Internetanbindung für ein Unternehmen realisieren

Inhaltsverzeichnis

1 Aufgabe / Sicherheit: Hacker, Cracker, Viren

1.1 Hacker

Als Hacker wird eine Person mit sehr fundiertem Computerfachwissen bezeichnet. Der Begriff „Hacker“ wird meist fälschlicherweise als kriminalisierende Bezeichnung verwendet, d.h. ein Hacker wird heute oft mit jemandem verwechselt, der Computer nur zu illegalen Zwecken einsetzt. Beispielsweise um in fremde Rechner oder Netzwerke eindringt, um dort Schaden anzurichten oder fremde Daten beschädigt. Grundsätzlich hat ein Hacker, der in fremde Computersysteme eindringt, eher rechtschaffene Absichten. Er glaubt an die Freiheit der Information oder sucht nach Informationen, mit denen er kriminelle Handlungen oder eine Verschwörung aufdecken kann.
Viele Hacker cracken nur zum Spass, manche im Auftrag ihres Landes, eines Geheimdienstes, als Wirtschaftsspione, oder nur um (im Auftrag des Betreibers) die Sicherheit eines Systems zu überprüfen.
Für unerfahrene Personen, die im Gegensatz zum echten Hacker ihre Werkzeuge nicht selbst programmieren, sondern stattdessen zum Zerstören von Systemen nur vorgefertigte Skripte und ähnliches verwenden, ist die abfällige Bezeichnung Script-Kiddie entstanden.

1.2 Cracker

In der Hackerszene werden unter Crackern Personen mit Computerfachkenntnissen verstanden, die im Gegensatz zu Hackern ihre Fähigkeiten grundsätzlich destruktiv einsetzen. Dazu gehört das mutwillige oder kriminelle Eindringen in fremde Computersysteme, auch mit Übernahme der Kontrolle über das fremde System, Belegen von fremden Speicherressourcen, Diebstahl von Rechenleistung für eigene Zwecke oder Diebstahl, Manipulation oder Zerstörung von Daten.
Der Ursprung des Begriffs „Cracker“ liegt in der englischen Umgangssprache (sog. Slang) und bezeichnet hier das Aufbrechen von etwas oder das (Zer-) Brechen der Wirkung eines Sicherheitssystems oder einer Sperrvorrichtung.

1.3 Viren

In der Fachsprache ist ein Computervirus eine nichtselbständige Programmroutine. Viren hängen sich an Computerprogramme oder Bereiche des Betriebssystems. Sie nehmen unkontrollierbare Manipulationen vor. Computerviren stören den regulären Betrieb des Computers und können bis zu kompletten Systemausfällen führen. Umgangssprachlich wird der Begriff „Computervirus“ meist auch für Computerwürmer und Trojanische Pferde benutzt.
Die Idee zu Computerviren leitete sich vom biologischen Vorbild der Viren ab.

In folgender Tabelle werden die Viren klassifiziert:

Virentyp	Beschreibung
Bootvirus	Bootviren nutzen die Funktionen von Computern aus, welche das automatische starten von Programmen beim Computerstart erlaubt, wie es z.B. für das Laden von Betriebssystemen notwendig ist.
Linkvirus	Linkviren schleusen sich in Programmdateien ein, so dass dessen Code beim Ausführen mit ausgeführt wird. Sie verbleiben meist im Speicher und infizieren Programme, wenn sie gestartet werden.

Makrovirus	Makroviren sind in Dateien wie z.B. Textdokumenten versteckt. Die in einer Makrosprache programmierten Programmteile (sog. Makros) können Prozesse automatisieren.

1.4 Würmer

Ein Computerwurm ist eine selbständige Programmroutine, welche im Computernetzwerk, an Computerprogrammen oder an Betriebssystemen Manipulationen vornimmt. Würmer sind den Computerviren konzeptionell sehr ähnlich. Die Abgrenzung besteht darin, dass ein Virus versucht Dateien auf einem Computersystem zu infizieren, während ein Wurm versucht, eine Zahl von Computern in einem Netzwerk zu infizieren. Ausserdem benötigt ein Virus ein Trägerprogramm. Wird dieses Programm ausgeführt so wird gleichzeitig auch das Virus ausgeführt. Ein Wurm ist ein eigenständiges Programm. Würmer werden überwiegend per E-Mail (meist als Datei-Anhang) weiterverbreitet, wobei der Datei-Anhang meistens eine 'doppelte Dateiendung' hat (z.B. Bild.jpg.exe). Hat der Benutzer die Optionen für die Dateiansicht von Windows nicht geändert, so wird ihm eine Bilddatei namens „Bild.jpg" angezeigt, obschon eigentlich eine Software dahinter steckt...

1.5 Trojanische Pferde

Als Trojanische Pferde bezeichnet man in der Fachsprache Programme, die sich als produktive Programme tarnen, aber in Wirklichkeit sog. Malware (aus engl. „malicious" = boshaft und Software) sind. In der Praxis auftretende Trojanische Pferde enthalten allerdings oft Spionagefunktionen oder Funktionen die es ermöglichen einen Computer via Netzwerk/Internet fernzusteuern (sog. Backdoors). Der wesentliche Unterschied zu Computerviren ist, dass ein Trojanisches Pferd ein normales Computerprogramm ist und nicht die Fähigkeit besitzt, sich selbständig (!) weiterzuverbreiten.

1.6 Hoax

Ein Hoax (engl. für Jux, Scherz, Schabernack; auch Schwindel) bezeichnet im Deutschen eine Falschmeldung, die sich per E-Mail verbreitet, von vielen für wahr gehalten und daher an viele Freunde weitergeleitet wird. Ein Hoax kann auch als moderne Form der Zeitungsente betrachtet werden.
Auch Kettenbriefe, die per Emails weitergeleitet werden, können zu den Hoaxes gezählt werden, denn hier existiert selten ein realer Hintergrund, der die Verbreitung rechtfertigen würde.

1.7 Antivirenprogramme

Ein Antivirenprogramm, oft auch als Virenscanner bezeichnet, ist eine Software, die ihr bekannte Computerviren, Computerwürmer und Trojanische Pferde aufspüren, isolieren und gegebenen beseitigen soll.
Um schädliche Software zu erkennen, hat jeder Virenscanner eine Liste mit Beispielen aller ihm bekannten Viren und Virentypen und anderer schädlicher Software, mit der er die zu überprüfende Software vergleicht. Diese Listen werden Virensignaturen oder Virendefinitionen genannt. Da ständig neue Viren und Würmer

auftauchen müssen die entsprechenden Listen ständig aktualisiert werden. Viele Scanner unterstützen heutzutage automatische Aktualisierungsmethoden. Antivirenprogramme werden im Hintergrund ausgeführt. Sie prüfen (abhängig von der Konfiguration) alle aktiven Dateien und Programme, was bei leistungsschwachen Systemen oft zu Leistungsengpässen führen kann. Selbstverständlich kann (und soll) ein System vom Benutzer manuell auf Viren geprüft werden.
Kein Virenscanner kennt alle Viren und Würmer. Ganz neue oder kaum verbreitete Viren und Würmer sind nicht in den Virendefinitionen enthalten und so für den Virenscanner nicht zu erkennen. Zwar verfügen einige Virenscanner über die Möglichkeit, auch nach allgemeinen Merkmalen zu suchen (sog. Intrusion Detection Systeme), jedoch sind diese Lösungen auch nicht immer ausreichend.

1.8 Schutz vor Viren

Anwender sollten niemals unbekannte Programme oder Programme aus unsicherer Quelle ausführen bzw. generell beim Öffnen von Dateien oder E-Mails vorsichtig sein. Durch Sicherheitslücken in den mit Dateien verknüpften Programmen können Schadprogramme auf verschiedene Weise aktiv werden. Durch die Autostartfunktion für CD-ROMs und DVD-ROMs können Programme bereits beim Einlegen eines solchen Datenträgers ausgeführt, und damit ein System infiziert werden.
Vor allem Microsofts „Outlook Express“ ist als sehr unsicherer Mail-Client aufgefallen, da es ohne Zutun des Benutzers fremde Software in E-Mails gestartet hat. Man sollte deshalb ein sichereres Programm benutzen (z.B. Lotus Notes).

Tipps zur Prävention vor Computerviren

- Dateien aus dem Internet (ob heruntergeladen oder per E-Mail erhalten) sollten nur angenommen werden, wenn man sicher ist, dass sie aus seriöser Quelle stammen (E-Mail-Absender können gefälscht sein) und nur geöffnet werden, nachdem man mit einem Antivirenprogramm die Virenfreiheit festgestellt hat.
- Das automatische Öffnen von Dateien aus dem Internet sowie das automatische Anzeigen von Dateianhängen sollte deaktiviert werden.
- Regelmäßig Betriebssystem und Software aktualisieren.
- Einen sicheren Browser und ein sicheres E-Mail-Programm verwenden.
- Schutzfunktionen des Betriebssystems nutzen. Dazu zählt insbesondere, nicht als Administrator mit allen Rechten, sondern als Nutzer mit eingeschränkten Rechten zu arbeiten, der keine Software installieren darf.

1.9 Genügt eine Firewall?

Eine Personal Firewall, wie wir sie unter Windows XP (ab Service Pack 1) mitinstalliert bekommen, kann theoretisch vor bösartigen Programmen, die sich über Schwachstellen in Serverdiensten weiterverbreitet, schützen. In der Praxis ist es jedoch besser, die kritischen Dienste zu beenden, da jedes Programm mit Internetzugriff (so auch die Personal Firewall) ein potentielles Angriffsziel darstellt. Des Weiteren sind Personal Firewalls gegen Computerviren fast immer unwirksam, da diese sich im Allgemeinen durch die Weitergabe infizierter Dateien durch die Benutzer verbreiten.

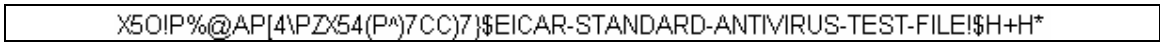
1.10 Genügt ein Antivirenprogramm?

Antivirenprogramme schützen nur vor bekannten Viren. Daher ist es bei der Benutzung eines solches Programms wichtig, regelmäßig neue Virensignaturen

einzuspielen. Diese werden meist vom Hersteller der Software bereitgestellt (z.B. McAfee oder Symantec). Unbekannte Viren können jedoch von manchen dieser Programme auch anhand ihres Verhaltens entdeckt werden. Diese Funktionen arbeiten jedoch meist unzuverlässig. Aus diesen Gründen sollte man diese Programme nur als Unterstützung ansehen und sich nicht allein auf ihr Urteil verlassen.

1.11 Testsignatur

Virensignaturen werden von Antiviren-Programmen zur Identifizierung von Viren genutzt. Sie stellen ein eindeutiges Erkennungsmerkmal dar.
Dieser 68Byte-lange Textcode definiert den Testvirus „Eicar“. Jedes Antiviren-Programm erkennt eine Datei mit diesem Code sofort als Virus, daher wurde der Code in diesem Dokument als Bilddatei abgelegt:



Quelle: www.eicar.org

1.12 Bekannte Namen aus der Szene

Kevin Mitnick (alias „Condor“) gilt als einen der bekanntesten Cracker. In seiner Karriere als Cracker soll er unter anderem mehr als 100mal in das Netzwerk des Pentagon sowie einige Male in das Netzwerk der NSA eingedrungen sein.
1988 wurde Mitnick das erste Mal inhaftiert: Acht Monate in Einzelhaft und weitere sechs Monate im Half Way House.
Am 15. Februar 1995 wurde Mitnick vom FBI erneut verhaftet und angeklagt, in ’einige der bestgesicherten Computersysteme’ der USA eingedrungen zu sein, unter anderem in NORAD („North American Aerospace Defense Command“), das Luftverteidigungssystem der USA auch gegen nukleare Angriffe.

2 Aufgabe / Sicherheit: Firewall Allgemeines

2.1 Sinn und Zweck einer Firewall

Firewalls (in der Fachsprache auch „Zugangsschutzsysteme genannt) sitzen an den Schnittstellen zwischen einzelnen Netzen und kontrollieren den Netzwerkverkehr zwischen den Netzen, um ungewünschten Verkehr zu verhindern und nur den gewünschten Verkehr weiterzuleiten.
Der häufige Einsatz einer Firewall besteht darin, den Verkehr zwischen einem lokalen Netzwerk und dem Internet zu kontrollieren und zu steuern. Ein komplexes Szenario stellt die DMZ (siehe 2.4) dar.

2.2 Vor was schützen Firewalls? - vor was nicht?

Firewalls schützen vor...
• Hacker/Cracker/Datenspione • Trojanischen Pferden • Externen (unautorisierten) Login-Requests

Firewalls schützen nicht vor...
• bösartigen Insidern schützen. • Verbindungen, die nicht über sie laufen. • Angriff aus dem Innern des Netzwerks • völlig neuen Gefahren schützen ("Ping-of-Death"). • Viren schützen.

Merksätze:

- Firewalls reichen folglich niemals als einziges Schutzinstrument aus!
- Jede Firewall ist nur so gut wie der Spezialist, welcher sie konfiguriert hat!

2.3 Angriffsarten

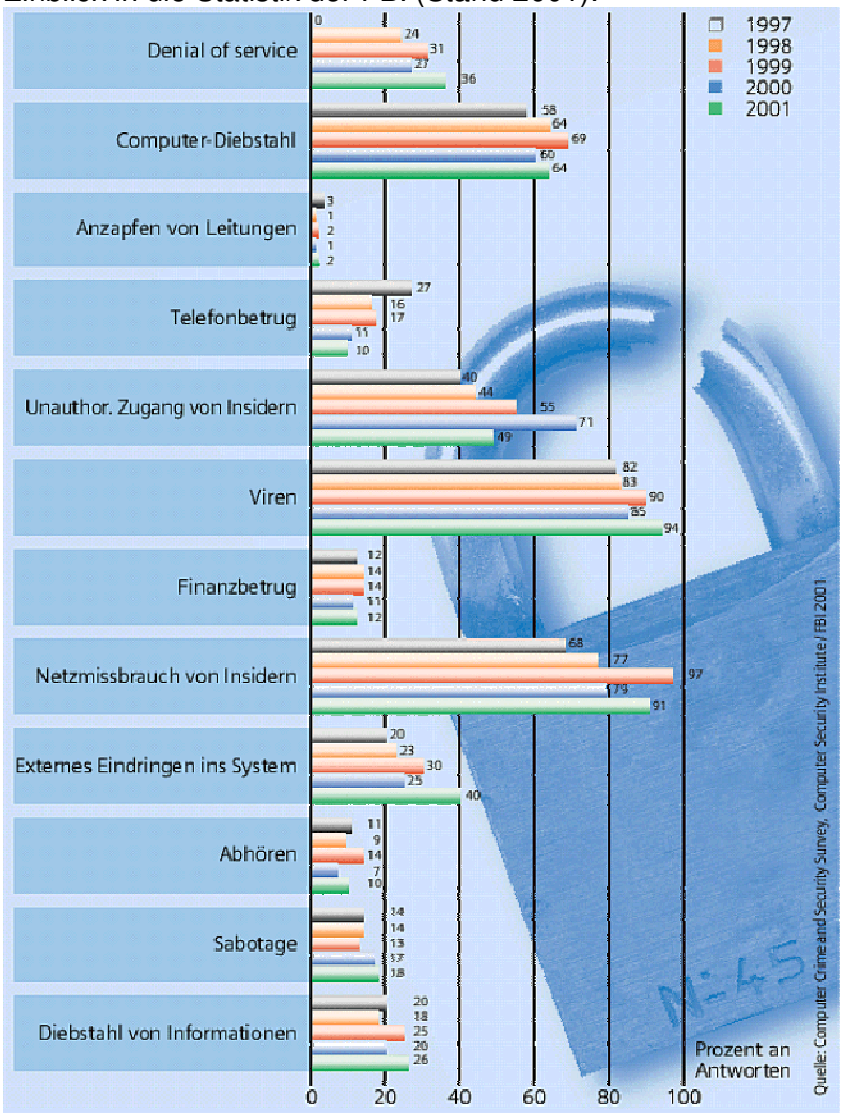
Eine Übersicht mit den häufigsten Angriffsarten:

- **Insider Angriffe**
  Wie Statistiken zeigen kommen die meisten Angriffe von Insidern aus dem eigenen Netzwerk. Gegen solche Angriffe gibt es nur selten gute Präventionsmöglichkeiten.

- **Brute Force Angriff**
  Die einfachste Art und Weise ein Passwort zu knacken, ist es durch Probieren zu erraten. Dazu werden mit Hilfe einer Software so viele denkbare Kombinationen wie möglich ausprobiert. Mit viel Glück errät man die richtige.

- **Denial Of Service Angriff**
  Als DoS-Angriff (Denial of Service attack, etwa: „Dienstverweigerungs-Angriff“) bezeichnet man einen Angriff auf einen Host (Server) mit dem Ziel, einen oder mehrere seiner Dienste arbeitsunfähig zu machen. In der Regel geschieht das durch Überlastung.

Einblick in die Statistik der FBI (Stand 2001):



Quelle: http://w4.siemens.de/Ful/de/archiv/pof/heft1_03/artikel18

2.4 Was ist eine DMZ?

Demilitarized Zone (DMZ, deutsch: entmilitarisierte Zone) bezeichnet einen geschützten Rechnerverbund, der sich zwischen zwei Computernetzwerken befindet. Der Rechnerverbund wird jeweils durch einen Paketfilter gegen das dahinter stehende Netz abgeschirmt.
Ein typisches Anwendungsbeispiel ist eine Firma, die einen eigenen Mailserver, Webserver (oder vergleichbares) betreibt. Weil öffentlich angebotene Dienste oft ein nicht unerhebliches Angriffsziel darstellen, kann man durch eine DMZ das Gesamtrisiko enorm minimieren.

2.5 Extranet

Ein Extranet beruht auf der gleichen Technik wie das Internet, kann jedoch nur von einer festgelegten Gruppe von Menschen genutzt werden. Extranets findet man zumeist bei großen Firmen, die ihren Kunden oder Geschäftspartnern aktuelle Informationen (Beschreibungen von Produkten, Preislisten) bereitstellen wollen, ohne dass diese Dokumente auch von der Konkurrenz eingesehen werden können.

2.6 Intranet

Ein Intranet ist im Prinzip vergleichbar mit einem Extranet, jedoch sind die Informationen nur von einer festgelegten Gruppe von Mitgliedern einer bestimmten Organisation zugänglich.

3 Aufgabe / Sicherheit: Firewall Technik

3.1 Firewall-Typen

Es wird prinzipiell zwischen folgenden Firewall Typen unterschieden:

3.1.1 Packet Filtering Firewall

Für solch einfache Aufgaben wie das Vergleichen von Quell- und/oder Zieladresse der Pakete, die die Firewall passieren, ist der Paketfilter zuständig. Er hat die Aufgabe, bestimmte Filterungen oder Reglementierungen im Netzwerkverkehr vorzunehmen. Ein Paketfilter definiert Regeln, welche festlegen, ob einzelne oder zusammenhängende Pakete das Zugangsschutzsystem passieren dürfen oder abgeblockt werden. Eine solche Regel wäre zum Beispiel: verwerfe alle Pakete, die von der IP-Adresse 192.100.10.1 kommen.

3.1.2 Content-Filter / Application-Level-Gateway

Eine Firewall kann aber nicht nur auf der niedrigen Ebene des Paketfilters arbeiten, sondern auch komplexere Aufgaben übernehmen. Ein Content-Filter überprüft zum Beispiel die Inhalte der Pakete und nicht nur die Meta-Daten der Pakete wie Quell- und/oder Zieladresse. Solche Aufgaben können zum Beispiel folgende sein:

- Herausfiltern von ActiveX und/oder JavaScript aus angeforderten HTML-Seiten.
- Filtern/Kennzeichen von Spam-Mails
- Löschen von Viren-Mails

3.1.3 Stateful Inspection Firewall

Die Stateful Inspection Firewall (zustandsgesteuerte Paketfilterung) ist eine typische Erweiterung für den Paketfilter. Dieser kennt den Status einer Verbindung und kann ein neues Datenpaket einer bestehenden Verbindung zuordnen. Diese Information kann als weiteres Filterkriterium herangezogen werden.