Internet

Schütze sich, wer kann!

Angriff aus dem Hinterhalt

In Zeiten, in denen die Vernetzung von Information und Daten in Wirtschaft und Gesellschaft durch das Internet immer grössere Bedeutung erlangt, zeigen sich immer wieder auch die Schattenseiten dieses neuen Mediums. Wenn ein Computer mit dem Internet verbunden ist, besteht eine Netzwerkverbindung. Aus dieser Öffnung des Rechners zur Aussenwelt ergeben sich auch Gefahren, wie die Attacke des neuen Computer-Wurms «Lovsan» Mitte August wieder einmal deutlich gemacht hat. Hatten wir seit «ILOVEYOU», «Nimda» oder «Bug-Bear» realisiert, wie gefährlich eine E-Mail hinsichtlich der Sicherheit unserer Daten sein kann, und auch gelernt, dementsprechend zu handeln, kam der Angriff dieses Wurms aus einer neuen Stossrichtung. Denn besonders perfid war, dass sich der Schädling nicht über E-Mail verbreitete. «Lovsan» bewegte sich ohne jegliches Zutun der Nutzer, führte zu unkontrollierten Rechnerabstürzen und öffnete nach Ansicht von Experten den Computer für Angriffe von aussen Besonders betroffen waren Privatleute und kleine Unternehmen, die über eine ADSL-Leitung permanent ans Internet angeschlossen sind. Betroffen waren aber auch die Bundesverwaltung und mehrere grössere Schweizer Unternehmen. Grund genug also, sich wieder einmal mit dem Thema Sicherheit zu befassen. Stichwort: Hilfe, die Würmer kommen! Macht die Luken dicht!

Thomas Vauthier
Th.vauthier@bluewin.ch

Grundsätzliches

Das Internet ist ein Verbund von Netzwerken, die wiederum aus Teilnetzen und diese jeweils aus einzelnen Rechnern bestehen. Alle die Rechner, die eindeutig in diesem Netzwerk adressierbar sind, werden als Internetrechner (Hosts), Rechner, die Daten abfragen, als Internet-Clients bezeichnet. Verbunden und identifiziert sind sie durch so genannte IP-Adressen. Hacker suchen aber mit Vorliebe systematisch ganze IP-Adressbereiche (z.B. einzelner Provider) für ihre Attacken ab.
Das grundsätzliche Problem besteht darin, die Kommunikation zwischen Client und Server für gewünschte Internetdienste zuzulassen und Angriffe auf den PC von aussen zu unterbinden.

Ein wenig Theorie

Der Begriff «Port» steht für softwaremässig vorhandene «Kommunikationskanäle» zwischen Client und Server. Die Ports sind von 0 bis 65535 nummeriert, davon von 0 bis 1023 für Standard-Internet-Dienste. Hier einige wichtige Portnummern:
- 20, 21 File Transfer Protocol (FTP) für den Datentransfer (z.B. Hochladen einer Homepage)
- 25 Simple Mail Transfer Protocol (SMTP) für den Versand von E-Mails
- 80 Hypertext Transfer Protocol (HTTP) für den Empfang von Webseiten
- 110 Post Office Protocol (POP) für den Empfang von E-Mails
- 119 Network News Transfer Protocol (NNTP) für Newsgroups (Diskussionsgruppen)
- 443 Secure Socket Layer (SSL) für die verschlüsselte Datenübertragung

Es ist sicher verständlich, dass diese und andere benötigte Ports für die Internetdienste geöffnet sein sollen, weil sie sonst nicht genutzt werden können. Andere Ports, über die möglicherweise Angriffe erfolgen können, sollen möglichst geschlossen sein. Dafür sorgt eine so genannte Personal-Firewall-Software (Feuerschutzwand).

Was ist eine Firewall?

Die Personal-Firewall-Software kontrolliert die Zugriffe auf alle Ports von und zum PC, wenn man mit dem Internet verbunden ist. Ungewollte oder unbekannte Kommunikationsversuche werden abgeblockt, gewollte Kommunikation wird freigegeben.
Ein Portscan ist eine systematische Suche nach bestimmten offenen Ports, durch die z.B. Trojaner oder andere «Würmer» eindringen können. Eine (Personal) Firewall kann so konfiguriert werden, dass sie diese Ports sperrt und somit eine Verbindungsaufnahme eines Hackers mit Ihrem Computer verhindert.
In einer «professionellen» Firewall kommen meist Paketfilter und Application-Level-Gateways zum Einsatz. In der Praxis wird diese in Netzwerken eingesetzt und besteht je nach Netzwerkgrösse aus einem oder mehreren separaten Rechnern, d.h., sie werden nur für diese Aufgabe genutzt. Dort wird somit der Datenfluss zwischen mehreren Netzwerken gesteuert, z.B. dem lokalen Netzwerk und dem Internet.
Da im Privatbereich ein eigener Rechner/Computer für einen solchen Zweck alles andere als ökonomisch ist, gibt es Firewall-Lösungen, zugeschnitten für dieses Marktsegment. Sie tragen den Namen «Personal Firewall».
Ich werde Ihnen in einem nächsten Beitrag einige Produkte aus dem grossen Angebot etwas näher vorstellen.

Wer braucht eine Personal Firewall?

Grundsätzlich jeder, der das Internet nutzt. Zu den besonders gefährdeten Anwendergruppen zählen aber:
- alle diejenigen, die über eine ADSL-Leitung permanent ans Internet angeschlossen sind
- Anwender, welche häufig neue Programme auf dem Rechner installieren
- Online- bzw. Netzwerkspieler
- Anwender, die Dateitauschprogramme wie Napster, Kazaa, Morpheus etc. benutzen

Fazit

Die Angelegenheit von neuen Angriffen aus dem Hinterhalt ist in der Tat trickreich. Abdichten kann ein Anwender sein System oder Netzwerk meist nur mit mehreren parallelen Massnahmen. Diese umfassen Virenschutz, Firewall, Analyse des Gefährdungdspotenzials durch den aktuellen Softwareeinsatz und umsichtiges Verhalten. Ein perfekter Schutz existiert auch mit einer Firewall nicht. Firewall-Software schützt zwar vor ungewollten Zugriffen auf den PC von aussen, schützt aber nicht vor Computerviren. Zur Abwehr von Virenattacken wird in jedem Fall eine Virenscanner-Software benötigt.
Für die Absicherung einer Netzwerkumgebung ist eine Personal Firewall nur begrenzt zu empfehlen und stark abhängig von den verwendeten Betriebssystemen. Hier ist das Beiziehen von Profis mehr als empfehlenswert.
Und: Wer ganz sicher gehen will, geht mit einem gesonderten PC in das Internet, auf dem sich keine sensiblen Daten befinden.

Fortsetzung folgt ...