14.06.2002

Internetsicherheit

Von
Clarissa Hannich
und
André Monson

Humboldt-Gymnasium
2. Semester - Informatik

INHALTSVERZEICHNIS

Seite 1 ..... Deckblatt

Seite 2 ..... Inhaltsverzeichnis

Seite 3 ..... Das Internet und seine „unbegrenzten Möglichkeiten“?!

Seite 4 ..... Die wahren Fallen des Internet
Seite 4 ..... Computerviren allgemein
Seite 4 ..... Vergleich von biologischen- und Computerviren

Seite 5 ..... Einteilung von Computerviren

Seite 6 ..... Das trojanische Pferd

Seite 7 ..... Einige weit verbreitete Viren
Seite 7 ..... Der Virus aus rechtlicher Sicht
Seite 7 ..... Wie man sich schützen konnte und kann

Seite 8 ..... Weitere Unsicherheiten im Internet
Seite 8 ..... Schutz vor direkten Angriffen

Seite 9 ..... Fazit

Seite 10 ..... Übersicht über die wichtigsten Schutzmaßnahmen
Seite 10 ..... Quellenangabe

Das Internet und seine „unbegrenzten Möglichkeiten“?!

Seit den letzten drei Jahren ist das weltweit attraktivste Medium in seiner Anwenderzahl explosionsartig gestiegen. Die Gründe hierfür sind eindeutig:
Es gibt keine einfachere, schnellere, billigere und informativere Quelle um Informationen in allen möglichen Bereichen zu allen Themen zu erhalten als das Internet. So ist heutzutage der Briefwechsel kaum noch zeitgemäß, wenn man doch mit einer E-Mail den Freund in Amerika in Sekundenschnelle erreichen kann.
Doch auch wenn es vieles erleichtert, kann es manchen Benutzer auch zur Weißglut bringen.
Die meisten Hobby-Surfer sind der vermeintlichen Auffassung, dass sie sich völlig anonym im Internet bewegen können, doch weit gefehlt...
Stellen Sie sich vor, sie würden in einen Erotikshop gehen und sich anschließend beim Gemüsehändler noch Beelitzer-Spargel kaufen. Und das alles auf Rügen, wo Sie niemand kennt. Sie wären anonym. Weder Ihr Name wäre bekannt, noch wüsste der Spargelverkäufer, dass Sie vorher in einem Erotikshop waren. Die meisten Internetbenutzer irren sich, wenn sie glauben das Internet biete dieselben Vorteile.
Und der Spargelverkäufer weiß es doch...
Sobald Sie eine Internetseite aufrufen, gibt Ihr Browser viele Informationen preis. Beispielsweise erhält der Websitebetreiber auf Abruf Ihre IP-Adresse, Ihre E-Mail-Adresse und sogar die Information, welche Seite sie zuletzt besucht haben. Der „Spargelverkäufer“ kennt zwar nicht Ihren Namen, er weiß aber jedoch, dass Sie zuvor im „Erotikshop“ gewesen sind. Aufgrund längerer Beobachtungen sind die Anbieter in der Lage, Ihre Interessen zu analysieren und für Marketingzwecke zu verwenden. Sie werden mit für Sie zugeschnittener Werbung überhäuft!
Des weiteren kann mittels Ihrer IP-Nummer der Standort Ihres Providers geortet werden. Dieser zeichnet in einer sogenannten LOG-Datei auf, welcher Benutzer dieses Providers zu welcher Zeit welche IP-Nummer besaß. Diese Dateien werden bis zu mehreren Monaten aufbewahrt. In Straffällen ist der Provider sogar gezwungen Ihren Namen und Ihre Anschrift herauszugeben. Somit ist im Allgemeinen, auf legalem Wege, keinerlei Anonymität im Internet geboten...
Es sei denn, man benutzt einen Proxy-Server. Dies ist ein Server, der Ihre Anfrage entgegennimmt, sich als Absender bei der angeforderten Seite einträgt und die Daten an Sie weiterleitet. Er geht gewissermaßen stellvertretend für Sie auf die angeforderte Website. Doch auch hier gibt es Nachteile. Der Proxy-Server ist ein stark ausgelasteter Datenknotenpunkt und verlangsamt somit

ihre Internetbenutzung. Der zweite Nachteil wäre, dass man auch hier nicht weiß, was hier mit den LOG-Dateien passiert.

Die wahren Fallen des Internet

Computerviren allgemein:

Der Name Virus wurde wegen der Ähnlichkeit der Funktionsweise der biologischen Viren gewählt. Hier ein anschauliches Beispiel:

Biologische Viren	**Computerviren**
Greifen bestimmte Zellen an	Greifen best. Programme (z.B. *.COM, *.EXE) an
Erbinformation der Zelle wird verändert	Programm wird manipuliert
In befallenen Zellen entwickeln sich neue Viren	Befallene Programme erzeugen weitere Kopien des Virus
Krankheiten treten nicht unmittelbar nach dem Befall auf	Infizierte Programme können längere Zeit fehlerfrei ablaufen
Jede Zelle wird nur einmal infiziert	Viren legen in der Regel in jedem Programm nur eine Kopie an
Viren können mutieren	Bestimmte Viren verändern ihre Struktur

Ein Computervirus ist ein Programm, dass der Sabotage bestimmter Teile, Dateien oder Programme eines Computers dienen soll. Ein solches Programm wird erst dann als Virus bezeichnet, wenn es erstens einen zerstörerischen Charakter hat und zweitens in der Lage ist Kopien von sich selbst in andere Programme oder sogar in andere Computer per Internet einzuschleusen. Alle mit einer Kopie verseuchten Programme, vermehren bei ihrer Ausführung den Virus erneut.

Der „klassische“ Virus war dazu gedacht, ganz gezielt und bewusst wichtige Dateien/ Daten des beispielsweise Kriegsgegners zu zerstören. Der Virus war hierfür besonders gut geeignet, da man zum einen nicht nachvollziehen kann, woher oder von wem der Virus stammt. Zum anderen ist er effektiver als eine „einfache“ Löschung der Daten, da selbst bei den vorher angelegten Sicherheitskopien der Virus sich einschleicht und bei deren Einsatz diese ebenfalls zerstört. Zuletzt ist das Ausmaß der Zerstörung enorm, da der Virus sich durch seine Selbstkopien exponentiell vermehrt. Anfang der 50er Jahre wurden die ersten Viren entwickelt und die Anzahl verdoppelt sich seitdem ungefähr alle acht Monate, weshalb sich bis heute ca. 1.000.000 Viren verbreitet haben.

Der „klassische“ Virus bediente sich der direkten Manipulation von Dateien, indem er Ziffern, Buchstaben oder ganze Datensätze austauschte. Zur Verdeutlichung der Zerstörungskraft stellen Sie sich vor, in Ihrem Portmonee werden Ihr Leben lang alle 50-Euro-Scheine durch 1-Cent-Stücken ersetzt...

Die neueren Viren reichen in ihrer Wirkung von grundlos ausgegebenen Fehlermeldungen bis hin zur Formatierung (kompletten Löschung) der Festplatte samt des verwendeten Systems.
Zur Verdeutlichung *dieser* Zerstörungskraft, stellen Sie sich vor Sie verlieren von einer Minute auf die andere alles für Sie Wichtige in Ihrem Leben, sodass Sie ohne irgendjemanden zu kennen, nackt, hungernd und ohne Geld auf der Straße säßen...

Einteilung von Computerviren:

- **Logische Viren:** Sehr einfache und auffällige Form, ein Virenprogramm tritt an die Stelle eines Anwendungsprogramms. Der selbe Effekt ist praktisch auch mit dem DOS-Befehl *RENAME* erreichbar.

- **Dateiinfektoren:** klassische Form eines Virus, "befällt" ausführbare Dateien (*.COM, *.EXE). Grundsätzlich kann dies auf drei Arten geschehen:

  a)Teile des ursprünglichen Programms werden überschrieben: Sehr plumpe und auffällige Methode, da das Programm funktionsunfähig wird.

  b)Virus wird an einer bestimmten Stelle (oft am Anfang) in das Programm eingefügt: Infektion kann bemerkt werden, da sich Dateigröße ändert.

  c)"Call-Viren": Im Programm ist nur ein kurzer Aufrufbefehl zu finden, Virusprogramm ist als Hidden File, im Arbeitsspeicher oder am günstigsten als eigener Interrupt abgelegt

- **Bootsektorviren:** Diese Viren schreiben ihren Code in den Bootsektor von Disketten bzw. Festplatten, wo er nicht nur schwer zu entdecken ist, sondern auch bei jedem Bootvorgang von einem infizierten Datenträger in den Speicher geladen wird und dort meist bleibt. Daher werden viele Bootsektorviren bei nahezu jedem Schreibvorgang auf einem verseuchten System übertragen.

- **Schlafende Viren, Trigger Viren:** Bleiben lange unbemerkt, da sie erst zu einem bestimmten Zeitpunkt (als sehr beliebt hat sich Freitag, der 13. erwiesen) mit ihrer Manipulation beginnen.

- **Trojanische Pferde:** Scheinbar nützliche Programme (oft Spiele), die während des normalen Ablaufes im Hintergrund die von vornherein programmierte Virenfunktion erledigen.

- **Polymorphe (evolutionäre) Viren:** Diese Art von Viren ändert ihren Code in jeder neuen Generation, d.h. sie kopieren einen mehr oder weniger stark veränderte Version weiter.

Manchmal wird auch die Wirkungsweise des Virus modifiziert. Sie sind die am schwersten zu erkennende Art von Viren.

- **Stealth Viren:** Tarnen sich, indem sie Aufzeichnungen des Zustandes (zum Beispiel den Eintrag über die Größe einer infizierten Datei) vor der Infektion manipulieren und sind daher kaum - oder nur sehr schwer - zu erkennen.

- **Macro Viren:** Sie sind die bislang jüngste Form von Viren und benutzen die Makrosprache einer Textverarbeitung (meist MS Word) oder Tabellenkalkulation, um ihre Manipulationsaufgabe auszuführen. Ihre Gefahr liegt darin, dass sie mit jeder im entsprechenden Programm erstellten Datei und nicht nur mit ausführbaren Programmen weitergegeben werden können, dass sie eher unauffällig ablaufen (viele Festplattenzugriffe sind bei Standardsoftware zur Gewohnheit geworden) und dass es derzeit kaum Programme gibt, die in der Lage sind, Macro Viren zu erkennen oder zu vernichten.

Das Trojanische Pferd:

Diese Virusart ist mit Sicherheit diejenige, von der man als privater Benutzer des Internet am meisten gehört hat. Als Trojanisches Pferd bezeichnet man ein Programm, das vorgibt, eine mehr oder weniger nützliche Aufgabe zu erfüllen, im Hintergrund jedoch andere, vom Benutzer nicht gewollte Aktionen vollzieht. Dies kann zum Beispiel das Ausspähen von Zugangsberechtigungen oder Daten sein, bis hin zum Formatieren der Festplatte. Verkürzt werden trojanische Pferde auch Trojaner genannt, obgleich diese Bezeichnung nicht ganz korrekt ist: Schließlich entstammt der Name der Sage von der Schlacht um Troja, als die Griechen über ein Versteck in einem hölzernen Pferd in die Stadt einfallen konnten. Das „Pferd“ ist beim Computer nun das Programm, das einen Nutzen vorgaukelt. Der „Trojaner“ wäre hingegen, der Anwender, der sich dieses „Pferd“ in die „Stadt“/ das System holt. Die im Programm verborgenen schädlichen Datensätze wären dann die im Pferd versteckten Griechen.
Ein besonderes Einsatzgebiet für trojanische Pferde ist das Ausspionieren von Zugangsdaten für Online-Dienste. Manche Trojaner spionieren nicht nur Nutzerdaten und Passwörter aus, sondern klinken sich in den Hintergrund des Systems ein und kann so auch per Tastatur eingegebene Passwörter abfangen.

Einige weit verbreitete Viren:

Name (n)	Herkunftsland	Typ	Symptome
Cascade, Fall(ing Letters), 1701,1704, etc.	Deutschland	*.COM-Infektor	Buchstaben purzeln vom Bildschirm
EDV, Cursy, Stealth	Frankreich	Bootsektor	Systemabstürze
Michelangelo	Schweden/ Norwegen	Bootsektor	formatiert Festplatte, reduziert Speicher
Scramble, One-Half-Virus	unbekannt	Stealth Virus	verschlüsselt Festplatte, wenn entfernt, kein Zugriff auf Teile der Festplatte
Stoned, Donald Duck, Hawaii, San Diego, etc.	Neuseeland	Bootsektor	Fehlermeldungen, Systemabstürze
Vienna, 648, DOS-62, Austrian, UNESCO	Österreich	*.COM-Infektor	Systemabstürze
Yankee Doodle Five O' Clock	Bulgarien	*.COM-Infektor	spielt um 17 Uhr Yankee Doodle

Der Virus aus rechtlicher Sicht:

In Deutschland ist es nicht verboten einen Virus zu programmieren, es ist lediglich verboten ihn in den Umlauf zu bringen. Das heißt es ist bereits der Versuch und die Anwendung selbst, Daten eines anderen in irgendeiner Weise zu manipulieren bzw. zu verändern, strafbar! Dies wird in der Regel mit Schadensersatzforderungen und einer Freiheitsstrafe bis zu fünf Jahren geahndet.

Wie man sich schützen konnte und kann

Da es sich bei den „klassischen" Viren meist um Zerstörerprogramme handelte die relativ einfach gestaltet waren, konnte man ihnen simpel mit speziellen Zugangskontrollen auf den Rechner entgegenwirken oder virenfreie Backups (komplettes System woanders noch einmal speichern) anlegen. Heutzutage reicht das nicht mehr aus, da die Viren wesentlich durchdachter gestaltet werden. Beispielsweise können sie mittlerweile jegliche Zugangskontrollen umgehen. Der allerbeste Schutz ist heute wohl keinerlei Art des Datenaustausches, sei es per CD-ROM oder Diskette, durchzuführen. Das heißt aber auch keinen Netzwerkzugang zu haben, auch nicht zum Internet. Nur dieser Schutz bietet die optimale Sicherheit.

Da diese Form des Schutzes eigentlich unmöglich ist wurden parallel zur Virenentwicklung Antivirusprogramme programmiert. Die Grundidee der Antivirusprogramme ist, dass sie alle

möglichen Strukturen der bisher bekannten Viren erkennen und das System nach diesen Strukturen absucht und gegebenenfalls ändert.
Die neueren Programme simulieren den gefundenen Virus erst in einem abgesicherten Modus und verändern die Datei anschließend. Doch hier sind die Nachteile klar. Das Programm ist nie aktuell weil ständig neue Viren programmiert werden, weshalb es auch nie alle Viren aufspürt. Um Abhilfe zu verschaffen gibt es neuere Überwachungsmethoden, die bereits beim Booten geladen werden und alle potentiellen Infektionsquellen prüfen. Eine weitere Art des Programms, speichert die Dateigrößen aller vorhandenen Dateien ab und vergleicht diese permanent mit den aktuellen. Hierdurch werden fast alle Viren gefunden, doch die Fehlalarmquote ist enorm hoch, da viele Dateigrößen absichtlich verändert werden. Die neuste und effektivste Virenerkennung ist mittels der „Fuzzy Logic“ möglich. Dies ist ein neues Programmierverfahren, welches nicht nur, wie bei z.B. Java, ein Wahr oder Falsch bei einer Wertabfrage zulässt, sondern auch Zwischenstufen wie vielleicht oder sogar eine Wahrscheinlichkeitstendenz. So kann man nahezu alle, auch neue, Viren erkennen, da auch diese auf einer bestimmten Programmbasis funktionieren, die durch „Fuzzy Logic“ erkannt wird.

Weitere Unsicherheiten im Internet

Natürlich gibt es nicht nur gefährliche Viren, sondern auch sämtliche Hacker, die erst in einem direkten Angriff auf einen privaten Computer bis hin zum Angriff auf ein ganzes Firmennetzwerk die Herausforderung sehen. Die Gefahr hierin besteht in der Tatsache, dass der Hacker den kompletten Zugriff auf die private Festplatte erlangt und somit Einsicht in sämtliche Dateien. Dies kann letztendlich dazu führen, dass der Hacker auf die Kosten des Opfers surft oder sogar eventuell gespeicherte Geheimzahlen oder Passwörter zu lesen bekommt.

Schutz vor direkten Angriffen

Wie vor der Infektion mit einem Virus gibt es auch hiervor nicht den optimalen Schutz. Trotz alledem gibt es wie gegen den Virus das Antivirusprogramm, gegen den direkten Angriff eine Firewall. Ein Schutzprogramm mit einer logischen Grundidee...
Stellen Sie sich vor, Sie sitzen in einem Raum mit zwei Türen. Durch die eine Tür bringt Ihnen der Postbote einen Brief, durch die andere kommt ein Einbrecher.
Wären die Türen abgeschlossen gewesen, hätten Sie vorher fragen können wer dort sei und Sie hätten den Einbrecher nicht hineingelassen. Und genau das ist das Prinzip der Firewall. Die Firewall

ist ein Programm, das überprüft welche Daten auf Ihren Rechner gelangen, woher sie kommen oder wer versucht auf Ihren Rechner zuzugreifen, bevor es die „Tür“/ den Port öffnet.
Doch was ist wenn der Einbrecher ein Brecheisen besitzt...? Die bessere Variante einer Firewall gaukelt dem Angreifer vor, dass Ihr „Zimmer“ gar keine „Tür“ hat und so schleicht sich der Einbrecher zum nächsten, bis er ein „Zimmer“ mit offener „Tür“/ offenem Port findet, wo er einbrechen kann. Doch so leicht wie es sich anhört ist es dann doch nicht. Würde man mit der Firewall alle Ports schließen, so bräuchte man kein Internet mehr, da keine Daten mehr ankommen würden und keine ausgesendet werden können. Oder können Sie durch geschlossene Türen gehen?!
Und das ist die komplizierte Seite der Firewall. Sie braucht genau angepasste Regeln, wann sie welchen Port öffnen und schließen soll, ein Ruleset. Um wirklich guten Schutz zu erreichen muss das Ruleset individuell auf jeden Benutzer eingestellt werden, was ein „Otto-Normal-User“ nicht kann. Es gibt im World Wide Web zwar auch schon vorgefertigte Rulesets, doch es ist klar, dass diese nur einen groben Schutz bieten.

Fazit

Den optimalen Schutz gibt es nicht, ein gewisses Restrisiko bleibt immer! Mit dieser These muss man sich als Internetuser abfinden, oder das Surfen lassen. Für den sichersten Internetgebrauch ist es zweckmäßig sich eine zweite austauschbare Festplatte zu kaufen, die man während der Onlinezeit absteckt, sodass sie nicht mehr mit dem Computer verbunden ist. Wenn man über etwas mehr Geld verfügt, sollte man sich einen zweiten Computer zulegen, auf dem man nur das Betriebssystem, ein oder zwei verschiedene Antivirusprogramme und eine Firewall installiert um verhältnismäßig sicher zu surfen.
Falls man sich keine der beiden Varianten leisten kann, sollte man sich trotzdem auf jeden Fall mittels Antivirusprogrammen und Firewalls schützen, doch Vorsicht: *„Ein Werkzeug ist nur so gut wie derjenige der damit umgeht!“*
So manche Firewall bewertet z.B. die Anfrage, ob der eigene Rechner im Netzwerk erreichbar ist als „Incomming Hack Attack“. Doch keine Panik, diese Meldungen erinnern eher an das Niveau der Bild-Zeitung.
Als Virusschutz sollte man mehrere aufeinander abgestimmte Antivirusprogramme installieren, um möglichst flächendeckend alle Arten abwehren zu können. Des weiteren sollte die Software mindestens monatlich geupdatet/ aktualisiert werden.

Durch die Vorgehensweise einiger Trojaner, die Tastatureingaben in den Passwort-Eingabefeldern abfangen, stellt auch der Verzicht auf das Abspeichern der Passwörter kaum noch einen wirksamen Schutz dar. Es kommt umso mehr darauf an, dass man nur Programme aus vertrauenswürdigen Quellen einsetzt. Denn jedes auf dem Rechner laufende Programm kann dort Daten ausspähen oder sogar manipulieren.
In Hinsicht auf die Anonymität muss jeder selbst wissen, wie er sich im Netz verhält, wie wichtig es für ihn ist unerkannt zu bleiben und ob er einen Proxy-Server benutzt.

Zuletzt noch eine Übersicht über die wichtigsten Schutzmaßnahmen:

- Die zweite Festplatte/ der zweite Computer
- Verschiedene Schutzprogramme
- Einrichten einer Firewall
- Sicherheitseinstellungen im Browser konfigurieren
- Proxy-Server verwenden
- Keine wichtigen und geheimen Daten auf der Festplatte speichern (z.B. Passwörter)
- Vorsicht vor Dateien aus unbekannter Quelle
- Vorsicht vor dem Tausch von CD-ROMs und DISKETTEn mit Freunden/ Bekannten
- Datensicherheit durch Steganografie (S-TOOLS, die Dateien verschlüsseln können)

Quellenangabe

- allgemein: Das Internet
- speziell: www.sicherheit-im-internet.de
- speziell: www.bhz.ch/itsicherheit.html
- speziell: www.aladdin.de/produkte/internetsicherheit/internet_sicherheit.html
- allgemein: Bücher
- speziell: „Internet-Sicherheit“ von Kai Fuhrberg, Dirk Häger und Stefan Wolf
- speziell: „Internet-Sicherheit, Browser, Firewalls und Verschlüsselung“ von Kai Fuhrberg