Schwachstellen bei der Internet-Sicherheit

von Kai-Oliver Detken

Grundsätzlich können vernetzte Computersysteme nie hundertprozentig gegen Angriffe von außen geschützt werden. Es ist jedoch möglich, einzelne Gefahrenquellen deutlich zu minimieren. Das größte Gefahrenpotential geht dabei immer von den Benutzern des Computersystems aus, insbesondere bei starker Unachtsamkeit von seitens der Systemverwalter. Kein automatisiertes System ist in der Lage, einen versierten Systemverwalter bei der Überwachung eines Computers zu ersetzen bzw. ihn daran zu hindern, seine Machtfülle zu mißbrauchen. Ebenso bestehen oft Gefahren durch rechtmäßige Benutzer, die entweder aus Unachtsamkeit oder aus kriminellen Antrieben die Sicherheit des Systems gefährden, beispielsweise durch unbedachte Wahl von Kennworten oder Datentransfer mittels Disketten nach innen und außen. Zentral hierbei sind die sog. programmierte Bedrohung (Programmed Threats) und die Bedrohung durch nicht autorisierte Eindringlinge. Je nach Herkunft und Absicht können diese mit mehr oder weniger Aufwand vom System ferngehalten werden.

Programmierte Bedrohung

Folgende programmierte Gefahren im Internet kann man zusammenfassen:

1. Virus: ein Stück Programmcode, das in der Regel in ein anderes Programm eingebettet wird, so daß befallene Programme anders arbeiten als sie eigentlich sollten. Meist verursachen diese Programme größere Schäden, indem sie auf der Festplatte sensible Bereiche überschreiben.
2. Dateiinfizierte Viren: Diese Viren hängen ihren Programmcode normalerweise an ausführbare Dateien, die bei Windows-Betriebssystemen mit der Endung .com und .exe bezeichnet werden. Zusätzlich werden auch systemspezifische Dateien wie .sys und .mnu davon angesteckt. Bei Windows-Systemen sind ebenfalls die Dateien mit Ausführungsrechten wie beispielsweise dynamische Programmbibliotheken nach der Dynamic Link Library (DLL) als Ziele beliebt, da sie zur Laufzeit eines Programms geladen werden.
3. System- oder Boot-Sektor-Viren: Diese Virenart ist in bestimmten Bereichen der Systemfestplatte (Master Boot Record – MBR) oder der Floppy-Disk (Boot Sector) zu finden.
4. Makro-Viren: Das sind Viren, die durch bestimmte Anwendungen verbreitet werden, die sich einer interpretativen Makrosprache bedienen. Indem diese Sprache wie etwa Visual Basic bei Microsoft-Anwendungen Zugriff bis auf die Systemebene zulassen, können solche Programme sehr großen Schaden anrichten.
5. Stealth-Viren: Gefährliche Programmfragmente, die so entworfen wurden, daß sie vor einer Entdeckung sehr effektiv geschützt sind. Zu den Merkmalen gehört das Verändern des Zugriffsdatums bei den befallenen Dateien oder der angezeigten Dateigröße. Zusätzlich sind Techniken vorhanden, die Fragmente vor Virenscannern verbergen, so daß kein wirklicher Schutz bestehen kann.
6. Würmer: Würmer sind ebenfalls Viren, die völlig eigenständige Programme enthalten. Diese Programme setzen sich auf die Festplatte oder den Hauptspeicher des Rechners, verändern dabei Daten und wandern häufig über das Netz weiter, um auch andere Rechner zu infizieren.
7. Trojanische Pferde: Programme, die vorgeben, ein anderes Programm zu sein, oder die sich in einem anderen, korrekt funktionierenden Programm selbständig einbetten, um an sicherheitsrelevante Daten heranzukommen.
8. Logische Bomben: Programme, die sich auf einem Rechner befinden und zu einem bestimmten Zeitpunkt oder durch einen bestimmten Vorgang ausgelöst werden.

Cracker und Hacker

Neben den programmierten Gefahren gibt es vor allem Probleme, die durch die direkte Beteiligung von Personen entstehen. In solchen Fällen sollte man die Einschätzung der Vorfälle nach der Motivation eines sog. Crackers vornehmen. Dabei muß zwischen Crackern und Hackern unterschieden werden.
Hacker versuchen, in ein System einzudringen, da sie sich für die Umgehung der Sicherheitsmechanismen interessieren. Sie zerstören dabei keine Daten und setzen keine Viren frei. So wie sie die Hintertür eines Intranets betreten haben, so verlassen sie das Netz auch wieder.
Cracker hegen hingegen von Anfang an kriminelle Absichten. Sie versuchen in ein Netz einzudringen, um sich persönliche Vorteile zu verschaffen und eventuell Daten zu zerstören. Neben dem tatsächlichen Schaden wie Datenverlust bzw. -diebstahl usw. besteht anschließend immer das Problem, die Integrität des Systems nach der Attacke wieder sicherzustellen.

Fazit

Solange man sich global nicht auf einheitliche Sicherheitsstandards und Implementierungen geeinigt hat, werden auch weiterhin Lücken im Internet vorhanden sein und ausgenutzt werden. Somit bleibt heute jeder für seine Sicherheit selbst verantwortlich und muß Kompromisse eingehen, wenn er nicht eine Netztrennung in Kauf nehmen möchte. Abhilfe wird es erst durch gemeinsame Standards wie z. B. SSL und IPsec und die Weiterentwicklung der Internet-Protokolle IPv6, DNSsec usw. geben. *(bk)*