Internet

Sicherheit im WWW

Web-Attacken abwehren

Das Internet birgt Gefahren, die auf den ersten Blick nicht erkennbar sind. Ist ein Rechner mit dem Internet verbunden, werden zwangsläufig Daten übertragen. Ob gewollt oder nicht, das bleibt dem User meist verschlossen. Generell lässt sich keine 100%ige Sicherheit für die IT-Systeme erreichen, wenn sie ans Internet angeschlossen werden. Die Gefahr, sich beim täglichen Surfen im Internet einen Virus einzufangen oder sonstwie ausspioniert zu werden, wird immer grösser. Antivirenprogramme alleine bieten hier nicht unbedingt hundertprozentigen Schutz, darum empfiehlt sich auch der Einsatz einer Personal Firewall. Vorbeugen ist allemal besser, als sich hinterher den Kopf zu zermartern... Dies umso mehr, als effiziente Programme zum Teil gratis aus dem Netz heruntergeladen werden können.

Thomas Vauthier
th.vauthier@bluewin.ch

Die vergangenen Wochen haben wieder einmal gezeigt, wie wichtig es ist, seinen PC vor Attacken verschiedenster Art zu schützen. Es muss nicht mal mehr zwangsläufig eine E-Mail oder eine Datei sein, über die man seinen PC infiziert – heutzutage stellt schon das reine Surfen im Internet eine potenzielle Gefahr dar. Viele Spionagetools finden den Zugang auf Ihren PC über verschiedene Netzwerk-Ports. Um sich bereits im Vorfeld zu schützen, bietet sich eine Kombination aus Virenscanner und Firewall an. Ist der PC bereits infiziert, muss man mit Datenverlust rechnen, damit das System wieder bereinigt werden kann. Im schlimmsten Fall hilft nur noch eine komplette Neuformatierung der Festplatte, was nicht nur mit einem enormen Zeitaufwand verbunden ist, sondern zusätzlich meist auch noch materiellen Schaden anrichtet. Vorsorge ist besser als Schadensbegrenzung!

«It is easy to run a secure computer system. You merely have to disconnect all dial-up connections and permit only direct-wired terminals, put the machine and its terminals in a shielded room, and post a guard at the door.»

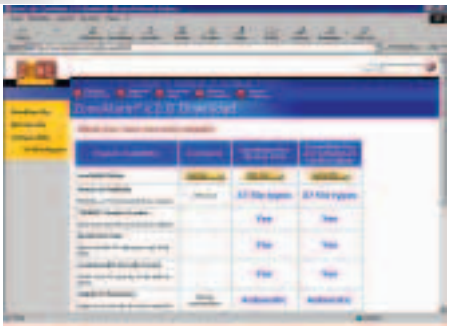
Eine **Firewall** (= Brandschutzmauer) ist ein System aus Hard- und Software, das an einem Punkt zwischen zwei Netzen installiert ist und nur zugelassene Kommunikation hindurch lässt. Unzulässige Aktionen werden abgewiesen, erkannte Missbrauchsversuche lassen sich protokollieren. Die Standardregel bei der Konfiguration von Firewalls sollte immer lauten: **«Alles, was nicht ausdrücklich erlaubt ist, ist verboten.»** Mit diesem restriktiven Ansatz setzt man sich weniger Sicherheitsrisiken aus.

Hier einige der interessantesten Tools, welche die Ports Ihres PCs überwachen und Eindringlinge abwehren helfen.

ZoneAlarm

ZoneAlarm gestattet nur vorher definierten Anwendungen, überhaupt auf das Internet zuzugreifen. ZoneAlarm überwacht die Internet-Verbindung und schlägt Alarm, wenn ein nicht autorisiertes Programm darauf zugreifen will. Erst wenn der Anwender das entsprechende Pop-up-Fenster mit Ja bestätigt, gibt ZoneAlarm den Zugriff frei. Für Notfälle gibt es einen Stop-Button, der sofort jeglichen Internet-Zugriff aller laufenden Programme blockiert. Zusätzliche Kontrolle bringt die Statistik, die das Utility für jede Anwendung führt.

Web: www.zonelabs.com/



Sphinx

Mit der Personal Firewall Sphinx lässt sich der PC wirkungsvoll vor Attacken aus dem Internet schützen. Vom Programm werden alle ein- und ausgehenden Verbindungen überwacht und protokolliert. Für die Konfiguration der Software stehen zwei Modi zur Verfügung: für Anfänger und Experten. Auf Wunsch führt ein Assistent Schritt für Schritt durch die einzelnen Einstellungen. Mit dem integrierten URL-Filter lassen sich unerwünschte Internet-Seiten von vornherein blockieren. Eine Statistikfunktion mit verschiedenen Auswertungsmöglichkeiten rundet dieses Sicherheitspaket ab.

Web: www.pcfirewall.de

Mcafee Personal Firewall

Mcafee Personal Firewall schützt Ihren PC vor allen bekannten Hackangriffen und Trojanischen Pferden, indem es sämtliche Netzwerk-Aktivitäten überwacht. Ohne Ihre ausdrückliche Erlaubnis kann nichts Ihr System verlassen oder in selbiges eindringen. Dabei merkt sich das Programm, was Sie in der Vergangenheit zugelassen oder geblockt haben und reagiert dementsprechend.

Web: www.mcafee.de

BlackICE Defender

BlackICE Defender beobachtet kontinuierlich die Internet- und Netzwerkverbindung und warnt vor möglichen Hacker-Angriffen. Dabei wird die IP-Adresse des Eindringlings angezeigt und die Art des möglicherweise unbefugten Zugangs. Somit eignet sich BlackICE Defender hervorragend, um unerwünschte Spione, also Hack-Attacken zu erkennen, und auch gleich deren IP-Adresse zu lokalisieren.

Web: www.networkice.com/

Norton Personal Firewall

Die Norton Personal Firewall erkennt, wenn vertrauliche Informationen wie Kreditkartennummern via Internet verschickt werden sollen und warnt mit Sicherheitshinweisen. Wählt man hohen Systemschutz, blockt die Firewall alle zuvor über den Button «Vertrauliche Info» erfassten Daten.

Unter «Benutzerdefiniert» lassen sich weitere Schutzfunktionen einstellen. Sobald Norton Desktop Firewall einen nicht autorisierten Zugriff auf das Internet feststellt, erscheint ein Warnhinweis. Hier kann man dann bestimmen, ob eine Anwendung auf das Internet zugreifen darf. Vorsicht ist hingegen bei Anwendungen geboten, die man nicht kennt oder die sich als System-Komponente tarnen. Im Hauptfenster erfahren User unter «Status», wie viele Aktionen Norton Personal Firewall seit dem Systemstart überwacht und geblockt hat.

Web: www.symantec.de

Fortsetzung folgt ...