbreiteten sie beim nächsten „Eindocken“ im internen Unternehmensnetz – ein „Bypass“ an der Firewall vorbei.
- Nach einer aktuellen Studie von Symantec ist die Zahl der von Trojanischen Pferden befallenen privaten DSL-Computern, so genannten „Zombie“-Systemen, die für die Spam- und Virenverbreitung missbraucht werden, im ersten Halbjahr 2004 auf 30.000 gestiegen – im zweiten Halbjahr 2003 wurden erst 2.000 „Zombies“ gezählt.

Um die Netzwerkverbindungen und Kommunikation mobiler oder privater Systeme ohne Firewall wirkungsvoll vor Angriffen aus dem Internet zu schützen, ist eine so genannte Personal Firewall unumgänglich. Eine Personal Firewall wird als Zusatzprogramm auf dem mobilen oder privaten System installiert und kontrolliert anschließend alle Kommunikationsverbindungen, die der Computer aufbaut. Dabei werden alle nicht explizit zugelassenen Verbindungen gesperrt und unerwünschte Verbindungsversuche von außen automatisch abgewiesen. Eine Personal Firewall schützt damit auch vor sicherheitskritischen (unbekannten) Fehlern im Betriebssystem eines Computers, die es Angreifern ermöglichen können, das System über eine bestehende Internet-Verbindung unter ihre Kontrolle zu bringen.

Windows XP Firewall

Grundlegende Funktionen einer Personal Firewall wurden von Microsoft im Betriebssystem Windows XP integriert. Für das aktuelle Service Pack 2 wurde die integrierte Personal Firewall erheblich verbessert: Sie kann nun – in der Professional-Version – über die zentralen Gruppenrichtlinien unternehmensweit einheitlich konfiguriert werden. Dabei kann zwischen einer Domänenkonfiguration (Arbeiten im Unternehmensnetz hinter der Firewall) und einer lokalen Konfiguration (direkter Anschluss ans Internet) unterschieden werden. In der Standard-Konfiguration werden alle Verbindungsaufnahmen von Außen abgeblockt.

Die Konfiguration der integrierten Firewall ist über das „Sicherheitscenter“ in der Systemsteuerung erreichbar. Geschützt werden automatisch alle Netzwerkverbindungen (Netzwerkkarte, WLAN, DFÜ-Verbindung)

Abb.: Konfigurationsmenu der Firewall in Windows XP (SP 2)

sowie Firewire- und Bluetooth-Schnittstellen. Dabei ist jedoch zu beachten, dass manche Provider spezielle Zugangssoftware anbieten, welche von der in Windows XP integrierten Firewall möglicherweise nicht unterstützt werden. In diesen Fällen sollte eine spezialisierte Softwarelösung als Personal Firewall eingesetzt werden.

Da die XP-Firewall Verbindungen, die vom System aus aufgebaut werden, nicht überwacht, ist die Nutzung einer spezialisierten Softwarelösung als Personal Firewall ohnehin zu empfehlen. Das gilt in jedem Fall für die Betriebssysteme Windows 95/98/ME oder Windows 2000, da diese keine eigene Firewall-Funktion beinhalten.

Grenzen

Eine Personal Firewall schützt allerdings nicht vor allen Angriffen. So ist für den Schutz vor Viren und Würmern zusätzlich ein (aktueller) Virenscanner erforderlich, der z. B. E-Mail-Anhänge auf Schaden stiftende Software überprüft und sie ggf. löscht. Auch vor schädlichen Webseiten-Inhalten, die entweder Schwächen in der Browser-Software ausnutzen oder unter Verwendung von Script-Sprachen bzw. über Active-X-Controls den Computer angreifen, schützt keine Personal Firewall, sondern nur ein zusätzlicher Content-Filter bzw. eine sichere Konfiguration des Browsers. Zahlreiche Hersteller bieten daher Personal Firewalls im Paket mit Content-, Spam- und Virenschutzlösungen an.

Eine Prüfung der Anfälligkeit eines direkten Internet-Zugangs für Angriffe aus dem Internet ist über kostenlose Online-Checks möglich, z. B. unter der Adresse *http://www.security-info.ch.*

Personal Firewalls werden von zahlreichen Herstellern angeboten, auch als Shareware oder Freeware, wie z. B. von Kaspersky[1], Kerio[2], McAfee[3], Sygate[4], Symantec[5] und ZoneLabs[6].

[1] http://www.kaspersky.com
[2] http://www.kerio.com
[3] http://www.mcafee.com
[4] http://www.sygate.de
[5] http://www.symantec.com
[6] http://www.zonelabs.com